



CYBER DEFENSE
MAGAZINE

2023

**SPECIAL
EDITION**

RSA[®]Conference | Where the world
talks security

Welcome to CDM's RSA Conference 2023 Special Edition

We're so excited to be able to welcome our colleagues, peers, and friends from around the world to RSA Conference for the thirty-second year!

This year's theme, Stronger Together, speaks to what we can accomplish when we work collectively – embracing new approaches and different perspectives that can affect the progress that shapes policy, establishes new best practices, and ensures our defenses become more effective. When collaboration is our foundation, the future is bright.

As always, we continue our mission to help cybersecurity professionals around the world get the knowledge they need to grow professionally and personally and protect their organizations from cyberthreats. And since cyberthreats are at work year-round, so are we. RSAC 365 cybersecurity learning provides seminars, webcasts, podcasts, reports, and more all year long. Plus, with our online RSAC Marketplace, you have the convenience of searching, filtering, and sorting our exhibitors' solutions anytime that's convenient for you.

In addition to all the learning opportunities the week of Conference, I encourage you to honor the community that is yours – take advantage of formal and informal networking opportunities as the connections you make, and people you meet, may be in your life forever. Whether you visit the Welcome Reception, RSAC Sandbox, the Women's Networking Reception, or demo the latest solutions in the Expo, you're sure to find like-minded peers. In addition to the conversations at RSAC, be sure to contribute to the online conversations by using our official hashtag #RSAC.

We hope to see you at RSA Conference this year.

Sincerely,

Linda Gray Martin
Senior Vice President
RSA Conference



RSAConference | Where the world talks security

Contents

Welcome to CDM's RSA Conference 2023 Special Edition.....	2
Beyond Anti-Virus 'Shark Nets': Why Current Approaches to Cybersecurity Need to Change.	12
<i>By Ms Camellia Chan, Founder and CEO of Flexxon</i>	
How to Improve your Security Posture and ROI	17
<i>By Mark Evans, VP Marketing and Packet Capture Evangelist at Endace</i>	
Security Leaders Are Finally Getting a Seat at The Table with Corporate Leadership – Make Good Use of Your Time There.....	24
<i>By Robert Herjavec, CEO of Cyderes</i>	
OT Zero Trust	28
<i>By Terence Liu, CEO of TXOne Networks</i>	
Enhance Employee Productivity by Adopting a Modern Approach to Password Security	32
<i>By Joshua Parsons, Product Marketing Manager at Enzoic</i>	
Complexity is Still the Enemy of Security	37
<i>By Gregory Hoffer, CEO of Coviant Software</i>	
Making a Business Case for Cyber Threat Intelligence: Unveiling the Value Realization Framework.....	41
<i>By Kaustubh Medhe, Head of Research and Intelligence at Cyble</i>	
Going into the Darknet: How Cynet Lighthouse Services Keep Cybersecurity Teams One Step Ahead of Hackers	47
<i>By Eyal Gruner, Co-Founder and CEO of Cynet</i>	
How To Survive a Ransomware Attack and Fix Ransomware Breach Face	50
<i>By Derek Nugent, Vice President of Revenue at Difenda</i>	
ChatGPT and You.....	55
<i>By Guy Rosefelt, Chief Product Officer at Sangfor Technologies</i>	

Strengths and Vulnerabilities of AI Applications to Health Care and the Protection of PHI, including Implications for the Confidentiality of the Doctor-Patient Relationship	60
<i>By Edward Maule, Chief Information Officer and Chief Information Security Officer at Advocate, LLC</i>	
2023 Predictions.....	64
<i>By Anurag Gurtu, Chief Product Officer at Strike Ready</i>	
A CEO's Guide to Not Becoming the Next Cyberattack Headline	66
<i>By Sheetal Pansare, President & Global CEO of Futurism Technologies</i>	
Advancements in AI Cybersecurity: Leveraging ChatGPT to Stay Ahead of Cyber Criminals	72
<i>By Brian Sathianathan, Co-Founder and CTO of Iterate.ai</i>	
Blockchain Startups Are Drawing Substantial Venture Capital Funding	75
<i>By Mohit Shrivastava, ICT Chief Analyst at Future Market Insights</i>	
Collaboration is Key to Building Industrial Cyber Resilience.....	81
<i>By Filipe Beato, Cyber Resilience Lead at the World Economic Forum's Centre for Cybersecurity and Natasa Perucica, Research and Analysis Specialist at the World Economic Forum's Centre for Cybersecurity</i>	
SAP Debugger's Power and Danger	87
<i>By Christoph Nagy, CEO of SecurityBridge</i>	
SIEM for SAP - Log Evaluation to Attack Detection	90
<i>By Christoph Nagy, CEO of SecurityBridge</i>	
The Cybercrime Blame Game: It's Time to Unite the Industry Against a Common Enemy.....	93
<i>By Brendan Kotze, Chief Executive Officer at Encore</i>	
Cyber Attack as an Asymmetric Threat	96
<i>By Milica D. Djekic, Independent Researcher</i>	
Understanding The Concept of Privacy By Design	104
<i>By Danijela Obradovic, Lawyer at Roberts & Obradovic</i>	
The Data Challenge: How to Map Data in A Distributed World	108
<i>By Dotan Nahum, Head of Developer-First Security at Check Point Software Technologies</i>	

Stop Backing Up Ransomware	113
<i>By James Gorman, Cyber Security Expert and Entrepreneur</i>	
Is Your Firm Ready for the SEC?	116
<i>By Jason Elmer, Founder and President of Drawbridge</i>	
How Must IT Leaders Develop Contingency Plans to Combat Geopolitical and Environmental Risks?	119
<i>By Mohit Shrivastava, ICT Chief Analyst at Future Market Insights</i>	
How the Increasing IT Talent Gap is Impacting the Cybersecurity Industry	124
<i>By Pete Sorensen, VP of Strategic Initiatives of ConnectWise</i>	
New Cyber Threats Calls for New Approaches	129
<i>By Mark Sincevich, Federal Director of Illumio</i>	
Leadership Is Still Washing Their Hands of Cyber Risk	132
<i>By John A. Smith, CEO of Conversant Group</i>	
Machine Identity Management: The Key to Managing Compliance Risk in a Multi-Cloud, Multi-Cluster World	136
<i>By Sitaram Iyer, Senior Director of Cloud Native Solutions at Venafi</i>	
Protecting Accounting Firms from Cyberattacks	139
<i>By Alan Hartwell, Chief Technology Officer at IRIS Software Group</i>	
Ransomware Takes No Prisoners	142
<i>By Monica Oravcova, COO and Co-Founder of Naoris Protocol</i>	
Reduce Healthcare Insider Threats with Identity and Access Management	146
<i>By Zac Amos, Features Editor of ReHack</i>	
Risk: Everything Everywhere All at Once	149
<i>By Marc Gaffan, CEO of IONIX</i>	
Top 7 Tips to Protect Your Endpoint Devices	151
<i>By Nicole Allen, Senior Marketing Executive at Salt Communications</i>	

Considering All Returns on a Cybersecurity Compliance Program	156
<i>By Doug Barbin, Chief Growth Officer and Managing Principal at Schellman</i>	
Secure Enterprise Collaboration Tools Are Critical in Light of Remote Work and Cyber-Attacks.	160
<i>By Allen Drennan, Principal and Co-Founder of Cordoniq</i>	
Stopping Criminals from Profiting Off Malware Requires a New Approach	164
<i>By CW Walker, Director, Security Product Strategy at SpyCloud</i>	
The Data Dilemma: Balancing Business Growth and Security	168
<i>By Noah Johnson, Co-Founder & CTO of Dasera</i>	
The Growing Necessity of Emphasizing Cloud Security in Business Operations	170
<i>By Deepak Gupta, CTO & Co-Founder of LoginRadius</i>	
Third-Party Cyber Security Risk Management: Best Practices	174
<i>By Sananda Dasgupta, Tech Industry and Cybersecurity Writer at Coloco</i>	
Why It Will Take Sophisticated AI Solutions to Fight AI Security Attacks	178
<i>By Rom Hendler, CEO and Co-Founder of Trustifi</i>	
1020 Cyber Security Professionals' Actions and Experiences When Applying for A New Role.	182
<i>By Torquil Macleod, Founder and Director of Via Resource</i>	
Closing The Cyber Marketing Gap with Investors	187
<i>By Patrick Kehoe, Chief Marketing Officer at Coalfire</i>	
Cyber Risk Quantification: A New Way to Understand Security Risks.....	191
<i>By Bruno Farinelli, Senior Director of Operations and Analytics at ClearSale</i>	
Evolution of the CISO Role	194
<i>By Jaye Tillson, Director of Strategy at Axis Security</i>	
Preparing Travel and Hospitality Companies for Cybersecurity in The Wake Of Travel Technologies	197
<i>By Shambhu Nath Jha, Associate Vice President of Fact.MR</i>	



ChatGPT: The Next Wave of Innovation or Your Biggest Security Threat?	200
<i>By Craig Burland, CISO of Inversion6</i>	
Is ChatGPT Ready to Disrupt Cybersecurity?	203
<i>By Anurag Gurtu, Co-Founder & CPO of StrikeReady</i>	
Communicating Cyber Risk.....	206
<i>By Tim Fleming, Strategic Advisor at Silverfort</i>	
Going On the Defensive: Turning the Tide on The Cybersecurity Vulnerabilities of Smart Home Devices With Value-Added Services	209
<i>By Craig Thole, SVP, Product Development and Operations at Assurant, Inc.</i>	
WOMEN IN CYBERSECURITY 2023 SCHOLARSHIP WINNER	213
Welcome to the Cyber Defense Global InfoSec Awards for 2023	214



CYBER DEFENSE MAGAZINE

is a Cyber Defense Media Group (CDMG) publication distributed electronically via opt-in GDPR compliance-Mail, HTML, PDF, mobile and online flipbook forwards All electronic editions are available for free, always. No strings attached. Annual EDITIONs of CDM are distributed exclusively at the RSA Conference each year.

Key contacts:

PUBLISHER

Gary S. Miliefsky
garym@cyberdefensemagazine.com

V.P. BUSINESS DEVELOPMENT

Olivier Vallez
olivier.vallez@cyberdefensemagazine.com

EDITOR-IN-CHIEF

Yan Ross
yan.ross@cyberdefensemagazine.com

MARKETING, ADVERTISING & INQUIRIES

marketing@cyberdefensemagazine.com

Interested in writing for us:

marketing@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine
Toll Free: +1-833-844-9468
International: +1-603-280-4451
New York (USA/HQ): +1-646-586-9545
London (UK/EU): +44-203-695-2952
Hong Kong (Asia): +852-580-89020
Skype: cyber.defense
E-mail: marketing@cyberdefensemagazine.com
Awards: www.cyberdefenseawards.com
Conferences: www.cyberdefenseconferences.com
Radio: www.cyberdefenseradio.com
TV: www.cyberdefensetv.com
Webinars: www.cyberdefensewebinars.com
Web: www.cyberdefensemagazine.com

Copyright © 2023, Cyber Defense Magazine
(CDM), a Cyber Defense Media Group (CDMG)
publication of the Steven G. Samuels LLC Media **Corporation**.

To Reach Us Via US Mail:

Cyber Defense Magazine
1717 Pennsylvania Avenue NW, Suite 1025
Washington, D.C. 20006

Welcome to CDM's RSA Conference 2023 Special Edition

Although this special issue is devoted to RSAC, I'd like to remind readers that Cyber Defense Magazine is conducting a contest. In the February, March, and April/RSAC issues of the magazine, one of the articles was written by Artificial Intelligence.

Every reader who correctly identifies all 3 AI-written articles, and names them in an email to us, will be entered in a raffle. The prizes will be items from the Cyber Defense Media Group offerings, such as an interview on CyberDefenseTV, or feature placement of your article on the CDM home page, or a gift card for those who prefer. Send your entry to me directly: yan.ross@cyberdefensemagazine.com

We are especially pleased to bring our readers so many relevant and compelling articles on the pressing issues facing cybersecurity professionals at this challenging time. We thank our many contributors for your participation in our important work. And we would like to emphasize the tremendous value derived from our partnership with RSAC for the benefit of our readers and contributors.

As always, we are delighted to receive both solicited and unsolicited proposals for articles. Please remember to submit all articles on the Cyber Defense Magazine writer's kit template, which incorporates the major terms and conditions of publication. We make every effort to close out acceptance of articles by the 15th of each month for publication in the following month's edition.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the Editor

Yan Ross, J.D., is a Cybersecurity Journalist & Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com



RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center



See for yourself why we are **Stronger Together.**

RSA Conference 2023 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From April 24 – 27, you'll get the chance to:

- Learn from world-renowned speakers and Keynotes.
- Explore the hottest cybersecurity solutions from over 600 global vendors.
- Harness the power of in person networking and interactive activities.
- Explore innovative ideas from up-and-coming companies.
- Step away from the daily grind to rejuvenate and refocus.

Learn more at rsaconference.com/cyberdefense23.

#RSAC



FOLLOW US



CYBER DEFENSE

MAGAZINE



www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensenewswire.com
www.cyberdefensewebinars.com
www.cyberdefenseemagazine.com
www.cyberdefenseconferences.com

Beyond Anti-Virus ‘Shark Nets’: Why Current Approaches to Cybersecurity Need to Change.

By Ms Camellia Chan, Founder and CEO of Flexxon



Shark nets have a notorious reputation: for failing at doing their intended job, giving a false sense of security, and causing great harm to wildlife.

When it comes to addressing the safety of beach goers, the issues with the outdated shark net approach are threefold:

A lack of control over the environment – in a vast natural ocean environment, these ‘safety nets’ repeatedly fail, whether through breakage, gaps that are too large, or anchor points coming loose.

Inability to account for the unknown – scientists estimate that there are over a million species of animals living in the sea; we may be aware of a specific danger but there are many others that lurk beneath the surface.

Continued reliance on human vigilance – a large surface area is difficult to patrol continuously, which means that gaps and lapses in monitoring are commonly overlooked.

The waters of cybercrime just as vast and murky

This real-world analogy perfectly mirrors the need for a revised approach to cybersecurity. In today's digital world, having to deal with a veritable ocean of an attack surface and unknown cyberthreats are two prominent challenges. Faced with this onslaught, it is unreasonable and sheer folly to expect human decision making to remain a large part of the cybersecurity chain.

At the cloud level, visibility over your infrastructure decreases astronomically. Today, organisations use thousands of instances of cloud services, which is near-impossible for the human mind or even your IT department to keep track of at all times. In August 2022, FortiGuard Labs reported that it had seen over 10,666 ransomware variants compared with 5,400 in the previous six-month period – representing a 100 per cent growth. There are simply too many variables beyond your control, which means that your IT experts and software-based defenses that patrol the external environment are fighting a battle against unseen foes, at all times.

Outside of the hardware level, organisations are playing in an ever-expanding open environment where they will be hard-pressed to protect themselves from all angles. In fact, between Q1 2021 to Q1 2022, the US ranked as the highest region globally to be targeted by ransomware, according to cybersecurity firm Group-IB.

The question then is how do we take control of the environment to protect our most important assets?

Your house, your rules

Revisiting the beach analogy. If I had to choose between the fallible safety net-protected beach and a swimming pool, I'd go for the latter. Why? Because I would know exactly what's in the water with me, and presumably would have control over that environment.

The same applies when devising a plan to keep cybercriminals away from your valuable data. In this analogy, the software is the ocean and the hardware is the man-made pool. Usage of the cloud is already highly prevalent and has undeniable business benefits. In fact, global expenditure on cloud infrastructure and services grew 13.5% y-o-y between 2020 and 2021., according to a study by IDC. Cloud computing was a lifesaver in the early days of the pandemic, as organisations shifted to remote working arrangements – and adoption will only continue to grow. This is why the idea is not to abandon the use of such a useful innovation, but rather to learn how to build a comprehensive defense posture to reap the benefit of digital innovation.

Specifically, your mission-critical assets such as employee and customer data, and company financial records, are absolutely essential to protect. Rather than allowing such information to float freely in the ocean of the cloud, you might already be storing the data with physical options such as physical servers or local storage devices.

Hardware-based security is also set apart by the fact that it is an extremely niche and specialised area, far more than software development. The US Bureau of Labor Statistics states that there are around 4.3 million software engineers in the US, compared to only 73,600 hardware engineers. This means that it takes a lot more than a casual hacker to launch an attack against your hardware.

While this is an important step in reducing your attack surface and defending against less sophisticated hackers, it unfortunately does not mean that you are safe yet – as the multiple incidents of data breaches in the past year alone have shown. Without an intelligent and fast-acting perimeter defense for hardware storage, hackers will still walk freely into your data vault, wreak havoc, and profit off your misfortune.

Control and sentry your perimeter

So how can organisations create an impenetrable perimeter that keeps would-be intruders out?

To protect data stored at the hardware level, you must create a controlled enclave environment, with limited access points, and continuous monitoring of actions made directly to the device. This is what we set out to do with the [X-PHY Cybersecure SSD](#).

Through the application of Artificial Intelligence (AI) and Machine Learning (ML), the X-PHY steps in to detect potential intrusions intuitively and continuously. Unlike the multitude of behavioural access patterns that AI-embedded software-based defenses must deal with, at the hardware level this can be simplified to just the read and write patterns.

This translates to far greater accuracy, response times, and success rates in detecting threats. Trimming the threat identification algorithms down to read and write patterns will also greatly eliminate the possibility of false positives, thereby removing the need for human intervention.

Joining forces to thwart cybercriminals.

The end-goal is to be able to continue benefiting from the countless digital applications that have elevated modern business operations, while protecting ourselves better from cybercrime.

Embracing the idea of a necessary alliance between the private and public sectors, and hardware and software-based defenses is vital and represents the next generation of cybersecurity defenses. To make that transition, a mindset shift across the industry is the first step. We cannot let the sheer volume of cyber incidents become a mere statistic for us as business leaders, it must serve as a wake-up call that jolts us into action.

Encouraging steps have been taken globally, from the multi-national taskforce set up by the [White House's Counter Ransomware Initiative](#) that encourages open discourse and smoother collaboration between the public and private sectors, to traditional B2B and B2C operators embracing the need for physical layer protection. As with introducing any new technological concept, a period of education and sandboxing is to be expected. We are heartened to have met with many like-minded corporations that are aware of the current state of cybersecurity and are looking beyond existing frameworks to strengthen

our defences. These organisations include Lenovo and ASUS, as well as distributors such as Digi-Key and World Micro. Such willingness to explore new avenues in creating a holistic cybersecurity posture is an important first step, and business leaders should adopt similar innovation and safety-led mindsets to rethink frameworks when building their organisation's IT infrastructure.

As guardians of each organisation, leaders must adopt this updated cybersecurity approach and advocate for a more holistic cybersecurity stack that comprises the seven layers of cybersecurity architecture identified in the OSI Model. Work with cybersecurity advisors, hardware solutions providers, educate your teams, and start integrating multi-layered hardware solutions into your infrastructure.

1 FortiGuard Labs Reports Ransomware Variants Almost Double in Six Months. Retrieved from: <https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reports-ransomware-variants-almost-double-in-six>

2 Ransomware Uncovered 2021/2022. Retrieved from: <https://www.group-ib.com/resources/threat-research/ransomware-2022.html>

3 Cloud Infrastructure Spending Closes Out the Fourth Quarter and 2021 with Strong Growth, according to IDC. Retrieved from: <https://www.idc.com/getdoc.jsp?containerId=prUS48998722>

About the Author



Camellia Chan is the CEO and Founder of Flexxon. She founded Flexxon in 2007 as a global company that specialises in next generation hardware-based cybersecurity solutions and industrial NAND flash storage devices. Camellia oversees the company's business development and growth, industry partnerships, and expansion to regional and global markets.

With a passion for innovation and a strong entrepreneurial spirit, Ms. Chan established the critical building blocks of Flexxon's brand and business in its early years and continues to guide the company forward by constantly pushing the boundaries of innovation. Ms. Chan is driven by the desire to use technology for good, and strives to create a safer space for citizens of the digital economy. Through the company's work in the cybersecurity space, Flexxon is charting a path forward that will not only help combat cybercrime more incisively, but deliver inclusive solutions. To achieve this, the company's solutions are designed to be cost-effective, user-friendly, and easily accessible.

Camellia can be reached online at flexxon@flexxon.com and at our company website <https://x-phy.com/>.

FREE SAAS SHADOW IT DISCOVERY

DON'T BE LEFT IN THE DARK

+ Self Onboarding

+ 3rd Party Apps Included

+ Compliances & Security Score Included!

- No Credit Card


- No Time Limit


- No Joke



TRUSTED BY:

 Fireblocks

 Intrusion


 OpenWeb

 Genesis

 Divvy

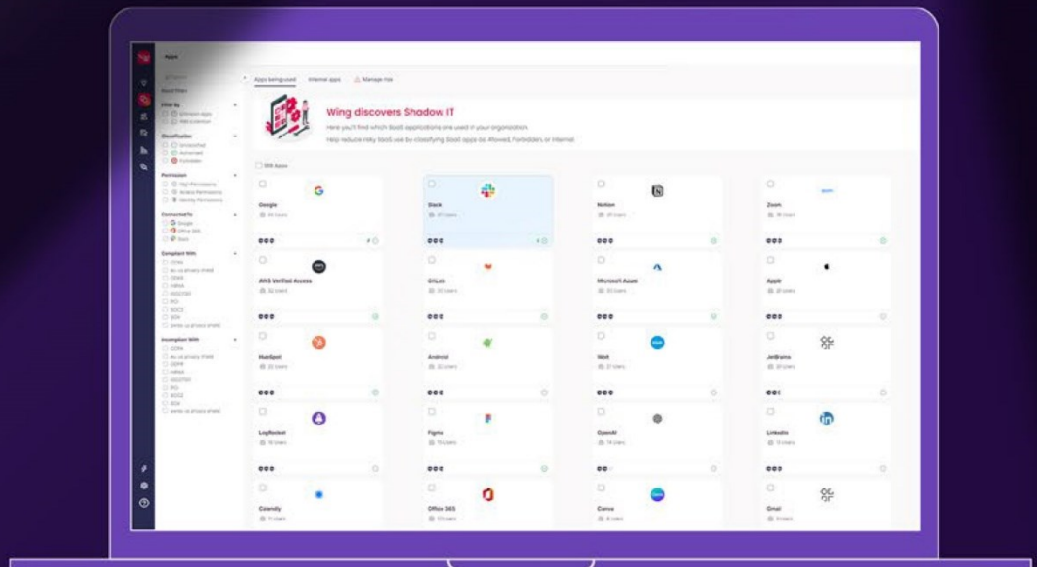
 accessiBe

 Cider

 MONTE CARLO

 BRANCH

 WING
Security



How to Improve your Security Posture and ROI

By Mark Evans, VP Marketing and Packet Capture Evangelist at Endace

Let's assume your security team has completed all the "low-hanging fruit" security essentials. They've made sure all the basic hygiene factors have been addressed – efficient patch management is in place, network and endpoint security and log collection solutions have been deployed, and alerting and security incident triage processes are working too. Not to mention, security awareness training is regularly conducted across the organization.

What, then, are the next steps to building a truly robust security posture? What do you need to put in place to help your teams combat the increasing flood of cyberattacks, eradicate alert fatigue, and prevent burnout? What will enable you to better manage security in an increasingly complex on-prem, cloud, and hybrid-cloud environment with multiple different vendor solutions in play?

How can you accomplish all this in today's climate of budget cuts, increasing workloads, and extreme shortage of skilled cybersecurity people?

Let's address four of the top cybersecurity challenges that organizations are grappling with, and what leading organizations are doing to address them.



Issue One: Stopping security teams from being overwhelmed.

Just about every article about cyber defense mentions alert fatigue – because it is a major issue in almost every organization. Security analysts are overwhelmed by the volume of alerts they receive and unable to do anything to reduce the load. The outcome is stress and burnout – then inevitably a threat is missed, resulting in the serious breach scenario that organizations were working so hard to avoid!

There's no single silver bullet to solving alert overload. But many organizations are embracing automation – leveraging SOAR tools – to eradicate some of the slow, tedious, manual work that analysts currently need to perform.

Simple mitigation tasks – such as isolating a suspect host and disabling compromised credentials – can be automated to reduce the risk of an initial attack escalating and give analysts more time to investigate and mitigate threats.

Additionally, the manual component of more complex investigation workflows – such as collecting and collating evidence – can be automated so that when an analyst starts an investigation, they have everything they need at their fingertips, rather than having to gather evidence manually and/or request data from other teams, both of which can add unnecessary delays to investigations.

Effective automation depends upon accurately identifying the type of threat that has been found and having proven playbooks in place to automate investigation workflows and streamline the human component of the process.

The best place to seek automation opportunities is by identifying what are the most prevalent incidents that consume the most analyst time. A common example is phishing attacks, where the investigation and remediation process are relatively well-defined. Automating or streamlining common workflows like this can free up considerable analyst time, while also ensuring consistent response.

Key to the successful automation of investigation and response workflows is ensuring all the evidence needed for a successful investigation is being captured and can be accessed by your SOAR solution. Investigations often fall short because critical evidence was simply never collected in the first place. Logs, flow data (NetFlow), and packet capture data must be available in addition to endpoint data and monitoring tool alerts.

Packet capture data can be particularly crucial in determining exactly what happened on the network and is an often-overlooked source of evidence. One of the first questions asked in any investigation is typically “what was this device talking to?”. The ability to quickly access and analyze a packet-level record of historical traffic that shows exactly what devices were talking to each other, and what was transmitted, can be an absolute game-changer for security analysts.

Issue Two: Protecting the crown jewels.

Obviously, it's important to protect the organization's most valuable assets above all else. But often the focus is on improving overall security posture and dealing with issues like alert fatigue. It's easy to overlook how to best protect the crown jewels.

Many organizations are implementing Zero Trust to help them restrict access to valuable data, systems and IP to only those individuals or systems that should have access.

This is a laudable initiative because it forces three things. First it forces organizations to identify what is most valuable. Secondly it forces them to clarify exactly who (or what systems) needs access to those resources. And lastly it forces organizations to examine both their network architecture and their authentication mechanisms.

Undertaking this analysis can help improve security posture across the board, as teams need to know and define what “good” looks like. Importantly, it also helps teams identify where additional monitoring and visibility is required to protect the crown jewels, and highlights which threats warrant the highest priority. If an attack is detected that may provide access to highly valuable assets, then it must be prioritized over attacks on assets of lesser value. Teams can also better target proactive security activity – such as threat hunting and deeper vulnerability analysis – in areas where it matters most.

Successful Zero Trust implementation depends on careful analysis of the environment and a methodical design and implementation process. But it’s also crucial to ensure, as you re-architect the environment, that you don’t create monitoring blind spots. Indeed, you may need to increase visibility in certain areas of the network to help better detect and defend against attacks on high-value, crown jewel assets.

You need the ability to test and validate your infrastructure as well as monitor it. So collecting the evidence you need – including network and endpoint data -- is crucial. Organizations frequently deploy additional evidence collection – such as continuous full packet capture – in segments of the network where high-value assets are located to ensure they have maximum visibility into all activity and can thoroughly test their defenses.

Issue Three: Gaining greater visibility into threats, as early as possible.

Detection tools must be as accurate as possible. That’s not an insignificant issue, given the difficulty of detecting attacks such as Zero Day threats, threats hidden inside encrypted traffic, and supply chain compromises like the Solarwinds “Solarflare” attacks that originate from trusted systems.

As network speeds increase, it’s critical to ensure that NDR, IDS and AI-based monitoring tools can keep pace. A monitoring tool that maxes out at 10 Gbps is going to flounder when network speeds increase to 40 Gbps or beyond and is going to have difficulty detecting threats that are hidden inside encrypted streams or that leverage common protocols such as DNS to disguise malicious activity, such as beaconing or data exfiltration.

AI-based detection tools can help supplement other monitoring tools by identifying anomalous behavior that might not have triggered alerts. But you also need the ability to quickly investigate these anomalies to determine whether they pose a real threat or are simply anomalous but not malicious. Again, it’s crucial for analysts to have the right evidence to quickly investigate and prioritize events and flag false positives back to detection tools to improve accuracy.

Accurately prioritizing alerts lets teams focus on the most important threats first. For this reason, streamlining the triage process is key. With the right evidence at their fingertips, analysts can prioritize and process alerts faster and more accurately. Automation can help with this too – for example, prioritizing those alerts that potentially threaten important resources, or target known vulnerabilities.

While improving detection is important, it's also critical to ensure that when detection fails (and inevitably it will) your security teams can go back in time to investigate historical activity – quickly and accurately.

Understandably, the focus of security teams is often on preventing and detecting real-time attacks. But the unfortunate outcome of this “real-time focus” is that putting in place the pre-requisites necessary to accurately reconstruct historical attacks becomes an afterthought. By the time more serious attacks – often not detected immediately – become apparent, the evidence of what happened in the initial stages of the attack often can no longer be found. Either the evidence was deleted by the attacker, or it was never collected in the first place.

The only solution to this issue is to make sure that reliable evidence is continuously collected and carefully protected. Network flow data and packet capture data are extremely valuable sources of reliable evidence because it is difficult for attackers to manipulate, delete, or avoid being tracked by them. Indeed, the fact that this data is being collected is typically invisible to the attacker.

By recording a complete history of what happens on the network – including all the rich, forensic evidence that full packet capture provides – analysts have the evidence they need to accurately reconstruct attacks -- even when the initial phase of the attack may have happened a week or a month ago. Let's face it, almost all incident investigation is looking at historical events that have already happened – so it's important to have the evidence you need to be able understand exactly what took place.

Access to reliable evidence lets analysts rapidly join the dots between what different monitoring tools may be showing them and quickly identify the root cause and scope of threats. The quicker you can see the connected phases of an attack early on, the better your chance of stopping that attack earlier in the kill chain and reducing the impact.

Issue Four: Getting better ROI from your existing investment in security tools and preparing for an uncertain future.

The security vendor landscape is daunting. There are hundreds, if not thousands, of solutions vying for your budget. All promising to remedy the shortcomings of the tools you've already spent money on.

Tempting as it might be to simplify things by looking for all-in-one solutions from a single vendor, this is often not a feasible or sensible option, there is truth to the saying “Jack of all Trades, master of none”. For one thing, you have existing investments in tools you have already deployed. For another, it's impossible for all-in-one solutions to provide the best option across all the areas of security that you need to cover. Even if you managed to find a miracle solution, the cybersecurity landscape changes so quickly that what might be fit-for-purpose now will likely be obsolete in a year or two.

So, what's the alternative?

It's essential to build a flexible and scalable infrastructure so that as your needs evolve, you can evolve your security stack to meet your needs without having to scrap everything and re-design again from the ground up.

Flexibility comes from the ability to deploy best-of-breed solutions for your organization's specific security requirements. The potential downside of this approach – and the reason all-in-one solutions initially seem attractive – is data can become “siloe” within specific tools or teams. The solution is to make integration capability a key attribute of any security tools you are looking to deploy - hopefully, you did this with the tools you have already in place!

Recognizing customers' needs to integrate solutions from different vendors is thankfully forcing vendors to focus on building this capability into their products. Integrating security tools dramatically improves visibility and flexibility – allowing you to collect and collate data to see related events in context. Integration is also essential to enable automated or streamlined workflows.

Again, it is imperative to understand what are the key sources of evidence that your teams and tools need access to if you want to ensure better ROI on your investments. The world's best detection tools can't be effective if they can't see all the data. The same goes for your teams.

As workloads move to cloud and hybrid-cloud environments, security teams are realizing they've lost visibility into network activity. As a result, many organizations are investing in solutions that give them greater control over, and visibility into, network traffic across the entire network. Building flexible and scalable traffic monitoring and evidence-collection into the infrastructure at the design level ensures your security teams always have visibility into what's currently happening on the network -- and can look back to see precisely what happened yesterday, last week or last month when needed.

Organizations are also realizing that the flexibility and scalability that cloud technology has delivered in the datacenter can be a feature of their security tool suites as well. Where traditionally security solutions were hardware based – firewalls, IDS and IPS appliances, and appliances for email or malware scanning, DDOS protection etc. – most security vendors now offer virtualized versions of their solutions for public, private, or hybrid cloud environments.

Virtualizing security functions can help eradicate “appliance sprawl” and allows organizations to design far more scalable, flexible environments where different security functions – often from multiple vendors - can be consolidated on common hardware to reduce both CAPEX and OPEX costs. Once these functions have been virtualized, the process of upgrading part of the security stack or rolling out new functionality is simpler, faster and cheaper. No longer do rollouts take months: they can now be done in hours or days. Moreover, deploying a new function is typically far less expensive because it is a software subscription rather than a costly hardware purchase. In short, virtualizing security functions can help organizations evolve to meet new threats quickly and affordably when gaps are identified.

Conclusion

Security practitioners often say effective security boils down to three things: People, Process and Technology. By focusing on making people more productive, processes more efficient, and infrastructure

more flexible and scalable, you can derive the greatest ROI from your efforts and investments. With a flexible infrastructure in place, you are better prepared to adapt and evolve to meet the challenges of an uncertain cybersecurity future as they emerge.

About the Author

Mark Evans is a Packet Capture Evangelist and has been involved in the technology industry for more than 30 years. He started in IT operations, systems and application programming and held roles as IT Manager, CIO, and CTO at technology media giant IDG Communications, before moving into technology marketing and co-founding a tech marketing consultancy. Mark now heads up global marketing for Endace, a world leader in packet capture and network recording solutions. www.endace.com.



CYBER CRIMINALS DON'T GIVE A \$#!T:

But we do, and we're
here to help!



SCADAfence

The Most Comprehensive
OT & IoT
Cyber Security Platform For
Critical Infrastructure &
Enterprises

www.SCADAfence.com

- About your project's scope.
- It's managed by a third party.
- It's a legacy system.
- It's "too critical to patch."
- About your outage windows.
- About your budget.
- That you've always done it that way.
- About your go-live date.
- It's only a pilot/proof of concept.
- About non-disclosure agreements.
- It wasn't a requirement in the contract.
- It's an internal system.
- It's really hard to change.
- It's due for replacement.
- You're not sure how to fix it.
- It's handled in the Cloud.
- About your Risk Register entry.
- The vendor doesn't support that configuration.
- It's an interim solution.
- It's [insert standard here] compliant.
- It's encrypted on disk.
- The cost-benefit doesn't stack up.
- "Nobody else could figure it out."
- You can't explain the risk to "The business."
- You've got other priorities.
- About your faith in the competence of your internal rules.
- You don't have a business justification.
- You can't show return on investment.
- That it's supposed to be "Air Gapped."

Security Leaders Are Finally Getting a Seat at The Table with Corporate Leadership – Make Good Use of Your Time There.

Looking to automation, engaging offensive security, and making the business case for building a robust cybersecurity strategy will help security leaders mature their program.

By Robert Herjavec, CEO of Cyderes

The cybersecurity threat landscape is vast, complex and ever-changing. It remains a certainty that the so-called attack surface – corporate networks, data, wireless systems and critical business processes – will continue to expand without letup at public and private companies alike. But for every measure there is a countermeasure, and so the deadly serious cat-and-mouse game continues.

The one thing that has not changed is the need to embrace constant change across the threat landscape. We are well into 2023 and already seeing shifts within cybersecurity and the economic landscape that affect security leaders.



We saw several predictions come to fruition in 2022:

Continued proliferation of identities: The complexity of digitally transformed enterprise environments – including a diverse set of endpoints, identities and internal and third-party access points – have created more vulnerabilities and opportunities for threat actors. Identity compromise continues to be adversaries' primary mode of attack.

Increasingly sophisticated attack techniques: From big game hunting (BGH) to the growth of ransomware-as-a-service (RaaS) and data leak sites (DLS), data extortion threat actors continue to innovate and evolve their tactics. New tactics such as Exmatter, [discovered last year by the Cyderes special operations team](#), indicate that threat actors are actively in the process of staging and developing the capability to outright destroy rather than encrypt data.

An overwhelming amount of security alerts and talent challenges: Increased sophistication and frequency of cyber-attacks has created an unmanageable deluge of alerts. Coupled with the continued talent shortage, more enterprises are turning to outside providers to manage these alerts, and those providers are consolidating to provide more comprehensive cybersecurity support for their customers.

Then there are some events in 2022 that simply could not have been predicted. For instance, the Russian invasion of Ukraine placed cybersecurity at the forefront of global conversations as concerns of cyber warfare and attacks on critical infrastructure spread across Europe and beyond. Business leaders also began to speculate whether threat actors would be emboldened to attack targets with greater force and frequency amid the chaos.

Later in the year when Joe Sullivan, former CSO of Uber, was found guilty of obstruction of justice and concealment of a felony, there was a new precedent set for security leaders. Suddenly, CISOs faced the added consequence that they could be held personally responsible for breaches.

In fact, there is an increasing number of laws coming out that aim to add extra layers of governance and oversight of cyber risk. For example, the SEC proposed last year that it would require public companies to disclose a breach within four days. And the White House is doubling down on regulation for industries considered critical to national security.

We were already starting to see the perception of cybersecurity shift at enterprises of all sizes, with leaders embracing security initiatives at the board level rather than confining them to IT. But the events of 2022 and increased governance has expedited this shift. In fact, the National Association of Corporate Directors (NACD) now recommends that boards of directors include at least one member with an information technology background.

The reality is that security leaders are no longer siloed — they now have a very important seat at the table. But to truly drive impact within their organization, they must evolve to take a security-oriented approach to the business, focus resources more strategically, and make it a priority to connect with leaders from across the organization.

The Cyderes [2023 Cybersecurity Conversations Report](#) is dedicated to the discussions recommended you have with your executive teams to do just that, helping you to mature your security program and stay ahead of the evolving threat landscape:

Look towards automation to modernize your SOC and focus resources on more strategic efforts:

Continued digital transformation and mass cloud adoption have created a modern business environment centered around incredible amounts of data. This has created a challenging environment for information security professionals as they attempt to stay on top of threats in the midst of so much added noise. Embracing automation can drive several key outcomes for your organization. When your security team isn't bogged down trying to manage an ever-increasing number of alerts, they are able to focus on higher-order tasks that deliver huge outcomes.

Engage offensive security to identify your greatest risks and map your security strategy: In the year ahead, expect to see increased demand for penetration testing and red/purple team offensive security services. This comes as more organizations recognize the need to pivot to proactive and continuous methods for defending their attack surface from advanced threats. Offensive Security allows enterprises to better prepare and protect enterprise IT infrastructure by closing gaps, improving controls and reducing risk. It also enables better quantification of risk, which is essential to determining the value of cybersecurity spending and managing its costs.

Make the business case for building a robust security program to your executive leaders: The first step in building your case for any investment in your cybersecurity program is to assess your current posture and identify what areas are in most critical need of improvement. Identify where you are today, what vulnerabilities exist, what your greatest risks are and what you need to do to mitigate those high-risk areas. Next, quantify the top risks likely to impact your organization. When you can put actual dollar values against the potential impact of specific risks in the event of a breach, your board will better understand how these initiatives add value to the organization.

Last year proved to be another year full of unexpected challenges and increased pressure on security leaders, but the events of the past year are putting us on the path to an even more secure, cyber-focused future.

Here's to a (cyber) safe 2023.

About the Author

Robert Herjavec is CEO of Cyderes. He is a globally recognized motivational, business, and cybersecurity leader. For the past 14 years, Robert has been well known as one of the Sharks and executive producer of the Emmy-award winning hit show, Shark Tank. He is a successful, best-selling author and has appeared on stage with crowds from 50 to 20,000 people and with luminaries such as Tony Robbins and Oprah. For more information about Cyderes, go to <https://www.cyderes.com/>





We will focus on your cybersecurity, so you can focus on your business.

We have the right mix of people, processes,
and technology to build your robust security
program and respond successfully to
any threat that comes your way.

**Cyber Defense
& Response.**

It's what we do.

cyderes.com

OT Zero Trust

The Last Frontier to Protect OT Environments

By Terence Liu, CEO of TXOne Networks

OT Zero Trust – a Device-Centric Methodology

In the IT world, the heart of Zero Trust is continuous verification, ensuring that every point of entry between connected services is from an authorized identity, at the proper time, from the expected source, through registered devices. This is a very human-centric and contextual process. Due to a high level of interaction between people through various services, any compromised personnel can pose threats to the entire organization.

In the OT world, devices and equipment are seldom bound to specific personnel. Despite its similarities in damage propagation to the IT world, OT countermeasures are totally different. Here at TXOne Networks, we advocate OT Zero Trust methodology, which is also a process of continuous verification. However, it is a device-centric, rather than people-centric, approach that covers all stages in the asset lifecycle. Every piece of equipment should be inspected before being sent to the production line, and all equipment should be continuously monitored and protected while in the process of manufacturing. IT people can easily sacrifice a portion of service availability for a boost in security during a given period.



But OT people need to do it the other way around because, in OT environments, system availability is king.

OT Zero Trust methodology is a framework wherein every asset is covered by at least one security countermeasure during its entire lifecycle. An asset's lifecycle includes pre-service inspection, endpoint protection, and network defense.

The Practicalities of OT Zero Trust Methodology

In our field experience, the No.1 hurdle for OT security managers hasn't been budgetary limitations, nor their professional knowledge of cybersecurity that prevents them from pursuing a higher level of security. It's a lack of manpower.

Imagine a factory plant with thousands of devices scattered over tens of acres, managed only by two professional OT security managers. That should paint a clear picture of why fancy IT security features are not the solution.

Only when OT Zero Trust is applied to practical security implementations will it make sense. Avoid bringing up more questions while trying to answer one. Pinpoint the exact path for the user to follow instead. The answer does not lie within the slight differences of detection rates among ill-suited solutions, but in an environment tailor-made to address OT-specific security requirements and conditions.

A Higher Call for OT Zero Trust – The Last Frontier of Defense

In our recent survey from 300 C-level executives or directors in charge of OT security, 94% of them experienced OT incidents that originated from IT. We see a clear trend that more and more ransomware-based outbreaks in OT are targeted attacks. If hackers can break through layered IT security defenses and retrieve all credentials to drop/spread ransomware in the OT space, deploying the same solutions in OT is not likely to help intercept malicious acts. The only solution is extensive OT security awareness – a contextual, situational awareness involving deep insight of OT activities.

In addition to examining the level of security with OT-specific signature intelligence, the Extended OT Zero Trust also reacts to items based on insights into the day-to-day operation norms in OT. For example, an Extended OT Zero Trust can confidently trigger the alarm when it sees a commonplace command over common protocols if the operation context never involved such protocols before.

This contextual awareness goes beyond traditional security approaches and requires a great deal of industrial insights and technologies such as AI; achieving this level of awareness is the ultimate goal of OT Zero Trust. Never trust. Always verify - and verify with industrial context.

To sum up, OT Zero Trust is a new but significant security paradigm that we need to shift into. We're eager to see it realize its potential and thrilled to be among its first pioneers.

About the Author

Dr. Terence Liu leads TXOne Networks, a cybersecurity company focusing on protecting OT and ICS with unique OT Zero Trust approach. Especially, TXOne's comprehensive solutions protect the mission-critical assets including the services and applications within as well as their network communication. The protection starts right after the onboarding of the assets, and throughout the staging, production, all the way to the maintenance phases, back and forth. Today TXOne has thousands of satisfied enterprise customers in a variety of verticals.

TXOne Networks official site <http://www.txone.com/>.





Industrial Cybersecurity. **Simplified.**



Keep the Operation
Running

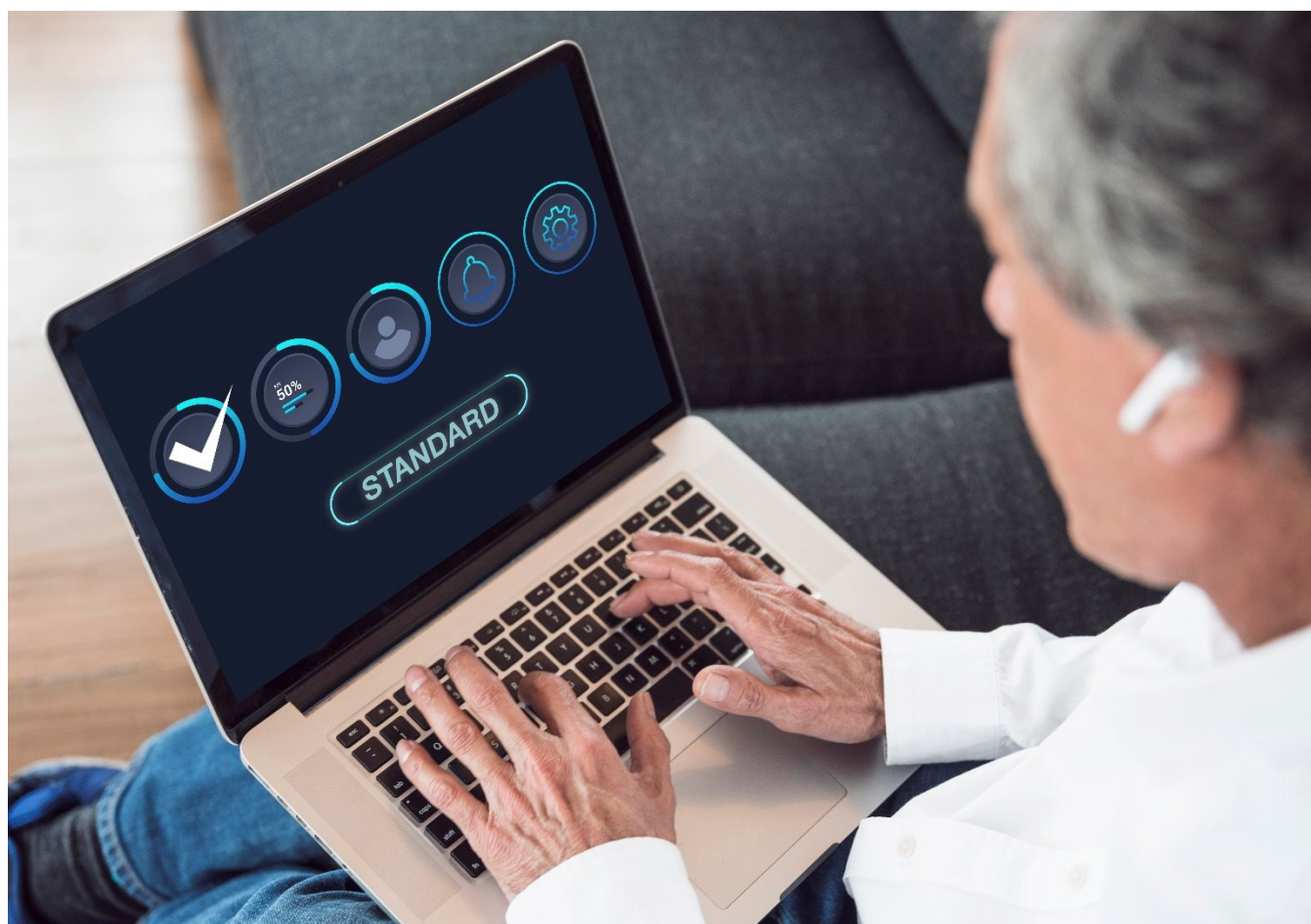
Copyright © 2023 TXOne Networks. All rights reserved.

txone.com

Enhance Employee Productivity by Adopting a Modern Approach to Password Security

By Joshua Parsons, Product Marketing Manager at Enzoic

For decades, enterprise security measures and employee productivity were seemingly at odds. In fact, 37% of respondents in a recent [Vanson Bourne](#) study indicate that security and regulatory policies are the chief inhibitors of their productivity and digital experience. Arguably, no area of security has been perceived as more counterproductive to employee efficiency than password management.



It's no secret that mandating a unique password for every account or system is a source of user frustration. Even in an enterprise environment in which access to many accounts is enabled via Active Directory, employees still find legacy password management approaches to be burdensome. They're not wrong—in fact, not only are these outdated policies a significant hurdle to productivity, but they also have an adverse effect on corporate security.

Security Shouldn't Come at the Cost of Productivity

Let us take a look at some of these legacy practices and why companies must abandon them in favor of a more modern approach to password security.

Eliminate Mandatory Password Resets

Enforcing periodic resets has been the traditional strategy for combating employees' poor password practices, like reusing them across multiple accounts, selecting generic ones like "Password" or "1234," or sharing credentials with colleagues. Multiple studies have documented that mandatory password resets require significant IT resources and don't enhance security, as people tend to choose simple passwords or make small changes to the root phrase when they know they will be required to change it again in the near future.

Abandon Complexity Requirements

Arbitrary password complexity requirements—such as including both upper- and lower-case letters, numbers, and special characters—are another legacy practice that inhibits productivity. Moreover, this approach often results in passwords that are easy for hackers to guess or crack. For example, "P@ssword1!" would meet all complexity requirements but is obviously a weak credential guaranteed to exist on a list of exposed passwords available to hackers on the Dark Web.

Get Password Security and Productivity in Lock-Step

The legacy practices above are just two examples that the National Institute of Standards and Technology (NIST) [now recommends against](#) due to their negative impact on employee productivity and account security.

So, what should companies be doing instead to secure passwords? A more modern approach is to screen all passwords against a list of commonly known and exposed credentials. After all, if a password is secure there's no point forcing users to change it every three months or comply with various complexity requirements. Many static lists of exposed credentials exist on the Dark Web and some companies even curate their own. However, given the staggering rate at which new breach data is exposed, the only way

to ensure password security is to continuously screen credentials against a dynamic database that is updated with the latest threat intelligence.

How Enzoic Gives Enterprises Password Peace of Mind

This is where Enzoic comes in. Our proprietary [credential screening solution](#) screens all proposed passwords against our continuously updated database. This extensive database contains billions of passwords exposed in data breaches and found in cracking dictionaries. In addition to complying with NIST's guidelines to screen passwords at their creation, Enzoic takes it a step further by vetting their integrity on an ongoing basis. Our database automatically updates multiple times per day, ensuring that every organization's password security reflects the latest breach intelligence without burdening the IT department with the details.

Zero Employee Friction

Another benefit of abandoning legacy password security approaches in favor of a modern credential screening solution is that verifying password integrity happens entirely in the background. Uncompromised employees gain efficient access to their accounts without adding additional steps or device requirements, as is the case with multi-factor authentication, one-time passwords, or other authentication mechanisms that introduce more friction. Should a previously secure password become compromised, companies can automate their response to force a password reset or use an existing secondary authentication method to verify the employee's identity.

Securing the Future of Hybrid Work

With the adoption of hybrid work environments, the need for secure passwords to combat this growing attack surface becomes increasingly important. A modern password management approach that continuously screens for credential compromise is the best way that organizations can secure this complex environment while simultaneously enhancing employee productivity.

[Click here](#) to learn more about how Enzoic's solutions can help you strike the right balance between password security and employee productivity.

About the Author

Joshua J. Parsons is the Product Marketing Manager at Enzoic, where he leads the development and execution of strategies to bring innovative threat intelligence solutions to market. He has had a lifelong interest in digital innovation and how it can be used to protect individuals and organizations from ever-changing cyber threats. A strong believer in giving back to the community, Joshua serves as a mentor to those interested in information security and marketing through his alma mater, the University of Michigan. Outside of work, he can be found at the nearest bookstore or exploring the city's local coffee scene.

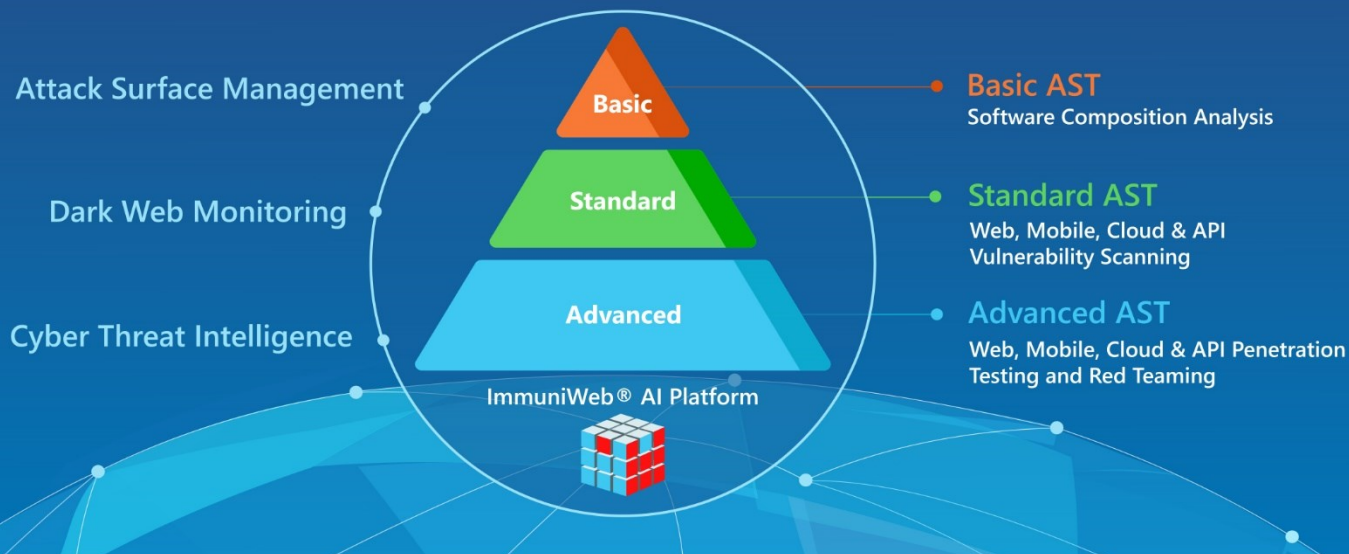
Joshua can be reached online on LinkedIn ([linkedin.com/in/jjparson](https://www.linkedin.com/in/jjparson)) and at our company website <http://www.Enzoic.com/>





The award-winning ImmuniWeb® AI Platform helps over 1,000 customers from over 50 countries to test, secure and protect their web and mobile applications, cloud and network infrastructure, to prevent supply chain attacks and data breaches, and to comply with regulatory requirements.

Risk-Based and Threat-Aware Application Security Testing (AST)



ImmuniWeb® Discovery

Attack Surface Management
and Dark Web Monitoring



ImmuniWeb® Neuron

Premium Web Application
Security Scanning



ImmuniWeb® On-Demand

Web Application Penetration Testing



ImmuniWeb® MobileSuite

Mobile Application Penetration Testing



ImmuniWeb® Continuous

Continuous Penetration Testing



www.immuniweb.com

Email: sales@immuniweb.com

Phone: +41 22 560 6800



Complexity is Still the Enemy of Security

Ease of Use, Ease of Integration Encourages Data Protection

By Gregory Hoffer, CEO of Coviant Software

In 1999 noted cybersecurity expert Bruce Schneier wrote in his Schneier on Security blog that, “The worst enemy of security is complexity. This has been true since the beginning of computers, and it’s likely to be true for the foreseeable future.” In the context of that post Schneier explained that complexities inherent in the design of technology products made it difficult to simultaneously test whether the product was secure. Whether software, hardware, or interconnected systems, you built a product to do a certain job and only when completed could it be tested to see if it was secure. Even then, Schneier observed, testing for security was not a high priority.



“This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere,” Schneier continued.

It's Not 1999 Anymore

The now common “security by design” approach was not yet in vogue, even though threat actors and cyberattacks were on the rise and recognized as a problem. Security flaws were an accepted part of using technology; a cost of doing business. A 1999 article from [CNN Sci-Tech](#) on cyberattacks reported that financial losses “rose to more than \$100 million for the third straight year.” How quaint. Fast forward to 2023 and some estimates have the total cost of cybercrime reaching a staggering \$8 *trillion* this year.

Today’s technologies are far from perfect, but cybersecurity is top of mind for most organizations, and the array of tools and services available to protect networks and data go far beyond the seemingly primitive firewall and anti-virus approach that was common a quarter century ago. Still, complexity remains an enemy of security, but not just in the way described by Mr. Schneier.

Even if created using the security by design approach, and tested to assure an absence of known vulnerabilities, when technology is difficult to use it can cause people to avoid using the product and instead find unsecure workarounds, thereby creating more security issues for the organization. At times those workarounds manifest as a stubborn refusal to abandon the old processes or, if that is not an option, to create a new way to complete whatever task is involved. That’s a natural response to change when the new way is (actually or merely perceived as) complicated. And when that happens, complexity’s enmity with security will rear its ugly head.

Workarounds are Anti-Security

We have seen this far too often in the realm of data transfer. Unfortunately, there is no shortage of easy and familiar ways of sending data from one place to another that are far from secure, so when that secure but complex process frustrates staff, they may look for an easier solution like email, file sharing utilities, or consumer-grade cloud services. These work just fine when you want to send grandma a bunch of photos and videos of the kids’ dance recital or the family’s summer trip to the Grand Canyon, but not when sending business-critical files. When these are the solutions that organizations use to send sensitive, even regulated, data like personally identifiable information (PII), [protected health information](#) (PHI), intellectual property, financial files, and data associated with [contractual obligations](#), it puts everyone at risk.

Some organizations believe they can solve the problem themselves by creating an in-house file sharing process that combines some existing components, open-source software, and a bit of ingenuity from someone on the IT team. Once again, the problem is usually that the resulting solution is a bit convoluted which can discourage its use. And roll-your-own tools are rarely ever documented by the person who created them, inevitably leading to problems when that person leaves the organization, gets sick, or goes on vacation.

Another thing to consider is: what happens when something breaks, a key piece of software becomes obsolete and unsupported, or a trading partner changes their standards? When the poop hits the fan ten years after the guy from IT who wrote the code left the company, where do you go for support? It's a lot to ask someone to try and solve a miasmic puzzle of code, bug fixes, extensions, and inexpertly bolted-on changes. Furthermore, in-house solutions lack features necessary for ensuring file security and for proving compliance with any applicable regulations. If a file goes missing and you can't prove that it was encrypted, the assumption must be that the data are compromised.

Make Security Easy

And finally, even when a commercial managed file transfer product is picked, there may be inherent complexities that make it difficult to implement and confusing to use. Too many customizations, both of features that should be standard and of some that are unnecessary, increase the chances of getting things wrong, either through omission or commission. And then there is the all-too-common bottom-up implementations that require vendor-specific "pseudo-coding" language to navigate to ensure you are getting all the functionality that is needed to do the job instead of intuitive top-down implementations consistent with the no-code ethic.

When the goal is to deliver a product that is supposed to help an organization conduct their business securely, it doesn't help to undermine those efforts by delivering a product that is difficult to use. A cynic might wonder if the complexity is not a bug, but a feature designed to get the customer to buy into costly support contract and, ultimately, fall victim to the sunk cost fallacy. That may be a good (if short-sighted) business strategy, but it is not a sound approach to cybersecurity.

We are All Security Stakeholders

The White House's recent *National Cybersecurity Strategy* states that, "To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community."

We believe that every technology vendor is a stakeholder in strengthening our national cybersecurity. As such, every technology vendor should work to make products that are secure by design, and that includes designed to be easy to install and use. Security should not be frustrating to the user. We are the ones with the skills to make the security experience integral to our products and easy for the user by using things like [process automation](#) to tackle essential steps that might be skipped or forgotten, to backstop the customer with alerts and documentation, and to not only streamline the functions our products perform, but to make the people and organizations who use our products more productive.

About the Author

Gregory Hoffer is CEO of San Antonio-based Coviant Software, maker of the secure, managed file transfer platform Diplomat MFT. Greg's career spans more than two decades of successful organizational leadership and award-winning product development. He was instrumental in establishing groundbreaking technology partnerships that helped accomplish Federal Information Processing Standards (FIPS), the DMZ Gateway, OpenPGP, and other features essential for protecting large files and data in transit.



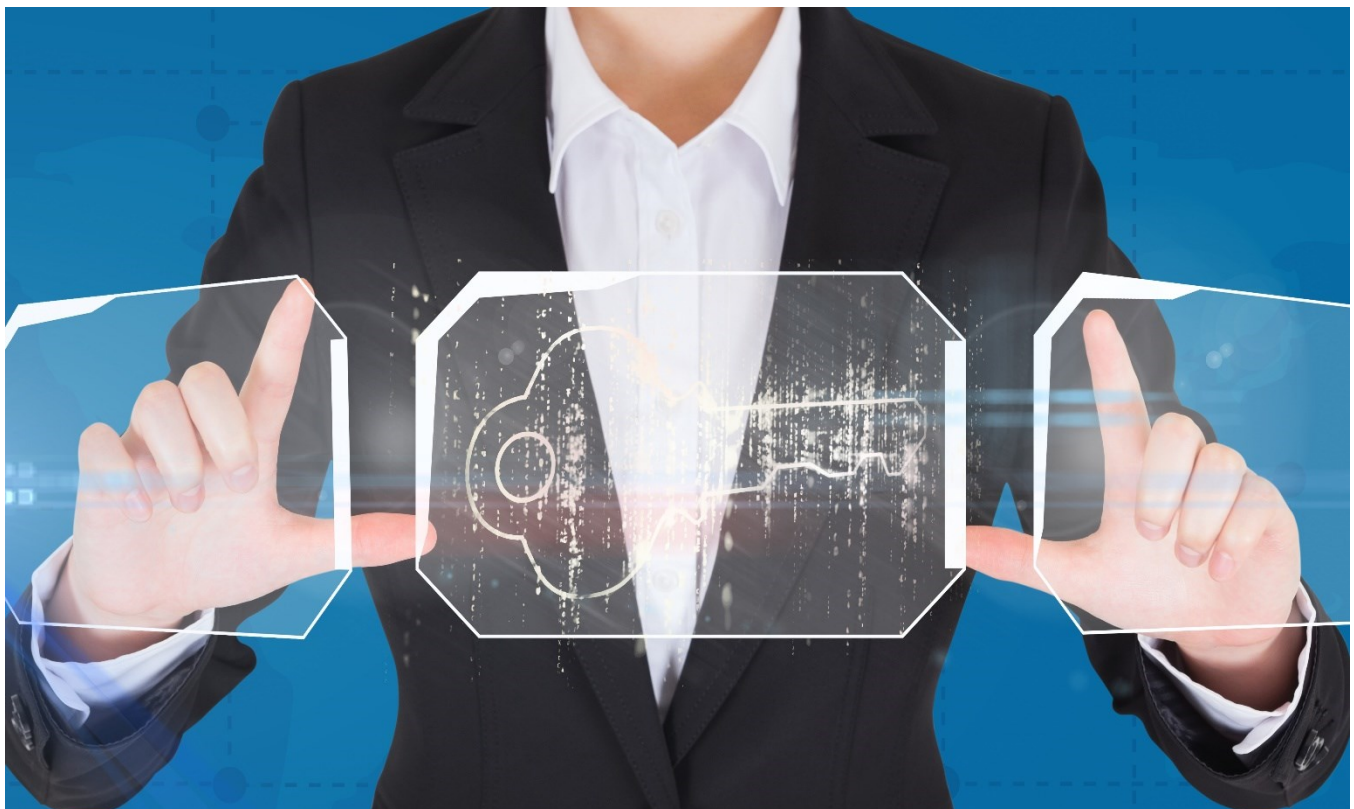
For more information visit [Coviant Software](#) online, or follow [Coviant Software](#) on Twitter and [LinkedIn](#).

Making a Business Case for Cyber Threat Intelligence: Unveiling the Value Realization Framework

By Kaustubh Medhe, Head of Research and Intelligence at Cyble

Cybercriminal motivations rarely change over time. A typical cyberattack is carried out for one of the following reasons -

1. Illicit financial gain via disruptive attacks such as ransomware, denial-of-service (DoS) or cryptocurrency theft
2. Intellectual property theft or corporate espionage for strategic competitive advantage
3. Sensitive data exfiltration for geo-political supremacy
4. Influencing public opinion by propagating a false/biased narrative through misinformation or disinformation campaigns for achieving socio-political objectives



What changes, however, is the approach and the modus operandi for carrying out such attacks.

In 2022, Threat Actors (TAs) were observed targeting security technology vendors and service providers that enjoyed a certain degree of trust and confidence in the industry.

In January 2022, Okta, a leading cloud-based identity management provider, was targeted in a well-planned attack, where TAs compromised a computer system of a customer support engineer employed with Okta's third-party IT services vendor. Using this as a pivot, the TA then swept Okta's internal network to access confidential information. While the attacker managed to get access to internal communication and ticketing tools only for a limited period and could not access any significant critical information, the incident demonstrated the relative ease with which an attacker can get past security defenses by abusing the inherent trust that an organization typically places on its third parties.

In June and July 2022, TAs targeted employees of Twilio – a leading customer engagement platform provider, with a well-orchestrated SMS phishing and Vishing campaign to steal their user accounts, passwords, and OTPs (One-time passwords used as a second factor of authentication) to access the sensitive contact information of its customers. The TAs also managed to register and link their own devices with a few customer accounts.

In August and December 2022, LastPass – the leading provider of Password management software reported a breach, wherein the attackers were able to access and copy sensitive customer information, that included not only end-user names, billing and email addresses, telephone numbers, IP addresses, but also sensitive vault data including usernames, passwords, and secure notes etc.

NortonLifeLock, another password management software vendor, reported that nearly 6000 customer accounts had been compromised via a credential stuffing attack, forcing the company to enforce a password reset and advising users to implement two-factor authentication.

Cyble's Darkweb Intelligence teams noticed several posts on cybercrime forums and the darkweb sites wherein TAs were seen soliciting access to cyber threat intelligence platform providers to get to their customers. Hackers also claimed to have successfully breached cybersecurity service providers offering security monitoring services, security assessment and penetration testing services, as well as data backup and recovery services. In addition, hackers were seen advertising the sensitive information of clients of victim companies on various cybercrime marketplaces and forums.

Recently, leading Cloud infrastructure and SaaS application providers such as Microsoft Azure and Atlassian have published detailed incident investigations wherein cyber TAs were seen bypassing the trusted SMS OTP based multi-factor authentication security by using stolen authentication cookies to login to the accounts of users. These user systems had been compromised using information-stealing malware.

Cyble's Threat Research team also discovered TA communication on the darkweb, associated with malware and phishing services being offered for sale and claiming to be designed in a way to bypass OTP-based two-factor authentication mechanisms to compromise a target. *Thus, OTP-based two-factor authentication is now being actively targeted and bypassed in advanced attack campaigns by skilled attackers.*

In addition, Cyble's researchers also encountered several posts on cybercrime forums advertising Extended Validation Code Signing certificates. These services enable criminals to digitally sign malicious code/binaries with digital certificates stolen from legitimate publishers to deceive the operating system and the anti-virus software into "trusting" these malicious binaries and allowing them to execute on the target's computer system. Thereby, they allow cybercriminals to install malware by bypassing the software security and anti-virus security mechanism on the victim's operating system.

By successfully attacking and bypassing "trusted" technologies and exploiting the trust relationship between organizations and their third-party service providers, TAs have now spawned a new trend that is expected to continue well into 2023 and beyond.

Our industry should brace for more such attacks in the future that target the trusted supply chain.

Social media has emerged as the next frontier for information warfare, with miscommunication and disinformation campaigns being routinely designed and launched to proliferate biased, false, or misleading information in masse to sway public opinion and cause financial, economic, or reputational damage to institutions and individuals. Coupled with the popularity of deep fake AI audio and video phenomenon, social media can amplify harmful content that could potentially have far-reaching ramifications for political regimes, the market performance of corporates, and personal reputations of people holding important positions in the public and/or private enterprise.

2022 saw glimpses of these risks materializing and causing widespread panic and confusion. A fake tweet from a Twitter account bearing the name and logo of Eli Lilly, the pharmaceutical company, announced that it was "making insulin free". This sparked widespread panic that led to the stock price falling by 4.37%. The Twitter account carried a blue tick mark signifying the account's authenticity, which further aggravated the confusion.

During the early days of the Ukraine-Russia conflict, a video portraying the President of Ukraine exhorting his people to lay down arms and surrender also emerged on social media and received much media attention. While the seemingly real looking video was quickly dismissed to be a creation of AI technology, it did trigger serious conversation and debate around the risks of misuse of deep fakes for sowing the seeds of distrust and suspicion and their potential for business and reputational damage to large corporations and enterprises.

Several organizations reportedly fell prey to smishing or vishing scams that involved a scamster creating a fake social media account or a chat messenger profile carrying an image of a senior executive or the CEO and coercing gullible employees into effecting a fraudulent wire transfer or a gift card transaction on their behalf.

Cybercriminals are increasingly adopting novel techniques that synthesize social media, artificial intelligence, and personal communication technology to target their victims via a highly personalized attack that aims to exploit the implicit trust relationship between brands, personalities, and individuals.

Several organizations have jumped on the proverbial digital transformation bandwagon exhorting their IT and software development departments to "move fast and break things". Open-source software underpins most such digital initiatives. With active communities of open-source software developers that freely share code and packages via public code repositories and also offer altruistic technical support,

software teams almost always turn to code re-use from various third-party sources such as GitHub and Node Package Manager (NPM) for accelerated code development.

While the availability of “ready to use” open-source software is a boon for rapid development and for meeting aggressive go-live deadlines, such methods unfortunately expose organizations to hidden software supply chain security risks.

Since late 2021 and throughout 2022, security researchers have reported several incidents where cyberattackers were found to have “poisoned” thousands of npm packages with malicious code designed to silently steal credentials, access tokens, API keys, install botnets or execute cryptocurrency mining software on developer systems as well as development/production servers. Such stolen information is then invariably used to launch a follow-up attack on the infected organization.

Because thousands of npm packages are being published monthly and used by over 60% of software developers, it is one of most lethal and stealthy attack vectors that can be used to launch mass scale attacks and compromise multiple organizations.

While network and endpoint security solutions have achieved decent adoption and penetration within the industry, the importance of software security and secure software development processes is lost on the average organization. As a result, software security lags the cyber threats that have evolved to take advantage of the general neglect and ignorance when it comes to securing the software development life cycle.

As is evident, the threat landscape is changing rapidly, and cyber adversaries have now turned to weaponizing trust and ignorance to target their victims with sophisticated tactics.

How can organizations counter such risks?

A few key initiatives that organizations can take to identify and manage such risks include -

1. Drawing up an inventory of trusted technologies and third parties and conducting a risk assessment to understand their exposure in the event that the trusted technology or supply chain partner were to be breached.
2. Designing and testing incident response plans to assist the organization to resume operations or recover securely in the event of a trusted attack.
3. Conducting organization-wide security awareness and training programs that educate staff on identifying and responding appropriately to newly emerging cyberattack campaigns designed to abuse trust.
4. Implementing multi-factor authentication mechanisms to prevent the risk of account compromise.
5. Reviewing and strengthening security configurations of their SaaS vendors
6. Reducing sensitive data sprawl to minimize the risk of data exposure from a breach.
7. Instituting a software security life-cycle program to identify the prevalence of risks due to open-source software and the necessary processes to secure the software supply chain.

Finally, organizations that wish to implement proactive cybersecurity should consider partnering with a cyber threat intelligence service provider to help stay up-to-date with evolving adversarial tactics and techniques. Actionable and timely information shared by threat intelligence providers can be used by information security leaders to make prudent risk-based security decisions and to implement critical policies or technical controls to reduce the likelihood of a similar attack from affecting their operations.

About the Author

Kaustubh Medhe – Head of Research and Intelligence at Cyble

Kaustubh Medhe is a security and privacy leader with over 2 decades of experience in information security consulting, audit, fraud risk management and cyber defence operations.

At Cyble, he leads Research and Cyber Threat Intelligence Services for clients globally.

Kaustubh is a Fellow of Information Privacy (IAPP) and holds the CIPP/E and CIPM credentials.



Kaustubh has executed and led information risk management programs for some of the largest clients in banking, insurance, retail and oil and gas industry in India, US, APAC, and the Middle East.

Prior to joining Cyble, Kaustubh was instrumental in setting up and operationalizing a threat intelligence enabled cyber defence centre at Reliance Industries, for one of the largest conglomerates globally with over 250K employees and 50K globally distributed assets (on-premises and the cloud).

Kaustubh was also associated with global managed security services providers such as Paladion (now ATOS) and Happiest Minds Technologies, where he led their Cyber Security and SOC Practice.

Cyble (YC W21) is a leading global cyber intelligence firm that helps organizations manage cyber risks by utilizing patent-pending AI-powered threat intelligence. With a focus on gathering intelligence from the deep, dark, and surface web, the company has quickly established itself as one of the pioneers in space. Cyble has received recognition from Forbes and other esteemed organizations for its cutting-edge threat research. The company is well-known for its contributions to the cybersecurity community and has been recognized by organizations such as Facebook, Cisco, and the US Government. You can visit the company website at <http://www.cyble.com>.



1 Platform- 6 Capabilities

Darkweb & Deepweb

Attack Surface Management

Brand Intelligence

Cyber Threat Intelligence

Vulnerability Management

Takedown & Disruption

[Learn More ►](#)



Going into the Darknet: How Cynet Lighthouse Services Keep Cybersecurity Teams One Step Ahead of Hackers

By monitoring the darknet, as well as underground forums, Cynet is able to identify and prepare for the latest cybersecurity threats before they reach deafening levels.

By Eyal Gruner, Co-Founder and CEO of Cynet

Data breaches are far from new, but the scale of attacks and sophistication of the attackers has reached all new levels in recent years. Since the pandemic, with the rise in remote work environments and work from home setups, compromised credentials became the most common initial access vector for data breaches in 2022 [according to IBM](#) – leading to rampant cybersecurity attacks. Because of the anonymity it offers, the darknet is fertile ground for bad actors looking to buy, sell, and trade large datasets of credential that can be used to access compromised accounts and systems left unchecked.



The alarming rise in compromised credentials led Cynet to launch its Lighthouse Service which monitors underground forums, private groups, and malicious servers for evidence of compromised credentials within the environment – taking its [MDR team \(CyOps\)](#) into the darknet and underground forums to search for potential cybersecurity threats before they become full-on attacks. Unlike traditional darknet monitoring services, Cynet focuses primarily on credential theft monitoring because of the swift rise in leaked credentials.

A Primer on the Darknet and Underground Forums

Unlike the internet we all use to work, shop, and connect online, users must download a special Tor browser or browser add-ons to navigate the darknet. Because there is no link between a user and the user's IP, the darknet requires specific access (software, configurations, authorization) – thus making it a prime location for illegal activity. Industry analysts estimate that the darknet accounts for 4% to 6% of internet content, with as many as three million users per day.

But the darknet is not the only gathering spot for cybercriminals. The internet we use on a daily basis (Clearnet) also houses underground forums that fuel and empower threat actors. The now seized "RaidForums" and its predecessor, "Breached," are two popular sites that can be accessed via common web browsers. While the two are accessible to the public, their forums are not accessible. A lot of these underground forums are inaccessible for most people and require certain levels of "street cred" among the community of hackers to enter. To access these forums, users often must be known on other similar forums or have other users vouch for them. Another option is to pay for access.

Because these forums still rely on anonymity, the communities have developed an ecosystem where users can buy credits and then transfer the credits into currency used to purchase databases, services, and malware posted on the forums.

By monitoring these forums, along with conversations and activity happening across the darknet, Cynet's research team is able to access the very places where threat actors share information, data, and malware with each other.

Things You Learn about Cybersecurity While Monitoring the Darknet

One of the primary cybersecurity insights Cynet has gained through its Lighthouse Service is that there is an enormous market for "Info Stealer" malware (malicious software that captures personal information from a computer). Once upon a time, hackers were heavily focused on attacking banking and financial information, but that's no longer the case. Cyber criminals are using "Info Stealer" malware to find compromised credentials for all organizations, actively planning large, sophisticated campaigns to target assets for both enterprises and small to midsize businesses.

This malicious activity has led to an entire ecosystem of compromised credentials available on darknet marketplaces in the last few years. And it's not just "Info Stealer" malware that's causing serious concerns

among cybersecurity professionals. Hackers are still leaning heavily on the tools they've been using since the dawn of cybercrime: ransomware, Trojans, Spyware and adware to name a few.

Lighthouse Services: An Additional Layer of Cybersecurity Protection for the Security Teams That Need It Most

No matter how effective your cybersecurity solution may be, company assets can still be compromised when used outside of the organization's security boundaries. When business devices (laptops, phones and tablets) are not secured by the organization's EDR or XDR platforms, they create a blind spot for the cybersecurity team charged with safeguarding the business. While security professionals are monitoring their networks watching for attacks, a hacker can simply walk into the perimeter using compromised credentials.

Cynet's Lighthouse Service helps prevent these attacks by monitoring daily activity on underground communities, hunting for new threats and pinpointing leaked credentials. Lighthouse's capabilities allow Cynet to link a host computer to any compromised credentials found so that it can help its clients identify the exact device that was compromised vs. trying to figure out which user was connected to the compromised assets.

Another worthy mention is Cynet's research team (Orion) that tracks new techniques and malware. The combination of Lighthouse and the Orion team's efforts validates that Cynet customers are protected both in the organization parameter and outside of it. Cynet can implement new detections to stop related attacks. Not only have Cynet customers gained an added layer of protection, Cynet is able to assist organizations that are not Cynet users, notifying multiple global CERT teams regarding critical infrastructure credentials that have been found within the darknet and underground communities.

As part of the cybersecurity industry, Cynet's ultimate goal is to create a safer world for companies and consumers alike. Its Lighthouse Service is another layer of defense for outside parameters – going into the darkest places online so that customers don't have to.

About the Author

Eyal Gruner is the Co-Founder and CEO of Cynet. He is also Co-Founder and former CEO of BugSec, Israel's leading cyber consultancy, and Versafe, acquired by F5 Networks. Gruner began his career at age 15 by hacking into his bank's atm to show the weakness of their security and has been recognized in Google's security Hall of Fame.

Eyal can be reached online at <https://www.linkedin.com/in/eyal-gruner/> and at our company website www.Cynet.com.



How To Survive a Ransomware Attack and Fix Ransomware Breach Face

By Derek Nugent, Vice President of Revenue at Difenda

Ransomware attacks have become a growing concern for businesses and individuals alike. Each year there are over 236.1 million ransomware attacks globally. The frequency of successful ransomware attacks has increased dramatically in recent years, and the damage caused by these attacks can be severe, including but not limited to emotional distress such as #RansomwareBreachFace, financial loss, data loss, business interruption, and reputational damage.

For example, in July 2021 a group of threat actors targeted the Florida-based software company, [Kaseya](#), using a vulnerability in their VSA software. The attackers compromised over 1,000 businesses worldwide and demanded a ransom of \$70 million in Bitcoin to release the encrypted data. The attack caused widespread disruption to businesses, with many unable to access their systems or data. Some businesses even had to shut down operations temporarily, and others lost valuable data.

Ransomware attacks like this one cost the world \$20 billion in 2021. That number is expected to rise to \$265 billion by 2031. Thousands of people are suffering from ransomware breach face every day.

CONSOLIDATION AND SIMPLIFICATION:

THE **FUTURE** OF CYBERSECURITY MANAGEMENT

Read the white paper

WWW.DIFENDA.COM | SALES@DIFENDA.COM | 1.866.252.2103



What is Ransomware breach face?

“Ransomware Breach Face” (#RBF) is a term coined by Difenda that refers to the reaction of people who unintentionally cause a cyber breach within their company. This can happen when someone clicks on a phishing email or receives a ransom note.

The main causes of #RBF are human error and lack of visibility into the security environment. Human error occurs when employees make mistakes such as downloading suspicious attachments, visiting malicious websites, or sharing sensitive information with unauthorized people, leading to a breach. In many cases, these actions are performed unknowingly, but they can have serious consequences.

The second major cause of successful ransomware attacks is a lack of visibility into the cybersecurity environment. Many organizations lack visibility into their network and endpoint activities, making it difficult to detect and respond to cyber threats in a timely manner. In many cases, cybercriminals will use encryption and other methods to hide their tracks, making it difficult for organizations to detect a ransomware attack until it is too late. This lack of visibility can lead to #RBF and other significant consequences for the business.

#RBF can cause major disruptions to business operations, as well as financial losses and damage to an organization’s reputation.

So, how did we get here?

Despite coming a long way from where we were five years ago, Ransomware Breach Face is at an all-time high and we are actually observing more serious ransomware breaches globally. Today, the average downtime caused by a ransomware attack is 12 days.

Some of the main reasons for increased successful ransomware attacks include:

1. As organizations continue to rapidly adopt emerging cybersecurity technologies, they are inadvertently complicating their operations and creating blind spots in their data protection infrastructure.
2. With a significant increase in remote work many organizations have struggled to secure their remote networks and endpoints, making them more vulnerable to ransomware attacks. With more employees working from home, attackers have more opportunities to exploit security gaps and breach an organization’s network.
3. Attackers are constantly evolving their tactics and techniques to bypass traditional security measures and exploit vulnerabilities in new ways.
4. The growth of the ransomware-as-a-service (RaaS) model has also made it easier for attackers with limited technical knowledge to launch ransomware attacks. RaaS providers offer turnkey solutions that include malware, hosting, and support services, making it easier for attackers to launch sophisticated attacks.
5. Cybersecurity analysts are receiving hundreds of alerts a day and security teams can’t determine what to look at or when to look at it. The sheer volume of data generated by cybersecurity tools, coupled with the constant changes in the threat landscape and regulatory requirements is creating a perfect storm that many organizations can’t handle alone.

To combat these evolving threats and more, organizations need to take a proactive and holistic approach to cybersecurity that includes a combination of people, process, and technology. Ultimately, it’s important

for organizations to prioritize cybersecurity as a strategic business initiative and invest in the resources necessary to protect their systems and data from the growing threat of ransomware attacks.

How To Survive a Ransomware Attack

In the unfortunate event that your organization becomes a victim of a ransomware attack, navigating the situation and minimizing the impact can be complicated. Working with a trusted and experienced cybersecurity partner can significantly streamline the response process and mitigate risk. Here's some best practices and tips for surviving a ransomware attack:

- **Disconnect affected systems:** The first step is to disconnect any affected systems from the network to prevent the malware from spreading further.
- **Assess the damage:** Quickly assess the scope of the attack, identify which systems have been affected, and determine the extent of the damage. This information is used to develop a customized plan of action to address the attack.
- **Secure systems:** Secure your systems to prevent further damage and protect your data from being exfiltrated. This may include applying software patches, deploying new security controls, or taking other remediation steps as necessary.
- **Data recovery:** Contact the proper authorities and get expert advice to determine whether or not to pay the ransom. In many cases, it is possible to recover data without paying a ransom if proactive processes are in place already.
- **Post-attack analysis:** After the attack has been contained, conduct a thorough analysis of the attack to identify any vulnerabilities in your systems or processes that may have contributed to the attack. Based on the findings, get expert support on creating a roadmap for remediations that can help prevent future attacks.
- **Invest in cybersecurity resources:** Ultimately, investing in cybersecurity resources is critical for businesses to survive ransomware attacks. This includes investing in the right people, processes, and technology to prevent, detect, and respond to ransomware attacks. Businesses should consider working with cybersecurity experts to develop a comprehensive cybersecurity plan and ensure they have the resources necessary to implement it effectively.

How Difenda Can Help Fix Your Face

Regardless of your initial reaction, it is important for individuals and businesses to take steps to protect themselves from the consequences of a ransomware attack. A well-established enterprise-class cybersecurity vendor with proven expertise and experience like Difenda can play a crucial role in helping businesses prevent and mitigate the risk of a ransomware attack.

Here are some ways in which Difenda can help:

1. **Risk Assessment:** Difenda can conduct a comprehensive risk assessment of your organization's cybersecurity infrastructure to identify vulnerabilities and weaknesses that could be exploited by cybercriminals. This includes assessing your organization's security policies, procedures, and technologies to determine their effectiveness in mitigating the risk of a ransomware attack.
2. **Security Monitoring:** Difenda can monitor your network and endpoints 24/7/365 to detect and respond to potential threats in real-time with managed SIEM, and Endpoint Detection and response capabilities.

3. Security Operations Center (SOC) Services: Leverage 24/7/365 SOC services to manage and respond to security incidents. This includes conducting incident response planning, testing and training, and managing security incidents from detection to resolution.
4. Cybersecurity Awareness Training: Ransomware education can provide employees with valuable preventative information about the latest cybersecurity threats and best practices for preventing and mitigating them. This includes training on how to identify phishing emails and other social engineering attacks that are often used to launch ransomware attacks.
5. Threat Intelligence: Difenda can provide access to threat intelligence feeds that provide real-time information about emerging threats and vulnerabilities. This can help your organization stay ahead of the curve and proactively mitigate risks before they are exploited.
6. Cloud Security: Difenda can help secure your organization's cloud infrastructure by identifying and mitigating vulnerabilities, monitoring cloud activity for threats, and providing secure access controls to cloud services.

More People Than Ever Are Falling for Ransomware Attacks. *Find out why in [The Ultimate Guide to Treating Ransomware Breach Face](#).*

About the Author

Derek Nugent is the Vice President of Revenue at Difenda. He is a managed security services expert that helps IT and security leaders map and augment their SecOps solutions. As a customer success evangelist, Derek has spent the last decade helping organizations across industry verticals identify and solve bespoke security and business use cases.

Derek can be reached online on [LinkedIn](#) and at difenda.com.





YOU'VE GOT SERIOUS #RBF

RANSOMEWARE BREACH FACE

Shocked by accidentally causing a cyber breach within their company, employees everywhere are suffering from Ransomware Breach Face - until now. Mitigate the effects of #RBF on your business with Difenda.

Let Us Help Fix Your Face

www.difenda.com | sales@difenda.com | 1.866.252.2103



DIFENDA

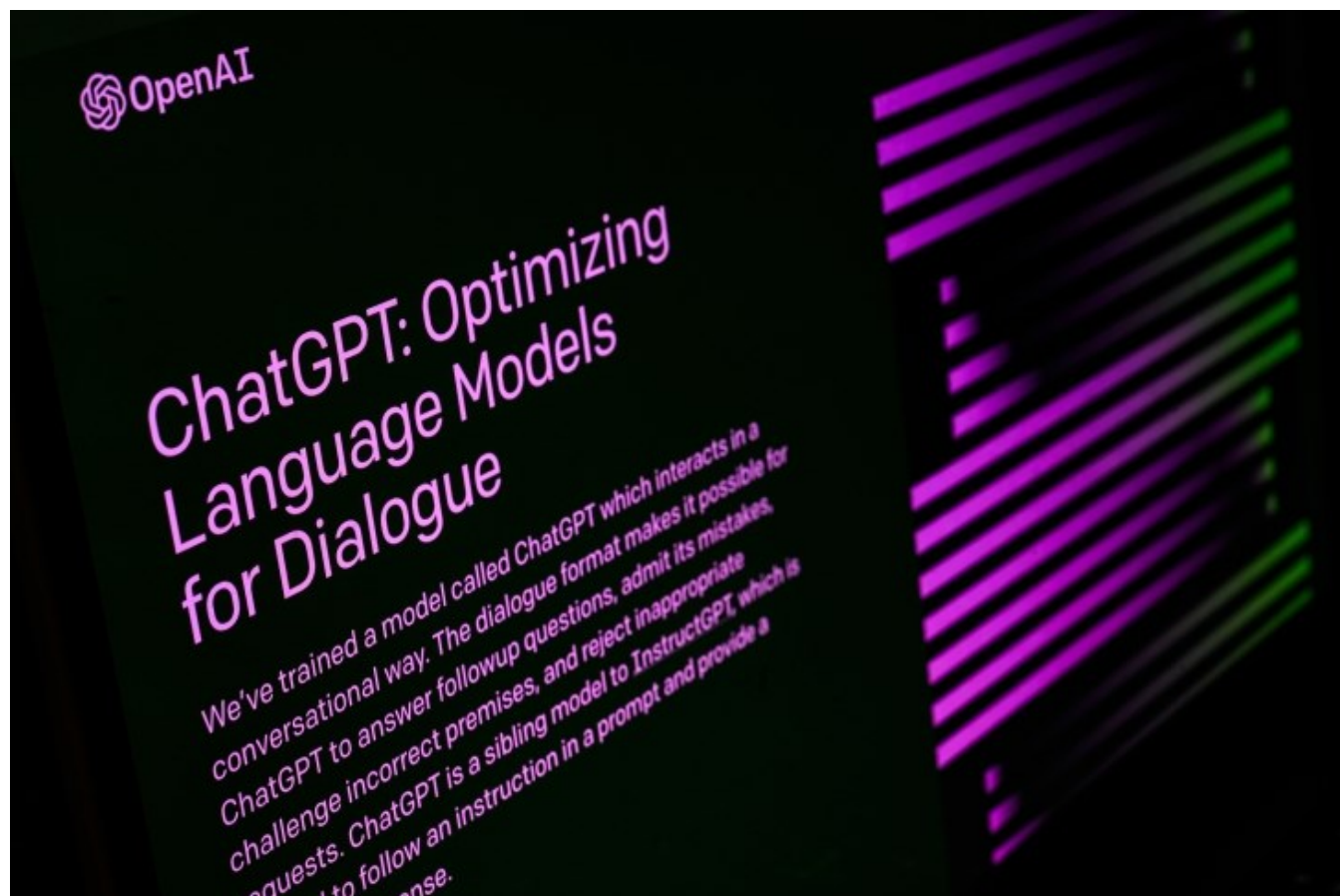
ChatGPT and You

Or I'm No Fool with Weaponized AI

By Guy Rosefelt, Chief Product Officer at Sangfor Technologies

Okay, I admit the title is clickbait to get you to read this article. There are articles about ChatGPT and its impact on civilization written daily, so I do not need to add to that body of minimal value. But weaponized artificial intelligence (AI) *is* a real-world problem and something that you need to be aware of.

If you saw my [interview](#) with Gary S. Miliefsky, the esteemed publisher of Cyber Defense Magazine, on Cyber Defense TV, I talked about how advanced persistent threats (APTs) have weaponized AI by using it to check the environment the malware is running in to determine if the environment is conducive for attack. This is not theory or TV science fiction; this is real and has been happening for a while.



Weaponizing AI

Previously, the typical level of intelligence that malware had was to watch the system clock and activate the payload on a certain date and time. Next came detecting if the malware was running in a virtual sandbox. The AI could detect if specific hardware was available, and the malware would shut down if it was not. Threat actors have since developed AI modules that evaluate specific environmental conditions to determine if malware should activate. Environmental factors include the domain the system belongs to, user accounts on the system, determining if it is being run in a virtual sandbox, what security software is running, and if it is possible to disable it.

That last check is very insidious as APTs can disable security software like Windows Defender. There exists in some APTs a powerful batch script called Defeat-Defender, which can shut down Windows Defender in any Windows system, prevent it from restarting, and hide the fact that it has been disabled so that the administrator is unaware. The APT will then go to sleep for a period of time, say two weeks, and then wake up to check if Defender has been re-enabled. If Defender has not been restarted, then the malware will continue its check to determine if it should activate. If Defender has been reactivated, then the APT will go back to sleep, never to return.

LotL: Defeat-Defender

- Powerful batch script that completely disables all Windows Defender processes and bypasses new Windows "Tamper Protection"
 - Can masquerade as a valid application
- "Tamper Protection" is designed to prevent disabling of real-time protection and modifying Defender registry keys using PowerShell or cmd
- Defeat-Defender then downloads and installs malicious files in startup folder without detection
- Disables
 - PUAProtection
 - Automatic Sample Submission
 - Windows FireWall
 - Windows Smart Screen(Permanently)
 - Disable Quickscan
 - Add exe file to exclusions in defender settings
 - Disable Ransomware Protection

User Account Control

Do you want to allow this app to make changes to your device?

Windows Command Processor

Verified publisher: Microsoft Windows

Show more details

Yes No

Page not available

Your Windows administrator has limited access to some areas of this app, and the files you need to access are not available. Contact IT support for more information.

Figure 1 Defeat-Defender (source: Sangfor Technologies)

The best example of weaponized AI being leveraged is the infamous SolarWinds Supply Chain Attack. This attack targeted numerous organizations in the United States and Europe, including hi-tech companies, communications companies, banks, schools, and government departments.

In December 2020, both FireEye and Microsoft detected lateral movement attacks that were later found to be a global operation. The attacks, [attributed to threat group APT29](#), implanted malicious code into a

core SolarWinds DLL file and distributed backdoor software through SolarWinds' official website. Using a technique called Living off the Land (LotL), the malicious DLL is called using the valid signed executable, SolarWinds.BusinessLayerHost.exe, and thus considered a trusted process. Trusted processes are not scanned by security software.

Once the malicious process was started, it began running a checklist of 9 environmental tests (see figure 2. SolarWinds Strict Environment Check) to see if it could activate undetected.

No.	Detection Mechanism
1	Check whether the name of the process that loads the malicious DLL file is SolarWinds.businesslayerhost.exe based on the hash value.
2	Check whether the last write-in time of the malicious DLL file is at least 12 to 14 days ahead of the current time. If yes, the malicious code will be dormant for about half a month before being executed.
3	Check whether the named pipe in hard coding is 583da945-62af-10e8-4902-a8f205c72b2e. This prevents repeated execution by multiple processes.
4	Check the ReportWatcherRetry configuration option for malicious reuse. The value of the ReportStatus item cannot be 3, which indicates the Truncate Exit state.
5	Check the domain of the current device. The domain name cannot contain character strings in the hash value verification blacklist patternHashes. The domain name cannot match the regular expression "(?i)([^\a-z])(test)([^\a-z])\$". This expression is mainly used to check whether the current domain name is for testing. It is deduced that the "(?i)(SolarWinds)" expression is used to detect whether the device is inside a SolarWinds office.
6	Check the first enabled non-loopback adapter and ensure that its IP address is not in the blacklist.
7	Check whether any of the 137 processes that are related to security software or services, such as WinDbg, Autoruns, or Wireshark, in the hash-formatted blacklist are running in the current environment, and stop such running processes if they exist.
8	Check whether any driver programs of the specified 13 security software, such as groundling32.sys, are running in the current environment.
9	Check whether the host parses "api.SolarWinds.com" as the destination IP address for instructions.

Figure 2 SolarWinds Strict Environment Check

Fighting AI with AI

The effects on businesses attacked with weaponized AI are significant and include:

- **Ransomware Infection:** Attackers use weaponized AI attacks to bypass security systems, build connections with their command & control (C&C) server, and automatically download ransomware executables.
- **Data Breach:** Attackers splice sensitive data and append as hosts to computer-generated domain names and send these as DNS requests to their servers. The hostnames are reassembled into exfiltrated data.
- **Assets Under Attacker Control:** Attackers control assets for illegal activity (Cryptomining/DDoS as a Service, etc.)

These cause disruption to business operations with great financial and operational impact.

AI-enabled malware can breach and infect an organization within 45 minutes. No human incident response team can detect and respond quickly enough. Organizations need tools with purpose-built AI models looking for specific behaviors. General-purpose AI models do not have the fidelity to detect different types of intermittent behavior over long periods of time. Behavioral detection should include building baselines of network traffic, user behavior, and application behavior. The models would then identify anomalous deviations, alert, and use SOAR (security orchestration, automation, and response) to command security products to respond using automated playbooks. This reduces the time needed to detect and respond to an attack from days and weeks to a matter of minutes.

Most organizations think that their security architecture is robust enough to combat APTs. Yet, ransomware is almost 100% successful, which means the most popular firewalls and endpoint protection are not sufficient to detect and block weaponized AI APTs, let alone go back and detect a breach. The next state-of-the-art security solutions must be AI enabled to detect the AI being used against them. The attackers may currently have the upper hand, but you can start evaluating new smarter tools to fight back.

About the Author

Guy is Chief Product Officer for Sangfor Technologies. He has over 20 years' experience (though some say it is one year's experience twenty times) in application and network security, kicking it off with 10 years in the U.S. Air Force, reaching rank of captain. After his time in the USAF building the first fiber to the desktop LAN and other things you would find in Tom Clancy novels, Guy worked at NGAF, SIEM, WAF and CASB startups as well as big-name brands like Imperva and Citrix. He has spoken at numerous conferences around the world and in people's living rooms, written articles about the coming Internet Apocalypse, and even managed to occasionally lead teams that designed and built security stuff. Guy is thrilled to be in his current position at Sangfor — partly because he was promised there would always be Coke Zero in the breakroom. His favorite cake is German Chocolate. Guy can be reached online at <https://www.linkedin.com/in/guyrosefelt/> and at Sangfor's official website: <https://www.sangfor.com/>.





Integrative Cyber Security Solution Portfolio



iSource



HSM/vHSM



HSA/vHSA



CloudView

Edge Protection



NGFW



DCFW



NIPS

Cloud Protection



CloudHive



CloudEdge



CloudArmour

Server Protection



BDS



vBDS

Application Protection



ADC



vADC



vWAF



WAF



ZTNA



XDR



NDR



CWPP



SD-WAN



Micro-Segmentation

Strengths and Vulnerabilities of AI Applications to Health Care and the Protection of PHI, including Implications for the Confidentiality of the Doctor-Patient Relationship

By Edward Maule, Chief Information Officer and Chief Information Security Officer at Advocate, LLC

Artificial intelligence (AI) has made significant advancements in the healthcare sector, and its potential is almost unlimited. AI-powered systems can analyze vast amounts of medical data, detect patterns, and offer insights that can help healthcare professionals make more informed decisions. However, as with any technology, there are strengths and vulnerabilities associated with AI in healthcare, particularly in relation to the protection of personal health information (PHI).



Strengths of AI Applications in Healthcare:

1. Diagnosis and Treatment:

AI applications can be used to analyze patient data and generate accurate diagnoses, allowing healthcare professionals to provide more effective treatments. AI can also assist in monitoring patient progress and predicting outcomes, allowing healthcare professionals to adjust treatments accordingly.

2. Precision Medicine:

AI can help identify genetic markers and personalized treatments that are tailored to individual patients, improving the accuracy and effectiveness of treatments.

3. Resource Optimization:

AI can help healthcare organizations optimize their resources by identifying inefficiencies in processes and procedures, allowing them to allocate resources more effectively and efficiently.

4. Remote Monitoring:

AI applications can be used to monitor patients remotely, providing healthcare professionals with real-time information about a patient's condition, allowing them to respond to emergencies quickly.

Finally, AI has the potential to increase efficiency in healthcare delivery. By automating routine tasks, such as data entry and administrative duties, healthcare providers can focus on patient care, leading to improved patient satisfaction and outcomes.

Vulnerabilities of AI Applications in Healthcare:

1. Security:

AI applications in healthcare require access to large amounts of personal health information, making them vulnerable to cyber-attacks and data breaches. This can lead to sensitive medical information being leaked or stolen, potentially putting patients at risk.

2. Bias:

AI applications can be biased based on the data they are trained on. If the data used to train the AI is biased, this can lead to inaccurate or unfair recommendations and treatments.

3. Overreliance:

Healthcare professionals may become over-reliant on AI applications, leading to reduced critical thinking and judgment. This can lead to misdiagnosis and ineffective treatments.

4. Lack of Regulation:

Currently, there are no clear regulations or guidelines for the use of AI in healthcare. This can lead to inconsistencies in how AI applications are used and a lack of accountability.

Implications for PHI and the Doctor-Patient Relationship:

1. Privacy:

AI applications require access to personal health information, raising concerns about patient privacy. Patients may be hesitant to share sensitive medical information if they are unsure of how it will be used or who will have access to it.

There is a concern around the potential for AI to violate patient privacy. As AI algorithms are often trained on sensitive patient data, there is a risk that the algorithms could be used to identify individual patients, even if the data has been de-identified.

2. Confidentiality:

The use of AI in healthcare raises important questions around the confidentiality of the doctor-patient relationship. As AI requires vast amounts of patient data to operate effectively, patients may be hesitant to share sensitive information with their healthcare providers. This could lead to patients withholding important information, which could negatively impact their care.

There is also a risk that AI could be used to identify individual patients, even if the data has been de-identified. This could lead to a breach of patient privacy and a violation of the doctor-patient relationship.

To address these concerns, healthcare providers must ensure that they have robust data security measures in place. This includes using encryption to protect patient data, implementing access controls to limit who can access patient data, and ensuring that all employees are trained on data security best practices.

Healthcare providers must also be transparent with patients about how their data will be used. Patients must be informed about how their data will be collected, stored, and used, and they must have the opportunity to opt-out of data sharing if they so choose.

Healthcare providers must always ensure that they are using unbiased AI algorithms. This includes ensuring that the data used to train the algorithms is diverse and representative of the patient population, and regularly monitoring the output of the algorithms for bias.

Conclusion

The use of AI in healthcare has many strengths, including the ability to analyze vast amounts of patient data quickly and accurately, improve patient outcomes, and increase efficiency in healthcare delivery. However, there are also vulnerabilities that must be addressed, such as the security of patient data, the potential for bias, and the risk of violating patient privacy. To address these concerns, healthcare providers must ensure that they have robust data security measures in place, be transparent with patients about data usage, and ensure unbiased AI algorithms. By doing so, the potential benefits of AI in healthcare can be realized while protecting the confidentiality of the doctor-patient relationship and the privacy of patient health information.

About the Author

Ed is IT Professional with over 10 years of experience leading teams, launching new technologies and managing complex IT projects. Throughout his career, Ed has overseen datacenter operations, corporate helpdesks, networks, data storage and cloud applications, for clinical, business and academic systems.

At Advocare, Ed leads an Information Services Department serving over 2,500 employees and 600+ healthcare providers. His team is responsible for the delivery of all IT services to nearly 200 Advocare Care Center offices. One of Ed's key initiatives includes the implementation of electronic health record (EHR) platform that allows Advocate patients to access their healthcare records via a secure internet and mobile app.

Prior to Advocate, Ed held various IT roles with Jefferson University Hospital and Kennedy Health. Ed holds a Master of Business Administration degree from Saint Joseph's University, including certification in the University's Leadership Development Program. He also has a Bachelor's degree in Information Technology from Thomas Edison State University. He maintains the Project Management Professional certification and is a Certified Information Systems Security Professional.

You can reach Ed at LinkedIn and through [Advocare](#), LLC website.



2023 Predictions

By Anurag Gurtu, Chief Product Officer at Strike Ready

In 2022, the global average total breach cost surpassed \$4.35M, and nearly two-thirds of organizations experienced more than one breach. As a result, CISOs are adopting various security strategies in 2023 that revolve around a human-centered approach to risk management. This theme will likely intersect with the trends below.



Role consolidation accelerates burnout.

Economic shifts and the global recession force companies to adapt, resulting in workforce reductions and restructuring. Moreover, with an ever-increasing threat landscape, cybersecurity teams, including security operations teams, are overwhelmed with work. Furthermore, resource consolidation leads to personnel wearing multiple hats, which contributes to accelerated burnout.

Voice assistance, mobile apps, and chat are modern norms

When millennials enter the workforce, they expect consistent forms of interaction that they are used to with consumer-centric apps. This need has translated into evolving product requirements such as making enterprise applications available on the mobile platform, supporting interaction with these applications using voice and text, and embedding capabilities such as virtual assistants. For the existing workforce, however, traditional access is still a necessity, including GUI and console access.

Rise of Generative AI

Investment firms are doubling down to invest in Generative AI. This AI includes technologies such as Deepfake detection, text-to-speech conversion across multiple languages, audio transcription, personalized support chatbots, and more. The ever-popular ChatGPT, Midjourney, and others have further accelerated this trend. However, it does not stop there. In an advanced form of Generative AI, users can interact with an AI bi-directionally. When applied to cybersecurity, an analyst asks a question about a threat; AI can answer this question and look for similar threats and help resolve them.

Closing thoughts

Empowering the millennial workforce in cybersecurity will be crucial to the success of CISOs in these challenging times. While security evolution coupled with technological advancement can help make cybersecurity very accessible, this creates a cautionary tale as these advancements will open a new class of 'non-technical' cyber attackers to take advantage of, e.g., the use of Generative AI to generate novel malware. Finally, the various governing bodies, such as the NIST AI Risk Management framework and the EU's AI Act, will help shape the success of AI. Personally, I'm looking forward to relaying voice instructions to my mobile device to assess my organization's security posture against an emerging threat and create a response to it without lifting a finger.

About the Author

Anurag Gurtu is Chief Product Officer of StrikeReady. He has over 18 years of cybersecurity experience in product management, marketing, go-to-market, professional services and software development. For the past seven years, Gurtu has been deeply involved in various domains of AI, such as Natural Language Understanding/Generation and Machine Learning (Supervised/Unsupervised), which has helped him distill reality from fallacy and the resulting confusion that exists in cybersecurity with real-world applicability of this technology. Gurtu was fortunate enough to have experienced three company acquisitions (by Splunk, Tripwire and Sun Microsystems) and an early-stage startup that went public (FireEye). Gurtu holds an M.S. degree in Computer Networks from the University of Southern California and numerous cybersecurity certifications, including CISSP, CCNP Security and more.



Anurag can be reached online at LinkedIn and at our company website <http://www.strikeready.co>.

A CEO's Guide to Not Becoming the Next Cyberattack Headline

By Sheetal Pansare, President & Global CEO of Futurism Technologies

Imagine you are a CEO waking up to a Class-action lawsuit simply because your IT department failed to comply with the necessary security compliances or worse, they didn't back up mission-critical business data exposing sensitive customer information to potential hackers.

Yes! Data breaches make hot news headlines almost every day! Many things can go haywire when it comes to containing a data breach: from outages to unplanned downtime and timely detection of an intrusion attempt to name a few.



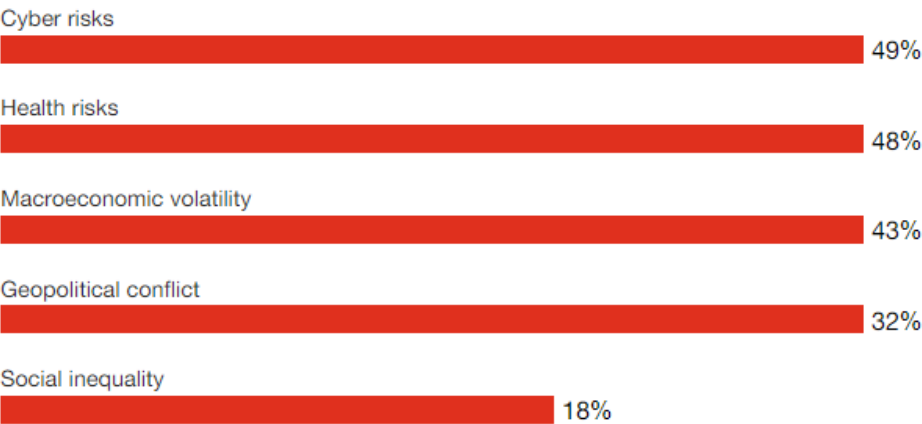
Did you know?

CEO of Optus (a leading Telco in Australia) took full accountability for a brutal data breach that jeopardized sensitive data of more than 9 million customers.

Now this can be hard for organizations that are led by leaders who undermine the importance of creating as well as maintaining a strong line of cyber defense. This is what happened with a leading French

hospital last year, which was left crippled by a Ransomware attack causing abrupt downtime of its critical systems forcing the healthcare provider to shift patients elsewhere while exposing sensitive patient data of millions.

Cyber tops the list of CEO concerns



Question: How concerned are you about the following global threats negatively impacting your company over the next 12 months?
(Showing only "very concerned" or "extremely concerned" responses)
Source: PwC, 25th Annual Global CEO Survey, January 2022.

Source: PwC

Why does cyber security need to be a priority for every CEO?

Cyber criminals see a feast of opportunities in today’s highly connected and digital-first economy. They are unleashing coming-of-age attack tactics on security and network systems on organizations. This is why CEOs ought to reevaluate every aspect of their security posture including people, process and technology.

Good news is that you as a ‘CEO’ can save your company from such unfortunate mishaps. Just knowing the fundamental security practices and concepts can help you make the right decision for your company.

Here’s what you as a ‘CEO’ ought to know about cybersecurity to avoid becoming the next cyberattack cover page story.

- **Good Cyber Hygiene Pays off**

Always make sure that your company follows good IT and cyber hygiene practice to keep all your systems and data safe. Also, remember that when an IT system reaches its 'end-of-life', its manufacturer or vendor no longer supports them thus, leaving them vulnerable to attacks. So patch now or pay later!

Did you know?

The infamous 'Log4j Vulnerability' has been giving sleepless nights to IT and security experts worldwide since its discovery (2021).

- **Don't ignore Endpoint Security**

When IT systems are removed or shut down from a network, they still tend to have personal information stored in them. To remove the data, these systems need to be 'wiped' before being discarded. This is where it counts to have a strong and unified endpoint management and extended detection and response (XDR) system in place.

- **No Company is Immune!**

Understand that any organization irrespective of its size is prone to cyber attacks. This is why you as a 'CEO' ought to assess the types of cyber risks your company faces and how those threats would impact your organization. CEOs when better understand these risks, can better tackle the impact and mitigate risks.

- **Security is not IT Issue Alone!**

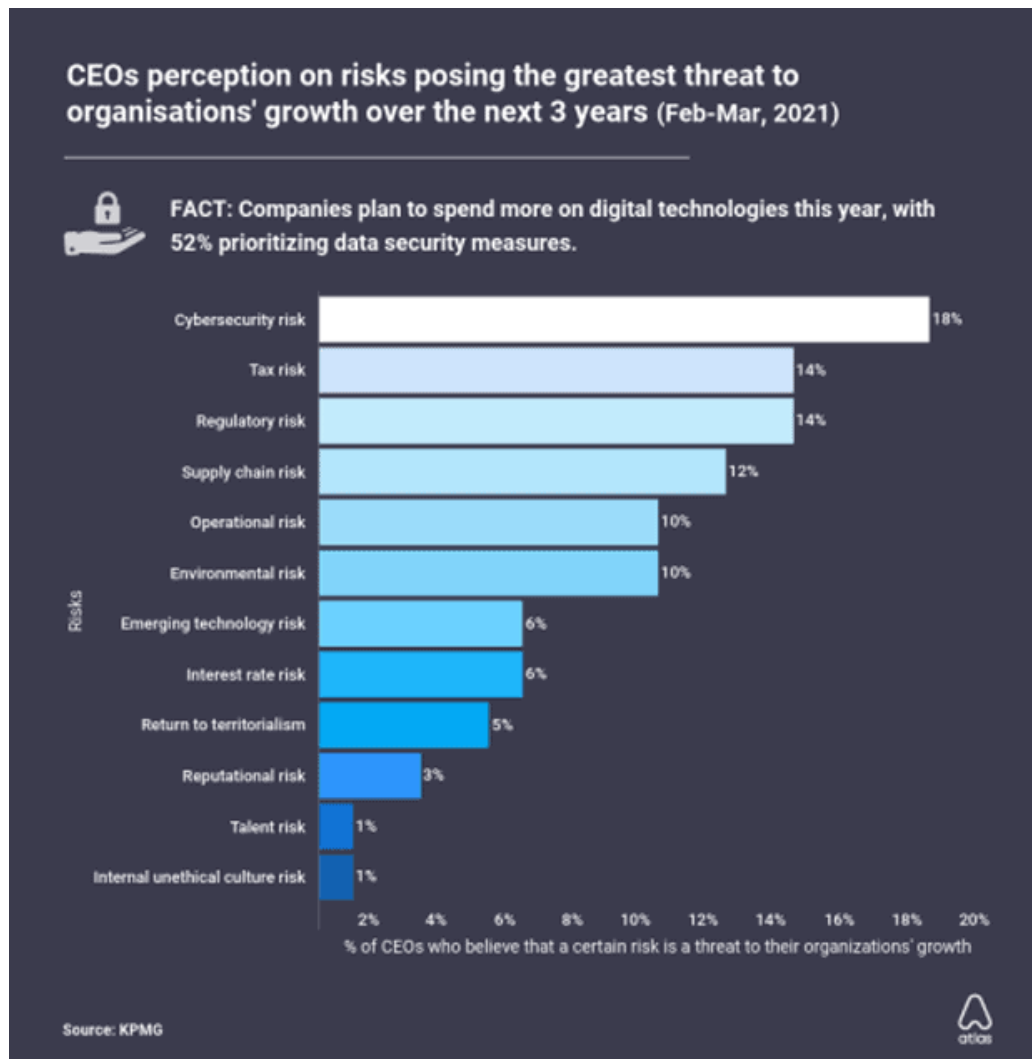
It is important for CEOs to understand that cyber security isn't just an IT issue, but a business issue. In fact, it is everyone's responsibility in an organization. While your security/IT teams hustle to up your guard against potential attacks, it is the responsibility of every stakeholder in the company to stay vigilant. If a company's information is compromised post an attack, it could lose customer trust affecting the brand's reputation followed by a legal suit. This is why it counts to have a strong managed identity and access management solution in place, which will not only help deploy the right layers of security, but will also bring in intelligent and context-based access decisions coupled with risk-based authentication.

Did you know?

Over 70% of enterprise data breaches involve insider attacks often executed by rogue or disgruntled employees.

- **Insider Threat Detection is a Must**

If your security or IT teams work separate from remote locations, make sure that they have frameworks and/or protocols in place ensuring secure access to mission-critical company database and systems. Having a powerful insider threat detection system can save the day here. It is advisable to seek expert help from a managed security services partner that will act as an extended arm to your security team taking over all the critical security tasks and operations.



Source: Loss Prevention Magazine | KPMG

Did you know?

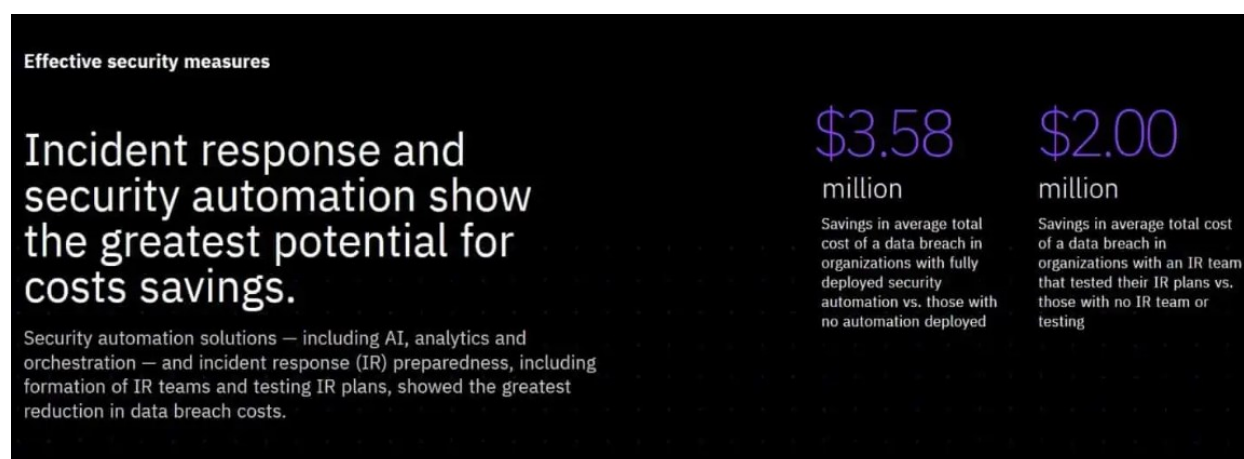
According to Verizon's 2022 Data Breach Report, four out of five breaches occur due to human based vulnerabilities and/or errors.

- **Cyber Awareness isn't just a One-Time Activity!**

Your employees are the ones that attackers target, manipulate and social engineer to coerce into your databases or systems. The single and most important factor in cybersecurity is the human factor. Yes! Even the most advanced security mechanism cannot protect your company if your employees fall for social engineering attack tactics. Educate your employees about the various types of attack tactics including or spear-phishing attacks, callback phishing attacks and new strands of Ransomware. Cyber awareness training needs to be a continuous process.

- **Have Complete Visibility of your IT Environment**

You simply can't protect an attack if you don't know that there exists a threat. Create an up-to-date list of your physical as well as digital assets. This is the key towards achieving end-to-end security. Understand the various types of threats and work with your IT/Security people in creating and deploying a solid incident response mechanism along with a disaster recovery plan.



Source: IBM

- **Communication is the Key**

Make sure to bridge any communication gap between you and your IT/Security team. For instance, many small organizations such as rural or community hospitals often lack the required expertise and tools to dodge cyber threats. It is imperative for CEOs of such organizations to establish strong communication with their IT/Security teams to understand their vulnerabilities and improve their security posture.

- **Security Automation is the Way to Go**

Investing in the right kind of tools and expertise can go a long way in securing your organization from coming-of-age attacks. A powerful threat protection solution, Security Information and Event Management (SIEM), will not only help you employ the best-of-breed security expertise and market-winning security intel and tool, but will also help you deploy the right layers of security. It will also help you abide by the various security compliances thus, strengthening your organization's security posture in the long run and most importantly, saving you from any kind of legal tussle.

Takeaway

Every other day, there's a new headline about some organization falling prey to a cyberattack or breach only to repent later. In most cases, the attack was not even detected for almost a year causing severe damage and data compromise. This is why it is advisable for CEOs to think like cyber investigators. Scrutinize the attacks that are in the news. Ask yourself what if my organization falls victim to such an attack? Adjust your priorities, strategies and educate your employees.

Don't take the bait! Be cyber smart!

The Future is Digital, The Future is Now!

About the Author

Sheetal Pansare is the President & Global CEO at Futurism Technologies based in the United States and has been an ardent evangelist of Digital Transformation (DX). Having been in the tech industry for over two decades transforming businesses worldwide delivering digital delight, he believes that now is the right time to reimagine how we see, perceive, and secure our digital world.

Sheetal P can be reached online at LinkedIn and at our company website <http://www.futurismtechnologies.com/>.

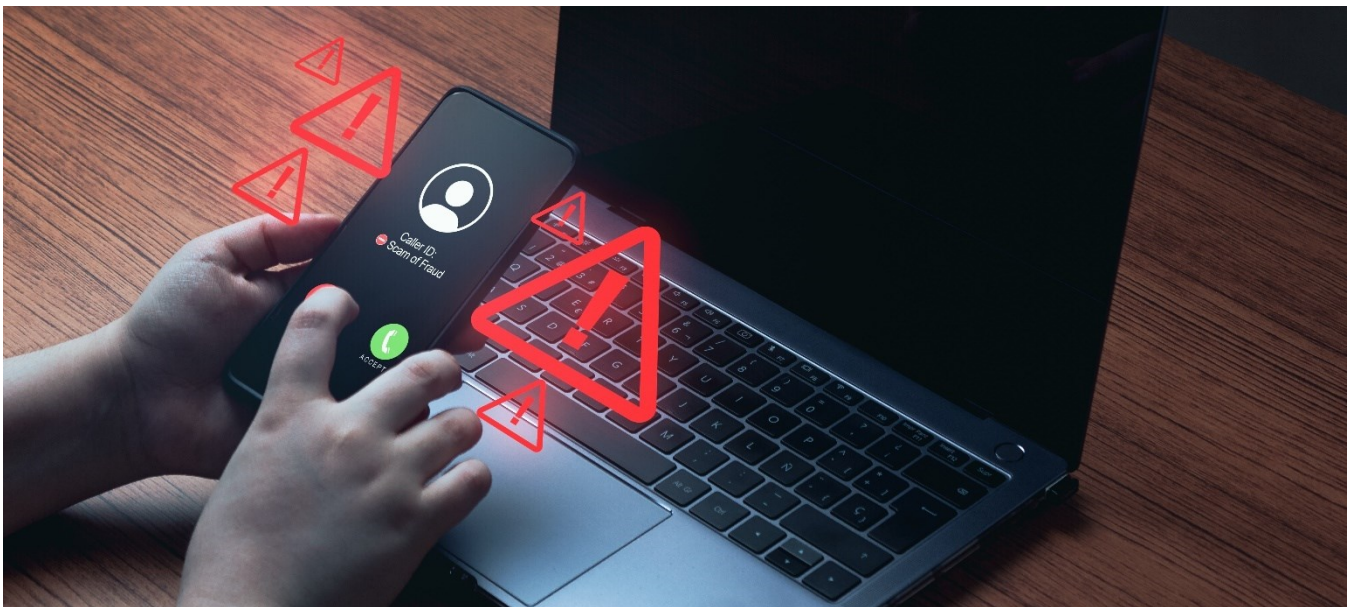


Advancements in AI Cybersecurity: Leveraging ChatGPT to Stay Ahead of Cyber Criminals

By Brian Sathianathan, Co-Founder and CTO of Iterate.ai

As our world becomes more and more digitized, the threat of cyber-attacks has become increasingly prevalent. The need for strong cybersecurity measures has never been more important, and the field of cybersecurity has rapidly evolved to keep pace with these changing times. One of the most exciting new technologies to emerge in the world of cybersecurity is artificial intelligence (AI), which has the potential to transform the way we approach security and protect ourselves from cyber threats.

At the forefront of this innovation is ChatGPT, a powerful AI language model developed by OpenAI. ChatGPT is designed to simulate human-like conversation and generate natural language responses to prompts. While it was not initially developed for cybersecurity purposes, it has the potential to be a potent tool in the fight against cyber threats.



So, how can ChatGPT be used to improve cybersecurity? One way is by helping to detect and analyze suspicious activity on a network. For example, if a security team notices unusual activity on their network, they could use ChatGPT to generate a natural language summary of the activity and help identify potential threats. Additionally, ChatGPT can be trained on vast amounts of data to learn patterns and identify anomalies, which can be used to proactively detect threats before they can cause damage.

Another way that ChatGPT can be used in cybersecurity is by automating certain security processes. For example, ChatGPT could be used to automatically generate and respond to security alerts, freeing up security professionals to focus on more complex tasks. Similarly, ChatGPT could be used to automatically

update security policies and configurations based on emerging threats, ensuring that systems are always up-to-date and protected.

One of the biggest advantages of ChatGPT is its ability to learn and adapt over time. By analyzing data on past cyber attacks and their outcomes, ChatGPT can develop an understanding of the tactics and techniques used by hackers, and use this knowledge to identify and prevent future attacks. This level of adaptability is crucial in the fast-paced world of cybersecurity, where threats are constantly evolving and becoming more sophisticated.

Of course, ChatGPT is not the only AI technology being used in cybersecurity. Machine learning algorithms, for example, are being used to train systems to identify patterns and anomalies that may indicate a potential threat. Similarly, behavioral analysis is being used to analyze user behavior and network activity to identify suspicious activity that may be indicative of a cyber attack. Predictive analytics is also used to analyze data on past cyber attacks and predict future threats.

Despite the many benefits of AI in cybersecurity, some potential risks and challenges need to be addressed. For example, AI systems may be vulnerable to manipulation or attack and may produce false positives or negatives if not properly calibrated or monitored. Additionally, there are concerns around the use of AI in cybersecurity, such as the potential for bias or discrimination in decision-making.

As with any technology, it is important to strike a balance between the potential benefits and risks. In the case of ChatGPT and AI in cybersecurity, the potential benefits are enormous. By leveraging the power of AI to analyze data, identify threats, and automate security processes, we can stay one step ahead of cyber criminals and ensure that our networks and systems remain secure.

At the same time, it is important to approach these technologies with caution and ensure that proper safeguards are in place to prevent misuse or abuse. This includes ongoing monitoring and evaluation of AI systems to ensure that they are functioning properly and producing accurate results. It also means ensuring that there are adequate checks and balances in place to prevent the misuse of AI in cybersecurity, such as appropriate training and oversight for security professionals.

Ultimately, the use of AI in cybersecurity represents a significant step forward in the fight against cyber threats. By leveraging powerful technologies such as ChatGPT and machine learning, we can stay one step ahead of cyber criminals and protect our networks and systems from attack. But it's important to remember that these technologies are only tools and that the human element of cybersecurity remains crucial.

Cybersecurity professionals must work hand-in-hand with AI systems to ensure that threats are detected and responded to in a timely and effective manner. This means developing a deep understanding of the technology, constantly monitoring and evaluating its performance, and ensuring that it is being used ethically and responsibly.

Moreover, it is important to recognize that cybersecurity is not just a technical problem, but also a human problem. Cybercriminals often exploit human vulnerabilities, such as social engineering tactics, to gain access to systems and steal data. Therefore, it is important to train and educate employees on cybersecurity best practices and to develop a culture of security within organizations.

The advancements in AI technology, including ChatGPT, represent a significant opportunity to improve cybersecurity and protect against increasingly sophisticated cyber threats. These technologies have the potential to revolutionize the field, enabling faster and more effective detection and response to threats, and automating many of the routine tasks involved in security operations. However, it is important to recognize that AI is not a panacea for cybersecurity challenges. It is only one tool among many, and its effectiveness depends on the expertise and experience of the professionals who use it. By combining the power of AI with human intelligence and expertise, we can stay one step ahead of cyber criminals and ensure that our networks and systems remain secure.

About the Author

Brian is the Co-Founder of Iterate.ai. He started his career at Apple where he was initially hired for his software development and encryption skills. For 6 years at Apple, he led iPhone and Intel Mac initiatives within the very private New Product Introductions (a.k.a. Secret Products) Group. His two core groups designed the security and activation platform for the first iPhone, for which he holds patents. After 8 years total, Brian left Apple to be Founder/President of Avot Media, a software platform used by firms like Warner Bros to transcode video for Mobile. Avot was acquired by Smith Micro [NASDAQ: SMSI]. At Smith, Brian became head of the video business and was responsible for strategy, vision, and integration. After Avot and Smith, Brian joined the seed-stage investment team at Turner Media, where he sought out startups in the Social, Consumer, Advertising, and Recommendation spaces. Over two years, he participated in 13 investments and one acquisition (BleacherReport). Two of his startups were acquired (one by Apple) during that period. Brian is now the Co-Founder and Chief Technology/Digital Officer of Iterate.ai, an innovation ecosystem launched in 2013. Companies like Ulta Beauty, The Pampered Chef, Driven Brands, and Circle K leverage the "intelligent low-code" capabilities invented and patented by Brian and his team. Interplay dramatically speeds up and simplifies digital and AI-based innovation. Largely bootstrapped and highly capital efficient, Iterate revenues grew 287% from 2017 to 2020. Brian can be reached online at <https://www.linkedin.com/in/briansathianathan/> and at our company website <https://www.iterate.ai/>



Blockchain Startups Are Drawing Substantial Venture Capital Funding

By Mohit Shrivastava, ICT Chief Analyst at Future Market Insights

Blockchain technology is becoming more popular owing to the various benefits businesses get from it- supply chain management, decentralized finance, data usage, control, and encryption. To ensure the smooth functioning of the technology, various companies require investments.

Venture capital (VC) investment is one of the main ways blockchain entrepreneurs finance their enterprises. Initial coin offerings (ICOs) used to be the main financing source for most blockchain projects, but strict regulatory oversight of ICOs has changed the dynamic. Hence, venture funding is essential to entrepreneurial as well as intrapreneurial blockchain enterprises, even when valuations are modest.



According to Future Market Insights, the global [blockchain technology market](#) is expected to grow with 44.3% CAGR from 2023 to 2033, providing ample opportunities for data decentralization in the future. And this is what the VCs are aimed at. Venture capitalists play the long game and invest their money patiently. They support innovation and are aware of the dangers involved. They support these firms knowing that there is a good chance that cryptocurrencies will play a significant role in the future of trade

and commerce. As a result, it is a risky industry with wide tails and uneven rewards. In this situation, the winner takes it all. VCs are always seeking 100x prospects, which carry extremely high risks. They keep investing in blockchain and cryptocurrency firms because they are aware that the rewards will eventually outweigh the dangers.

Simultaneously, the venture capital sector might be drastically altered by blockchain technology in a variety of ways. For starters, it could be simpler for entrepreneurs to raise capital without using the conventional VC procedure. The amount of money VCs spend in businesses and the fees they charge may decline as a result of this.

In this blog, we will discuss what is drawing the attention of VC firms toward blockchain technology, how large-scale flocking of the VC firms will take place in the third quarter of 2022 towards blockchain start-ups, and why the VC firms supporting these crypto companies.

Benefits of venture capital funding for blockchain firms Several venture capital firms are continually investing in blockchain businesses since they see great promise in the field. As a result, VC companies are forging strategic partnerships with blockchain entrepreneurs and investing in the market to make money. In turn, this has made this an advantageous sector for venture capital companies due to the excitement around blockchain technology and the growing usage of cryptocurrencies.

There is now a high potential for growth and increasing demand for investments in blockchain firms. As a result, blockchain venture capital companies are making investments in the sector to make money. Several factors make the sector profitable for investors, including the ones listed below:

- The potential for blockchain to expand is enormous. For instance, in 2013, Coinbase received \$20 million from renowned VC firm Andreessen Horowitz. The same is currently valued at \$12B in 2023. Investors are seeking growth prospects like this. This demonstrates that the sector is rapidly expanding and has a lot of room for growth.
- The advent of blockchain technology has changed the internet as people know it, and Web3 is the wave of the future. Several firms are now using blockchain to create decentralized apps. This future is getting closer because of the industry's development and expansion. Venture capital firms have invested in this technology due to the industry buzz.
- Blockchain investment is a desirable investment choice due to its flexibility. Blockchain venture capital financing is particularly attractive since a crucial component of the fundraising process involves the exchange of NFT tokens rather than shares. Venture investors thus perceive the blockchain business as having possibilities for investment.

The third quarter of 2022 saw large-scale flocking of VCs toward this technology.

Decentralized finance (DeFi) along with Web3 were the principal targets of the early-stage startup capital from some of the most prominent private investors in the third quarter of 2022, despite a drop in total venture capital investments.

Web3 - a phrase used to characterize a hypothetical future phase of the internet - enterprises working on decentralized software projects in addition to blockchain-based products and services attracted the most capital during the quarter, with \$879 million invested across 24 agreements. Some of the largest transactions in the industry have been funded, including a \$300 million Series B funding for Mysten Labs and a \$200 million Series A funding for Aptos Labs, two innovative blockchain networks that could challenge existing giants such as Solana and Ethereum.

And these investments continue to eye for various start-ups, considering their growth potential in the long run. Such developments are expected to bring in more opportunities for blockchain firms, aid them to take up risks, and aim for high gains in the future.

Blockchain offers investors better security.

The blockchain is a digital ledger that keeps track of all online transactions. This public information is dispersed over a computer network, making it nearly hard to hack or alter. In light of this, the blockchain is frequently hailed as being the most secure method of data storage.

The blockchain provides more transparency and security in the context of venture capital funding. The specifics of an agreement, such as when a venture capital company invests in a business, are documented on the blockchain network. All participants in the transaction then have access to this information, making sure that each individual is on the same page.

Additionally, the usage of smart contracts allows for automating some elements of the transaction, such as the distribution of payments. This increases process efficiency and lowers the possibility of human mistakes.

In the end, the venture capital sector may undergo a transformation owing to the blockchain. It may assist VC firms in establishing confidence with their investors and portfolio companies by making agreements more safe and transparent. This may then result in increased funding entering the VC ecosystem, spurring development and expansion.

Investors get a faster transaction

Blockchain technology is shaping the future of venture capital funding. The way startups solicit money and investors trade and monitor their portfolios might both be fundamentally changed by distributed ledger technology. The fact that blockchain permits quicker transaction times is one of its key advantages. This is so that a third party's verification or approval of the transaction is not required. Particularly when compared to the conventional banking system, this may save a tonne of time.

Blockchain technology also has the benefit of being more secure. This is so that every transaction can be validated before being published on a public ledger. Due to this, it is highly challenging for someone to fraudulently change the transaction history. The possibility for blockchain to upend the conventional VC model is arguably its most fascinating feature. VCs now frequently make early investments in firms before pulling out when they are sold or go public VCs may now invest in vouchers that represent shares in startups thanks to blockchain technology. This enables them to benefit more directly and liquidly from the company's success. Additionally, it more closely matches their interests with those of other stakeholders in the firm.

In conclusion, blockchain technology has the potential to revolutionize the venture capital sector. It claims to speed up, secure, and increase transparency in transactions. Investors may have more influence over their portfolios and raising funding may be simpler for startups as a result. This might ultimately result in greater innovation and better results for all parties concerned.

Investments are made to support the crypto-ecosystem

Venture investors have placed more bets on cryptocurrency start-ups in 2023 than they did in the last ten years altogether. The venture capital divisions of cryptocurrency firms, whose continuing growth will be dependent on the ecosystem's expansion, made a significant portion of the investments in the last few years.

For instance, the investment arm of the Coinbase cryptocurrency exchange, Coinbase Ventures, supports businesses developing infrastructure like Solana, a blockchain network; companies providing crypto financial products like BlockFi; projects for decentralized finance, also known as DeFi projects, where automated transactions are managed by code; and organizations working on the metaverse's digital economy, where users trade digital goods for their virtual lives.

Coinbase Ventures closed more deals than any other venture capital company in the third quarter of 2021. The major objective of the investing arm is to promote the crypto ecosystem. The VC company doesn't use return as its key criteria to assess Coinbase Ventures' performance. Blockchain technology as well as the open-source database architecture that powers cryptocurrencies are projected to progress the internet and eventually replace the incumbent IT behemoths, according to Coinbase and other cryptocurrency startups.

UNICEF's Venture Fund

The UNICEF Venture Fund welcomed eight fresh firms in 2021 that are creating blockchain-based, open-source solutions for enhanced financial inclusion. This was the debut cohort with over 50% of the firms being created or headed by women, the first cohort to extend the Fund's investment portfolio to Rwanda, and even the first cohort to acquire both USD and cryptocurrency in initial financing.

To connect the businesses to UNICEF's activities in their countries throughout the investment term, UNICEF made use of its extensive network. As part of the professional assistance program, UNICEF also offered technical as well as strategic support. Just two years have passed since they started working with this cohort, and in that time, the companies have identified strategic methods to support and expand their efforts, including methods for UNICEF to have access to the created digital infrastructure. Each firm in this cohort was chosen by UNICEF solely because it is paving the way for financial inclusion but also because it offers a solution to problems that have been identified as cross-cutting by UNICEF's program divisions, such as growing access to resources, community engagement, accountability, and the effectiveness of funding flows.

For instance, another Portfolio Company was bought in 2022, proving sustainability as well as scalability. IDT Corporation, a leading supplier of cloud communications, fintech, and traditional communications services, purchased Leaf Global Fintech, which created a virtual bank for refugees as well as vulnerable groups to enable asset storage and exchange across borders even without the requirement for a smartphone. This acquisition will enable Leaf to grow its effect and assist even more migrants, merchants, and unbanked individuals.

Leaf expanded its solution across three African countries during its period with the Fund, initiated an NFT collection of artwork created by refugees, and is currently pilot-testing a digital microlending platform. As a result, they influenced over 40,000 beneficiaries and increased direct financial services access for 7,000 refugees and members of vulnerable populations. As a result, several governmental and non-governmental organizations are eager to celebrate their continued growth with such blockchain start-ups and VC investment.

Conclusion

The venture capital sector may even be drastically altered by blockchain technology in a variety of ways. For starters, it could be simpler for entrepreneurs to raise capital without using the conventional VC procedure. The amount of money VCs spend in businesses and the fees they charge may decline as a result of this.

The emergence of token sales, which are a type of cryptocurrency-based crowdfunding, might potentially have an impact on VCs. Startups can generate money through token sales by offering digital tokens that can be utilized to access the company's goods or services. This could make it possible for entrepreneurs to completely avoid VCs.

Finally, blockchain technology may make it simpler for entrepreneurs to monitor their development and convince investors of their value. This may result in VCs needing to perform less due diligence and ease the process of selling their investments.

All of these adjustments would have a significant effect on the venture capital and blockchain startup industries. However, it's crucial to keep in mind that blockchain technology is still in its infancy, so it's unclear how any of these developments will turn out just yet. Therefore, while it's possible that blockchain technology could disrupt the VC sector, it's yet too early to predict how.

About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Insights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and consulting engagements across ICT, Electronics, and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate in Engineering in Electronics & Communication.



<https://www.linkedin.com/in/shrivastavamohit/>

Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!

Our company website <https://www.futuremarketinsights.com/>

Collaboration is Key to Building Industrial Cyber Resilience

By Filipe Beato, Cyber Resilience Lead at the World Economic Forum's Centre for Cybersecurity and Natasa Perucica, Research and Analysis Specialist at the World Economic Forum's Centre for Cybersecurity

Industries are in the midst of a digital transformation where infrastructure and systems are being connected to the internet and emerging technologies, such as artificial intelligence and internet of things (IoT), are being embraced to optimize performance and improve day-to-day industrial operations. The number of technologies finding their way into industrial operational environments and the new categories of connected objects is both impressive and bewildering. To illustrate, forecasts suggest that the number of industrial internet of things (IIoT) connections will reach [36.8 billion in 2025, an increase of 107% from 2020](#).

While digital technologies and connectivity unlock new business growth and efficiency opportunities in industrial environments, they also contribute to the expansion of the cybersecurity threat landscape, presenting risks that can lead to financial, reputational, legal and even physical and environmental damage.

In the face of proliferating cyber threats, it is no surprise that the value of the [global industrial cybersecurity market](#) is expected to grow to \$29.41 billion in 2027, at a 8.2% compound annual growth rate in the period 2019-2027.



Cyber threats to critical infrastructure are increasing and challenging public safety, society and economic stability.

While no industry is spared cybersecurity threats, some are more susceptible than others to risks with far-reaching consequences. Critical infrastructure organizations, including those in energy, healthcare and manufacturing, have become a key target for malicious actors, [with more than 60% of attacks in 2021 targeting operational technology](#). Gartner, the technological research and consulting firm, even predicts that cybercriminals are likely to weaponize operational technology and cause “harm or kill humans” by 2025.

The energy sector, which is crucial for the running and development of every other industry, has suffered a number of cyber incidents in recent years which have not only disrupted operations and the supply chain but also contributed, at times, to panicked consumer behaviour and higher energy prices. Such effects were, for instance, felt in May 2020 when a ransomware shut down the Colonial Pipeline, a major gasoline and jet fuel pipeline spanning 5,500 miles.

The healthcare sector has also suffered. A report by Check Point says that cyberattacks rose by 86% [in 2022 compared to 2021](#). On average, the industry experienced roughly 1,410 [security breaches](#) every week. Such attacks often result in disruption of access to critical health data, such as prescriptions, laboratory results, as well as patient admission and discharge functions.

While such attacks expose patients to both cyber and physical risks, they also bear a significant cost for healthcare institutions. For the past 12 consecutive years, the health industry, more than any other industry, endured the highest data breach costs reaching a record \$10.1 million [in 2022](#).

With the proliferation and rapid adoption of innovation and digitalization resulting in connected factories and products, the manufacturing industry [became the most targeted sector](#) in 2021, with 65% of the incidents leading to disruption of operations and supplies and tampering the quality of end products. At a time when supply chains are under stress, a cyber event could be hugely damaging for the global economic outlook.

Managing cyber risks is not easy task, especially when industries are facing three main challenges:

- **Divergent culture and priorities:** Historically, a culture gap prevailed between the approach taken towards enterprise and industrial operational technologies, particularly regarding security. With both environments converging, an integrated approach on security is required.
- **Diversity of technologies:** Organizations rely on modern, proprietary and legacy technologies, some of which were built to last a lifetime but without necessarily cybersecurity in mind. In addition, innovation and adoption of emerging technologies expand the complexity of managing cyber threats.
- **Multifaced and complex ecosystem:** The hyperconnectivity and complex supply chain networks and dependencies, where trust is extended to third-party providers with different cybersecurity practices and levels of maturity, is a further challenge to security.

Moreover, these three challenges coexist with external factors that shape the cybersecurity space.

Geopolitical instability as a trigger for leadership action

As conflicts take on a digital dimension, there is growing concern among cyber and business leaders that [“global geopolitical instability is moderately or very likely to lead to a catastrophic cyber event in the next two years”](#). This is particularly worrisome for organizations operating critical infrastructure, such as energy, healthcare and manufacturing – which are increasingly becoming a target for nation-state actors, hackers and other attackers motivated by political, economic, or strategic gains. Multiple sources indicate that at least 150 cyber incidents have taken place since geopolitical tensions have intensified. Such developments are influencing leadership action on cybersecurity with recent findings suggesting that global geopolitical instability has had a moderate or substantial impact on cyber strategy for 74% of business and cyber leaders.

Regulation as a driver of cyber resilience

In addition to the business sector, governments and regulators are also driving efforts to ensure that cybersecurity is strengthened in nations and regions by updating regulations and proposing new standards, in particular for critical infrastructure. Recently, the European Commission proposed a Cyber Resilience Act to address the inadequate level of cybersecurity inherent in many products, or inadequate security updates to such products and software. The act complements existing legislation such as the NIS2.0 Framework which was recently approved by the European Parliament and European Council and [aims to bolster the EU’s cybersecurity capabilities and resilience by expanding its coverage to include more sectors](#).

In light of growing cyber risks, the US government has also sought to improve the cybersecurity of key industries. In May 2021, following the Colonial Pipeline attack, President Biden signed an executive order outlining a number of measures to modernize cybersecurity. Among other things, it led to the signing into law of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, whereby critical infrastructure organizations need to report cyber incidents and ransomware payments to the Cybersecurity Infrastructure Security Agency (CISA).

In response, CISA published a set of technical rules to protect critical infrastructure information and launched a [strategic plan for 2023-2025](#) to collectively reduce risk and build resilience to cyber and physical threats to the nation’s infrastructure.

Nations in the Asia-Pacific region have also been active in updating cybersecurity strategic plans to address threats to the industrial environment and operational technologies. Singapore, for example, updated its Cybersecurity Strategy in 2021 to feature resilient infrastructure as a key pillar; [Japan in 2021](#) included new approaches to advance digital transformation and cybersecurity; and Australia launched

the [Security Legislation Amendment \(Critical Infrastructure Protection\) Act](#) in 2022 providing additional obligations and guidance for critical entities.

All these activities demonstrate how nations are taking concerted measures to address growing cyber threats to critical infrastructure industries. Some governments are also engaging and seeking international partners to develop mechanisms to share learnings and improve collaborative action.

How to transform cyber resilience into a global team sport?

The dependency on the digitalization and connectivity of critical infrastructures is growing exponentially and so are the risks. At the World Economic Forum, multistakeholder communities have been collaborating to take global action at both an industry and cross-industry level to strengthening cyber resilience.

Independent of the industry, there are three key actions that would help organizations and ecosystems strengthen cyber resilience.

1. Make cyber a business imperative while capitalizing on digitalization.

Businesses are moving towards more digitalization, connectivity and emerging technologies for strategic and competitive value. These drivers, along with the growing sophistication of cybercriminal operations, increase the risks and the potential impact of a cyberattack. It is important, therefore, to ensure that cyber resilience is part of the business strategy from the outset. To that end, business executives need to recognize and understand the associated challenges in order to apply correct prioritization and mitigation actions to capitalize on the business benefits. Organizations should establish a comprehensive cybersecurity governance model while leveraging existing global frameworks and standards, build a holistic view of the ecosystem and its broader impact, and ensure that resilience and security by design is embedded in operations and business decisions.

2. Embed cybersecurity in the organization's DNA

To achieve this, organizations need to cultivate a cybersecurity culture in the workplace at all levels – from operations to leadership. At the leadership level, cyber leaders should proactively communicate with executives and the board to convey cybersecurity as a business imperative and strategic priority. Cyber practitioners should communicate in business terms rather than confusing executives with technical jargon. The leadership should also understand that organizational cybersecurity is a shared responsibility guided and coordinated by the chief information security officer and, as such, is not the responsibility of any single individual. At the employee level, a cyber-aware culture can be promoted through periodic training and cybersecurity campaigns to increase education and highlight secure procedures.

3. Ensure collaboration across the ecosystem

With the increasing complexity of industry and cross-industry supply chains and ecosystems, it is key that critical infrastructure organizations have a holistic view of their ecosystem and work closely to build resilience. Cyber incidents are a question of when, not if, and to mitigate vulnerabilities early and respond to threats more rapidly in real time, businesses should collaborate with government officials and regulators before security breaches occur to ensure incident reporting and information sharing systems are well understood. Cooperation should also extend to third parties that provide goods and services to critical infrastructure organizations. Organizations are as strong as their weakest link and attackers will target these weak links in supply chains to compromise the other entities in the network. To that end, ecosystem players should share cyber-threat information, and develop and test incident scenarios to better react in case of attacks.

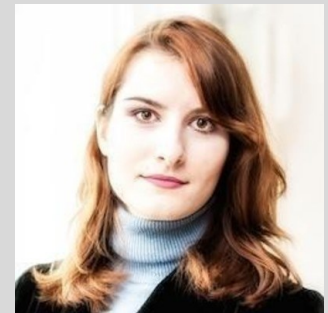
Cyber resilience is not a destination but a continuous journey. As such, it cannot be regarded as a one-time, or a one-actor effort. At a time when the cyber threat landscape is in constant flux, it requires cross-organization and cross-industry collaboration to ensure business continuity and security.

About the Authors

Filipe Beato is a Lead at the World Economic Forum's Centre for Cybersecurity, where he is responsible for Cyber Resilience initiatives driving collaborative action to strengthen cyber resilience across industry ecosystems, such as Energy and Manufacturing. Filipe is a cyber resilience and digital professional with a focus on strategy, transformation and innovation on public-private sectors with 10+ years of experience in helping organizations shaping and delivering their global cyber and digital strategies and transformations by bridging a strong technical background with business strategy. Filipe holds a PhD in Applied Cryptography from the University of Leuven, MSc in Computer Science from the University of Bristol, and BSc in Computer Engineering from the New University of Lisbon.



Natasa Perucica is a Research and Analysis Specialist at the World Economic Forum's Centre for Cybersecurity, where she co-leads activities of the Centre's Cyber Resilience in Oil and Gas initiative. She is also involved in the Centre's efforts on cyber capacity building and skills development. She received her bachelor and master's degree in Political Science from Université Catholique de Louvain in Belgium and is currently pursuing a PhD in Social Theory, Digital Innovation and Public Policies at Università degli Studi di Salerno.



Filipe Beato and Natasa Perucica can be reached through Mr. Sahil Raina – sahil.raina@weforum.org
Media Relations Lead at the [World Economic Forum](https://www.weforum.org/)

SAP Debugger's Power and Danger

By Christoph Nagy, CEO of SecurityBridge

It must have been a few years ago that I participated in a webinar where the Service Advertising Protocol ("SAP") representative explained a recently corrected vulnerability. The correction did not remove the problematic code but only introduced an additional check. Which, in my opinion, is the normal procedure. However, after the explanation by the SAP speaker, an interposed question came from the audience. The question was: How does the fix protect against attackers who use SAP Debugger to skip the check? In response, the spokesperson vehemently emphasized that an SAP system in which users have debugging privileges (coupled with changes to program variables); cannot be protected from compromise.

The combination of the debugger authorization with the said possibility to change the program variables is called, in SAP lingo, *Debug & Change*. To support the statement of the SAP expert, let's look at: What is the SAP Debugger? and What can it do to the system?



What is SAP Debugger?

The SAP Debugger, also known as the Advanced Business Application Programming (ABAP) Debugger, is one of the most important development tools offered by SAP. An ABAP developer or a technical SAP consultant uses it to analyze problems or to simulate program flows. Usually, the debugger is simply used to understand a certain behavior in SAP ERP and to identify or understand customizing options. Provided that a user has the appropriate authorizations, the debugger can be called from all ABAP screen-based transactions using function code /h. The SAP ABAP Debugger can also be used in OData, WebDynpro for ABAP, etc.

What can I do in the SAP Debugger?

In addition to the generally known functions such as the step-by-step processing of source code and the analysis of values of program variables, there are still some hidden features not known by everyone.

Did you know that you can start a remote debug session with the SAP Debugger, where you can analyze - or influence - a user's SAP session? The feature is not new, by the way, as evidenced by this blog from 2013: Remote ABAP Debugging (<https://blogs.sap.com/2013/04/29/remote-abap-debugging/>)

Alternatively, you can let the cursor jump from line 1 to next without executing the source code in-between.

So-called breakpoints can also be set dynamically. Breakpoints stop the debugger, or to be more precise, the cursor at a certain point in the program flow.

Additionally, to the ability to view the values of a program variable, there is also the option to change values. SAP offers the possibility to authorize this function granularly. More about this in the section: How can I protect myself?

What risks arise from the SAP Debugger?

It was rightly pointed out by the speaker of the SAP webinar mentioned at the beginning of this article that the debugger can be used to compromise the system, provided that the attacker holds or acquires the authorizations to do so.

Some examples spotted in the wild:

- Bypass authorization checks by resetting the return code (SY-SUBRC) or setting the cursor.
- Changing values in program variables to infiltrate or manipulate the database
- Modification of the program flow to obtain an abort or a change of the end-result.

Now you must know that if an attacker accesses the coveted *Debug & Change* permission, he typically does not base the attack on the debugger only but uses it in the Reconnaissance phase or in the Gaining

Access section. The SAP Debugger can also be a helpful tool in wiping the evidence of the SAP attack since everyone knows the SE16 trick: How to edit SAP tables in Debug Mode using SE16. (<https://sapboost.com/how-to-edit-sap-table-in-debug-mode-using-se16>)

This, of course, makes it more important to recognize an anomaly in usage behavior. It is even better if so-called *indicators of compromise* are detected at an early stage in order to be able to identify attacks.

How can you protect yourself?

Although these functions of the SAP Debugger can be restricted via authorizations, you will quickly notice that developers cannot work without extensive authorizations. Of course, the work of the SAP developer is mainly done in the development system. Therefore, there is no need to allow SAP Debug authorization, especially in combination with change permission of program variables in a system with productive data. So, you should ensure that this critical authorization combination is or will never be assigned in a productive SAP environment.

Use the authorization object "S_DEVELOP" and prevent object type "DEBUG" in combination with activity:

- '02' - Changing values of fields and (as of Release 6.10) the function >Goto statement, and
- '90' Debugging of sessions of other users.

You can achieve additional protection by regularly and promptly analyzing the activities in the associated SAP logs, in this case the SAP Security Audit Log (SAL).

However, this can be very time-consuming. In particular, the reliable detection of anomalies or an indicator of compromise for the SAP system requires additional analyses. If you do not have time to do this manually, market solutions can help.

About the Author

Christoph Nagy has 20 years of working experience within the SAP industry. He has utilized this knowledge as a founding member and CEO at [SecurityBridge](https://securitybridge.com)—a global SAP security provider, serving many of the world's leading brands and now operating in the U.S. Through his efforts, the SecurityBridge Platform for SAP has become renowned as a strategic security solution for automated analysis of SAP security settings, and detection of cyber-attacks in real-time. Prior to SecurityBridge, Nagy applied his skills as a SAP technology consultant at Adidas and Audi. Christoph can be reached online at christoph.nagy@securitybridge.com.



SIEM for SAP - Log Evaluation to Attack Detection

By Christoph Nagy, CEO of SecurityBridge

To detect attacks on SAP, you need to evaluate the security logs in SAP.

While many organizations have spent the past few years protecting the perimeter, business-critical systems are now becoming the priority of security operations. In this article, we will look at what a Service Advertising Protocol (“SAP”) SIEM might look like and what data and processes are necessary to enable desired conclusions.

Many readers are already familiar with SIEM - an abbreviation for Security Information Event Management. The best-known vendor solutions are Splunk, IBM QRadar, and MS Sentinel, but there are many other providers. SIEMs read security logs from various sources and use an intelligent aggregation of the data to derive conclusions about suspicious activities or malicious user behavior.



What data from SAP Applications needs to be collected?

Before deep diving into the process flow, we must look at which SAP logs have to be read out. SAP produces many protocols and logs that are necessary to create transparency in the business process.

This is not easy, especially since most SIEM adapters for SAP take an all-or-nothing approach for onboarding new log sources. For example, if we took the SAP system log, all entries must be transferred, although only 5% would be necessary for [SAP Security Monitoring](#).

A selective transfer of the entries necessary for the correlation would also have a positive side effect on the licensing costs for the SIEM product used, given that these usually are paid according to "log volume per day". Back to the question - which SAP logs are security-relevant? These are only the most relevant logs:

4. SAP Security Audit Log
5. SAP System log
6. SAP HANA audit log
7. SAP Gateway log
8. SAP Java audit log
9. SAP Profile parameter

For further conclusions in the Threat Monitoring for SAP process, you must transfer the user master and selectively change documents.

Bird's-eye view of SAP SIEM

For enterprise-wide attack detection, our goal is to combine as much information as possible. This is the only way to define the attack patterns that are afterward continuously searched for.

In the SIEM, it will combine the SAP logs with security logs from other sources:

- Server and Desktop OS
- Firewall / VPN
- Physical infrastructure (e.g., access control systems)
- IPS and IDS
- Identity Management
- System Health, Performance Monitoring Information
- Network and accessories
- Anti-Virus
- Databases

You must take the following steps in the SIEM process to create reliable alerts. First, you must read the data promptly. This also involves the normalization of the different source formats. Traditionally, mapping the SAP logs already presents the first challenge to customers since the event logs (e.g., CEF) can handle hardware or operating system logs better than the application logs.

Many SIEMs try dividing the data into categories directly in the onboarding process. The customer defines these categories during the definition phase and can become a valuable tool later during processing.

Validations must be in place to ensure the integrity of the monitoring solution including those logs that are not disabled and (or) manipulated. Especially with SAP, an insider can change the logs already in the application stack or flip a switch that prevents the output of security-relevant information.

Once the integrity of the data is ensured, the correlation can begin. This area is extensive and can be very specific, which depends on the customer deployment scenario. As a rule, the actors are identified and then attributed. Actors can be, for example, Windows users or an SAP account. Attribution is the process responsible for assigning attributes and properties. Information about the threat actor will be enhanced, with various attributes, such as the used operating system, SAP log-on version, geo-location, and IP-Range.

With all this information, you can now create alarms. For example, if a user who usually works at the U.S. office and with a Windows laptop now logs in from Asia and uses a Linux system, this could lead to an alarm. Of course, to detect SAP insider attacks, the information must be specific and detailed.

Detection of malicious SAP activities and distinguishing them from “regular” admin activities requires defining what is normal, and [which activity represents an anomaly](#). In-depth knowledge of SAP security is necessary for this. Critical, remote-enabled function modules, as well as database tables with sensitive content, must be known.

About the Author

Christoph Nagy has 20 years of working experience within the SAP industry. He has utilized this knowledge as a founding member and CEO at [SecurityBridge](#)—a global SAP security provider, serving many of the world's leading brands and now operating in the U.S. Through his efforts, the SecurityBridge Platform for SAP has become renowned as a strategic security solution for automated analysis of SAP security settings, and detection of cyber-attacks in real-time. Prior to SecurityBridge, Nagy applied his skills as a SAP technology consultant at Adidas and Audi. Christoph can be reached online at christoph.nagy@securitybridge.com.



The Cybercrime Blame Game: It's Time to Unite the Industry Against a Common Enemy.

The need for the cybersecurity industry to work together in order to combat the rising threat of cybercrime.

By Brendan Kotze, Chief Executive Officer at Encore

When someone breaks into a house, who would you hold responsible: the intruder or the victim? Naturally, most of us wouldn't blame the victim for not having secured their house well enough - we'd blame the thief for breaking in.



Why then, do we not hold this same view when it comes to cybercrime?

When a cyber-attack occurs, people are very quick to point fingers at the victim, the general view being that the business failed to implement the necessary security practices. However, cybersecurity is a complex and integrated problem that requires total visibility into every control in order to find a solution; there isn't a switch that automatically makes you secure.

It's not as simple as locking the few doors and windows on your house; it's the equivalent to deadlocking and placing bouncers on thousands of inconspicuous endpoints across the network.

This isn't to say that all organisations are blameless; poor cyber hygiene still exists across industries that needs to be addressed with haste. But we need to break the habit of playing the blame game, and work together against a common enemy.

A single breach triggers an enormous fallout.

To put this issue into perspective, we can refer to one industry in particular that frequently finds itself in the sights of global cybercriminals: the world of finance.

This lucrative sector not only faces relentless bombardment from attackers, but they must also then manage the equally damaging repercussions once customers and partners catch wind of their predicaments.

Banks especially face a fall in share price once an attack becomes public knowledge. They also risk losing customers if there is a perceived risk to personal finances and private information. At the end of the day, banking is built on trust and once that trust is broken, it's extremely challenging to re-establish.

Beyond their customers, banks also face fines from regulators and privacy boards, and if a cyber-attack is not handled with care and proper disclosure, employees lose trust in the organisation.

The victim of cybercrime is therefore impacted from multiple angles, whether that be their consumer base, internal staff, regulators, the wider community, or even insurers who could refuse cover. Ultimately, when it comes to a cyber-attack, there is a shared responsibility with more than one party at fault, just as there are more victims beyond the original target. For example, if a bank is charged with higher insurance premiums, as is often the case post-breach, this inevitably trickles down to the consumer in the form of increased banking charges.

More victims, more responsibility

When personal information is stolen, whether that be banking details, names or addresses, this often then translates into other forms of crime such as identity theft, false transactions and even physical crime. For example, a criminal might be able to gain access to a personal email or social media account as a result, which can then be used to identify when a victim is away from home, leaving the house

vulnerable. Stolen banking information can also result in indirect monetary fraud when the information is used to legitimize phishing emails.

It is easy to focus the blame on certain individuals, such as data processors, when something goes wrong but there needs to be more back-end support from a cybersecurity perspective, as well as support from a governance standpoint given how highly regulated this particular industry is.

Cybersecurity is already considered a grudge purchase given the astronomical costs of running it, without an easily demonstrable ROI in the absence of a breach. As with all investment, there needs to be a round-the-clock business incentive. However, since cyber-attacks are now inevitable, we can argue the incentive already exists. It's just a case of translating that to the organisation.

What are the next steps?

Victim blaming and shaming needs to be addressed as it simply compounds the issue. We need to accept shared responsibility with mature accountability in place in order to solve this complex issue.

At the end of the day, it's critical infrastructure within the economy that's being targeted, and even though they are private institutions, the impact of a cyber-attack creates devastating ripple effects beyond the company itself and its clients, as we've seen with attacks on businesses such as the Colonial Pipeline incident in 2021. The regulatory and government support (dare I suggest financial rebates and incentives for responsible security spending) behind these types of organisations should therefore match the risk at a national level.

When some of the world's largest and most established organisations are being targeted and breached – their security systems armed to the teeth with advanced technology – it's clear that attack campaigns are becoming more sophisticated by the day. We shouldn't be so quick to assume that businesses are in the wrong. If the necessary security practices are not in place, the right authorities will and should address non-compliance.

In the meantime, we should be working together as an industry to support these businesses and turning our attention to the real enemy that is already planning its next attack.

About the Author

Brendan is the CEO of Encore, the unique industry tool that combines Cyber Asset Attack Surface Management and External Attack Surface Management. It provides complete visibility over an organisation's estate to present a consolidated view of your security posture.

Brendan brings more than 13 years of progressive technical and business expertise, and his knowledge and methodologies have advanced through years of fundamental network communications work.



Cyber Attack as an Asymmetric Threat

By Milica D. Djekic, Independent Researcher

Abstract: Cyberspace is yet unsafe environment for communication and data transfer. Hacker's organizations can target many servers, datacenters and endpoints relying on capacities of only one workstation. That means cyber attack is a multiple-user threat which can affect a plenty of networks. The information-communication infrastructures are critically vulnerable to a wide spectrum of hacking campaigns. The bad guy on another side of the grid will see what is going on with targeted machine and easily doing drag-and-drop of malware applications cause sabotage with such a network. Cybercrime is a crime area by the Interpol and there are the entire legal regulations and case procedures which can guide law enforcement officers how to combat that criminality applying the best practices. The modern Police Forces are capable to resolve a lot of criminal justice investigations as there is still strong dependability on emerging technologies and current cyber assets. The main appeal to defense community of today is to assure manageability of the risk in high-tech surrounding as coming industrial tendencies could dictate those requirements. This study will carefully analyze all cyber challenges being obvious in the practice attempting to suggest some possible responses to those criminal scenarios.

Keywords: cyber defense, risk, intelligence, criminology, asymmetric warfare, etc.



Cybercrime is a criminal responsibility of someone affecting security, privacy and the other interests in virtual spot. The consequences of the high-tech criminality can be far reaching and potentially dangerous to national and global population. Hacker's operations are normally launched from some IT equipment and they can threaten many. The hacker's organizations which goal is to assault national needs deal with threat to critical infrastructure as impacts to such an asset can be catastrophic. In other words, that's a direct interfering with country's safety and security using advantages of new technologies. The ongoing best practice in criminology can tackle such a case, but there is yet need to take into consideration passive methods of defense as prevention is for a reason in such a case it is possible to save as many as it is feasible. Cyber defense is from strategic importance to any nation and state as it can mitigate risk and protect community from potential drawbacks. The major motive for hacking is a profit and those law breakers do not hesitate to attack anything being from vital significance. The ultimate imperative of recent strategies was safety as something being convenient to many, but today it's clear it's needed to go a step higher in order to protect lives, businesses and infrastructure from arising threats. [1, 5] The best practice in policing is strongly attached to dependability of offenders on information-communication grid as anyone spending time there leaves footage and throughout detail analysis it is possible to locate any threat relying on cyber systems. Many brilliant ideas in security have demonstrated some weaknesses, because there is still risk from human factor being a part of the system. Service demands a lot, but there is a great appeal for better background investigation and timely confirmations of officers as they can become insider threats which intentionally or unintentionally do a leakage of the confidential findings. Combating such a challenge is uneasy and takes a lot of knowledge and experience as even the system members can be corrupted working against the interests of their society and encouraging concerning behavior of their people. The aim of the crime actors is to involve as many individuals as they can into illegal activities as their motto is they are stronger when there are many of them. That can significantly compromise an image and reputation of such a society within international cycles as the majority of the honest world can feel need to punish anyone supporting crime. The bad guys will always challenge and the mission of the good guys is to protect innocent people being the victims of such an occurrence, so far.

The 21st century has brought new technological revolution, as well as the heaps of security challenges. Cybercrime costs global economy trillions of dollars per annum, but some sources claim that the overall loss could be much bigger. Cyberspace has become a battlefield for cyber criminals and cyber warriors as it can be used to access anything being online. Sitting in front of screen or using a cellular phone can turn into horrifying experience as hackers are capable to do tracking, sabotage or espionage of anyone's accounts, devices or the other IT assets. Indeed, cyber security has developed some counter-measures to reflect those inconveniences and some tendencies in science and technology can see the light at the end of the tunnel. In other words, the situation is concerning, but there are some remarks it is possible to tackle such a crime.

Combating cybercrime is a criminology question and the current trends suggest nowadays best practice in case management is a powerful weapon in the hands of the investigators. Also, it is clear that there is not yet full awareness how corruption can be dangerous in generating novel insider threats which can try to ruin the system from inside. The crime's environment has evaluated into respectful ecosystem which

has caused the zero-trust order across the globe. [9] The criminals are stronger when they are together and they will mostly cope with strict rules and hierarchy within their syndicates. In their belief, there is always the method to trick the authorities and make the common people experiencing unrest in their communities. In expert's opinion, sometimes is so tricky to challenge criminal and terrorist organizations as they can react putting under risk both – people and resources. Apparently, the investigation seeks from the Police to be very discrete, because if the criminals find out someone is conflicting with their interests they can provide a furious response blackmailing many to stop operating against their needs. The ongoing crime's organizations are capable to shake the entire global landscape as they deal with power in their hands. In addition, virtual surrounding is a place where is feasible to conduct asymmetric warfare operations causing dramatic impacts to many. It seems cybercrime is a challenge to the modern authorities as it is the mix of technical and security matters. Managing risk in cyberspace is a tough task and some guidelines indicate there will be the huge need for a deep understanding of those issues.

Criminology is a science about the methodologies, techniques and approaches how to identify; process and resolve some criminal justice incident which should get its epilog on the court. On the other hand, it is important to understand crime as an attack to the legal system and its values. The mankind has a long history and through any past epoch the countries have coped with the laws being invoked to determine the rights, obligations and responsibilities of the community members living under such a rulership. If anyone would dare to breach the legal regulation that person would be punished following that time's investigation steps. With the progress of civilization the conditions have changed, but any approved country dealt with the authorities being trained to enforce the rules and protect people from the crime. The similar situation is even today as all legitimate states must guarantee the law enforcement on their territory as that is the only way to be a part of the United Nations which role is to assure legacy and human rights in regards with modern criteria of the legal societies. [16] Throughout history, there have always been geo-strategically important regions and those areas are commonly transit routes for crime's organizations. The past of those fields was turbulent and usually the place of conflicts, unrests and crises. If the local authorities are not capable to ensure the governance on their territory such a country might become the spot where crime blooms. In such a sense, it's obvious why the international collaboration in criminology is needed as the criminal and terrorist organizations cannot recognize the borders and in today's connotation they have a status of the transnational security challenges. Therefore, the identical case is with the cybercrime as anyone being online can become the victim of hacking. Further, high-tech criminality especially cannot recognize the limits as their actors can access the infrastructure at any point of the world producing so dangerous consequences to all. Hackers do not need to show their ID document in order to attend some place in the world; they only need to figure out IP address and such an asset will be all theirs.

Background Information

Under the modern condition any device being on the web can be used as a hacking tool. Downloading and installing the hacker's software on an object is simple task and the entire internet is overwhelmed with so handy tutorials, hacker's forums and similar online content. In other words, it's easy to become a cyber criminal and some experiences suggest that even the secondary school students can deal with skill being sufficient to make the first steps in such a crime area. The tendency shows cybercrime underworld recruits new members at that age and once thrown in such a business they can stay there for a long period of time. Average cyber criminal has a potential to turn into the other crime areas which makes him getting the hybrid threat. Typical case in criminology is that anyone with that skill can be suitable for drug trafficking, financial crime, human smuggling and even terrorism. Preparing the high-tech campaign takes time and effort and many crime organizations know how to take advantage over their cyber warriors. Only one hacking machine can cover a plenty of targets making out of attacked devices a grid which receives commands from a centralized workstation being capable to exploit all available vulnerabilities within an hour or two. The developed economies have a tendency to cope with smart technologies which means their peripherals communicate through TCP/IP channel and not via cables which is the case in the previous generation of computers. That means such a centralized system copes with network sharing capacities putting any device into grid and assigning it its IP address. [1-4] The modern marketplace offers some solutions on the web which can be applied to discover IP addresses and the other details in the network 4.0. The skillful hackers can demonstrate a wide spectrum of capabilities and sometimes it is a challenge to prevent cyber operation. The law enforcement agencies need to work smart in order to cut the information exchange in the cyberspace and carefully choose a moment to find out when the threat's plan is uncovered and further open for being mitigated. The next generations hacking challenges can be far more notorious than at present, but cyber industry yet needs to think about advancements which are at least a step ahead of the threat.

High-Tech Operation Challenges

Cyber technologies capture the majority of the information-communication systems which serve to deliver the findings from one point to another. Those technologies are highly sensitive to hacker's attacks as they can be approached from anywhere if they are in the network. Professional defense equipment can expose the devices even if they are not on the web, while the ordinary hacking tools are useful only if the object is online. The nightmare to hackers is once they access the cyberspace they will leave a trace within such an asset. The modern best practice in criminology shows that those cases can be resolved in an investigation fashion as there is the strong skill with the authorities worldwide. In addition, some fundamental researches across the globe can offer the helpful inputs to the entire high-tech industry. The cyber industry is so powerful drive which role is to offer a betterment of many coping with cutting-edge systems. It's time of cyber-physical revolution and the majority of current professionals deal with skill to improve and innovate what already exists, as well as provide some novel paths in their area of expertise. The cyber campaigns can offer a wide domain of the potential threats to people, businesses and

resources and those challenges should be tackled intelligently as the ongoing century has given unrests and crises over the globe. In order to protect the international interests in the world the cyber community must put a lot of effort developing tactics and strategies how to manage the risk within the virtual surrounding.

Characteristics of Asymmetric Landscape

The point of the asymmetric battlefield is a small group of the challengers will try to attack the numerous enemy. In other words, it's not about the warfare between two or more equally powerful sides, but mainly the conflict of some crime organization with the entire country or even the global community. The modern age is witnessing such a situation as the minority of the world's population believes it can get a power and dominance over the rest of the people. Combating asymmetric threat is very demanding as those folks cope with well-developed techniques of pushing their interests in the world. Cyber attacks are also asymmetric risk as it is possible to use a small army of the high-tech warriors which are capable to assault a heap of the targets within several hours causing so impactful harm. Apparently, after conducting a campaign the hackers normally select to escape and sometimes it is a challenge to locate them. The best policing practice can offer some response to such a criminality mostly through the international cooperation as cybercrime is a transnational offense.

Feasible Responses to Hacking

The usual cyber attacks can affect the accounts, endpoints, communication and anything being correlated with the web experience. The internet grid is available mostly with any place in the world and hackers know how to exploit its vulnerabilities. There are three sorts of cyber security such as prevention, surveillance and incident response. The leading experts in the field recommend to attempt to balance amongst those three types of defense. The perfect outcome to that challenge is to make an equal distribution of those key pillars once something is going on in the cyberspace. Also, the cyber security marketplace copes with some skill gap, but even in that case it is necessary to take an ingenious approach getting roads which probably exist, but they are not aware today.

Cybercrime as a Criminology Matter

According to some global Police and security associations, any abnormalities in the cyberspace are recognized as a crime. Those occurrences are normally described in some legal regulation, so skillful Police officers can determine a sort of the criminality and suggested punishments. The way which leads from the initial information to case conclusion must be crossed with investigation procedures that serve to make the case by the accepted laws. From expert's point of the view, the policing is a multidisciplinary area as it involves both – natural and social sciences professionals. Indeed, anyone in such an organization has some role and the main imperative is to assure solidarity between the staffing that serves for the same mission.

Considerations and Impacts

Some findings suggest that the cybercrime costs the global economy more than 5% of the world's gross product. Those are very wasted finances and if there would be a method to save those losses many people would be happy and secure. The high-tech attacks are the real disaster of the modern time and true headache to many governments over the world. Indeed, one of the ultimate challenges to nowadays criminology is how to reduce a rate of that offense as the population across the globe could work peacefully in order to impact a total productivity and effectiveness to their societies.

Conclusion

Asymmetric landscape has challenged the world throughout history as it brings a disbalance to many spheres of the lives and works. It's obvious than ever the security could be the most significant tendency in the future as the overall world literally creeps for better days. This century is an age of the challenges, so the entire defense community is needed to be united in order to protect global values and standards.

References:

- [1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.
- [2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine
- [3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine
- [4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine
- [5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine
- [6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine
- [7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine
- [8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine
- [9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine
- [10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal
- [11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine
- [12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine
- [13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine
- [14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine
- [15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine
- [16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books “The Internet of Things: Concept, Applications and Security” and “The Insider’s Threats: Operational, Tactical and Strategic Perspective” being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert’s channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with a disability.



Understanding The Concept of Privacy By Design

By Danijela Obradovic, Lawyer at Roberts & Obradovic

"Privacy by Design," a concept first introduced by former Ontario Information and Privacy Commissioner [Ann Cavoukian](#), is a comprehensive approach to privacy that goes beyond simply meeting regulatory and legal requirements. It involves incorporating privacy into all aspects of an organization, including its objectives, priorities, project management, and operations. [Privacy Lawyers](#) and IT professionals should understand the principles behind this important privacy framework.

The Privacy by Design framework is based on seven (7) principles:

Principle 1: Proactive, Preventative Approach - Organizations should anticipate and prevent privacy risks before they occur.
Principle 2: Privacy as Default Setting - IT systems and business practices should include the maximum degree of privacy protections by default.
Principle 3: Embedded in Design - Privacy should be incorporated into the design and architecture of IT systems and business practices.
Principle 4: Full Functionality, Positive-Sum Approach - Privacy and security, as well as privacy and revenue, can both be achieved.
Principle 5: End-to-End Security - Privacy and security measures should cover the entire lifecycle of data.
Principle 6: Visibility and Transparency - Organizations should be transparent about their privacy standards and practices and be open to independent verification.
Principle 7: User-Centric Approach - Organizations should prioritize the privacy interests of individuals and provide strong privacy defaults, appropriate notice, and user-friendly options.

The aim of these principles is to promote privacy as an integral aspect of organizational objectives, priorities, project management, and operations. We will discuss these seven principles in more detail below:

Proactive, Preventative Approach

The first principle emphasizes the anticipation and prevention of potential privacy invasions, rather than waiting for them to occur and offering remedial measures afterwards. This approach adopts a preventative attitude towards privacy risks, rather than addressing them after they have taken place. In essence, Privacy by Design aims to stop privacy infractions from happening in the first place, rather than reacting after the fact.



Privacy as Default Setting

The second principle, aims to provide the highest level of privacy protection by integrating privacy measures into all aspects of IT systems and business practices. Regardless of the individual's actions, their privacy is protected by default through the implementation of privacy-focused design and architecture. This means that personal data is automatically shielded from potential privacy breaches, eliminating the need for individuals to take any extra steps to safeguard their privacy.

Embedded in Design

The third principle indicates that privacy should be integrated into the very foundation of IT systems and business practices, rather than being added on as an afterthought. This results in privacy becoming a fundamental aspect of the system's core functionality, without compromising its performance.

Full Functionality, Positive-Sum Approach

Positive-Sum, not Zero-Sum, takes a “positive sum” view of privacy and recognizes that organizations need not choose between privacy and security or between privacy and revenue, as both can be achieved.

End-to-End Security

The fifth principle requires organizations to implement end-to-end privacy and security measures covering the entire lifecycle of data once privacy has been embedded into the design of IT systems and business practices.

Visibility and Transparency

The visibility and transparency principle requires organizations to be transparent with users and ensure that all interested stakeholders have visibility into their privacy standards and practices. Organizations should also consider obtaining independent verification of the robustness of their privacy systems.

User-Centric Approach

The last principle calls for organizations to adopt a user-centric approach and prioritize the privacy interests of individual users and customers. This can be demonstrated, for example, by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

In Canada, the CPPA (Canadian Personal Information Protection and Electronic Documents Act) contains no explicit reference to Privacy by Design or its seven foundational principles. However, the Standing Committee on Access to Information, Privacy, and Ethics has recommended that privacy by design be made a central principle and that its seven foundational principles be incorporated into Canadian privacy legislation, where possible.

In Quebec, on the other hand, privacy legislation (Bill 64) has incorporated Privacy by Design concepts. The legislation requires organizations that collect, use, or disclose personal information of individuals located in Quebec to implement privacy-by-default settings and ensure the highest level of confidentiality without any intervention by the individual concerned. Organizations must comply with these requirements, even if they do not have a physical presence in Quebec.

Canadian organizations operating in Europe should also be aware that Privacy by Design is an explicit legal obligation under the GDPR (General Data Protection Regulation). Article 25 of the GDPR imposes a duty on controllers to put in place technical and organizational measures that effectively implement data protection principles and integrate necessary safeguards into the processing of personal data to ensure protection of data subjects' rights. Pseudonymization and data minimization are explicitly mentioned as examples of appropriate measures.

Privacy by Design is a comprehensive and proactive approach to privacy that recognizes the importance of embedding privacy considerations into all aspects of information technology, networked data, and all organization.

About the Author

Danijela is a lawyer with significant experience in solving complex business challenges. She has a general corporate practice, with expertise in privacy law, regulatory compliance, risk management and corporate governance. Her clients range from medium size businesses to multi-national conglomerates. Danijela holds an engineering degree, having graduated with distinction from University of Waterloo, and has significant experience as an engineer at a top-tier energy corporation. She earned her Juris Doctorate degree from Osgoode Hall Law School. Danijela's commercial insight and technical know-how allow her to deliver practical solutions to clients. She is currently based in Toronto, Canada.



The Data Challenge: How to Map Data in A Distributed World

By Dotan Nahum, Head of Developer-First Security at Check Point Software Technologies

Here's a quick-fire question: do you know where all your sensitive data is? As businesses of all sizes generate, accumulate, store, and process more data records in more places than ever, it's increasingly challenging to classify and track all that data – not to mention make use of it.

On the one hand, enterprises rush into digital transformation with their isolated data silos and outdated legacy code. On the other hand, 86% of developers admit they do not consider application security a top priority when coding. Somewhere in between are CISOs facing burnout as they attempt to enforce code



security best practices, privacy regulations, and compliance standards into the chaotic process that is the software development lifecycle.

In this post, we'll look at mapping your distributed data is necessary, what challenges you'll face along the way, and how you can overcome them.

Why is data scattered in the first place?

Whether you like it or not, most data produced, stored, and processed by business applications is distributed by nature. Both logical and physical data distribution is necessary for any application to scale in functionality and performance. Organizations store different data types across different files and databases for various purposes.

The classic example of data distribution within a company is buyer and client data. One SME can have data on leads, warehouse orders, CRM, and social media monitoring spread over dozens of internally developed and third-party SaaS applications. These applications read and write data at different intervals and formats to owned and shared repositories. In many cases, each also has various schemas and field names to store the exact same data.

Application development processes distribute a significant portion of data within the application architecture, especially regarding serverless, microservice-based architectures, APIs, and third-party (open source) code integration. So, the critical question isn't why we distribute data in our applications. Instead, it's how we can manage it effectively and securely throughout its lifecycle in our application.

Mapping distributed data: is the effort worth the reward?

"Shift left" application security, big data security, code security, and privacy engineering are not new concepts. However, software engineers and developers are only beginning to adopt tools and methodologies that ensure their code and data are safe from malefactors. Mainly because, until recently, security tools were designed and built for use by information security teams rather than developers.

Privacy by design is nothing new either, but in today's hectic velocity and delivery-driven developer culture, data privacy still tends to be neglected. It often remains ignored until regulatory standards (like GDPR, PCI, and HIPAA) become business priorities. Alternatively, in the aftermath of a data breach, the C-suite may demand that all relevant departments take responsibility and introduce preventative measures.

It would be great if all software services and algorithms were developed with privacy by design principles. We'd have systems planned and built in a way that makes data management a breeze, which would streamline access control throughout the application architecture and bake compliance and code security into the product from day one. In short, it'd be absolutely fantastic. But that's not the case in most development teams today. Where do you even start if you want to be proactive about data privacy?

The first step in protecting data is knowing where it resides, who accesses it, and where it goes. This seemingly simple process is called data mapping. It involves discovering, assessing, and classifying your application's data flows.

Data mapping entails using manual, semi-automated, and fully automated tools to survey and list every service, database, storage, and third-party resource that makes up your data processes and touches data records.

Mapping your application data flows will give you a holistic view of your app's moving parts and help you understand the relationships between different data components, regardless of storage format, owner, or location (physical or logical).

Don't expect an easy ride.

Mapping your data for compliance, security, interoperability, or integration purposes is easier said than done. Here are the hurdles you can expect to face.

Depiction of a moving target

Depending on your application's overall size and complexity, a manual data mapping process can take weeks or even months. Since most applications that require data mapping are thriving and growing projects, you'll often find yourself chasing the velocity of codebase expansion and deploying additional data stores throughout micro-services and distributed data processing tasks. However, you spin it, your data map is obsolete as soon as it's complete.

The ease of data distribution

Why do new data stores pop up faster than you can map them? Because it's so easy to deploy new data-based features, microservices, and workflows using cloud-based tools and services. As your application grows, so does the number of data-touching services. Furthermore, since developers love to experiment with new technologies and frameworks, you may find yourself dealing with a complex containerized infrastructure (with Docker and Kubernetes clusters) that may have been a breeze to deploy, but is a nightmare to map.

The horrors of legacy code

As enterprises undertake digital transformation of their legacy systems, they must address the data used and created by those systems. In many cases, especially with established enterprises, whoever originally wrote and maintained the legacy code is no longer with the company. So it's up to you to explore the intricacies of service interconnectivity and data standardization in an outdated environment with limited visibility or documentation.

Integrating security and privacy engineering in your applications

It's no secret that data is stolen every day. So much so that you can pretty much guarantee that your email address is included in one or more datasets for sale on the dark web.

What can you do to protect your application and data from the greed of cyber criminals and the scrutiny of regulators?

Scan your code to map your data.

Modern CI/CD pipelines and processes employ Static Application Security Testing (SAST) tools to identify code issues, security vulnerabilities, and code secrets accidentally pushed to public-facing repositories. You can employ a similar static code analysis technique to discover and map out data flows in your application.

This approach maps out the code components that can access, process, and store the data, thus mapping out the data flows without fully crawling the content of any database or data store.

Enforce clear boundaries for microservices.

In a microservice architecture, each microservice should (ideally) be autonomous (for better or worse). But where does each microservice end and another begin regarding sensitive data?

You can identify the boundaries for each microservice and its related domain model and data by focusing on the application's logical domain models and related data. Then, attempt to minimize the coupling between those microservices.

Shift left for privacy in a distributed world

Data security and privacy are rarely a priority for application developers. So it's no surprise that application data can float around your cloud assets and on-premises devices uncatalogued and unmanaged. However, in 2023 you can't afford to neglect data privacy laws and potential data security threats lurking in your code.

Mapping the data flows in and out of your application is the first step to shifting privacy left and integrating privacy engineering, compliance, and code security in your CI/CD pipeline.

About the Author

Dotan Nahum is the Head of Developer-First Security at Check Point Software Technologies. Dotan was the co-founder and CEO at Spectralops, which was acquired by Check Point Software, and now is the Head of Developer-First Security. Dotan is an experienced hands-on technological guru & code ninja. Major open-source contributor. High expertise with React, Node.js, Go, React Native, distributed systems and infrastructure (Hadoop, Spark, Docker, AWS, etc.) Dotan can be reached online at (dotann@checkpoint.com) and <https://twitter.com/jondot> and at our company website <https://www.checkpoint.com/>.



Stop Backing Up Ransomware

By James Gorman, Cyber Security Expert and Entrepreneur

When utilizing cloud technology for workloads, companies often assume that their current backup strategy is sufficient for the cloud environment. However, having good backups has been a basic form of Cyber and IT resilience for over 35 years. While many IT organizations have established a backup strategy in the past, they have yet to adapt it to address new technologies and emerging threats.

Many organizations store their backups on media storage on-site or off-site storage, cloud-based storage, or another company-managed facility. However, as these traditional strategies and legacy solutions migrate to critical cloud-based workloads, they may need to be more suitable to ensure the resilience and recovery of cloud-based workloads. The cloud operates differently than traditional on-premise systems in that it is programmable, ephemeral, and on-demand, requiring a different approach to backup strategies to ensure the resilience and recovery of cloud-based workloads. Legacy backups can present a problem when migrating to the cloud, and they are not designed to be cloud-native and may need to be more effective in detecting and removing cyber threats and corruption. Restoring and testing these backups can be time-consuming and disruptive to daily operations. A corrupted backup can cause



significant issues when attempting to restore from backup to live production, resulting in disruptions and delays in restoring operations. This corruption is especially problematic if the backup itself contains the ransomware problem.

Some Startling Statistics:

- Ransomware attacks hit 80% of organizations in 2021. ([Pollfish](#))
- More than 60% of those hit by the attacks paid the ransom. ([Pollfish](#))
- The average ransomware payment was \$570,000 in the first half of 2021, up from \$312,000. ([Mimecast](#))
- 58% of organizations infected with ransomware agreed to pay a ransom in 2021, compared with 34% in 2020. ([Proofpoint](#))
- Of those, 32% had to make an additional ransom payment to regain access to their data/systems. ([Proofpoint](#))
- Ransom demands are five times higher when data exfiltration is involved. And that's happening six times more often in 2022 than in 2019. ([Arete & Cyentia](#))

Cyber Criminals are getting more competent and more professional.

As cyber criminals become more skilled and professional, they can launch attacks that evade detection for extended periods. According to one study, the delay between a malware infection and the execution of a ransomware attack can be as long as 72 days. This delay means that even if an organization has “done everything right,” like having backups that go back one or two months, they may still be restoring infected applications. Restoring the ransomware is a worst-case business scenario. Companies need to implement solutions that specifically protect against backing up ransomware. One such solution for the cloud is a Cyber Recovery Service, which can help ensure the integrity of application during and after a potential attack.

Cyber Recovery Service

Elastio provides a Cyber Recovery Service.

- not just backups
- not just malware detection
- not just recovery services
- not just another pretty dashboard

Elastio's Cyber Recovery Service offers comprehensive protection for your AWS workloads. It not only backs up your data but also ensures that it is free of ransomware and corruption. With Elastio's technology in place, you can have peace of mind knowing that your backups are malware-free and restorable. The service also provides a mechanism to restore a part or the whole application without interruption to current operations. Recovery testing can be performed, proving that your team has done Disaster Recovery training and can document it for audits such as SOC 2, HITRUST, PCI, or CMMC.

Elastio's founders have extensive experience in the industry and have been leaders in backup, recovery, and data security for decades.

Elastio auto-detects new workloads in your AWS environment, scans them for ransomware, and creates highly recoverable, immutable backups that are compressed and deduplicated for cost efficiency. [Download our guide](#) to defending your cloud backups from ransomware to learn more.

About the Author

James is a Cyber Security Expert and entrepreneur with experience securing, designing, deploying, and maintaining large-scale, mission-critical applications and networks. James leads teams through multiple FedRAMP, NIST, ISO, PCI, and HITRUST compliance audits, and he has helped numerous companies formulate compliance and infrastructure scalability strategies. His previous leadership roles span from CISO to VP Network Operations & Engineering to CTO and VP of Operations, at companies as diverse as GE, Epoch Internet, NETtel, SecureNet, Transaction Network Services, AuthX, Certify Global, SecureG, Cyber Defense Media Group, and OnePay.



James can be reached online at (jgorman@cyberdefensemagazine.com, @jgorman165, etc..) and at our company website <https://hard2hack.com/>

Is Your Firm Ready for the SEC?

How To Prepare for the Regulations of Tomorrow

By Jason Elmer, Founder and President of Drawbridge

It is no secret that cybersecurity regulations are on the rise: in 2022, the U.S. Securities and Exchange Commission (SEC) proposed cybersecurity rules that would affect all firms in the alternative investment industry. In addition to the processes already examined such as risk assessments and vulnerability management, the SEC also proposed conducting compliance checks around board oversight, incident response and annual reviews that require enhanced reporting. While these are only proposals for now, they represent a revolutionary shift in how the SEC will conduct due diligence in the future.



For many firms, new layers of cybersecurity and new compliance requirements can seem overwhelming. But if the SEC proposed rule changes tell us anything, it is that firms must take a proactive rather than reactive approach to ensuring their cyber posture ahead of the new rules expected in 2023, following the SEC reopening the comment period for another 60 days. Cybersecurity is no longer a checklist item to

be considered once a firm has achieved a certain level of AUM or funding – cybersecurity is a top consideration for firms of all sizes, and the SEC will not differentiate based on size.

A cautionary tale can be found in EyeMed, an Ohio-based vision care benefits company that was required to pay a \$4.5 million fine for failing to conduct a necessary risk assessment and violating the New York State Department of Financial Services cyber rules. This costly mistake could have been avoided had they conducted ongoing vulnerability assessments and implemented a multifactor authentication process for their email system. In addition to the fine, EyeMed was given three months to conduct a risk assessment and provide the regulator with a clear plan to improve its cybersecurity practices to avoid serious mistakes in the future.

The EyeMed incident shows that cybersecurity is a compounding issue that cannot be solved overnight. It requires firms to take charge and create comprehensive, technical and actionable plans that can be quickly executed so firms can stay one step ahead of looming threats. The key piece of preparation for SEC compliance is in “owning” a firm’s cybersecurity. Technology solutions can make this process easier for firms and empower them to take a proactive approach to their cybersecurity defenses, such as implementing data flow mapping to perform in-depth vulnerability analysis. These types of solutions are not only required for regulatory compliance, but also vital to protect the integrity of the data and information firms deal with daily.

While certain technical controls like policies, risk assessments and cybersecurity training can be outsourced, there are additional actions that firms will be required to complete, including:

- Internal team training to comply with the proposed 48-hour incident reporting deadline
- Data flow mapping to understand vulnerabilities and enable firms to implement the required mitigation tactics
- Board reporting on the fund’s current and future cybersecurity preparedness ownership becomes particularly important in this case.

Many firms historically left cybersecurity in the hands of IT providers or MSPs, particularly those firms without a CISO. That is no longer adequate. Cybersecurity today must be reviewed to protect sensitive data and information and prevent the significant cost of non-compliance. The stakes are even higher in the face of the new SEC regulations, and firms that fail to incorporate cyber into their strategic business operations and budgets may end up paying for it elsewhere, both in fines and in the loss of consumer trust.

Ensuring a firm’s effective cyber posture is not an overnight process – it requires ongoing risk assessments and an actionable road map to identify existing vulnerabilities and correct for the future. With appropriate planning, technological investment and empowerment from board members, firms will be able to meet and exceed the SEC guidelines – and become proactive in their fight to protect against cyberattacks.

About the Author

Jason Elmer brings more than 20 years of cybersecurity and IT infrastructure experience to his role at Drawbridge. As Founder and President, he is responsible for driving the firm's day-to-day operations, expanding its geographic and technology footprint and leading the company for global growth and scale. His management background includes multiple executive leadership roles and extensive experience delivering business critical FinTech software and solutions that meet the specialized needs of hedge funds and private equity managers.

You can find out more about Jason's work at <https://drawbridgeco.com>



How Must IT Leaders Develop Contingency Plans to Combat Geopolitical and Environmental Risks?

By Mohit Shrivastava, ICT Chief Analyst at Future Market Insights

In today's geostrategic context, geopolitics and technology are inextricably linked, but many IT professionals who prioritize digital transformation pay comparably little heed to the geopolitical and environmental threats.

If one wants their plans for technological adaptation and digital transformation to be successful as an IT leader, one must have a thorough understanding of the geopolitical and environmental risks that may affect their firm. The success of the organization depends on it, in reality. It has been noted that the geopolitics of technology and business are important components for the purpose-led growth of any company.

The dangers might range from industrial policy concerns to cybersecurity threats to shifting technical regulation. One of the most obvious instances of the relationship between technology and geopolitics is cybersecurity. These risks can threaten governmental organizations, which will affect the data in various IT companies. Such risks are propelling the demand for IT contingency plans like cybersecurity



insurance. According to Future Market Insights, an ESOMAR-certified market intelligence firm, the global [cybersecurity insurance market](#) is expected to garner a 19.1% CAGR from 2023 to 2033.

Governments are also progressively promoting self-sufficiency in critical technology through industrial strategy, which is fueling geopolitical competitiveness. Long term, this might pose serious dangers to the IT industry. Therefore, these hazards might prevent IT organizations from expanding and prevent them from creating effective backup strategies.

Thus, in this blog, we will discuss the importance of a cyber risk balance risk for data protection, how can IT leaders mitigate the risks via gaining organizational resilience, and how the Governance, Risk, and Compliance (GRC) programs doubling the security of data.

Opting for a cyber risk balance sheet can offer protection.

Cybersecurity is one of the most visible manifestations of the relationship between technology and geopolitics. Cyberattacks motivated by geopolitics may have a big impact on cybersecurity, risk management, and digital transformation strategies. While no firm is immune to such attacks, those that have robust data security systems, well-trained workers, and effective cyber defenses are expected to be less vulnerable. As a result, many IT leaders are looking to a cyber risk balance sheet preparedness strategy as a reliable IT contingency plan.

One "power move" that executives may undertake to enhance their decision-making about cyber risk is to create a cyber risk balance sheet. This straightforward change in corporate behavior and risk thinking integrates cyber hygiene with the current corporate risk management mechanism in a way that fosters knowledge, promotes wise conduct, and incentivizes sensible investments. This is achieved by making the various invisible ledgers of cyber hazards apparent via the power move of the cyber risk balance sheet.

A board member can advise their cyber leaders to assign their teams the duty of developing and evaluating a cyber risk balance sheet that lists the cyber incidents that might have a meaningful financial impact on the firm. The following are the essential processes in creating a cyber risk balance sheet:

Create a methodology for quantifying cyber risk that is suited to the organization's risk profile. Using Factor Analysis of Information Risk (FAIR), along with other industry standards like NIST SP 800-53 as well as ISO 27005, this may be built.

Identify the most important cyber threats that affect the company and assess the likelihood of the threat, the assets at risk, and the efficacy of the cyber controls currently in place to minimize them.

Create a balance sheet that combines planned or present investments in cyberspace with the likelihood of in-scope cyber threats and liabilities.

Once this balance sheet is completed, periodically examine and discuss it using the cost in dollars of cyber threats as a foundation for comprehending and converting the underlying impact on the bottom line. This ledger may be used to assess the effectiveness of current security efforts and to require Chief Information Security Officers (CISO) to justify additional cyber spending in terms of a profitable return on

investment. For example, a \$2.5 million investment in system security in the next 3 years reduces cyber risk by almost \$7 million on the cyber risk balance sheet.

Leaders can focus on building organizational resilience.

The frequency as well as the complexity of challenges across risk categories, from geopolitics to economic instability, from climatic changes to public health, and from talent to supply chain, are what is driving today's challenges for various IT companies globally. Business leaders must take action right now to meet these difficulties head-on and seize the possibilities they present by involving their workforce and establishing a sense of mission. In light of this, IT organizations must strengthen their organizational resilience.

Organizational resilience is the capacity to recover from negative experiences, learn from them, and come out stronger against recurring problems. It is better to approach resilience building from three angles:

Operational

It takes emergency service planning, workforce flexibility, crisis management, and technology to ensure that companies can operate under unfavorable conditions to develop innovative methods to serve consumers and safeguard staff amid unanticipated catastrophes.

Financial

Greater flexibility in capital allocation enhances diversity and streams of return in the face of uncertainty and supports agility in the face of the unexpected. Enterprises may become more resilient to unforeseen occurrences and generate more sustainable profits by experimenting with and swiftly learning from risk reduction and investment possibilities.

Human

Businesses that have leaders that are concerned about the requirements of each employee's own emotional, physical, financial, as well as social health and who foster a shared, corporate sense of purpose prosper under challenging circumstances.

Governance, Risk, and Compliance (GRC) programs are being implemented by various IT companies for better security.

Governance, Risk, and Compliance (GRC) is a methodical strategy to manage geopolitical and environmental risks, comply with all industry and governmental laws, and integrate IT with business objectives. It consists of methods and tools for integrating technology innovation and adoption with a

company's governance and risk management. The GRC strategy is used by businesses to reliably accomplish corporate objectives, eliminate ambiguity, and adhere to regulatory obligations.

By implementing GRC programmes, businesses may enhance their decision-making within a risk-aware culture. An effective GRC program may help key stakeholders set policies from a shared perspective and conform to regulatory requirements. GRC harmonizes the firm's overall policies, decisions, and activities.

Utilizing these GRC practises, corporations are able to make a range of data-driven choices. They may keep an eye on their resources, set guidelines or frameworks, and employ GRC tools and software to swiftly reach conclusions based on data. GRC streamlines corporate procedures around a common culture that supports moral standards and promotes an atmosphere that is conducive to growth. It oversees the creation of an effective corporate culture and encourages moral decision-making inside the business. It also improves a business' cybersecurity tactics.

Businesses may utilize data security measures to preserve customer data together with private information by utilizing an integrated GRC approach. Due to the increasing cyber risk that puts user privacy and data at danger, the company must create a GRC plan. It enables companies to follow data privacy regulations like the General Data Protection Regulation (GDPR). By establishing a GRC IT strategy, an IT department may boost customer confidence and protect its company from risking it to any geopolitical and environmental hazards.

Innovations like the Internet of Things (IoT), operational technology (OT), and quantum may expose the organization to risks related to data privacy, third-party security, identity fraud, and IT regulatory compliance in complicated technical contexts. To centralize and supervise risk management while satisfying compliance and reporting requirements, an IT executive must combine these contact points.

For instance, IBM® provides all-inclusive, product-neutral GRC and data privacy, as well as identity and access management (IAM) services from planning through execution, offering direction, and helping to choose, implement, and automate various risk management programs. Thus, to mitigate the numerous geopolitical and environmental risks, IT leaders might use programs as their IT contingency plans.

Conclusion

For various businesses, geopolitical and environmental risk refers to the possibility of global political unrest to endanger the operational and financial stability of corporations. Different IT leaders must comprehend the specifics of the link between corporate globalization and geopolitics, chart the "sites of risk" for corporate entities in their operations, and adopt forecasting tools to improve their enterprise resilience concerning threats from terrorism and conflict to develop a conceptual model to mitigate this risk. To advance this process, CEO leadership is also essential.

Analytics might be a different escape route. For enterprises to successfully manage risks and boost employee and business resilience, analytics and data are essential enablers. At the moment, organizations have access to a wide range of data on topics including insurance payments and losses, benefits, and skills, employee compensation, and cyber, climate, and capital threats.

Analytics as well as artificial intelligence may help leaders develop practical insights and viewpoints. They may better identify their needs, prioritize them, and allocate resources effectively by employing predictive modeling.

Numerous business leaders have been challenged by recent events, but their responses have demonstrated that managing uncertainty is achievable. Organizations may become stronger and more future-ready by concentrating on the techniques mentioned above.

About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Insights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and consulting engagements across ICT, Electronics, and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate in Engineering in Electronics & Communication.



Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!

Mohit may be reached at <https://www.linkedin.com/in/shrivastavamohit/>

and at our company website <https://www.futuremarketinsights.com/>

How the Increasing IT Talent Gap is Impacting the Cybersecurity Industry

By Pete Sorensen, VP of Strategic Initiatives of ConnectWise

In the rapidly evolving digital landscape, technology solution providers (TSPs) are having to deal with an unprecedented number of staff vacancies on their teams. What's more concerning is that the current IT Talent Gap and tech labor shortage are making it nearly impossible to fill these critical roles.

Although these shortages are reaching all areas of the tech industry, specific sectors, like cybersecurity, have been affected more than others. Despite the overwhelming need, cybersecurity continues to be one of the hardest-hit sectors of the IT talent gap because it's a necessity within all industries. The vast majority (86%) of Small- and Medium-size Businesses (SMBs) place cybersecurity within the top five priorities for their organization. And six in 10 will invest more in cybersecurity because it reduces the risks for their organization, according to the IT Talent Gap report.



While most cybersecurity companies are focusing on digital transformation, the new cloud-based technologies they need to turn to in the wake of the pandemic, and how they will handle rising inflation costs, many tech leaders are overlooking much more alarming truths within the industry.

The Critical Connection Between Cybersecurity and the IT Industry Talent Gap While the IT talent gap is an immense issue, causing similar pains in multiple corners of the globe, solving the cybersecurity talent gap is a sub-issue that's just as important, if not more, given the dire consequences a cyber-attack or breach can have on an organization's critical infrastructure, sensitive information, private data, business operation, and overall reputation.

The State of SMB Cybersecurity in 2022 report revealed several interesting statistics related to the issue:

- 78% of organizations across all industries said they plan to increase their cybersecurity spending over the next year.
- 31% cited broad-level pressure in this area compared to 14% in 2020.
- 94% of organizations said they'd be willing to move to a new cybersecurity provider that offered the right solution for their business.
- Additionally, 39% said they'd even be willing to pay more for a company that could provide that said solution (versus 30% in 2019).

What's at Stake for SMBs if the Cybersecurity Talent Gap Continues?

While the IT Skills Gap is causing similar pain points for all business leaders, solving the challenges posed by the cybersecurity industry talent gap is mission-critical to help SMBs survive the current backdrop of economic certainty and an increasingly complex cyber threat landscape.

Cybersecurity is one of the most significant IT sub-sectors in the global marketplace due to several contributing factors—namely the growing number and increasingly damaging effects of digital attacks.

In fact, over 60% of SMBs have experienced a financially damaging cyber-attack in the past 12 months, according to research.

The biggest reason is an increase in the number and effect of digital attacks. Also, many industries are calling for increased compliance legislation, necessitating more in-depth cybersecurity protocols.

Now, the question becomes: with this increased demand, how does the IT talent gap specifically play out for the cybersecurity sector?

IT companies that continue to fall short when it comes to finding talented, specialized labor begin to see drastic declines in key areas of their businesses. Failure to fill these highly skilled tech roles makes IT companies less secure, less efficient, and less effective. With so much of our world running on data and IT infrastructure, this may be one of the biggest industry challenges of our time.

Root of the Cause: Why Is There a Cybersecurity Skills Gap With Such High Demand?

Although data shows that the number of open cybersecurity positions dropped from 3.12 million to 2.72 million in October 2021, the cybersecurity talent gap actually grew during that period. What makes this even odder is that IT cybersecurity professionals reported overall higher job satisfaction and happiness levels from working in the field.

Data from one study shows that 2021 was the best year for cybersecurity workers, and employees in the field showed a job satisfaction rate of 77% that year, which was the highest job satisfaction rate in the history of the survey.

So, it stands to reason that one of the gaps in this particular IT sub-sector might have to do with questions surrounding on-site, hybrid, or remote work options. Only 15% of cybersecurity professionals expressed interest in returning to an office environment full-time, which has led to an above-average wave of resignations within this industry.

It's also important to note that changes to the job itself had a hand in this resignation wave. In the wake of the global pandemic, it wasn't just cybersecurity pros going remote—everyone did. The move to remote work resulted in a nightmare for industry professionals plagued with more headaches and more security risks that made it even more challenging for experts in the field to do their job.

North America is also facing a unique IT “size gap” due to the insurmountable medium-sized tech businesses experiencing intense competition from international mega-firms regarding things like market share and profitability. Naturally, the same competition takes place on a national scale when recruiting premier talent.

Automation to Ease the Burden on Cybersecurity Pros

The idea behind automation and the technology skills gap is to reduce the demand for talent by reducing the reliance on people. This can be especially effective in the security world, where things like patching, disaster recovery, and threat detection can all be automated and reduce the need for specialized talent.

Automation can indeed reduce the need for specialized cybersecurity talent, but IT execs need to be careful not to fall into the trap of relying solely on it. Some highly-skilled talent will still be needed to run and monitor these systems. So, while automation does relieve some of the pressure caused by the labor shortage in the cybersecurity sector, it doesn't solve it completely.

Budgets and expenses also limit the deployment of automation cybersecurity platforms throughout the industry. While this technology is becoming more and more established by the day, it's still relatively new. IT execs will need to carefully examine AI/automation platforms to see what they can afford and what services will be most impactful to their business.

Here are just a few ways IT companies are using automation to their advantage when it comes to cybersecurity:

- Offer customers 24/7 support solutions
- Streamline project management and automate routine tasks to increase employee satisfaction
- Improve business insights through real-time data capture and analysis
- Decrease unnecessary threat alerts and service calls
- Speed up threat detection and response times

While the list above is a great start, AI technology will continue to take on more responsibility in the future and hopefully drastically reduce the global pain felt by the IT skills gap.

Internal Training Programs to Upskill Employees

It's also important for companies to invest in an internal process for professional development opportunities to help widen the IT skills gap in cybersecurity. The benefits here are two-fold:

1. It shows employees that their employers are invested in their long-term success.
2. Employers benefit from a workforce with new and improved capabilities that enable them to tackle a wider variety of tasks in the short term.

The beauty of these programs is that they can be linked to specific needs or areas of specialization.

For example, by linking cybersecurity training to specific requirements or career plans (CompTIA, ISC2, etc.), organizations can craft and mold existing talent to fit their needs. This is particularly essential in areas like cybersecurity where roles are significantly outstripping supply.

Expanding Hiring Pools

The diversity and inclusion topic can be a loaded one because it forces tech employers to take a good, hard look in the mirror. IT companies need to be honest about whether or not they're taking advantage of the entire tech talent pool available.

Many minority groups find themselves underrepresented in the IT world. Part of the problem may be that employees and executives in the space have a massive disconnect on this issue. Only 24% of women and minorities experience a feeling of belonging within the IT industry compared to 75% of executives who feel like they do belong. What can IT leaders do to make these individuals feel more comfortable?

To achieve more diversity in IT roles, executives need to improve the diversity of the talent pool as a whole. Mentorship programs are a valuable tool in this area. A senior-level employee taking a new, minority employee under their wing can go a long way toward making them feel that they belong.

The Conclusion: Building a Cybersecurity Talent Foundation in IT

IT firms and SMBs need to think long and hard about the workplace systems and environment they're creating, and whether or not they're setting themselves up to attract new talent. In addition, they also need to consider implementing tools and strategies that allow their existing teams to be as productive as possible. Navigating this is the only way to keep your business best-in-class as we move into the future of the IT landscape and help reverse the trend of this growing global IT talent gap and increasing cybersecurity threats and breaches.

About the Author

Pete Sorensen, VP of Strategic Initiatives at ConnectWise. Pete Sorenson serves as the Vice President of Strategic Initiatives at ConnectWise—the world's leading software company dedicated to the success of IT solution providers (TSPs) through unmatched software, services, community, and marketplace of integrations. Pete joined ConnectWise in early 2018 and prior to that, he held several leadership positions during his 10-year tenure at DuPont Pioneer.

Website Link: <https://www.connectwise.com/>

Facebook: <https://www.facebook.com/ConnectWise>

Twitter: <https://twitter.com/ConnectWise>

LinkedIn: <https://www.linkedin.com/in/peter-sorensen-574abb48/>



New Cyber Threats Calls for New Approaches

By Mark Sincevich, Federal Director of Illumio

Data compromises hit record numbers in 2021 with [1,826 occurrences](#) reported, up 23 percent from 2017. In the last two years alone, 66 percent of IT managers experienced at least one supply chain attack and 76 percent experienced at least one ransomware attack. As cyber incidents become more advanced, agencies or commands must change their approach, or they'll continue to see the same results. They need to move beyond a traditional "prevention and detection" mindset and toward a Zero Trust Architecture.

For years, IT leaders across federal agencies have focused on preventing breaches and keeping cyberattacks from penetrating the network. But, as digital transformation continues to expand the modern attack surface and the nature and frequency of attacks evolve, that mindset must shift from *stopping all* attacks to also *minimizing* the impact of an attack and finally to *assume breach*. The reality is attacks are inevitable – and every agency is a target.

At a high level, a Zero Trust architecture moves beyond traditional security measures (i.e., perimeter-based security) and requires all users, whether inside or outside the organization's network, to be authorized before being granted access to specific applications or data. Predicated on three core



principles, “assume breach,” “least privilege,” and “constantly verify” a Zero Trust approach aims to shrink the initial attack surface and empower organizations to operate through a “never trust, always verify” lens.

Zero Trust also views users from a holistic approach and centers around five core pillars: identity, devices, networks, applications and workloads, and data. Traditionally, perimeter-based security has focused only on the first three pillars: identity, devices, and networks. However, if a cyberattack or malware can pass the first three pillars, the attack can then move freely across workloads or applications. Zero Trust Segmentation (i.e., microsegmentation) is designed to stop the lateral movement of cyberattacks, quickly minimizing the impact when an attack occurs.

In simple terms, think of microsegmentation like a hotel. Just because you're able to get into the lobby of the hotel (bypassing firewall defenses) doesn't mean you're able to automatically access your room. Because every room has a keycard, you can only access yours once you're checked in and once your access (via personalized keycard) is granted. And an example of constantly being verified, if you are meant to check out at 11am and you go out of your room and try to access your room at 11:30am, your access will be denied. You will have to go to the front desk and get re-authenticated.

Microsegmentation is the foundational component of the workload and application pillar of Zero Trust and plays a critical role in establishing any resilient security strategy. In fact, you cannot have an effective nor a complete Zero Trust security stack without having a microsegmentation solution. Ensuring agencies have an action plan in place and are taking small steps forward will ultimately better position them to combat and withstand evolving threats.

Where to Start with Microsegmentation

While many agency IT leaders recognize that microsegmentation is crucial to keeping up with evolving cyberattacks, it's important to understand that resilience requires a coordinated effort – requiring dedicated resources and new ways of thinking. To start implementing microsegmentation and “assume breach” successfully, agencies can:

- **Set Up a Zero Trust Task Force** – Zero Trust implementation is often hindered by bandwidth and competing priorities. Agencies can benefit from an internal task force to help guide the process. The Air Force's journey to Zero Trust implementation is a great example. This command is currently leveraging outside cyber, engineering, and program management to establish a Zero Trust Task Force. This dedicated responsibility – and allocated budget – is moving the needle on Zero Trust progress within the command.
- **Begin with a Network Map** – Agencies must start with real-time application and workload visibility into their network. You cannot protect, or defend against, what you can't see. This includes maximizing visualization and establishing a real-time map of applications, workloads, and interdependencies. This network discovery process provides agencies with the ability to find risky ports and prioritize where to start.

Cyberattacks aren't slowing down anytime soon – and as they evolve in both frequency and sophistication, agencies need to consider new ways to protect IT environments. Today's newfound emphasis on Zero Trust and resilience is one way to do this.

By prioritizing Zero Trust technologies – like microsegmentation – early on, agencies are better empowered to reduce cyber risk while accelerating Zero Trust outcomes quickly. This ultimately empowers them to focus more time, energy, and resources on furthering other mission critical objectives.

About the Author

Mark has 23 years of experience working with the DoD and Intelligence Community implementing technology solutions. He has worked for hardware and software vendors in the visualization, the backup and recovery, and the cybersecurity space in addition to the command-and-control market for over 10 years where he specialized in Cyber and Joint Operations Centers. He has written over three white papers and numerous articles on the topic of cybersecurity. He is a graduate of the University of Maryland, College Park and is a current member of the Civil Air Patrol (CAP) where he is his squadron's cyber education officer.



Mark can be reached online at <https://www.linkedin.com/in/mark-sincevich-4660957/> and at our company website <https://www.illumio.com/>.

Leadership Is Still Washing Their Hands of Cyber Risk

By John A. Smith, CEO of Conversant Group

Where it comes to owning responsibility for cyber risk, executive leadership has moved in and out of the spotlight like character actors in a play for over a decade. Circa 15 years ago, most IT teams went it alone, working to “keep the lights on” while also attempting to secure the enterprise against threats. Once cyberattacks and related global headlines became too voluminous to ignore, we (rightly) began hearing calls for [CEOs](#) and [boards of directors](#) to get involved—these attacks had become too catastrophic for senior leadership to defer awareness, decision-making, and blame. As breach damages soared, several CEOs were ousted. Finally, many executives answered the call, briefly taking the stage in security operations.

But it didn’t last long; companies worldwide found a loophole enabling them to defer risk back to IT in the form of an organizational change—the appointment of a Chief Information Security Officer (CISO)—offering up a technical leader with a high enough title that CEOs could move quietly back into the shadows. Exit, stage right. As an unsurprising aside, it was a series of cyberattacks by Russian hackers that inspired the [appointment of the very first](#) CISO ever—Steve Katz--by Citicorp in 1994. However, it



was many years and hacks later that first the government, and then the financial services industry, and then others adopted this role.

So, have these top executives taken responsibility, and has the CISO role mitigated risk? I argue that they largely have not, but it is crucial to understand why. Without full leadership awareness of the threats, risks, and potential consequences of attacks, IT teams are not able to obtain the buy in and budget necessary to fully understand their risk estate and mitigate it. And ultimately, as we will discuss, CISOs and IT are still largely on the front lines of accountability and blame today. Yet, sadly, they are unable to affect the security outcome without support from the top and resources from external parties. Our aim is not to disparage CISOs or IT; but rather, argue that given the current structure, support, and focus of the CIO role and IT department, they are set up to achieve suboptimal results and all the blame when things go south.

Why the CISO Model Still Fails to Address Cyber Risk

When companies scrambled to appoint CISOs *en masse* around 10-15 years ago, some brought in new blood—the most experienced security and compliance leaders appropriate for their needs. Others, particularly in the mid-sized business ranks, simply reorganized, elevating current senior IT staff to the title. In either case, it accomplished a few things that moved the actual end goal of security even farther away (and this dynamic continues today).

First, it provided a buffer and deferment layer between the CEO/board and the ranks of IT struggling daily with too much risk, too little staff, and insufficient budget allocation to secure the business. I don't necessarily blame boards and CEOs for this; security is *hard*. Most executives don't understand it; it's considered a highly technical cost center that presents a complex problem with thousands of moving parts you can't ever fully solve. Senior leaders have many conflicting priorities, all of which are screaming for budget and requiring solutions. While some are very technically knowledgeable, most aren't, and finding one person to shoulder the load is an obvious (though inadequate) solution.

Unfortunately, executives can never fully pass off this responsibility because data is far too central to the organization's ability to function. Because top leadership, boards, and even private equity firms make critical budget allocation decisions, they must be made to understand the vulnerabilities, potential solutions, and the real-world results of failure to act (in a language they can understand). Then, they must own the decisions on which risks to take based on budgetary allocations. While CISOs have a powerful title, we see in our daily work they still have less access to the board than they truly need to sway top leadership. They need a voice—and they need the right information to make top leadership truly understand what is at stake.

Second, in our experience, most (but not all) CISO's are quite focused on aligning their security programs against compulsory and recommended compliance frameworks like NIST, CIS, HIPAA, FedRAMP, and the like. These frameworks don't focus enough on ensuring the underlying security controls and technology are configured and orchestrated in a manner to prevent a breach. They are also static: they don't iterate in real time with the very fast-changing threat actor tactics or rapidly shifting organizational threat surface. In other words, CISOs and IT teams often don't know what they don't know—where the

threats truly exist in their environment, what needs to be fixed and how, and this puts them in an even weaker position to present accurate information to those holding the purse strings. I don't blame them, either—IT has a huge span of control, and even security-focused staff can quickly lose pace with current threat actor techniques when in their single corporate environment for a length of time.

Finally, while this model has provided a layer of culpability to shield the CEO and boards in the event of a catastrophic breach, so what? Who cares about blame (aside of the hapless, blamed CISO) when the organization's finances, reputation, and market position are a pile of ruin? Blame is a pointless game. Class action lawsuits are still likely to be undeterred anyway if the organization was found to be negligent in proper security practices, regardless of how compliant they are with frameworks and statutory requirements. CISOs and their associated teams must be focused on preventing this destruction so businesses, jobs, and industry can continue unabated by focusing on where the real risk lies—not in their written policies, regulations, and frameworks, but in the underlying tech stack and its configuration and orchestration.

This can be done by leveraging external, rigorous, and regular assessments of all key systems, applications, and controls. Threat intelligence must be applied to an organization's technology orchestration, and this can only be accomplished by a CISO operationalizing a risk register on the principle of Zero Trust. Zero Trust is not a single or set of processes, people, or products; it is an orchestration of all three. These activities, along with internal/external penetration tests and internal and external vulnerability scans (no less than monthly), must be leveraged as feeders to the operationalized risk register, which can then be presented to executive leadership in terms understood by them (dollars and potential damages). Executive leadership operating as a team, not just the CISO or any group or individual in IT, should be responsible for accepting discovered risks for the organization.

IT Teams Need Support: Top Down, and Outside In

It's time for CEOs, boards, and even private equity firms to enter the stage again and get educated. It's essential that they truly understand what is at stake—who is to blame isn't the core issue. They must be involved and provide the leadership and resources that CISOs and technical teams need to secure the organization.

It's true that CEOs and boards have many competing priorities. But when the business is decimated by a catastrophic breach, there is no greater priority than that—and by then, it is often too late to shine a spotlight on it.

About the Author

John A. Smith is the CEO of Conversant Group and its family of IT infrastructure and cybersecurity services businesses. He is the founder of three technology companies and, over a 30-year career, has overseen the secure infrastructure design, build, and/or management for over 400 organizations. He is currently serving as vCIO and trusted advisor to multiple firms.

A passionate expert and advocate for cybersecurity nationally and globally who began his IT career at age 14, John Anthony is a sought-after thought leader, with dozens of publications and speaking engagements. In 2022, he led the design and implementation of the International Legal Technology Association's (ILTA's) first annual cybersecurity benchmarking survey.

John Anthony studied Computer Science at the University of Tennessee at Chattanooga and holds a degree in Organizational Management from Covenant College, Lookout Mountain, Georgia. John can be reached online at our company website <https://conversantgroup.com/>.



Machine Identity Management: The Key to Managing Compliance Risk in a Multi-Cloud, Multi-Cluster World

By Sitaram Iyer, Senior Director of Cloud Native Solutions at Venafi

Financial services may be an industry in which [mainframes still do much of the heavy lifting](#), but increasingly it's also at the center of a new wave of cloud computing innovation. An estimated 60% of North American banks plan to invest in cloud technology in the future, [according to one estimate](#). However, as individual customers spread their risk by migrating workloads to multiple Kubernetes clusters across multiple public cloud providers, they may be unwittingly introducing new security risk.

That's due to a resulting explosion in the volume of cloud assets, all of which have identities that must be securely managed. The only way to do so in dynamic and volatile environments like these is to turn to third-party tooling for automation and control.



A multi-cloud, multi-cluster world

According to [one report](#), 92% of enterprises had a multi-cloud strategy last year. Deploying workloads across multiple public clouds can be particularly useful for organizations in highly regulated industries like financial services. It may help them meet compliance-based data sovereignty and availability requirements – by ensuring that sensitive information is stored in the right jurisdiction and that systems remain up-and-running even if one provider fails. A multi-cloud strategy also enables banks to take advantage of best-of-breed capabilities offered by specific providers. And it helps to mitigate the risk of vendor lock-in – which may also be a concern for regulators.

As multi-cloud has grown in popularity, so have containers and microservices – which offer a vehicle in which to run workloads across these different cloud environments. In many cases, it is Kubernetes that is used as the de facto system for automating, deploying and managing these containers. Again, at this level, financial services companies are choosing to run them not just in a single cluster but in multiple clusters – and across multiple cloud environments – to reduce vendor lock-in, enhance performance, and improve availability and resiliency.

But government and financial regulations also require businesses to assert a level of control over these environments in order to mitigate cyber risk. This should include not only human identity and access management, but also managing the digital certificates and keys that comprise machine identities.

When the auditors come knocking

What do we mean by machines in this context? It could refer to anything from devices to workloads, applications, containers and clusters. Fail to keep these identities up-to-date and secure and the “machines” they are linked to will become vulnerable to hijacking and exploitation – potentially leading to data breaches, ransomware, crypto-jacking and much more. That’s because machine identities effectively secure and encrypt communications between these cloud assets. Fail in this, and financial services organizations could expose themselves to significant reputational and financial risk.

The bad news is that there are several roadblocks to effective machine identity management. Containers in particular are dynamic and ephemeral – appearing and disappearing all the time. Each new one needs a digital certificate, which may ultimately only last an hour or two. Multiply this out over multiple clusters and clouds, and the numbers quickly become mind-blowing.

[Research reveals](#) that the average organization used nearly 250,000 machine identities at the end of 2021 – but that this figure will more than double to at least 500,000 by 2024. Three-quarters of surveyed CIOs said they expect digital transformation initiatives to increase the number of machine identities in their organizations by at least 26%. We would expect similar findings in the financial services sector.

The challenges are multiplied by the fact that cloud native identity management tools don’t work across other providers’ environments and don’t allow for continuous monitoring of machine identities. This can lead to duplicated effort, extra expense and critical security gaps. It will also put financial services firms at risk of failing risk management audits – [which will at the very least](#) require them to show an inventory

of every machine protected by a certificate and possibly answer additional questions on critical assets. Depending on the audit, significant fines could follow.

A win-win

In short, this is a job that has quickly become unmanageable for human security teams. Instead, they require a single, automated machine identity management solution to work across all cloud and container environments. It should automatically configure, renew and revoke certificates, delivering cross-cluster visibility to help teams check the status of machine identities and answer any auditor questions with confidence. Automated error displays down to the individual certificate-layer would enable them to easily click through and remediate – further enhancing overall security posture.

With a control plane for managing machine identities, financial services security teams can have the peace-of-mind that complex cloud environments will remain secure, even as they continue to evolve. And both they and developer teams will have more time to work on higher value tasks to support the business. That's a win-win all round.

About the Author

Sitaram Iyer is Senior Director of Cloud Native Solutions at Venafi. He believes security should be one of the primary considerations organizations make as they make their cloud native journey. With a plethora of cloud native technologies out there, it is critically important to empower developers and platform teams with services that allow them to build and deploy applications more securely.

Building a zero-trust model as you adopt strategies to use Kubernetes and service meshes can be challenging. At Venafi, we understand this and work with large enterprises who are looking to address these challenges.



Sitaram can be reached online at [LinkedIn](#) and at our company website www.venafi.com.

Protecting Accounting Firms from Cyberattacks

Cybersecurity Practices Must Be A Top Priority For Firms This Busy Season

By Alan Hartwell, Chief Technology Officer at IRIS Software Group

Financial service firms are a top target for cybercriminals given the highly sensitive client data they house, as demonstrated by the [268 financial services](#) data breaches in 2022 alone. The latest was [revealed](#) by Brian Tankersley, former CPA Practice Advisor tech editor, on LinkedIn when hackers tried to request Electronic Filing Identification Numbers (EFIN) from unsuspecting users.

Cybercriminals are in no way slowing down, and we can expect attacks to continue increasing in frequency and sophistication. Cybersecurity Ventures [predicts](#) a ransomware attack will occur every 2 seconds by 2031 and cost victims \$265 billion annually.



For firms looking to prevent breaches and safeguard valuable client data, cybersecurity practices must be a top priority.

Significant company impact

The latest cyberattacks targeted CPAs and tax preparers during a busy tax season, potentially allowing hackers to acquire sensitive financial data. A security breach can be extremely detrimental to firms, causing irrevocable damage to client trust and a firm's reputation – not to mention monetary loss.

Once cybercriminals steal data from a company, reputational and monetary damage could be long-lasting. One popular technique for cybercriminals to utilize sensitive data is requesting a high ransom payment from the firm and threatening to leak the data if the ransom is not paid. Theft can also lead to a loss of intellectual property, impacting a company's growth, and the loss of current and prospective clients.

As the cybersecurity landscape swiftly changes, cyber criminals are exploiting any weakness they can find, meaning taking the path of least resistance and keeping out-of-date security systems puts firms at high risk. On-premise systems are inherently easier to exploit than cloud-based systems, especially when firms do not have dedicated time each day to update security patches and ensure all programs are running as they should.

Protecting your organization

With trust being a vital component to a CPA-client relationship, cybersecurity must be a critical safeguard to protect your client's data. Every cyberattack is going to be different and there is no way to know how your client's data could be mishandled.

Less robust cybersecurity systems can be a target for cyberattacks, so it's important to have an appointed Chief Data Protection Officer or third-party dedicated to your cybersecurity. Ensuring that your anti-virus software is consistently updated, and multi-factor authentication implemented to prevent fraudulent access is a priority. Another top concern should be digital document storage and how your firm will protect data from breaches. This is especially true if you have acquired companies, as extending all cybersecurity systems across acquisitions will minimize risk.

Educating staff about cyber risks on a regular basis is also a key way to keep your organization secure. This training should include phishing, personal data protection and cybersecurity best practices. Fostering a culture of safe cyber practices will keep employees conscious of cybersecurity best practices.

Extending this expectation to third party vendors can be the best opportunity to protect your firm from a future breach. Be sure to ask about cybersecurity protocols, data protection measures, functionality, integrations and capabilities. A cloud-based SaaS is going to be the best way to ensure the security of your data. SaaS providers often have the resources to dedicate time and personnel to ensure system security for their clients. It is often hard for firms to exert the same level of security diligence on on-premises systems due to resource constraints that inhibit hiring dedicated cybersecurity staff. Turning to

cloud-based systems offers a cost-effective solution and allows you to focus on what's most important – your clients.

While integration of cloud-based technology has been slow to adopt within the accounting industry, it is essential for safeguarding the future of a firm. With proactive protections in place, your firm can focus on safeguarding your vital corporate and customer data and focus on delivering value to your clients.

About the Author

Alan Hartwell is the group chief technology officer at [IRIS Software Group](#). He is responsible for evolving IRIS' cloud software offering and further developing its product engineering capabilities to support its increasingly international expansion. Hartwell brings over 25 years' senior level experience supporting and leading the acquisition, consolidation and integration of products and technologies.

Alan can be found on [LinkedIn](#) and at our company website <https://www.irisglobal.com/>.



Ransomware Takes No Prisoners

By Monica Oravcova, COO and Co-Founder of Naoris Protocol

The recent Killnet cyberattack that disrupted contact between NATO and military aircraft providing aid to victims of the Turkish-Syrian earthquake, is a clear indication that cybercriminals do not discriminate. Anyone, any company and any organisation is a target.

While ransomware was not indicated, the Distributed Denial of Service (DDoS) attack briefly shut down the website of NATO Special Operations Headquarters and disrupted communications with Strategic Airlift Capability, an organisation that relies on NATO for assistance with humanitarian airlifts.

“Computer as a Target” cybercrime like the one above, used to be a rare occurrence, as this type of attack required a high level of expertise and a number of actors working in tandem to execute. Now however, cybercriminals are collaborating, and setting up infrastructures and organisations that have all the hallmarks of legitimate companies, replete with marketing, administration, sales and human resource teams.



Ransomware as a service (RaaS) fuelling attacks

“Computer as a Tool” cybercrime however, is much more prevalent because the skill set required to execute attacks is less demanding. In these cases, the attacker relies on human error or ignorance to exploit a device or network. The statistics are alarming, phishing attacks on mobile devices make up [60%](#) of cyber fraud and [95%](#) of data breaches are caused by humans. Organised crime syndicates are now selling RaaS (ransomware as a service) tools to would-be hackers, it's estimated that a ransomware attack occurs every [39](#) seconds, and in a recent Microsoft report the number of password attacks reached [921](#) attacks per second in 2022, an increase of 74% in just one year.

Attacks on such strategic and important organisations like Nato (and a host of other organisations including [Royal Mail](#) and [American Airlines](#)) should be limited to movie screens, unfortunately, the breaches are very real and the threat is growing. Best estimates predict that the financial fallout from cyberthreats in web 2 and web 3 could cause A \$10 Trillion cyber damage headache by 2025.

Why the battle is being lost

According to Statista, [revenue](#) in the Cybersecurity market is projected to reach US\$173.50bn in 2023 and the average Spend per Employee is projected to reach US\$8.19k, so there is a lot of money being thrown at the problem.

There's a myriad of reasons why traditional cybersecurity is failing, fundamental issues include the exponential increase in ransomware precipitated by the pandemic and the hasty shift to remote working (an increase of 148% in 2020 alone). This shift to BYOD (bring your own device) and cloud computing happened with little time to put strategies and technology in place for IoT security. Due to business revenue decreases in almost every sector during the lockdowns, IT budgets were cut and staff were culled, resulting in a skills gap, and this culminated in increased cybersecurity weaknesses.

These core issues played right into the hands of cybercriminals and they took full advantage. Innovation in cybercrime technology is as, if not more, robust than cybercrime prevention technology. Cyber criminals have funding, knowhow, time and incentive to sharpen their skills. While payouts for ransomware according to a [Chainalysis report](#) revealed that funds sent to known ransomware addresses globally fell from \$765.5 million in 2021 to \$456.8 million in 2022, it's premature to celebrate. Even though there is increasing resistance to paying ransoms, there is still the sticky issue of compromised data. The hackers still have access to the data they stole and will no doubt be selling it to other nefarious actors.

Using teaspoons to dig a trench

In an increasingly decentralised and networked world, current cybersecurity solutions are no match for cybercriminals. While cybersecurity mesh architecture (CMSA) championed by Gartner is gaining traction it doesn't go far enough.

Current cybersecurity is centralised, configuring network devices to operate in silos, all served by [cybersecurity](#) software that operates from opaque systems that can't be audited. In essence, every new

device added to a network becomes a single point of risk to the network it serves. Hackers use these weaknesses to launch their malware through phishing and smishing attacks. Given that the majority of individuals operating devices on networks are ill-informed about the dangers of ransomware installed via phishing and smishing, companies are sitting ducks for this kind of attack.

Until cybersecurity solutions are decentralised and distributed; unifying the governance of all devices so they operate in harmony, ransomware attacks will continue to rise.

The need for decentralised security is becoming more urgent, it's estimated that global [ransomware damage alone will cost \\$256B in 2031](#). With decentralised security, each device becomes a cyber-trusted validator node that monitors every other device in the network in real time, removing traditional points of failure. It monitors the system's metadata, OS levels etc. of the devices programmes and Smart contracts (if web 3), and not the activity of the user.

In a decentralised cybersecurity environment, when a hacker interferes with code, there would be an instant alert and the device could potentially be locked out of the network, preventing the full infrastructure from being compromised. This ensures both Web2 and Web3 operate safely, bringing decentralised trust and security enforcement to centralised spaces.

Detection of risks and governance lapses in complex environments or networks, should happen in seconds, not months, which is currently the case. According to IBM, the average breach lifecycle takes 287 days, with organisations taking 212 days to initially detect a breach and 75 days to secure it.

For now, we are going to see an increase in attacks as technology is trying to understand web3 and catch up with web 2. The best defence is education - it's vital that all employees and individuals are trained on their role in combating cybercrime. Given that 95% of all hacks are caused by human error, this would be a very worthwhile investment.

About Naoris Protocol

Naoris Protocol is the Decentralised CyberSecurity Mesh for the hyper-connected world. Our disruptive design pattern makes networks safer as they grow, not weaker, by turning each connected device into a trusted validator node. A robust Blockchain protocol that every company can use to protect against the escalating levels of cyber threat.

Devices are rewarded for trusted behaviour, fostering a secure environment. Participants earn \$CYBER staking rewards for securing the network.

The more users, businesses, and governance structures that use the Decentralised Cybersecure Mesh, creating networks of networks, the stronger and more secure it becomes.

About the Author

Monica Oravcova, COO & Co-Founder of Naoris Protocol . Experienced leader with 15+ years in IT and Cybersecurity for Telco, Finance and Manufacturing, led operations and executive teams for FTSE 100 clients AT&T, IBM and Apple, managing budgets over \$100M. Passionate evangelist and thought leader for women in Deep Tech.

Monica can be reached online at [LinkedIn](#) and at our company website <https://naorisprotocol.com/>.



Reduce Healthcare Insider Threats with Identity and Access Management

By Zac Amos, Features Editor of ReHack

Identity and access management (IAM) refers to the policies, procedures and technologies used to manage and control access to digital resources and systems. IAM plays a crucial role in cybersecurity, particularly in mitigating insider threats. Insider threats occur when employees, contractors or third-party vendors with authorized access to sensitive systems and data intentionally or unintentionally misuse their privileges, resulting in security breaches, data loss or theft.

Health care organizations are [particularly vulnerable to insider threats](#) due to the sensitive nature of the data they handle, including medical records, personal information and financial data. Learn how to protect such critical information with identity and access management.



Understanding Identity and Access Management

IAM is a comprehensive framework that ensures users and entities can access the resources they need to perform their jobs effectively while preventing unauthorized access. It involves managing the digital

identities of individuals and entities who need to access resources, ensuring they have the appropriate level of access based on their roles and responsibilities.

IAM also involves authentication and authorization mechanisms, which verify user identities and control their access to resources. Its solutions typically involve the following components:

- **Identity Governance and Administration (IGA):** IGA involves managing the life cycle of digital identities, ensuring user identities are accurate, up-to-date and aligned with organizational policies and procedures.
- **Authentication:** Authentication mechanisms verify the identity of users before they can access resources. Common authentication mechanisms include passwords, biometrics, smart cards and tokens.
- **Authorization:** This controls user access to resources based on their roles and responsibilities. Authorization mechanisms include role-based access control (RBAC), attribute-based access control and mandatory access control.
- **Single Sign-On (SSO):** SSO enables users to access multiple resources using a single set of credentials, streamlining the authentication process, and reducing the risk of password fatigue and unauthorized access.
- **Identity and Access Analytics:** This provides insights into user behavior, enabling organizations to identify anomalies, suspicious activity and potential security threats.

How IAM Can Help Protect Against Insider Threats in Health Care

By implementing a robust IAM framework, health care organizations can offer training [to reduce the 25.9% turnover rate](#), control who has access to what resources, and monitor and manage access in real-time, reducing the risk of insider threats. Here are some specific ways in which IAM can help protect against insider threats in health care.

1. Access Control

Health care organizations can manage access in real-time and regulate who has access to what resources, thanks to IAM. They can also [lower the risk of data breaches](#) and theft by adopting access controls to ensure only authorized individuals can access critical data and systems. For instance, health care organizations can use RBAC to assign access permissions based on predetermined roles, verifying users can only access the resources they need to perform their jobs.

2. Identity Governance and Administration

By implementing IGA, organizations can make sure only authorized personnel can access sensitive data and systems. For example, health care organizations can use IGA to manage user accounts and permissions, ensuring profiles are only created for authorized personnel.

3. Multi-Factor Authentication (MFA)

MFA requires users to provide two or more forms of authentication before they can access resources, such as a password and a biometric scan. This can significantly reduce the risk of unauthorized access, as attackers must compromise multiple factors to gain access. For example, health care organizations can use MFA to ensure only authorized personnel can access sensitive data and systems, reducing the risk of data breaches or theft.

4. Privileged Access Management

Privileged access management (PAM) is the process of managing and restricting access to accounts with [elevated admission to sensitive data](#) and systems, such as administrator accounts. PAM can help health care organizations verify only authorized staff use privileged accounts and are routinely reviewed and watched for unusual activities. Health care companies can also use it to limit access to sensitive information and systems to those employees who need it to perform their jobs.

5. Continuous Monitoring and Analytics

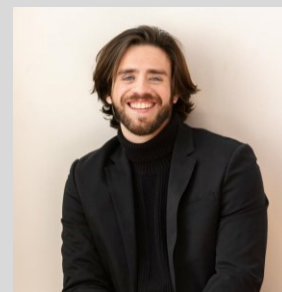
IAM solutions can enable health care organizations to monitor user activity continuously and manage access permissions in real-time. This can help organizations detect and respond to insider threats quickly. For example, health care organizations can use analytics to monitor user behavior and identify anomalies, such as accessing data outside their regular working hours or attempting to access resources they are not authorized to others.

Eliminate Insider Threats in Health Care

Identity and access management solutions can effectively mitigate these threats by controlling access to data and systems, managing identities and monitoring user activity in real-time. By implementing a comprehensive IAM framework, health care organizations can significantly reduce the risk of insider threats and safeguard sensitive patient data and systems.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on [Twitter](#) or [LinkedIn](#).



Risk: Everything Everywhere All at Once

It's Time to Get Proactive About Risk Reduction

By Marc Gaffan, CEO of IONIX

The first quarter of 2023 is being dominated by a singular theme, re-thinking risk. We came into the year facing the most anticipated recession of all time. The Federal Reserve is hiking rates at a furious pace. This is having its intended impact on the economy, particularly on the housing market. “Don’t Fight The Fed” was the rallying cry of Wall Street strategists. Instead, the market took off like a rocket in January. By the end of the month, the Bears were getting weak, and many were giving in. Fear of missing out (“FOMO”) is a powerful thing.

A few weeks later the gains are gone. Investors are again rethinking their strategies for the rest of the year. Are we headed for a rebound or another leg down? What’s the bigger risk, missing the rally or fighting the Fed?

In the technology sector, a seismic change in the nature of risk took place in early March, when The National Cybersecurity Strategy ([“NCS”](#)) was released. Its top priority was to, “rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.”

So, what does that mean for practitioners? According to the Strategy, “Shifting liability for software products and services to promote secure development practices.” That’s right. If you develop software or



deliver software as a service, you are responsible for its security. This will lead to many changes in software development and application security. It turns out the DevSecOps debate is only getting started.

Another example of rethinking risk is the sudden collapse of Silicon Valley Bank. Is your money safe in the bank? That is the ultimate reevaluation of risk. One anecdote from the weekend of worry drove home how connected, and vulnerable, we are. It was a small business owner who had no banking relationship with Silicon Valley Bank. He would not be able to make payroll. Why? His payroll firm was a client of the bank, and the payroll funds froze. As Tony Dwyer, Canaccord Genuity's Chief Market Strategist said in a note to investors, "The risk is not in what you can see, it is in what you cannot see."

When it comes to securing your organization, how should you be thinking about risk right now? What are you not seeing? The first thing to understand is risk extends far beyond the assets of your organization.

Digital transformation drives growth. It also increases cyber risk. As your organization leverages third-party infrastructure and SaaS apps and becomes more connected, you also become more vulnerable. Their security is now your problem. You are in a similar position to that small business owner and his payroll vendor.

Now is the time to get proactive about risk reduction. One of the most impactful things you can do to reduce risk is to reevaluate your extended attack surface. Here are three proactive things that you can do to frustrate threat actors and reduce risk facing your organization.

- Map external risks that put your organization in danger. Always be ready to answer the question: what assets do we have out there, and what are they connected to or reliant on? Then, if any of these create an attack path, block it.
- Unused and abandoned assets are an attack surface goldmine for cyber attackers. Often these assets have access to sensitive systems and data. It is best practice to remove assets as soon as possible when no longer used or necessary.
- Speaking of best practices, patching your infrastructure remains a missed opportunity. It's also one of the simplest vulnerabilities to mitigate.

We are all thinking about risk right now. For those responsible for cybersecurity, the challenges are many. With an understanding of your true extended attack surface, you can take these proactive steps to reduce risk.

About the Author

Marc Gaffan is CEO of [IONIX](https://www.ionix.io), formerly Cyberpion, the leader in Attack Surface Management. With a focus on building and scaling companies, Marc has led startups to become industry leaders with thousands of worldwide customers. Marc has 20 years of cybersecurity experience, most notably founding Incapsula, growing the company to \$100M ARR, and its acquisition by Imperva. Marc can be reached at <https://www.linkedin.com/in/marc-gaffan/> or at our company website <https://www.ionix.io>.



Top 7 Tips to Protect Your Endpoint Devices

By Nicole Allen, Senior Marketing Executive at Salt Communications

The threat landscape has become more sophisticated due to the new hybrid working lifestyle and companies' use of connected devices has resulted in an ever-increasing number of attack surfaces. Phishing and ransomware assaults are two of the most common and persistent endpoint threats. In order to safeguard all of the new remote endpoints, [COVID's](#) quick change to working from home modified some security objectives. Employees operating their devices outside your network perimeter are, without a doubt, particularly vulnerable to cyberthreats. Organisations should keep in mind, however, that they must also defend their own resources and systems.



How does endpoint security work?

Endpoint security protects end-user devices and the data travelling to and from them by adding additional layers of security. Antivirus and [malware protection](#), malicious activity detection, [mobile phishing](#) prevention, [internet browsing protection](#), and [data encryption](#) are all examples of this protection.

As discussed above, phishing and ransomware are two of the [most common](#) endpoint threats. [Phishing attacks](#) can be distributed through genuine applications and used for a variety of goals, including

monitoring user activity, collecting login credentials, sending ransomware and other malware, and gaining access to a company's network.

Ransomware is the number one cyber threat to businesses, according to [Secureworks researchers](#). These attacks are raising the stakes by creating a high demand for stolen credentials and data, as well as broadening the toolkit of threat actors. Since the early days of ransomware, threat actors have understood that data is money and have honed their approaches. [Ransomware](#) has changed the game, so you'll need to rethink how you secure your endpoints from this threat.

In order to protect all your employees and organisations as a whole against the latest cybersecurity threats, Salt offers the following recommendations:

1. Beware of common web app threats

The presence of software vulnerabilities and threats to online apps is something that all business owners will have to recognise and [protect themselves](#) against. A well-functioning web application is frequently backed up by a security infrastructure that includes a number of complicated components. Databases, operating systems, firewalls, servers, and other application software or devices are all included. What most people don't realise is that all of these components need to be maintained and configured on a regular basis in order for the web application to function effectively.

[Directory traversal attacks](#) are still being used against insecure web apps, allowing attackers access to sensitive data on the server hosting the online service. In the end, the attacker may gain access to sensitive data or perhaps complete control of the system. Administrators can reduce the risk of these attacks by updating their web application and server software on a regular basis and using [intrusion prevention systems](#) to secure their servers.

2. Have a data access policy

Many firms [lack](#) the simplest data storage, access, and usage protocols. Any organisation that wants to protect its data must define the data classification levels. In the case of personal or financial data, for example, data can have public, limited, or critical access. Since not every employee in a firm needs access to all of the company's data, a [data storage strategy](#) is more than merely encrypting data and hoping for the best. That's why an effective data storage strategy should include access restrictions for who can access and use data, as well as for how long.

Each type of data should be defined in terms of which workers and departments have access to it. User authentication mechanisms, such as [two-factor authentication](#), can be used to accomplish this. As well as at all times any security breach should be immediately reported to the protocol's administrators.

3. Consider all devices not just one

A device is considered an endpoint if it is [connected](#) to a network. With the rise of [BYOD](#) (bring your own device) and [IoT](#) (Internet of Things), the number of individual devices linked to a company's network can easily approach the tens (and hundreds) of thousands.

Endpoint security is frequently [focused](#) on laptops and desktops, but tablets and smartphones are just as critical. This is particularly true today that the workplace has evolved to more agile working methods. Endpoints (particularly mobile and remote devices) are a favourite target of adversaries because they serve as [entry points](#) for threats and malware. Think of the latest wearable watches, smart devices, voice-controlled digital assistants, and other IoT-enabled smart devices as examples of mobile endpoint devices that have [evolved beyond](#) Android and iPhones.

As a result, verify that all company-issued devices, including mobile phones and tablets, need to have [endpoint protection](#), and discourage the use of personal devices unless they have suitable company-approved security or communications installed.

4. Keep certifications and technology updated

Most businesses resent the [numerous procedures](#) required to maintain regulatory compliance, but these restrictions frequently assist businesses in a variety of ways. They aid in the identification of data that could be a target for hackers, as well as the procedures that must be followed to protect this data from cyber-attacks. An organisation can better defend itself from costly data breaches by implementing suitable compliance rules.

Data integrity and reliability are also improved by adhering to [compliance rules](#). While many standards are focused on data security, others maintain business continuity so that your company can respond promptly to a crisis, both physically and online. Furthermore, the standards benefit employees and customers by improving the ethics employed to operate the company and to retain data.

Government regulations, industry standards, and software licence agreements must all be followed by [all enterprises](#). That means you need to know where all of your endpoints are, what's running on them, and how they're used. Ensure that your company's endpoints are patched on a regular basis, and that all licensing adheres to the most recent compliance and regulatory standards.

5. Update your security and recovery plans on a regular basis

It's also crucial to keep in mind that a security or data recovery plan is a [living document](#) that needs to be updated on a regular basis. Developing a solid disaster and security recovery plan is a time-consuming process that delves into the nitty gritty of your business and how you'll handle a worst-case situation. It has numerous business-critical components, and collaboration with third-party experts should be explored in order to achieve the [best-fit approach](#).

Reviewing your security and disaster recovery strategy on a regular basis is essential for ensuring that it accurately depicts your environment and responds to the risks and repairs required for [business continuity](#). If you've added additional mobile, [IoT](#), or on-premise resources, update your security and disaster recovery plans to reflect any new or changed network infrastructure.

6. Educate all employees on the risks

In your IT environment, your employees are the [most common](#) attack vector. It's the motivation behind phishing attacks, email attacks, and other forms of cybercrime. Employees might thus be your biggest weakness or greatest strength in terms of cybersecurity, if you follow that logic. It all boils down to the education you provide them.

As a result, you must do proper [staff endpoint training](#). For the record, this does not imply that you should meet every six months or even every quarter. Instead, make it a regular occurrence, such as a monthly or bi-weekly meeting or (for remote workers) some kind of training programme. Education is useless if it isn't reinforced on a regular basis, and especially if it isn't adjusted as new threat intelligence emerges.

[Every employee's actions](#) play a critical role in guaranteeing your network's security. Employees can do a lot to help, whether it's not clicking on a phishing link or choosing a more unique password. Since many employees are unaware of the dangers, it is essential to educate them on fundamental security practices.

7. Have a secure communications system for all endpoint devices

With an ever-increasing number of mobile users needing access to sensitive data, your company faces new security concerns linked to endpoint security every day. Protecting your data, which is likely your most valuable asset, with a [secure communications system](#) has numerous advantages.

Having secure communications enables professionals to conduct secure calls and message threads while maintaining complete communication privacy. [Salt Communications](#), for example, protects your company's data from attackers from outside your organisation. Organisations will be able to maintain control over their communications and feel secure in any event that arises during their day-to-day operations. As well as having complete administrative controls for monitoring users, tracking activities, and executing corporate policies in order to accomplish complete endpoint security, regulatory compliance, and business improvement at the bottom line.

Beyond the endpoint

Endpoint [threat protection and visibility](#) are essential for detecting threats in your company, but there will always be gaps due to unknown or unprotected endpoints. [Endpoint telemetry](#), when paired with regularly updated threat information and data from network and cloud security controls, gives you a more complete picture of potential threats to your business.

Maintaining cybersecurity in the face of [COVID-19-driven](#) organisational transformation can aid in the prevention of phishing and ransomware attacks. Remote working is a growing trend that shows no signs of slowing down. To safeguard your organisation and cut down on wasted staff hours each year, you need effective detection and protection on these remote endpoints.

As a precaution, verify that all company-issued devices, including mobile phones and tablets, have endpoint protection. Feel free to contact Salt to secure your communications with our award winning [secure communications system](#) which enables professionals to conduct secure calls and message threads while maintaining complete communication privacy.

If you require any additional assistance, please contact our experts for more information on this subject at info@saltcommunications.com or to sign up for a free trial of Salt Communications or to [speak with](#) a member of the Salt Communications team.

About Salt Communications

Salt Communications is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt Communications is headquartered in Belfast, N. Ireland, for more information visit Salt Communications.

About the Author

Nicole Allen, Senior Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online at ([LINKEDIN](#), [TWITTER](#)) or by emailing nicole.allen@saltcommunications.com) and at our company website <https://saltcommunications.com/>



Considering All Returns on a Cybersecurity Compliance Program

By Doug Barbin, Chief Growth Officer and Managing Principal at Schellman

C-Suite executives have many variables to consider when they are implementing changes or making investments at an enterprise level. They are reckoning with a fragile economy, downsized teams and heightened inflation rates—putting budgeting and cost concerns top of mind, and rightfully so. However, too often, business leaders get caught up in the everyday consumer mindset of bargain-hunting for products or services that require exceptional accuracy and efficiency. This is none truer than for organizations shopping for a cybersecurity compliance assessment.

The cybersecurity industry itself is facing challenges as well. The adoption of data privacy regulations – from [CMMC](#) to [GDPR](#) and [CCPA](#), expanding security threats and additional digital footprint complexities have further complicated and increased costs for trusted and secure cybersecurity operations. To further



burden decision-makers, cybersecurity insurance premiums are [peaking](#) for those who worry about or experience a breach.

While this may entice business leaders to look for affordable cybersecurity assessment auditing programs above all, it's important to note [the average cost of an enterprise data breach was \\$4.35 million](#) in 2021. So, while cost is an important factor in any business purchase, it should not and cannot be the only factor when conducting a security assessment. Instead, when researching different cybersecurity auditing partners and programs, Chief Information Security Officers (CISOs) should consider return on assessment investment (ROAI).

Understanding ROAI measurements

ROAI measurements leverage a combination of factors, including an auditing firm's reputation and resources—enabling leaders to take a more strategic approach to decision-making. It also considers the working relationship that an auditing firm will have with a business, accounting for process-related efficiencies and workflow synergies. In essence: it covers the largest impacts of a compliance program, beyond cost.

Assessment firms with enhanced expertise, scale and capabilities of cybersecurity auditing can provide higher quality and level of service with a lower operational cost per report. With ROAI in mind, businesses are encouraged to dig deeper, beyond the dollars and cents, to determine which providers can bring the auditing efficiencies and scope of auditing services needed to remain compliant, mitigate disruptions and help the company save on costs later down the line. Most importantly, the customers that rely upon an organization will better trust them if the organization is holistically considering its audit partners.

Auditing efficiency and why it's valuable

Businesses that aren't considering ROAI tend to gravitate to the low-cost, "easy-button" providers they see pop up in their newsfeeds, inboxes or while scrolling through social media. Unfortunately, those easily recognizable providers that throw massive budgets into marketing campaigns to showcase their savings, aren't always what they claim to be once a working relationship is established. And, when put into practice, there are unforeseen "costs" to actually working with them. For low-cost cybersecurity auditing firms, this is also true.

Everyone will claim they're efficient when pitching you, but oftentimes, [low-cost audit firms](#) will propose and price their engagements based on a perfect case scenario. They disregard mentioning any add-on fees for additional services or how they support you on an ongoing basis. Once a company signs a contract, they are often at the mercy of the auditor. If the firm decides to enact several rounds of changes to the original, agreed-upon audit contract—a tactic known as "amendment creep"—the company may be subject to price increases and additional licensing audits that cost the business time, resources and productivity, as well as their assurance that they chose the right provider.

An ROAI approach considers the effects of a firm's auditing efficiency to mitigate contract amendments and business disruptions. Cybersecurity auditing firms offering 5% or less for the number of amendments they can propose to a contract after an agreement is made typically deliver high-quality audits without any of the added costs or headaches. This is because, as uncovered with ROAI, they have the confidence, resources and expertise to customize to customer needs within a certain price range.

Ditching the “bolt-on” cybersecurity assessment

General administrative efficiencies go hand in hand with auditing efficiencies for IT teams. No cybersecurity operation is the same. Thus, auditing programs must possess the flexibility and scalability to adequately integrate into and meet the needs of each business's unique digital infrastructure.

Low-cost audit firms often lack the agility and resources to adapt to quickly evolving business needs or meet the varying requirements of different regulatory bodies. These firms often use predetermined auditing templates that negate customization to provide a tailored experience for a CISO's team. These templated auditing programs can also be another way for low-cost cybersecurity firms to charge additional fees for adjustments needed to remediate auditing needs or for implementing processes to solve for inaccurate or imprecise audit results.

When choosing a cybersecurity auditing partner, CISOs must weigh a firm's agility and ability to provide fast, efficient and personalized auditing programs to adapt to their business's evolving needs. Additionally, auditing firms that offer highly flexible and scalable assessment programs can often cover auditing requirements for any regulatory agency. This enables companies to implement a cohesive cybersecurity auditing program, partnering with a single assessment firm—reducing the time wasted and complexities of finding and working with multiple firms.

By assessing cybersecurity needs beyond cost, CISOs will discover the administrative value they can find in their cybersecurity assessment, leading to less time spent preparing for an audit; less time spent educating your auditors; less time spent responding to duplicate requests; and less time re-writing reports. This, in turn, streamlines cybersecurity assessment processes, which reduces workloads, eliminates business disruptions and leads to unforeseen cost savings later downstream.

For companies that want to uplevel their cybersecurity compliance programs, the cost cannot be the sole consideration. By making cost a small component of your company's larger security narrative and using ROAI measurements, CISOs can take a more strategic approach to risk assessment. Choosing a cybersecurity compliance program based on expertise, flexibility and scale ensures IT teams are not only getting the efficiencies and agility necessary to keep up with ever-evolving compliance needs but are also gaining a knowledgeable and trusting auditing partner to help navigate their cybersecurity journey.

About the Author

Doug Barbin is the Chief Growth Officer and Managing Principal at Schellman. Doug Barbin is responsible for the strategy, development, growth, and delivery of Schellman's global services portfolio. Since joining in 2009, his primary focus has been to expand the strong foundation in IT audit and assurance to make Schellman a market leading diversified cybersecurity and compliance services provider. He has developed many of Schellman's service offerings, served global clients, and now focuses on leading and supporting the service delivery professionals, practice leaders, and the business development teams.



Doug brings more than 25 years' experience in technology focused services having served as technology product management executive, mortgage firm CTO/COO, and fraud and computer forensic investigations leader. Doug holds dual-bachelor's degrees in Accounting and Administration of Justice from Penn State as well as an MBA from Pepperdine. He has also taken post graduate courses on Artificial Intelligence from MIT and maintains multiple CPA licenses in addition to most of the major industry certifications including several he helped create.

Doug Barbin can be reached online at <https://www.linkedin.com/in/douglasbarbin/> and at our company website <https://www.schellman.com/>.

Secure Enterprise Collaboration Tools Are Critical in Light of Remote Work and Cyber-Attacks.

By Allen Drennan, Principal and Co-Founder of Cordoniq

Cyberattacks escalated in 2022 as critical industries remain a frequent target of cybercriminals. New data from Check Point Research revealed that [global cyberattacks rose by 38% in 2022](#) over the previous year. Many of these attacks were led by small hacker groups focused on exploiting collaboration tools used in work-from-home environments.

With critical industries and infrastructure under attack, [cybersecurity remains the top investment priority for CIOs](#) as firms need to manage escalating threats. Ransomware is a leading cause of data breaches, and key, high-profile targets include healthcare organizations, universities, financial institutions, telecommunications, as well as [governments](#).

Ransomware attacks are not only costly but more [difficult to identify and contain](#), according to a report from IBM. Last year, the average cost of a ransomware attack reached \$4.54 million, while additional consequences range from loss of data to eroded trust from customers.

The reality of cyberattacks is that malicious actors will access data any way they can and will exploit any vulnerability. Phishing, stolen credentials, and social engineering are among the [leading attack vectors](#). However, AI and apps such as [ChatGPT](#) are emerging as new threats, as bad actors are exploiting these apps to write malware and devise more sophisticated social engineering attacks.



CISOs and cybersecurity professionals are under tremendous pressure to stay up to date with the latest trends, prepare for threats, and ensure that software, tools, and platforms are secure. Protecting collaboration tools must be a cybersecurity priority for organizations of all sizes.

Remote work and distributed teams persistently at risk

As distributed teams and remote work environments are now permanently in place for enterprise organizations, collaboration tools are a critical part of an optimal hybrid and remote work experience. But with the large number of employees working from multiple locations, there are more opportunities for malicious actors than ever before.

Secure integrations of platforms and tools are critical, as the number of devices and access points are creating multiplying levels of attack surfaces that are more difficult to track and manage.

Some business tools that were once intended for limited use are now ubiquitous across organizations. Adding another challenge is the way teams are accessing these tools across multiple devices, both corporate-owned and personal. The risks of compromised credentials, devices and tools that are not adequately secured are compounded.

Collaboration tools and platforms are a pervasive source of threats, including communication, document, and content sharing tools. Industries that handle sensitive information, for instance, financial and accounting, management consulting, or government agencies, must be hyper-vigilant about data security. Confidential and sensitive data, from corporate secrets to Personal Identifiable Information (PII) and financial information are often key targets of cybercriminals.

Securing software and tools must be part of the culture of cybersecurity that needs to start from the C-suite. Creating a cybersecurity-minded culture includes creating policies and education about protecting data and systems. Passwords, secure devices and zero trust approaches are essential. However, choosing secure software platforms and integrations, starting with software that is built securely from the ground up, is also a key strategy.

Strategies to secure collaboration tools and integrations

Most firms use a variety of business tools day-to-day, many of which are used to collaborate, communicate, and share data. To ensure that these tools are secure, firms need to focus on a few key practices. For instance, good password hygiene, zero trust architecture and multi-factor authentication are a must, regardless of where employees are working. It's important for teams to maintain these practices across all devices, apps and transmissions.

Organizations, meanwhile, need to make sure their employees have access to the tools that give them optimal remote work experiences, which means using advanced and highly secure collaboration tools and technology. If the firm's tech stack suits their needs, employees are less likely to download unauthorized apps or tools.

Software products that aren't adequately secure can leave firms open to vulnerabilities. Good patch management is a critical step in reducing security risk from software. Another proactive approach can be taken when selecting PaaS, SaaS or other software that will be integrated with other tools. Look for solutions that have security baked into the SaaS product throughout the development process and not bolted on as an afterthought.

API driven platforms are good choices for secure integrations of tools and apps, but it's crucial to make sure that APIs are secure. API vulnerabilities, such as broken user authorization and authentication, mishandled authentication token management and outdated transport layer security implementations, can lead to hacking and data breaches. Strong API security testing and monitoring can help mitigate the risk of attacks on API integrations.

Consider a solution that works on private cloud networks to safeguard data, content and privacy. Private cloud networks can provide elevated security for servers, network, data and applications and give the organization more control over security and remote access.

When selecting video conferencing and collaboration platforms, look for solutions built securely from the ground up, with true end-to-end security with the latest TLS standards and not merely symmetric encryption. Secure solutions should also offer the organization complete control of all aspects of the collaboration platform, including all live and interactive user experiences.

Cybersecurity will remain a key ongoing priority for enterprises even as they face expected budget cuts as well as cybersecurity talent shortages. Cyber threats are constantly evolving, and malicious actors will find new ways to exploit vulnerabilities. But keeping security top of mind while considering collaboration tools and platforms can help to mitigate some of the risks.

About the Author

Allen Drennan is Principal and Co-Founder, Cordoniq. When he founded Nefsis Corp. in 2005, Allen introduced a cloud-based, video conferencing online service, cited by Frost and Sullivan as the first of its kind. He achieved this by building engineering teams to create a mobile and desktop solution that successfully blended web and native code into a seamless online service.

Over his career Allen has designed, built and deployed large-scale SaaS solutions for real-time video and collaboration, and created new technology for mobile video user interfaces, messaging, text, voice and video communications. Some of these solutions have been recognized in Gartner's Magic Quadrant and featured in major industry publications over the years, such as eWeek, PC Magazine, USA Today, New York Times, The Wall Street Journal, CyberDefense Magazine and more.

A frequent contributor to open-source projects, Allen also writes about highly technical software engineering topics for iOS, Android, Linux, MacOS and Windows.

Allen went on to found [Cordoniq, Inc.](https://www.cordoniq.com/), bringing together many of the team of senior engineers who created Nefsis and OmniJoin, as well as new talented team members, to create the next generation of truly secure, state-of-the-art video conferencing and collaboration.

Allen can be reached online at LinkedIn <https://www.linkedin.com/in/allen-drennan-0359a822/> and at our company website <https://cordoniq.com/>.



Stopping Criminals from Profiting Off Malware Requires a New Approach

By CW Walker, Director, Security Product Strategy at SpyCloud

The first three quarters of 2022 saw the total detection of over [62.29 million](#) new types of malware – approximately 228,000 new threats every day.

While security teams and company leaders focus their attention on the mitigation of ransomware, stealer malware - the quiet precursor - slips through the cracks. Infections are often notoriously difficult to identify and seem to have no immediate consequences. In fact, large corporations, regardless of industry, may suffer from malware [for years](#) before an exposure is detected.

Many organizations overlook that ransomware is often a direct result of stealer malware infections. Cybercriminals use the information siphoned from exposed devices to carry out attacks, making proper malware remediation essential for a robust security strategy.



What's worse, as enterprises deploy innovative solutions and tactics to prevent infection, companies with work-from-home policies and employees using BYOD or personal devices to access corporate applications often create new malware opportunities.

To combat this silent threat, enterprises need a new, more comprehensive remediation process that accounts for darkweb activity and provides more visibility into often unknown and ephemeral malware infections.

The Malware Landscape Is Evolving

One reason malware is difficult to detect is that there are very few indicators when a device is compromised.

For example, if an employee accidentally clicks on a link holding [infostealer malware](#), the malware can install, siphon data, and uninstall itself in five to 10 seconds, leaving little to no evidence of the infection. In a matter of seconds, the employee's credentials and session cookies are in cybercriminals' hands.

Likewise, popular info stealers like RedLine Stealer malware are often deployed through phishing emails, links in social media comments, malvertising, or malicious YouTube "tutorials." If an unaware employee downloads the malware, bad actors have free reign to use the stolen credentials and data to impersonate the user, decreasing the odds that they will be identified as suspicious.

While existing antivirus software offers protection against well-known types of malware, newer variations, such as Redline Stealer, Raccoon or Vidar are much more difficult to detect. Coupled with evolving botnet delivery methods that can evade detection and the fact that many malware infections occur outside of traditional, secure parameters, it's no surprise companies are struggling to address the threat.

Another crucial aspect to consider is the ongoing threat of exposed data. Traditionally, wiping known malware from the infected device is the most common remediation approach, but it fails to address the already-siphoned information now in the hands of [Initial Access Brokers \(IABs\)](#).

IABs are individuals or groups who package malware-stolen data and sell it on the darkweb. Cybercriminals buy this freshly stolen data and are granted all the information needed for initial network access, making it easy to bypass industry-standard prevention methods like multi-factor authentication (MFA) and deploy ransomware.

As if that wasn't enough, data sold by IABs is valuable as long as it has not been reset. For example, although the 2019 [Facebook breach](#) exposing millions of data points happened several years ago, it's possible credentials stolen in that attack are still active, making it an ongoing threat to that platform, its employees and its users.

A recent rise of IABs illustrates the underlying factor driving the increasing frequency of malware attacks – a thriving underground economy that weaponizes and monetizes network access.

Current cybersecurity measures are unable to close the gaps that lead to initial malware infections and fail to account for the fallout after a device has been compromised. While endpoint detection and application security monitoring are being used as temporary solutions, it's not enough.

The Bigger Picture Involves More Comprehensive Remediation

While employee education is the essential first step for a robust security defense, everyone makes mistakes. With the increasing frequency of malware attacks, it's getting harder and harder to entirely avoid infection. Instead, leaders should proactively mitigate the threat with a Post-Infection Remediation (PIR) approach.

PIR is a series of steps woven within standard malware infection responses that aims to address the lasting threat of exposed data.

The approach works like this: once the Security Operations Center (SOC) has identified an infected device, the IT team takes the standard first step of clearing the infected device. Enterprises in parallel use darkweb monitoring tools and human intelligence (HUMINT) teams to scan the underground for stolen information. The solutions and teams find the user data and trace it back to the initially compromised asset.

Once armed with this knowledge, SOCs begin remediating all compromised credentials and applications impacted by the attack. This can include third-party workforce applications such as Single Sign-On (SSO), code repositories, payroll systems, VPNs, or remote access portals. If all exposed data is reset, it's unlikely a full-blown ransomware attack will occur.

By going straight to the source of the threat – the darkweb – SOCs gain insight into all exposed devices and applications. SOCs may not monitor personal devices, but if the stolen data is linked to said device, teams can act to remediate these previously unseen entry points, better protecting the organization and the user.

PIR is more comprehensive than legacy, machine-centric malware response processes. Where these methods emphasize device remediation and neglect to consider user identity, PIR takes a more identity-centric approach, considering the personally identifiable information (PII) at risk.

Using this approach, leaders and executives can equip themselves for future success against evolving malware practices. Regardless of whether infected devices are being monitored, IT teams will have full visibility into the scope of the threat, significantly shortening the exposure window for ransomware and other critical threats while closing previously unseen security gaps.

About the Author

CW Walker, Director, Security Product Strategy at SpyCloud, is a cybersecurity and threat intelligence expert. He started his career in government as a threat intelligence analyst and has always been passionate about understanding and creating stories that can be told through the collection and analysis of interesting data. He has led teams of solutions engineers at multiple threat intelligence companies and currently supports SpyCloud's cybersecurity product strategy. He holds a BS in Political Science and Economics and a Master's Degree in Strategic Intelligence Studies.

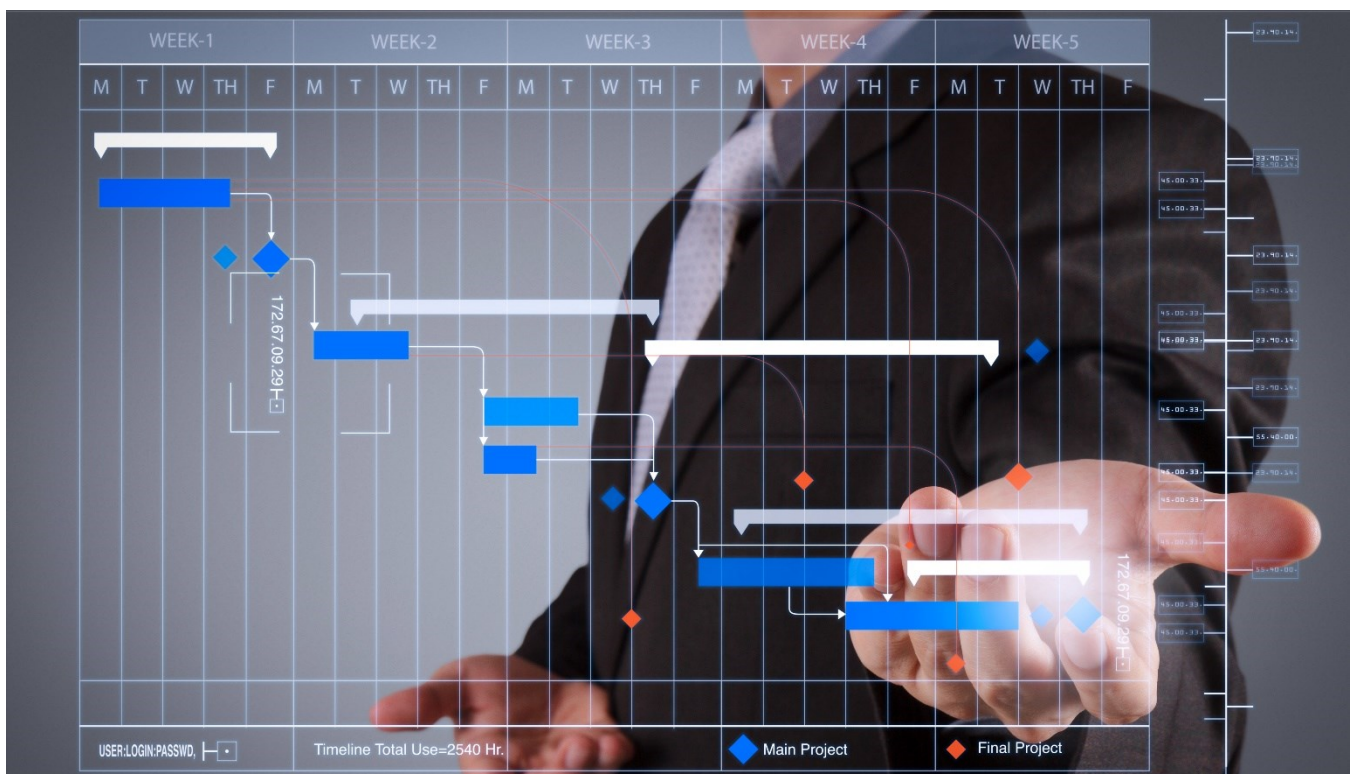
CW can be reached online at <https://www.linkedin.com/in/cwrwalker/> and for more information about SpyCloud, visit <https://spycloud.com/>.



The Data Dilemma: Balancing Business Growth and Security

By Noah Johnson, Co-Founder & CTO of Dasera

In today's digital age, data is the lifeblood of business growth. With large amounts of data sprawled across multiple platforms, companies must catalog and organize their data to derive actionable insights. But with data's value comes risk, and companies must ensure the data they collect and use is secure.



To start, companies must inventory their data and catalog it, both structured and unstructured data, whether in databases, cloud storage, or on-premises systems. This step is crucial to identify all data sources, including shadow data lurking on unsecured devices.

Once the data has been identified, it must be classified based on sensitivity so that data such as PII, PHI, and financial data can be secured accordingly. Companies should work with data owners and stewards to classify the data and determine who should have access.

Access control must be implemented to limit who has access to sensitive data, both internal and external, to the organization. This includes limiting access to those who need it for their job functions and implementing multi-factor authentication to ensure only authorized users can access the data.

Auditing and monitoring tools should be implemented to track all access to sensitive data, both successful and unsuccessful attempts. This can help detect potential breaches or data misuse, enabling a quick response to mitigate the risk.

Finally, policies and procedures should be implemented to ensure ongoing compliance with regulations, such as GDPR, CCPA, and HIPAA. This includes reviewing access controls, auditing logs, and conducting regular vulnerability assessments.

Securing data in today's environment requires an approach that aligns business objectives with data security. Companies can mitigate the risks associated with operationalizing their data while driving business growth by taking inventory of data sources, classifying data, implementing access control, encrypting data, monitoring access, and ensuring compliance.

While many solutions are available to help companies achieve these goals, it's important to carefully evaluate each solution to ensure it meets the company's specific needs and aligns with its goals. Ultimately, the solution should provide complete visibility and control over all data sources, identify sensitive data, assess risks related to data usage, access privilege, and misconfigurations, and enable automation of business policies with a no-code policy framework.

Utilizing data to its full potential can be a game-changer for businesses looking to stay ahead of the curve. By harnessing the power of data, companies can optimize their operations, personalize customer experiences, identify new market opportunities, and a million other use cases that can affect growth. However, this growth potential also brings new risks, such as data breaches and regulatory compliance violations proving security teams must take a proactive approach to data security. By cataloging and securing data from the start, companies can confidently use their data without fearing exposing sensitive information or regulatory non-compliance. By implementing a comprehensive data security solution that aligns with their data-driven goals, companies can mitigate these risks and maximize the value of their data. The benefits of a robust data security strategy are clear: improved operational efficiency, increased customer trust, and reduced risk. With the right tools and processes in place, companies can unlock the full potential of their data and drive business growth.

About the Author

Noah Johnson is Co-Founder & CTO of Dasera. He received his Ph.D. in Computer Science from UC Berkeley and founded three companies based on his academic research, including Dasera. Noah developed the first practical system to provide differential privacy for general SQL queries. This work was featured in Wired and Gizmodo, and serves as the technical foundation of Dasera's products.

Noah can be reached online at [LinkedIn](#) and at our company website www.dasera.com.



The Growing Necessity of Emphasizing Cloud Security in Business Operations

Ensuring the protection and reliability of cloud security for business success

By Deepak Gupta, CTO & Co-Founder of LoginRadius

In today's digital age, businesses of all sizes rely heavily on cloud technology to store, process, and access their critical data and applications.

While cloud computing offers numerous benefits, it also poses significant security challenges that can jeopardize the confidentiality, integrity, and availability of sensitive information.

Cyberattacks are becoming more frequent and sophisticated, and businesses that fail to implement robust cloud security measures are at a higher risk of data breaches, theft, and other cyber threats. Therefore, businesses must emphasize cloud security now more than ever.



Let's uncover the aspects of cloud security and learn more about the cloud security tools and technologies that can be pretty useful for enterprises leveraging the cloud in the long run.

Why Cloud Security Cannot Be Ignored in Today's Business Environment

With the rapid adoption of the cloud, businesses are undeniably jumping on the digital transformation bandwagon. However, the risks of cloud working environments couldn't be overlooked.

Here are the reasons why cloud security matters now more than ever:

1. **Remote Workforce:** The COVID-19 pandemic has accelerated the shift towards remote work, and many businesses have migrated their data and applications to the cloud to enable employees to work from anywhere. However, this has also increased the attack surface for cybercriminals, who can exploit vulnerabilities in remote access tools, weak passwords, and unsecured devices to gain unauthorized access to sensitive data. Robust cloud security measures such as multi-factor authentication, encryption, and secure VPNs are crucial to protect against these threats.
2. **Compliance Regulations:** Businesses in regulated industries such as healthcare, finance, and government must comply with strict data protection and privacy regulations such as HIPAA, PCI DSS, and GDPR. Failure to comply with these regulations can result in hefty fines, legal penalties, and reputational damage. Implementing cloud security measures that align with these regulations is essential to avoid compliance risks and protect sensitive data.
3. **Data Breaches:** Data breaches can have a devastating impact on businesses, leading to loss of revenue, customer trust, and reputation. Cloud security threats such as phishing, malware, and ransomware attacks can compromise data confidentiality and integrity, making it imperative for businesses to implement security measures such as data encryption, network segmentation, and threat detection and response tools.
4. **Cloud Misconfiguration:** Cloud misconfiguration refers to the improper setup of cloud resources such as storage, networks, and servers, which can result in unintended exposure of sensitive data. Robust cloud security measures such as identity and access management, configuration management, and compliance monitoring can prevent misconfigurations and protect against data exposure.

Tools and Technologies to Reinforce Cloud Security

1. **Encryption:** Encrypting data both in transit and at rest is crucial for cloud security. Encryption helps to ensure that data remains private and is only accessible by authorized users. This is important for organizations subject to regulations such as HIPAA, PCI-DSS, or the GDPR. Tools like AES and SSL/TLS can be used for encryption.
2. **Multi-factor authentication:** Implementing multi-factor authentication (MFA) adds an extra layer of security to user accounts by requiring a combination of something the user knows (such as a password), something the user has (such as a phone), and something the user is (such as a fingerprint). Multi-factor authentication can help reduce cloud security risks and ensure customers and businesses are secure in the cloud landscape.
3. **Adaptive authentication:** Adaptive authentication evaluates the risk level of each login attempt and adjusts the authentication requirements accordingly. This helps ensure that only authorized users can access sensitive data. Adaptive authentication systems can use a variety of risk factors to determine the level of authentication required for a given login attempts, such as the user's IP address, the device being used, and the time of day. If the system detects a high risk, it may require additional authentication methods such as multi-factor or biometric authentication.
4. **Virtual Private Cloud (VPC):** A VPC is a logically isolated section of the cloud where you can launch resources in a virtual network. This can increase security by keeping sensitive data isolated from the public internet. By isolating resources within a virtual network, a VPC helps to reduce the risk of unauthorized access to sensitive data. This can help organizations maintain their data's confidentiality, integrity, and availability.
5. **Regular security audits and vulnerability scans:** Regular vulnerability scans can help identify potential security weaknesses and ensure that your cloud environment remains secure over time. By regularly checking for vulnerabilities and potential threats, organizations can identify and address security issues before they become significant problems. This helps to reduce the risk of data breaches and other security incidents.
6. **Network segmentation:** Network segmentation helps to keep different parts of your cloud environment separate and secure. This can help to prevent unauthorized access and minimize the impact of security breaches. By dividing the network into smaller segments, network segmentation helps to reduce the potential attack surface and limit the effects of security breaches. This makes it more difficult for attackers to access sensitive data or systems. Moreover, network segmentation allows organizations to control network traffic flow between different segments, reducing the risk of unauthorized access or data leaks.
7. Organizations can use these tools and technologies to effectively reinforce cloud security and protect their sensitive and customer data from potential threats.

In Conclusion

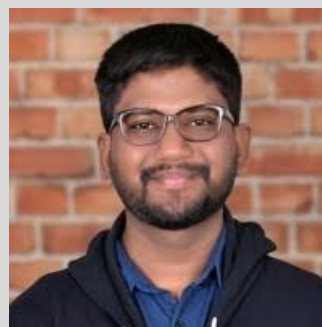
Cloud security is critical for businesses to protect against cyber threats and ensure sensitive data confidentiality, integrity, and availability.

By implementing [robust cloud security](#) measures such as multi-factor authentication, encryption, network segmentation, and threat detection and response tools, businesses can mitigate security risks and maintain their reputation and competitive advantage in the market.

Moreover, these security measures help businesses maintain a good reputation in the market since brands that are concerned about customer information security are highly admired by global customers.

About the Author

Deepak Gupta is the CTO and Co-Founder of LoginRadius, a rapidly-expanding Customer Identity Management provider. He's dedicated to innovating LoginRadius' platform, and loves foosball and winning poker games! Connect with him on [LinkedIn](#) or [Twitter](#).



Third-Party Cyber Security Risk Management: Best Practices

By Sananda Dasgupta, Tech Industry and Cybersecurity Writer at Coloco

Businesses are becoming increasingly reliant on third-party services for their various operations. In today's interconnected business landscape, it is practically impossible for any business to survive without collaborating with third-party vendors, suppliers, partners, contractors, and service providers. When this collaboration happens in a digital space, it adds up to the existing cyber security threats.

These third-party entities regularly interact with your IT infrastructure and may have access to your confidential data and privileged information. It increases the attack surface for the hackers who can use the vulnerabilities in that third-party system to steal your information or launch an online attack.

Third-party Cyber Security Risk Management- Why it is Important?

Third-party cyber security risk is becoming a pressing concern for businesses of all sizes and industries. Data suggests organizations worldwide use an average of [110 software-as-a-service \(SaaS\) applications](#), and the number is ever-increasing.

Now think that each of these SaaS vendors offers services to hundreds or even thousands of clients. In software supply chain attacks, hackers inject malicious code into an application to infect all users.



Technology research and consulting firm Gartner predicts that by the year 2025, [at least 45% of organizations](#) worldwide will be impacted by supply chain attacks.

Companies on the receiving end of such attacks lose millions of dollars for incidents that are outside of their direct control. Moreover, each incident of data breach severely impacts the organization's reputation. According to the data collected by the National Cybersecurity Alliance, [up to 60% of small businesses](#) go out of business and file for bankruptcy within 6 months of suffering from a data breach or other cybersecurity incidents.

Thus, in this environment of the growing threat of third-party cyber security risk, companies must have a well-planned strategy to mitigate the risk.

Third-party Cyber Security Risk Management- 5 Best Practices

Effective third-party cyber security risk management strategy involves assessing the potential risks associated with each third-party relationship, implementing appropriate controls and safeguards, and continuously monitoring for potential vulnerabilities and threats.

Here are 5 best practices that your organization should adopt to minimize potential security vulnerabilities and threats that arise from the use of third-party vendors, suppliers, or partners who have access to your business's systems, data, or network.

Assess the security measures implemented by your vendors

The recent Gartner report suggests that [over 80% of businesses](#) could identify third-party risk only after initial onboarding and due diligence. It shows that the traditional assessment method fails to detect new and evolving cyber security threats. You must update your due diligence process in order to identify all the risk factors.

Before entering into a contract with a vendor, service provider, or any other third-party entity, make sure you are thoroughly updated on their security protocols. If there is a lack of transparency in their security policy document, ask pertinent questions to ensure you know what security measures they implement to protect the system. Assess the vendor's security testing to confirm the company has effective detection and response plan. Also, enquire about the past cyber security incidents experienced by the vendor and how those incidents impacted their clients.

Establish clear security requirements in contract

The security requirements of a company depend on the risk tolerance level. It is important to communicate to your vendor about your security expectations. Establish clear security requirements for all third-party vendors, including data security and privacy standards, incident response protocols, and

monitoring and reporting obligations. Include these requirements in all vendor contracts and agreements and conduct regular audits to ensure compliance.

The security requirements should specify the type of data the third-party vendor will have access to and outline the measures that the vendor should take to safeguard the data. If the third-party vendor handles personal data or sensitive information, the security requirements should also cover privacy requirements. These requirements might include compliance with relevant data protection laws, such as GDPR or CCPA, and implementing appropriate privacy controls to protect sensitive information.

Also, specify the procedures that the third-party vendor needs to follow on the occasion of a security breach. This includes notification protocols, mitigation measures, and steps to contain and resolve the incident. Your contract document should also outline the monitoring and reporting obligations that the third-party vendor must follow. These might include regular security audits, reporting security incidents or breaches, and regular communication with the business regarding the vendor's security practices.

Keep yourself up to date on your vendors list

Organizations often lose track of the services they use and the data the vendors have access to. It can be disastrous for your third-party cyber security risk management strategy.

Maintain an accurate vendor list and regularly review their access to data to limit the exposure of sensitive data to only those who need it. It will reduce the risk of data breaches or leaks and limit unauthorized access or misuse of sensitive data.

Moreover, you will have more control over your system when you have clear knowledge about your vendors and their access to data. For example, if a third-party vendor has access to highly sensitive data, you can implement additional security controls or ask the vendor to deploy a more stringent security protocol for that particular set of data.

An updated vendor list will also help you respond quickly if a security incident occurs. When you know who all have access to the data, you can immediately identify the relevant vendor and take appropriate measures.

Implement continuous monitoring and limit access

Continuous [network monitoring](#) is critical for identifying and addressing potential cybersecurity risks in real time. Continuously monitor your network traffic to spot any irregularities. It will help you quickly recover if an [incident of cyber-attack](#) through a third-party system occurs.

Your team should also continuously monitor the vendors for security risks. The monitoring should include regular security audits, penetration testing, vulnerability scanning, and ongoing risk assessment. It will help you evaluate the effectiveness of third-party vendors' security practices and detect any vulnerabilities and weaknesses in their systems and applications. You can consider hiring third-party auditors to use their expertise.

Also, consider implementing robust role-based access control. Make sure the only vendors with access rights need it to do their job. Depending on the nature of their service, vendors may need to access data or systems only for a limited period of time. Make sure their access rights are withdrawn once the job is done.

Have a response plan

No amount of security precautions can make your system 100% immune to cyber security threats. Cybercriminals are coming up with more sophisticated methods to penetrate the system. This means that despite the best effort of your third-party vendors and partners, cyber security incidents may still occur. You should have a detailed response plan in place that outlines the steps to take in the event of a security breach involving a third-party vendor.

An incident of security breach can be messy, and it can confuse your employees as well as the vendors. Make sure all your employees know their roles when such incidents happen. Your response plan should include procedures for notifying affected parties, mitigating the impact of the breach, and conducting an investigation into the cause of the breach.

Takeaway

In today's complex business ecosystem, businesses need to take proactive steps to manage and mitigate cyber security threats by implementing an effective third-party cyber security risk management strategy. The steps mentioned here will help create a secure environment for businesses to run their operation and minimize security vulnerabilities and threats that arise from third-party vendors, suppliers, or partners. By following these best practices, companies can [improve their cyber security and productivity](#) and can quickly recover even if a security breach incident occurs.

About the Author

Sananda is a writer at Coloco where she writes on tech industry and cyber security. She works as an independent writer and works with diverse range of clients. Her writings are regularly published on various online blogs and magazines. Sananda can be reached online at sananda7ster@gmail.com or <https://www.linkedin.com/in/sananda-dasgupta>.



Why It Will Take Sophisticated AI Solutions to Fight AI Security Attacks

By Rom Hendler, CEO and Co-Founder of Trustifi

We live in amazing times, when advanced AI-based text generating engines like ChatGPT can scan the Internet for information and create an intelligible, relevant narrative on any topic. That's terrific news for companies looking to compose quick and easy blog posts or web site copy. But unfortunately, it's opened up a Pandora's box of potential security threats. An engine like ChatGPT puts dangerous tools into the hands of the malicious actors who orchestrate phishing and malware attacks on business email databases.

Carefully composed and effortlessly fluent, imposter emails created by ChatGPT can easily lure users into revealing critical log-in credentials that can compromise a company's security. And the more AI-sourced details these fraudulent emails contain, the harder they are to discern from a legitimate message coming from one of the user's actual favored vendors. Phishing attempts are one of the leading causes



of network breaches. Some of the most devastating attacks endured by this country's corporations have started with a single compromised password.

How Does ChatGPT Do Damage?

ChatGPT utilizes AI-based “transformer” algorithms—based on the same principles that connect human neural cells—to scan the internet for germane material based on keywords, prompts, or other search parameters, generating what's referred to as “natural language text.” This same capability can be leveraged by malicious hackers to create phishing emails and malware designed to infiltrate a corporate network with far more speed, efficiency, and stealth than ever before.

Not only does this type of technology create natural language, it can also aid programmers in creating code—and we all know not all code is leveraged for good. Sophisticated AI allows hackers to create blocks of nefarious code almost instantaneously; or to automate portions of a cyberattack launch, such as the initial infection code.

In the case of phishing and imposter attacks, the ability for AI-based bots to scrub the internet for accurate details on a victim's identity makes it nearly impossible for those users to recognize the attack. Gone are the days when phony emails were glaringly marked by spelling mistakes and generic requests for information. Today's attacks will include the name of the user's actual bank or healthcare provider, it will refer to their home city or local pharmacy (“geo-phishing”), or will supposedly have come from a vendor with whom the user regularly transacts.

Data is gathered with lightning speed through AI bots, pulled from existing references that populate the internet. The email incorporating these details then typically supplies a link leading the recipient to a brand imposter site where they will volunteer their user names and passwords.

The New Wave of AI-generated Security Threats

Just as CAD-based design programs now allow anyone with basic computer knowledge to function as a designer, advanced AI content generators deliver programming capabilities and automated coding shortcuts to even the least accomplished of wanna-be hackers. It is exponentially expanding the base of criminals who can crank-out malware.

The rise of AI technologies like ChatGPT, Replica, and YouChat stands to produce a frightening escalation of malicious activity targeting business networks, since it hands-over powerful tools to the ill-intentioned. The increase in cyberattacks will likely include a wave of activity that targets email data, since these systems are typically a point of entry for malware, viruses, and other threats.

Malicious software only needs to compromise a single account to infiltrate an entire network. Many viruses will sit dormant on the system for a length of time, to avoid detection that can be traced back to the date of infection, making the breach harder to mitigate. The viral code is later activated and works its way through the network, scraping data for sale, collecting private credentials, or conducting denial-of-service activities.

Fighting Bad AI with Good AI

So what can organizations—or the individuals who use email systems from both their offices and their homes—do to protect themselves from these sophisticated AI-powered threats? The only valid strategy is to utilize the same level of advanced AI technology in the cybersecurity solutions that protect their email data.

The biggest challenge for companies looking to secure their networks is determining whether or not their security solutions rely on sophisticated AI. The assumption is that all solutions leverage these methods, yet it's often not the case. Many traditional security solutions, including some of the most entrenched brands in the marketplace, rely on the blacklisting of known IP addresses as their main line of defense against malicious activity. Many established solutions were designed before this escalation of AI-based cybercrime and are still catching up, as opposed to newer solutions that have been designed from the get-go with AI-powered scanning tools.

It's true that a great percentage of spam attacks come from IP addresses that have been previously established as malicious. But blacklist/whitelist filtering doesn't account for AI-based bots that read through millions of internet references, interpreting contextual messages to create ultra-convincing, natural language spoof emails.

Security solutions must employ the same level of AI technologies, leveraging these protocols to scan inbound emails for red-flag keywords and phrases—the same way nefarious code will scan for data on their victim's hometown and business partners. These AI-powered solutions will either flag, block, or quarantine questionable emails using keywords such as “credit card,” “invoice,” or “wire transfer.”

This is a true situation of fighting fire with fire. Only AI-based algorithms will be able to detect the cleverly worded, accurately targeted, and naturally composed imposter emails that are soon predicted to reach business environments. If an organization's cyber security solution does not employ advanced AI tools, they will be underprepared for the influx of well-crafted phishing attacks and malware.

Depend on Encryption

Another way to fight against powerful AI-related breaches is to implement the use of email encryption throughout an organization, which keeps sensitive material from being accessible to hackers and AI bots. Advances in encryption technologies have produced solutions that are simple to use, where encryption can be automated to comply with regulations such as HIPAA or the GDPR, taking the burden of deciding what content is sensitive and out of the hands of the individual user. Effective encryption allows protected messages to be opened and decrypted with a single click, just as easily as a non-encrypted email. Powerful solutions will auto-encrypt the recipient's reply as well.

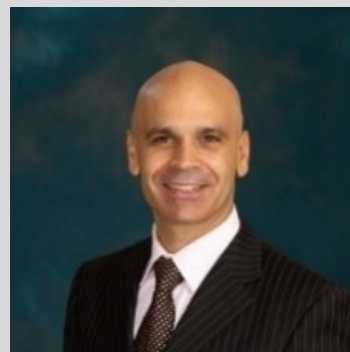
Effective encryption will not impact the user's ability to breeze through their inboxes. Organizations should look for an encryption solution that incorporates tokenization, a break-through capability that allows the non-sensitive portions of an email to be read just as easily as any other email. The tokenized portions

(e.g. a credit card number, or healthcare identification information) can be retrieved at the recipient's convenience. This can significantly contribute to an organization's productivity while providing superior protection.

So although AI-based platforms continue to hand over vital capabilities to bad actors, at least there is hope for organizations to protect themselves with the same level of AI-powered technology in their cybersecurity solutions. Companies must make sure their solutions utilize these AI-based tools if they expect to keep pace with the risks of this new frontier in natural language generation.

About the Author

Rom Hendler is the CEO and Co-Founder of Trustifi, a cyber security firm offering email encryption solutions delivered on a software as a service platform. Rom is a member of the Forbes Technology Council and has extensive C-level executive experience at Fortune 500 companies. He was a key player in opening and operating integrated resorts around the world with a total investment exceeding \$15B. Trustifi leads the market with the easiest to use and deploy email security products providing both inbound and outbound email security from a single vendor including encryption with tokenization, data protection, anti-virus and anti-malware. Its unique, cloud-based storage model is helping the companies in the SMB and enterprise marketplaces rethink their approach to cyber security. See more information about Rom at www.trustifi.com.



1020 Cyber Security Professionals' Actions and Experiences When Applying for A New Role.

By Torquil Macleod, Founder and Director of Via Resource



At Via Resource, we strive to provide a supportive service to our candidates and clients. As the world shifts and everyone becomes more online, Cyber Security as a profession has grown because there is more personal and sensitive data vulnerable to an attack. The rise of Cyber Security has had a huge impact on businesses as professional industries are scouring to hire Cyber Security talent to protect their online presence, assets and customer data.

Our research focuses on the current market to candidate's views of how the recruitment process has changed, and to establish what candidates find attractive in employers and job opportunities. We carried

out an industry survey from 22nd November 2022 – 5th December 2022, asking 1020 candidates their thoughts when applying for a new role.

Torquil Macleod, Founder and Director of Via Resource comments:

“We are incredibly grateful to all the candidates who took the time to complete our survey as we look to understand how the market has changed. The feedback gathered will help us to improve candidate experience and help inform our clients. We want to ensure candidates receive the best experience possible with quality support, advice and guidance from Via Resource to find their perfect role.”

Audience of the survey

Out of the 1020 professionals surveyed, 171 (16.8%) respondents were from the UK and 849 (83.2%) respondents were from the US. With the top three areas working in:

1. Security Engineering & Architecture (35%)
2. Governance, Risk & Compliance (27%)
3. Network Security (21%)

The top three seniority of within their organisation follows:

1. Manager, 8 years + (32%)
2. Senior, 5 – 8 years (25%)
3. Associate, 2 – 4 years (18%)

Changes within the market

Cyber security jobs are in high demand with 78% respondents believe there will be an increase in roles. However, 88% believe there is a cyber security skills gap, where a recent report Cyber Security in Focus, features responses from cyber security directors, security operations directors and VPs of product security in EMEA and North America. Where 87% of respondents admitted they are suffering skills shortages, with over a third (35%) claiming positions were left unfilled after a 12-week period. 60% of organisations also admitted they have been struggling with finding cyber security talent, and 52% reported difficulties with retaining employees. Meanwhile, seven out of 10 leaders worldwide say hiring women and new graduates are among their top three challenges.

Three areas identified by respondents to reduce the skills gap include:

1. Attract talent (31.7%)
2. Train and apply employee skills (28.9%)
3. Encourage employees innovative thinking and practical ability (25.3%)

How Candidates Apply for A New Role

Cyber security professionals apply for roles in a mixture of ways with applying on a company website being the most popular channel with 54% of the candidates, is an unexpected for this to be the most popular when it was only 31% last year. However, the reason for this could be those applying directly to the company may be competing against a smaller pool of applicants, which will naturally decrease the competition. Also this helps delivers the applicants credentials to employers in their preferred format, as opposed to the one utilised by an external job site. Some organisations also provide more detailed information about job openings on their website, compared to the descriptions on job listing sites.

Using a recruitment Consultancy comes second, 53% of candidates reported finding un-advertised Cyber Security roles where hiring organisations have chosen to be more discreet. Candidates also preferred not having to negotiate salary package with potential employers, this part of the process made many applicants feel uncomfortable. Other ways of applying for a new role include using their own personal networks (42%), LinkedIn (35%) and job boards (11%).

44% of candidates surveyed checked company reviews before applying for a role, in particular Glassdoor. Cyber security professionals pay close attention to the ratings and reviews which can significantly influence whether they choose to move forward with the application process. On average candidates spend 21 minutes to complete each application.

What Candidates Want from An Organisation

When a candidate has applied for a role on average, they would expect a reply either within three working days (41%) or up to a week (39%) mentioning if they have been successful to the next stage or not.

If a candidate is successful to the next stage interviews, they are happy to incorporate phone and online interviews with the final stage to be in person interviews (16%). However, most candidates (41%) are only wanting to participate with online interviews due to technology allowing us to do so. After each interview stage it is important for candidates to receive detailed feedback with 42% of candidates strongly agreeing and 42% agreeing. This is an incredibly important statistic as the importance of employer branding and candidate experience is hugely important in today's employment market. The ideal number of interview stages is seen to be three to four depending on the seniority of the role, this is to avoid interview fatigue for both employers and candidates.

What candidates want within the role

We asked 1020 cyber security professionals if they had to rank the most important thing, they look for in a new role the sequence is as followed:

1. Salary/day rate
2. Career progression
3. Employee Benefits
4. Workplace Culture/Environment

5. Skills
6. Job responsibilities
7. Job Title
8. Training

Salary is regarded as one of the most important factors while making a choice between roles, therefore putting salary ranges in job advertisements may give organisations a competitive advantage when trying to attract candidates. That's because most candidates look first at a position's compensation and benefits when scanning a job posting, then at the job's required qualifications and skills.

Even with training being the lowest importance to candidates 95% of candidates surveyed would be happy to take on additional training to learn skills (1% more than last year).

Job Benefits

When an organisation provides company benefits, this helps recruit and retain the best employees, boost morale, and improve company culture and benefit from a more productive workforce. Therefore, when candidates apply for a role, they would be looking at the benefits package which could be a way to differentiate one organisation to its competitors. Due to COVID-19, the working culture has changed by providing a more flexible working culture which is important to candidates (36%) and the ability to work from home (23%). Where technology is enabling businesses to continue to function, communicate effectively and maintain positive morale through video conference calls, virtual coffee catches ups and screen-to-screen team socials.

As employees spend most of their time working, offering a health program is crucial. Health benefits can improve overall productivity at work, reduce absenteeism, improve dietary habits of employees, and promote positive behavioural patterns. This is why candidates have chosen other benefits including health insurance (45%), employee rewards platform (38%), bonus scheme (34%) and gym membership/wellness programme (29%).

Conclusion

Several new insights into the individuals working in and applying for cyber roles, the cyber security skills gaps that affect employers, and the challenges that organisations face when it comes to training and recruitment. The main lessons we draw are as follows:

1. Skills gap - The skills gap presents significant challenges to organisations attempting to stay ahead of the cyber risk landscape. It is expected organisations to focus on hiring and retaining niche cyber talent along with outsourcing strategies to remain agile and optimise operational processes in 2023.
2. Education - Schools, universities and training providers to give a holistic skillset, covering the relevant technical skills and soft skills that employers demand, and the ability to implement those skills in a business context. Organisations must also support existing talent through ongoing training.

3. Support - Burnout is rampant today at many organisations, especially when there is such a shortage of skilled people, it's easy for anyone unhappy to leave and find a better opportunity elsewhere. However, there are also critical cyber security needs that must be met.
4. Recruitment - Sourcing the right talent at the right time can prove arduous for any company. But the process becomes even more challenging when you work within a niche industry or sector. In these situations, a specialist recruiter can help find the perfect candidate for a hard-to-fill role.

This insight gained from information and cyber security professionals shows the new thinking when applying for a cyber security role. Which in turn helps Via Resource when speaking to organisations to guide them with the best job packages, interviewing process and onboarding successfully where candidates can fit perfectly into the role.

About the Author

Torquil Macleod, Founder and Director of Via Resource. Tor has spent the last 10 years helping organisations build high performing Information Security teams. His experience spans from the development of large-scale recruitment and training programmes to helping Start-ups make the right security hire. His insight is from first-hand experience of the real Cyber Security Skills Market.

Tor can be reached online at <https://www.linkedin.com/in/tormacleod/> and at our company website <https://www.viaresource.com/>.



Closing The Cyber Marketing Gap with Investors

Positioning security as a stakeholder value proposition

By Patrick Kehoe, Chief Marketing Officer at Coalfire

With breaches and shutdowns making daily headlines, no one wants to do business anymore with companies that can't assure buyers that they're on top of their security programs from supply chain to point of sale. As a result, cyber risk exposure has become a dominant factor in customer purchasing decisions. And now, with COVID and the cloud, enterprise risk posture has become a critical factor for investors.

For equity shareholders, venture firms, acquirers, and merger candidates – and a growing constituency of external stakeholders and internal employee stock option programs – a company's security and compliance credentials are becoming just as important as its financial statements.



SEC Changes the Game

It's human nature to hide flaws and imperfections, but daily headlines blaring the latest breach have inspired the Securities and Exchange Commission to turn that instinct upside down with new disclosure requirements. A proposed SEC ruling will force public companies to disclose material security incidents within four days. "Material" means anything that could impact a company's stock price – which is nearly impossible to determine that fast. This implies legally actionable consequences based on far more uncertain criteria than the conventional governance and compliance standards that security managers are used to dealing with.

If this proposal becomes law, it will eclipse the historical impact of the Sarbanes-Oxley Act 20 years ago, which was implemented by Congress in reaction to corporate accounting scandals. When public companies adopt this new level of reporting, it will inevitably trickle down into the greater private sector, forcing the hand of corporate communications and investor relations teams to engage immediately with constituents, especially investors.

The Path to Cyber Investor Confidence

There's a lot of work to be done to refocus marketing on cyber with a strategy of ultra-transparency! In a recent Forrester survey, security decision-makers ranked investors last on their list of stakeholders to receive cyber performance reporting. In stark contrast, investors surveyed by RBC Global Asset Management identified security as one of their most important governance issues.

In this significant change management moment, marketing teams, legal, and investor relations professionals must adopt a new discipline: integrate cyber assurance into customer and investor communications. Here are the top-five enterprise strategies to help close the gap between security posture and market confidence:

- Establish an investor relation cyber program
 - Build and leverage a corporate Trust Center that is featured prominently on your company's website and within investor communications. The Trust Center should showcase risk management priorities, security policies, privacy assurance practices, and compliance information across all divisions and product lines.
 - Within the Trust Center, use compliance frameworks as your "seals of approval." These provide proof points that connect security posture with operational resilience and brand trust.
- Link security posture to performance metrics
 - Provide visibility to investors through presentations and regular financial reporting that validates management's intentions and demonstrates your cyber program's effectiveness. Investors value quantitative, objective metrics regarding cybersecurity performance and outcomes, always in context with policies, controls, governance, and procedures.

- Convey your risk philosophy.
 - We can't eliminate risk, so we rely instead on experience and intuition that inform a strategic hierarchy of vulnerabilities and philosophies that drive remediation strategies.
 - Convey a pragmatic strategy that identifies the company's unique threat landscape and what types of attacks it's likely to face.
 - Make sure to communicate what factors can be controlled, what risks the company is willing to take, and how those decisions are made.
- Incorporate the supply chain
 - Work with all supply chain partners to ensure they meet your security standards and that you meet theirs.
 - Commit to each other and to your mutual customers and stakeholders that you adhere to the highest standards and best risk management practices along physical and digital supply chains.
- Leverage a multi-pronged communication approach
 - Prepare PR, IR, and legal teams to move with every incident. Collaborate using the Trust Center to develop a "damage report" process that makes sense of breaches when they happen and communicates remediation strategy in real-time.
 - Integrate security posture into periodic financial reporting. After one of history's worst identity thefts in 2017, Equifax bounced back with a corporate overhaul, including an annual report that specifically communicates and elevates security as an investor value proposition.
 - Confirm to the board of directors that security costs for tools and controls can translate into platform-enabled, seamless systems that deliver better financial performance.
 - Integrate Trust Center content into sales team materials and communications. If presenting the company for acquisition or future financing, incorporate security culture and updates into your pitch deck.

Circle of Trust

All stakeholders want confidence in their relationships and within their spheres of influence. No one wants to buy from or do business with companies they can't rely on. No one can afford to buy and hold the assets of a company – or allow that company to acquire or merge with another – without an enhanced level of trust in today's cloud-exposed environments.

Management must re-calibrate security and trust as bedrock business principles and prioritize transparency and cyber integrity throughout all enterprise communications.

About the Author

Patrick Kehoe is Chief Marketing Officer at Coalfire. He has over twenty-five years of experience working with software, hardware, and service providers in High Tech and cybersecurity markets, where he has successfully built and deployed growth strategies and innovative marketing approaches. Prior to joining Coalfire, Mr. Kehoe served as Chief Marketing Officer for Arxan, where he and the team analyzed application security vulnerabilities and deployed solutions to protect applications. Previously, he held leadership positions at Siemens Enterprise Communications (now Unify), a global provider of communications software and services, where he was responsible for North American marketing and partner business, and he oversaw the development of the strategic plan and drove market awareness and pipeline generation. Prior to his work at Siemens, Mr. Kehoe spent nearly 20 years with Booz Allen Hamilton and MarketBridge, a sales and marketing professional services firm, providing business and IT strategy consulting services.



Mr. Kehoe has a track record of success in the Americas, Europe, and Asia, and has spoken at conferences and corporate events on a variety of sales and marketing topics. He holds a degree in Computer Science from Vanderbilt University and an MBA from the Darden Graduate School of Business, University of Virginia.

Cyber Risk Quantification: A New Way to Understand Security Risks

CRQ can identify security improvements, prioritize implementation, and justify security investments. Here's how to make it work for your organization.

By Bruno Farinelli, Senior Director of Operations and Analytics at ClearSale

Digital fraud and security risks are always with us, and they're constantly changing as businesses open new channels and adopt new technologies that criminals work to exploit. Data breaches are an especially thorny problem, with millions of customer records breached every year, and even password managers becoming vulnerable targets. Fraud continues to increase year over year, with identity fraud and fraud-related scams leading to \$52 billion in losses in 2021 in the U.S. alone.

Meanwhile, hybrid work policies, automation and IoT implementation, social and metaverse commerce, and other trends are adding complexity to the technology and channel attack surface. All of this is



happening while companies face a continued shortage of cybersecurity talent and are re-evaluating their spending in light of slowing global economic growth. Security and risk management leaders need to identify the specific risks their companies face and communicate those risks in a way that other stakeholders can understand to justify technology and talent investments.

Cyber-risk by the numbers

Increasingly, security executives are using cyber-risk quantification (“CRQ”) to understand their holistic risk profile. CRQ can aid in planning security improvements to prevent data breaches, compliance penalties, fraud, and lost customer trust. It can also provide the metrics that leaders may need to demonstrate to board members and the C-suite the risks of underinvestment in security.

CRQ is an activity described by Gartner as “any risk assessment that measures risk exposure and expresses it in financial or business-relevant units.” CRQ can be as simple as a scale that ranks the likelihood and potential cost impact of specific risks. It can also be quite complex, with AI-enabled statistical modeling and ongoing risk analysis. Forrester describes the variety of CRQ approaches as “anything from a threat heat map to a 5×5 grid to a list of the latest threats with a flowchart of how the firm is addressing them.” By 2024, 68% of security decision-makers plan to implement CRQ that uses AI and ML.

Regardless of the specific method used, CRQ can help bridge one of the most widespread issues that security leaders face: a lack of C-suite understanding of an organization’s cyber risks and their potential financial consequences. In 2021, just half of IT leaders thought their organizations’ executives “completely understand cyber risks.” By quantifying risk in a way that allows for the creation of benchmarks and KPIs, CRQ can help IT leaders show the value of security investments and present those investments as ways to protect and even drive growth. As Deloitte’s 2023 Global Future of Cyber Survey says, cybersecurity is “becoming an essential part of the framework for delivering business outcomes.”

Understanding existing cyber risk frameworks

Leaders who want to implement CRQ have a variety of frameworks they can choose. Factor Analysis of Information Risk (FAIR) is the best-known option, and it expresses risk “in financial terms” to give all stakeholders a common way to understand and talk about risk.

This approach differs from existing qualitative risk management frameworks. The NIST Cybersecurity Framework (CSF) is a federally sponsored rubric for evaluating risk across organizations. Federal agencies are required to assess their cyber risk with this tool, but organizations in other industries have adopted it voluntarily, particularly within critical infrastructure and manufacturing. Other frameworks like those published by ISACA and MITRE can also help with comprehensive risk identification but don’t express it in dollars.

All of these frameworks require lots of data and time to deliver useful results, which can be a daunting prospect for IT leaders whose teams are already stretched thin. The time involved can also undermine the impact of the framework findings, because real-time data is the preferred resource for decision making.

Applying new CRQ solutions

New CRQ vendors offer a way to gain risk insights faster by automating data collection and analysis. Forrester describes several optimal use cases for CRQ tools, including to quantify existing risk, to describe ROI of current security investments, to prioritize risk remediation, and to build the case for new investment. The analyst firm also describes the CRQ space as emergent and dynamic, with most products “in the prototyping phase.”

Because the space is relatively new and changing quickly, Forrester recommends choosing CRQ solutions that support specific use cases, rather than trying to find a one-size-fits-all provider to handle holistic risk quantification. Any proof-of-concept should focus on a single use case in order to prove value related to one decision that needs to be made. From there, it may be possible to expand use cases with the same vendor, run another proof-of-concept with a different vendor, or choose another vendor for a different use case.

Data from each quantitative analysis can be used to establish benchmarks for progress in terms of risk reduction and ROI, so IT can track and report progress. As CRQ solutions become more mature and comprehensive, security leaders will have more options to evaluate and describe risks, make plans to reduce those risks, and make the case for investment that protects their organization.

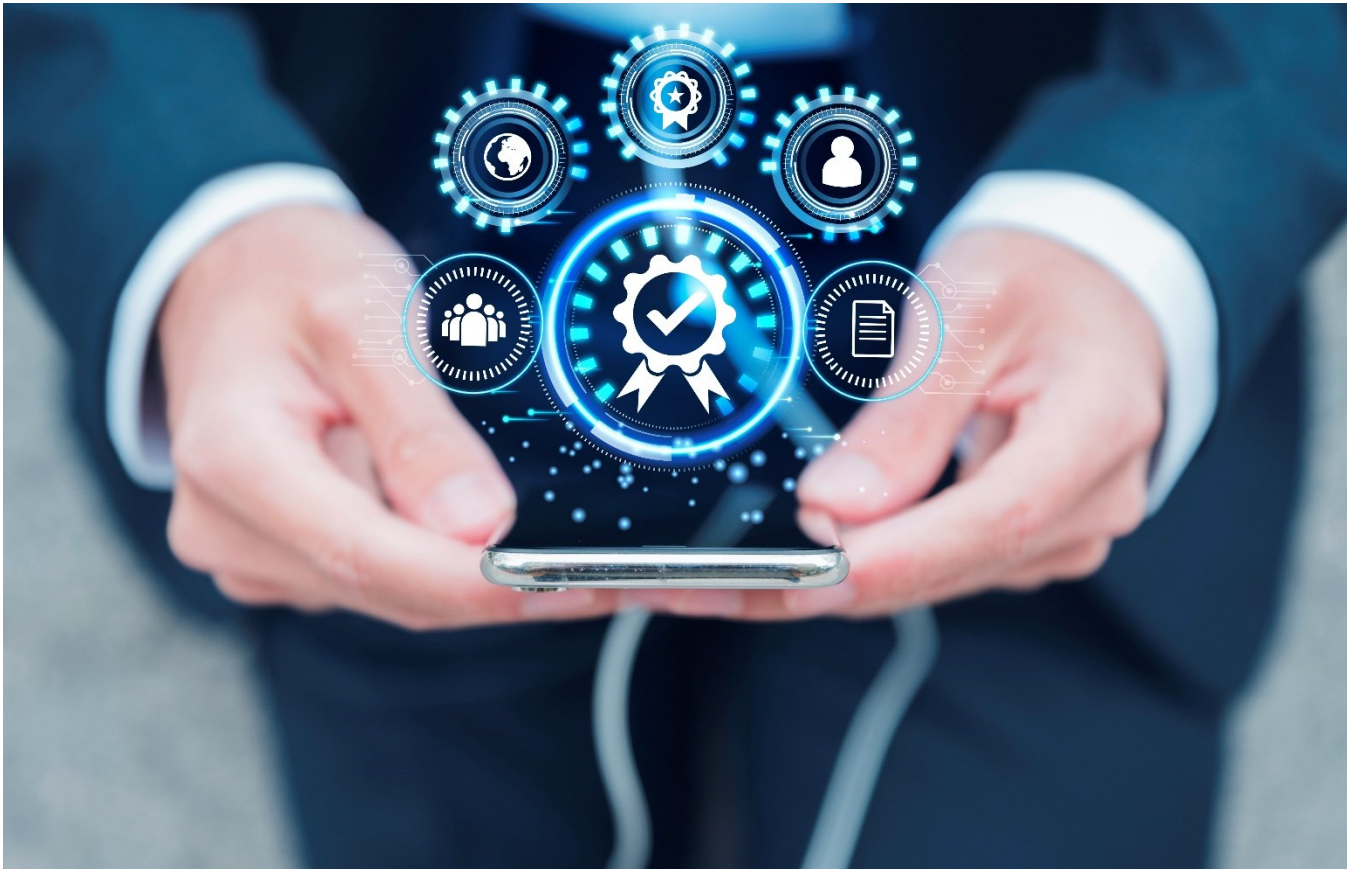
About the Author

Bruno Farinelli is an expert in biometrics and browsing behavior, and serves as Senior Director of Operations and Analytics at ClearSale. Bruno holds a Bachelor's degree in Statistics from top Brazilian University UNICAMP and an MBA in Business Intelligence from one of the most well-known Technology Institutes in Latin America FIAP. Follow on [LinkedIn](#), [Facebook](#), [Instagram](#), [Twitter](#) @ClearSaleUS, or visit <https://www.clear.sale>.



Evolution of the CISO Role

By Jaye Tillson, Director of Strategy at Axis Security



Evolution of the CISO Role

The Chief Information Security Officer (CISO) role is relatively new in the corporate world, with its origins dating back to the late 1990s. The role has evolved significantly since then, and it now plays a crucial role in the success and security of organizations.

History of the CISO Role

The CISO role can be traced back to the late 1990s when businesses began to realize the importance of securing their digital assets. As the use of the internet and digital technologies increased, so did the risks associated with cybersecurity threats.

In response to these threats, organizations created roles dedicated to information security management. These roles were initially known as Information Security Managers (ISMs) which were often part of the IT department. They were responsible for ensuring the confidentiality, integrity, and availability of the organization's information.

Over time, the role of the ISM evolved to include broader responsibilities, such as risk management and compliance assurance, the title changed to Chief Information Security Officer (CISO) which reflected the growing importance of the role and the increasing responsibilities associated with it.

Evolution of the CISO Role

The role of the CISO has evolved significantly since its inception. Initially, the CISO was responsible for technical aspects of information security, such as implementing firewalls, intrusion detection systems, and other security technologies. However, as cyber threats became more sophisticated, the CISO's role expanded to include risk management, compliance, and incident response.

Today, the CISO plays a critical role in the success of an organization. They are responsible for ensuring that an organization's information is secure, that the organization is compliant with relevant regulations, and that it is adequately prepared for and can respond to cyber incidents.

Importance of the CISO Role

The importance of the CISO role cannot be overstated. Cybersecurity threats are increasing in frequency and sophistication, and organizations must be prepared to defend against them. A data breach can have severe consequences for an organization, including loss of reputation, loss of revenue, as well as legal and regulatory consequences.

The CISO is responsible for ensuring that the organization's data is secure and ensuring that the organization complies with relevant regulations and that it can respond to cyber incidents effectively. However, it should be noted that the CISO cannot do their job alone, and it is essential to have a team of people who can help implement and manage information security management systems effectively. The team should consist of professionals with diverse skills and expertise, including risk management, compliance, and incident response.

Effective teamwork is crucial to the success of the CISO. It is essential to have clear communication channels, well-defined roles and responsibilities, and a culture of collaboration to ensure that everyone is working towards the same goals.

Where the CISO Should Report

The reporting structure of the CISO can vary depending on the organization. In many cases, the CISO reports to the Chief Information Officer (CIO). However, there is a growing trend toward having the CISO report directly to the CEO or the Board of Directors.

Reporting to the CEO or Board can give the CISO more influence and authority, which can ensure that the organization's cybersecurity posture is taken seriously. It also highlights the importance of the role and ensures that the CISO has the necessary resources to carry out its responsibilities effectively.

Conclusion

The role of the CISO has come a long way since its inception in the late 1990s. Today, the CISO plays a critical role in the success and security of an organization. As cyber threats continue to evolve, the importance of the CISO role will only continue to grow. Organizations must have a dedicated and well-resourced CISO to protect their digital assets and prepare for cyber incidents.

The CISO is critical in ensuring that organizations are protected from cyber threats. With the increasing frequency and sophistication of these threats, it is more important than ever to have a dedicated and well-resourced CISO and team in place. By working together, they can develop and implement effective information security management systems to protect organizations' digital assets and respond to cyber incidents efficiently.

About the Author

Jaye is a technology leader with a proven track record in delivering global strategic and enterprise-wide programmes totaling over \$1billion. He provides technical advisory to global mergers and acquisitions across multiple countries and cultures, large scale global transformation programs, enterprise-wide cyber security governance, digital strategic planning, and the creation of operational efficiencies.

He has spent over 20+ years understanding the challenges of defining and implementing enterprise strategies and translating these into the design and deployment of enterprise-wide platforms and infrastructures. His expertise includes the globalisation of IT platforms to create cost and resource efficiencies, resilience, and improved information flow to support executive decision making.



Jaye has led multiple large strategic technology programmes and is a critical asset for the success of organisations undergoing global transformation. He has built and trained several globally reaching teams, capable of successful execution of strategic plans. He is currently responsible for the budget, costing, fiscal planning, cost reduction and global people management at a large technology manufacturing organisation.

He is recognised as a mentor and coach in his area of expertise and observes industry and market trends to ensure his technology recommendations fit the business strategy. He is a senior technical lead, is seen as the go-to person within the business for all technical questions and is seen as a role model in the organisation.

Preparing Travel and Hospitality Companies for Cybersecurity in The Wake of Travel Technologies

By Shambhu Nath Jha, Associate Vice President of Fact.MR

Technology has touched every aspect of our lives and became an integral part of them. This has further going on the defensive changed the way we eat, shop, and spend our time. Right from booking a dinner table in a restaurant to booking a flight, technologies have made it easier than it was ever before. With these massive applications, such technologies are leveraged by users across many sectors. Even the travel sector has been impacted by ongoing technology advancements. Today, we can organize our entire trips, and book hotel rooms, flights, sightseeing tours, and other activities, all from a mobile device.



Technology has completely changed the way we travel, making our journeys more enjoyable and practical. What we currently refer to as travel technology is this significant transformation of the tourism sector driven by the integration of technologies. The use of e-commerce and IT in hospitality to save time, reduce cost and generate seamless travel experiences for customers is increasing industry competition.

As per Fact.MR's research, the global demand for travel technologies is estimated to increase at a CAGR of 8% from 2023 to 2033. Currently, the global travel technologies market is valued at US\$ 6 billion at present and is predicted to reach a market size of US\$ 13 billion by the end of 2033.

Recognizing trending travel technologies is essential for companies for addressing the possible security concerns and application scope to gain a competitive edge. For this business requires market research that provides industry-specific insights. FactMR's research solutions are opted for by leading firms making it a market consultant brand one can trust.

Travel Technologies are Transforming the Travel Experience in Significant Ways

Technology has a crucial role in the hospitality sector, allowing businesses to streamline operations, improve customer service, and increase efficiency. Technology can help hotels and restaurants increase revenue, and improve customer satisfaction. It can also help them better manage their resources and provide a better overall experience.

AI solutions that use machine learning also offer insights into customer behavior, interests, and preferences about travel destinations, accommodations, extras, airlines, car rental agencies, costs, and other factors.

Chatbots are used to provide 24/7 customer support and interactions. Furthermore, these can also assist in making bookings, processing payments, and generating conversation as a travel companion.

For instance, hotels that use IoT enable their visitors to use their cell phones to operate various internet-enabled items in their rooms. They have access to control TVs, thermostats, lighting, and more.

Growing Concerns Over Cyber Security: Demanding Wise use of Travel Tech.

According to a survey exploring digital economy footprints, the online travel booking segment is anticipated to grow and surpass 823.59 million users by end of 2023. There is no doubt that travel technologies have made bookings faster, easier, and more efficient. Furthermore, with AI and VR one can stay connected even while traveling. However, this ease can cost you the loss of privacy and is often challenged by cyber threats.

AI is raising cyber concerns in the travel sector by introducing new vulnerabilities that can be exploited by malicious actors. AI-powered systems are increasingly being used to automate processes such as customer service, ticketing, and baggage tracking. However, these systems are vulnerable to attack and manipulation, which can lead to data breaches, identity theft, and other malicious activities.

Additionally, AI systems can be used to launch sophisticated phishing campaigns and other cyberattacks. Finally, AI-powered systems can be used to manipulate the pricing and availability of travel services, leading to unfair practices and consumer exploitation.

The Top Cyber Security Concerns Related to Travel Technologies

- **Data Breaches:** Travel companies store a large amount of sensitive customer data, including credit card numbers, passport information, and other personal details. This data is vulnerable to cyber-attacks and data breaches, which can lead to identity theft and financial losses.
- **Phishing Attacks:** Travel companies are often targeted by phishing attacks, which are attempts to steal personal information by sending malicious emails or links.
- **Malware:** Malware is malicious software that can be used to gain access to a company's systems and data. Travel companies are particularly vulnerable to malware attacks, as they often have multiple systems and networks that are connected to the internet.

Future Roadmap: Fundamental Cybersecurity Tips for Travel Companies

Unsecured Wi-Fi networks can be used by hackers to gain access to a company's systems and data. Travel companies should ensure establishing a comprehensive security policy is the first step in ensuring cyber security for travel sector companies. This policy should include guidelines for data protection, access control, and incident response. Countries like Denmark, UK, and USA are ranked as top nations having defending policies to handle cyber threats.

Companies need to monitor both incoming and outgoing communication for malware. Uninterrupted usage of unsecured sites and corporate servers should be blocked. Strong passwords and data protection measures are essential. Companies can instruct employees from opening an email attachment from unknown sources. Data encryption is another standard solution to prevent cyber-attacks. Doing a cyber-security audit is always preferable once the fundamental safeguards are in place.

Due to the huge volume of private, sensitive information, they save in their databases, hotels, and travel agencies are popular targets for cybercriminals. As these companies use layers of personal data where cyber ignorance is escalating. The companies are shifting their business model to digital which also opens the scope for cyber-attacks where a robust cyber security strategy is essential to deal with travel technologies risk management in 2023.

About the Author

Shambhu Nath Jha, Associate Vice President, Fact.MR. Shambhu helps enterprises and corporate to envision where the world is heading, and how their business is transforming. Perpetual variance is an inherent attribute of how businesses function, and the change cycle has shrunk, and he helps clients to understand these excellence fundamentals. Decision makers and SBU heads across industry verticals require a cognitive nudge from Shambhu to shield their enterprise from the awaiting risk.

Shambhu has over a decade of experience in helping clients to attain business excellence across several sub-domains of Food, Healthcare, Healthcare IT, Technology, and Sports. He understands how technologies along with transforming the supply chain ecosystem integrate with the existing business ecosystem and influence enterprise output. Shambhu can be reached online at <https://www.linkedin.com/in/essienjaevicelresident/> and at our company website <https://www.factmr.com/>.



ChatGPT: The Next Wave of Innovation or Your Biggest Security Threat?

By Craig Burland, CISO of Inversion6

ChatGPT, an artificial intelligence language model developed by OpenAI, is in the midst of the hype cycle where every success or failure is shouted from the rooftops. Its millions of users generate millions of queries per day with probably an equal number of posts, comments, and articles. Since its public go live in November 2022, it has garnered significant attention and dramatically exceeded expectations, surpassing the AI models before it. The platform uses deep learning algorithms and vast amounts of text data to generate human-like responses to natural language inputs. It has a wide range of capabilities, including text generation, language translation, and answering complex questions wrapped in human-like speech. Potential applications include customer service, content creation, data analysis, and education. Unfortunately, it has also been used to write malware, craft phishing, cheat on term papers, and plan fictitious crimes.

Across the recent history of innovation, there's a tendency to react with excitement, uncertainty, and even fear. The steam engine sparked fears of job loss alongside ideas of revolutionizing transportation. The first airplanes generated wonder and amazement at human accomplishment and fears of military



applications. Computerphobia reached its peak in the mid-1980s, marked by fears about humans losing jobs or becoming dependent on devices for critical thinking. Organ transplantation, space travel, DNA manipulation, etc. have all elicited strong reactions that emphasized both amazing potential and dreadful consequences, finally settling into an equilibrium that is nuanced and complex.

As a cyber defender and risk manager, it's vital to see both sides of this innovation and develop an approach that balances the potential threat and business opportunity. Uncertainty and fear would demand blocking all access to ChatGPT and the API. Excitement and wonder would propose feeding terabytes of data into the platform for its near-prescient insights. Before either approach, further consideration is warranted. Let's take a few examples of GPT's more high-profile concerns and counter-balancing opportunities:

A few weeks ago, ChatGPT was criticized in numerous articles for enabling creation of advanced, polymorphic malware. While most of the articles left out key facts like the web version didn't actually produce the malware and that ample human intervention was required, use of ChatGPT as a malware engine was theoretically possible. However, one must also consider the potential benefit of using ChatGPT to stub out software for developers, speeding new product development. The promise of low-code or no-code applications with the assistance of a tool like ChatGPT is now more than marketing hype. Take a more specific use – writing a routine to encrypt a large store of content. The resulting code could be used to secure an important transaction or ransomware. ChatGPT doesn't know or understand the difference.

More recently, the internet was abuzz with news that hackers had bypassed the ChatGPT controls to create new service offerings like phish email automation. The original article (it has since been updated for clarity) left out the key point that the bypass was merely the use of the API which currently doesn't have all the constraints of the web version. (API abuse is currently prohibited by OpenAI policy, not a technical control.) Like the scenario above, while the API can be used to generate phish – until OpenAI detects and terminates the access – it can also be used to generate phish testing campaigns and awareness posts that vary in content and tone, keeping the message fresh.

Currently, there are numerous articles about how to turn off the response controls, enabling ChatGPT answer without filters eliminating answers that potentially enable unlawful activity. While these claims are proving dubious upon further scrutiny, consider the potential uses in threat modeling or role playing. Asking ChatGPT to act as an insider threat and it will decline. Asking ChatGPT to help you, as a CISO, to brainstorm ways an insider can harm your organization becomes an insightful method to verify your defenses. In a 10-minute span, ChatGPT can guide you from a 10,000-foot view down into the weeds. In this example, ChatGPT could walk one through high-level threats like monitoring cloud storage down to a user-awareness quiz about social engineering attacks that included answers! Extending the use case to role playing, think about the tremendous value of interacting with an AI programmed to emulate malicious behavior in helping people prepare for real scenarios.

The impact of ChatGPT may mark the beginning of an AI race as the big players – Microsoft, Google, Baidu, Meta, Amazon – invest millions upon millions to build the most complete AI platform. They'll push the envelope of innovation, adding features and functionality as desired, then following with mitigations and controls as required. Like the innovations before it, we'll be enthralled with the excitement and possibility as we simultaneously wrestle with the uncertainty and fear. We'll climb and climb until we reach

the peak of expectations, then slowly slide into disillusionment. Finally, our perceptions will evolve from black and white to nuanced and complex. Like the innovations before it, we will come to understand that ChatGPT is just a tool. A complex and intriguing tool, but a tool nonetheless. We should not fear it. We should not revere it. We should consider it, understand it, and then use it.

About the Author

Veteran cybersecurity leader, Craig Burland, CISO, Inversion6 works directly with the firm's clients, building and managing security programs, as well as advising them on cybersecurity strategy and best practices. He has decades of pertinent industry experience, including leading information security operations for a Fortune 200 company. He is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Global Security, and Oracle Web Center. Craig can be reached online at LinkedIn <https://www.linkedin.com/in/craig-burland/> and at our company website <https://www.inversion6.com>.



Is ChatGPT Ready to Disrupt Cybersecurity?

By Anurag Gurtu, Co-Founder & CPO of StrikeReady

We've seen so many advancements in artificial intelligence within just a few years. ChatGPT is definitely one of the most recent ones - and a name that has been on the minds of many people. It's essentially a chatbot that uses artificial intelligence to have a "conversation" with you. ChatGPT is one of the most advanced options of its kind and boasts over 100 million users already. If you've tried ChatGPT yourself, then you already know just how powerful this tool is, but did you know that it could hold the potential to disrupt the cybersecurity industry?



Data Analysis And Predictive Functionality of AI

In just a decade, the number of data breaches that happen in the US increased significantly. About 662 breaches happened every day in 2010. And by 2021, companies in the US recorded over 1000 of these breaches on a daily basis. When your company is affected by a breach, it can take a long time to recover and contain it. In fact, the average time it takes to contain these data breaches is about 80 days.

This is an important area where ChatGPT and similar technologies can be useful. The problem with these breaches is the fact that there is usually a significant amount of data that cybersecurity experts and other

staff need to go through. This type of assessment is crucial to see the scope of the data breach or attack, but can take a very long time to complete.

ChatGPT can be a very valuable tool when it comes to incident response. The faster a situation is assessed, the quicker you can take appropriate action. You'll be able to feed the data to the ChatGPT API in order to obtain assistance with the incident response. The bot can help with analyzing your system logs and configurations. This can help you identify where and how the breach happened, and also gain a better view of what data was leaked during the attack.

This is not where the help offered by ChatGPT ends, however. You'll be able to take advantage of ChatGPT to generate scripts and prompts to strengthen the security of your network. It's a great way to reduce the risk of another attack that leads to a breach in the future.

ChatGPT can also help you determine the potential risk of a phishing attack. This is due to its potential when it comes to analyzing data you enter into the chatbot. By simply pasting text from an email or a social media post into ChatGPT, the bot analyzes the language and writing. You'll be able to ask ChatGPT if the text seems suspicious and could be linked to one of these phishing attacks before opening any attachments or links.

This particular factor also makes the AI technology useful in employee training programs. You can use ChatGPT to generate texts that are typically found in phishing emails, then present these examples to employees. By educating your staff on things to look out for in emails that contain susceptible attachments, you are able to further strengthen your defenses against attacks.

ChatGPT And Ethical Hackers

Not all hackers are criminals. Ethical hackers focus on helping to strengthen a company's cybersecurity by offering simulated hacking services. The use of ethical hackers can help a company identify faults in their security systems.

ChatGPT is also a great tool for ethical hackers, as well as experts who focus on penetration testing. These hackers can use ChatGPT in order to generate messages for emails and social media posts that will be used in phishing simulations. It's also possible to ask ChatGPT to provide step-by-step instructions on identifying vulnerabilities and to write a script that will be useful in penetration tests.

Following the testing procedures, ethical hackers can use ChatGPT to assist with writing scripts and commands that can be used after the exploitation. These scripts can then ensure the ethical hacker is able to determine how much data can be breached through the vulnerability that they discovered.

What Are the Downsides To These Technologies In Cybersecurity

The developments in AI surely offer certain benefits for cybersecurity, but we should not overlook the downsides and errors that may accompany these technologies. As we mentioned previously, the technology can assess large amounts of data and then provide predictive output or summaries.

Hackers who gain access to valuable information could also take advantage of these features. When the hackers need to scan through a large amount of data, they could turn to these software solutions in order to quickly find the information that holds the most value. By summarizing existing data that the hacker has access to, the software might also become a tool used to identify patterns that could make breaching passwords easier.

Conclusion

With several emerging technologies that use ChatGPT's APIs and similar AI functions, many companies are trying to strengthen cybersecurity. The use of these technologies can make the process of filtering through data, summarizing reports, and even predicting attacks much easier. We looked at some of the main ways in which the tech is going to disrupt cybersecurity in the upcoming future.

About the Author

Anurag Gurtu is Co-Founder & CPO of StrikeReady. He has over 18 years of cybersecurity experience in product management, marketing, go-to-market, professional services, and software development. For the past seven years, Gurtu has been deeply involved in various domains of AI, such as Natural Language Understanding/Generation and Machine Learning (Supervised/Unsupervised), which has helped him distill reality from fallacy and the resulting confusion that exists in cybersecurity with real-world applicability of this technology. Gurtu was fortunate enough to have experienced three company acquisitions (by Splunk, Tripwire and Sun Microsystems) and an early-stage startup that went public (FireEye). Gurtu holds an M.S. degree in Computer Networks from the University of Southern California and numerous cybersecurity certifications, including CISSP, CCNP Security and more.



Anurag can be reached online at [LinkedIn](#) and at our company website <https://www.strikeready.co>.

Communicating Cyber Risk

CISOs struggle with the board amidst an economic downturn.

By Tim Fleming, Strategic Advisor at Silverfort

Cyber risk is now nailed firmly to the board table. A seemingly never-ending procession of high-profile data breaches and attacks causing operations to grind to a halt has seen to this. Fighting for priority amongst other business siloes has become less of a problem for the CISO.

However, a perennial issue that does still hold cyber risk back in the boardroom is that of communication. Interactions can still sometimes feel like they're taking place in different languages, or are focussed on disparate objectives, something the accomplished security leader must seek to avoid.



Clouds on the economic horizon make this even more important. As a slowing global economy weighs on sentiment, the people, processes, and technology which make up a security leaders risk posture come under the microscope. Harder questions are asked about priorities. You must justify where your chips are laid.

Against this background, communicating with the board effectively becomes even more important.

Organisational impact as a unifying language

Now more than ever, a common language becomes crucial. As the economy tightens,

so does the focus of the organisation on what is truly important – operational uptime, customer trust, reputation, regulatory compliance and, typically, the ability to continue generating revenues.

This is the lens through which discussions must be held. It's not about cyber risk, but operational risk. In an economic downcycle the point must be made that, while the root cause of the problem might be micro, the impact could be macro. However, with the devil lying in a fragmented tangle of technical details far away from operations, this is often lost in translation.

Take Colonial Pipeline for example. The shutting down of the pipeline was caused not by a direct attack on OT systems, but a knock-on effect of billing infrastructure being compromised and a fear of lateral movement into critical areas. Imagine trying to convince a board in advance that such a seemingly tangential risk would ultimately stop 380m litres of oil from flowing, every day. Doing so would have required a mastery of big-picture storytelling, just enough technical nuance, and a need to not appear a scaremonger.

Making an effective cost argument for risk initiatives

In contrast to being able to articulate big picture impacts, security leaders in challenging economic cycles also need to articulate and defend the finer details of how they are prioritising investment. OPEX will invariably come under the spotlight as the security function is quizzed on potential cost savings.

Against this backdrop, communicating the 'bang for buck' from specific defensive capabilities is important. By breaking out the cost of security initiatives line item at a time and highlighting how much risk is addressed by each, management teams can better understand the impact of expenditure. This is where risk frameworks can be a useful tool. By summarising how a seemingly fragmented set of security initiatives mesh to secure operations, it communicates where investment performs best. Just as importantly, it highlights where exposure will occur should cost savings be sought.

Take, for example, identity programs. A strategic approach to identity is an increasing part of board level conversations because it represents a highly effective investment against a broad swathe of cyber-attacks. While, to date, conventional controls have only covered small sections of the identity threat surface – security teams are waking up to the wholesale risk reduction benefits that can be achieved by understanding where these gaps lie and preventing malicious access. Doing so stifles lateral movement - stopping threat actors carrying out a wide range of attacks. Highlighting the return on investment from such initiatives will stand security leaders in good stead with their boards.

Equally important in such conversations is making the case for protecting the workforce as much as possible. During tough times, it is tempting for senior teams to cut heads to make quick cost savings. While, on paper, this represents a short-term gain – the lost investment in people will be hard to replace when the inevitable upswing occurs – requiring an expensive and lengthy process down the line. Positioning your people as a cost-effective defensive investment, rather than an overhead, is crucial.

Bring senior stakeholders along with you

The final piece of the puzzle when communicating cyber risk strategy is stakeholder management. Understanding which members of the senior team have influence, directly or otherwise, over budgets and strategy is increasingly important to CISOs.

Start with building a map of the people who the security function has a bearing on and vice versa, whether technical or otherwise. Then, bring them in early to the decision-making process to ensure joint ownership of any proposed strategy or initiatives. Disgruntled stakeholders, often the cause of difficult questions and friction, are often the result of a lack of understanding about where cyber risk fits into their area of operations. This can be avoided with clear, transparent conversations. A CISO who takes the time to educate the right people will enjoy a far smoother path at the board level.

Ultimately, the debate around communicating with the board is not a new one for senior security leaders and the industry has come on leaps and bounds over the last few years. Current market conditions, however, add pressure as they intensify the need to justify resources. By collaborating with your target audience, framing communications in business terms, and being aware of where investment can be applied for maximum impact, CISOs are in good stead to weather the worst of it.

About the Author

Tim Fleming is a Strategic Advisor at Silverfort. Having recently retired from Deloitte, Tim Fleming is now working as a consultant and advisor across the areas of cyber security and CIO advisory including IT strategies, and operations.

With extensive experience in the IT sector across many organizations and industries, Tim brings a wealth of knowledge to assist companies in their technology challenges in areas such as IT Strategy and Governance, IT operations, and cyber security. Tim's experience would be invaluable to organizations in industries including media, financial and professional services.



Currently, as one of Tim's roles, he is working closely with Silverfort Inc, a cybersecurity software provider with a unique and ground-breaking approach to identity protection and lateral movement protection.

Tim can be reached online at (<https://www.linkedin.com/in/tim-fleming-60651937>) and at our company website <https://www.silverfort.com/>.

Going On the Defensive: Turning the Tide on The Cybersecurity Vulnerabilities of Smart Home Devices With Value-Added Services

By Craig Thole, SVP, Product Development and Operations at Assurant, Inc.

While the rise of internet-enabled smart home devices generates the opportunity to create an advanced, intuitive smart home ecosystem, at the same time their arrival also creates the conditions for more security vulnerabilities within the connected home. This fact isn't lost on consumers: according to Assurant and Parks Associates' most recent white paper – [‘Protect the Connected Home: Home security Meets Personal Privacy’](#) – 72 percent of consumers are now preoccupied with the security of their smart home products and their network in general. With news of hacks and unauthorised access to personal data increasingly fueling consumer concerns about the inherent vulnerabilities of connected devices and systems, many are left wondering what options are available to allow them to prioritise their household's data security and privacy. Consumers want to know that their homes and families are safe from intruders (both physical and virtual) and that their digital identities and personal data cannot be compromised and will remain out of the hands of nefarious actors.



Against the backdrop of an ever-evolving and dynamic threat landscape, consumers might now be persuaded to turn their attention towards the personal-data privacy solutions and security service options that deliver the most advanced safeguarding and home monitoring systems. In the last few years, reported instances of smart home attacks have seen hackers remotely controlling smart lights and smart TVs, unlocking IoT enabled doors, and

remotely turning on and streaming video from smart cameras. Now there is a growing awareness that despite the prevalence of smart home devices for the purpose of protecting homes against theft, damage, or accidents, smart home devices also represent a real risk in terms of lowering personal data security. When it comes to protecting the entire connected home, home security dovetails neatly with personal privacy in a way that makes the meaningful expansion of peace-of-mind offerings the next logical step in the evolution of device protection services. In this context, home security providers are well positioned to devise combined bundles of device protection plans and data privacy services, thereby allowing them to leverage their skills, assets, and service relationships founded on trust with customers that provide them with the right to make these offers. The long-term consequences of this development include lowering the barrier to wider smart device adoption, an increased positive perception of product value, and increased consumer confidence when it comes to adopting new products.

Data security and privacy: ensuring future smart home success.

The majority of consumers are concerned about data security, and their concern is warranted and supports their need to be vigilant. Parks Associates found that of the consumers they polled during the course of their research, approximately one-half of those with connected devices have experienced at least one data privacy and security issue. As device users continue to accumulate products to build-out their connected homes, the risk of becoming a target for acts of privacy invasion or a victim of hacking also rises. The natural fears related to this evolution are also supported by the research, with almost three-quarters of households signaling concern or high concern about the presence of spyware and viruses finding their way onto their smart devices and subsequent malicious interference and disruption.

As the consumer data highlights, a typical home has 16 connected devices with smart home device owners owning an average of eight smart home devices in total. While the increased adoption of such devices is a positive development for the broader connected home market, integrating a growing number into one's smart home set-up also adds to the level of risk and the number of problems experienced. In fact, for those with multiple smart home devices, the higher the anxiety about data privacy tends to be.

Clearly, with the rapidly developing connected device environment taking shape and the inevitable corresponding emergence of threats, it's time to rethink the comprehensive security and device protections on offer.

New solutions to old problems

The existence of real concerns regarding privacy and unauthorized access to smart devices have the power to stymie the connected smart home dream before it really has a chance to take flight. For this reason, leading tech giants, OEMs, and other disruptive smart device start-ups need to address the issues head on and come up with satisfactory and practical solutions to guarantee that consumer data remains fully protected at all times. And with concerns over data vulnerability and privacy serving as a barrier to consumers acquiring devices, cybersecurity and similar holistic protection features could be instrumental in enticing "on-the-fence" customers to explore and commit to device purchases that will allow them to embrace the connected home model. The addition of a monitoring subscription on top of such purchases could make all the difference in terms of winning the hearts and minds of consumers.

The companies that are now tentatively investigating the opportunity of value-added services to serve the smart home market need to think strategically when conceptualizing and devising these new offerings. As the objective is

to alleviate the fears of existing and potential connected device owners, they must appeal to two different constituencies: the uninitiated prospective purchasers and the existing owners of smart devices. Depending on how they go about designing, tailoring, and selling these bundles, such companies have the power to influence how all consumers use their smart home devices in a way that achieves maximum value and satisfaction. Additionally, they may also be able to fulfil the role of ‘trusted advisor’ in supporting consumers to choose their additional future smart home devices in the future.

Building trust in the smart home

The on-going and largely unaddressed uncertainty surrounding the safety and privacy of connected devices and their associated data has led to increased interest in add-on security services for smart devices. With only 37 percent of consumers trusting the companies that have access to their personal data, the technology companies looking to offer security add-on services have a significant task on their hands to earn their confidence. But at least they have a captive audience: as the white paper underlines, 67 percent of consumers report interest in a cyber security add-on from the security provider that guarantees their equipment cannot be monitored or controlled by unauthorised people. Smart home customers see the value of increased protection and privacy in their home, and as a result may be ready to respond positively to a comprehensive bundle of value-added services.

Delivering peace-of-mind services to restore confidence in the smart home vision

Fundamentally, security providers and the manufacturers of smart home devices have the opportunity to add value to their existing service offerings by transcending simple monitoring solutions and diversifying into additional service elements that deliver peace-of-mind to customers. These include self-monitoring alerts, premium technical support (‘White Glove service’), advanced data privacy solutions, video storage and warranties. Offering this type of ongoing and reliable technical support beyond the onboarding process and instalment of smart home devices not only incentivises consumers to build-out their smart home by purchasing new devices, it also strengthens the customer relationship. At the same time, those companies whose ambition it is to deliver comprehensive security, both for the home that the system is contained in, as well as the devices that comprise the security bundle, have the opportunity to positively reset consumer expectations in relation to the management of their security and privacy concerns.

Fortifying the secure smart home of the future, today

As smart home and security devices continue to grow in adoption and use, concerns around data security and privacy amongst consumers will also persist. Owners of smart homes require security systems that deliver peace of mind and the assurance that their smart devices will operate seamlessly and securely. In light of this, many consumers may be drawn to the security providers that are demonstrably taking steps to improve data privacy and minimize the risk of security breaches within the smart home. As a result, holistic privacy protection is a valuable add-on service that can restore the confidence of both potential and existing users of smart security systems and devices. Additionally, these add-on services will entice consumers to see new value in this next-generation premium support, add stickiness and satisfaction through the services provided, and strengthen brand loyalty.

About the Author

Craig Thole is the Senior Vice President of Product Development and Operations at Assurant, a Fortune 500 Company. Assurant is a leading global business services company that supports, protects and connects major consumer purchases. Craig can be reached via [Assurant.com](https://www.assurant.com).



WOMEN IN CYBERSECURITY 2023 SCHOLARSHIP WINNER

This year's 1st winner is Kylie Amison

About the Winner

I am a recent graduate of George Mason University where I obtained my Bachelor of Science degree in Cybersecurity Engineering with a minor in intelligence analysis. I currently only hold one certification, the CompTia Security +, but plan to get both the eMAPT and CEH. I am working full time at a leading mobile security company, NowSecure, as an Application Security Analyst where I do all types of fun things like exploit vulnerable apps, secure mobile application development, and contribute to exciting projects and important initiatives that are consistently highlighted throughout the security industry.



In addition, I also work part time with startup company, Auspex Labs, as a Cybersecurity Software Developer, where I am the main developer on DiplomacyTM, a geopolitical threat intelligence engine that combines a broad assortment of metrics and NLP sentiment analysis to calculate nuanced and real-time threat scores per nation state. Working at Auspex has been pivotal in my knowledge in creating secure software and has given me the opportunity to not only develop my first product, but to also start my own startup company, productizing the software and capabilities created in DiplomacyTM. Which brings me to my final achievement, I am now co-founder and CTO of Xenophon Analytics, a company that grew from shared interests in international political affairs and my project of building the geopolitical risk engine.

Throughout all of these experiences and my coursework at GMU, I have gained essential skills in secure software development, risk management, data analysis, Python, penetration testing, and mobile security. When I'm not researching or coding, you can find me watching anime, reading Sci Fi, or playing with my dogs! I have aspirations of going back to school to get a graduate degree in either Digital Forensics, or Cyber Law (maybe both?). My ultimate goal in life is to learn every single day, and I'm proud to be doing just that.

With her award, she has received an opportunity for a part-time internship with CDM as a cybersecurity reporter and blogger.

Reach out to her with story ideas:

marketing@cyberdefensemagazine.com

Award Winners



Welcome to the Cyber Defense Global InfoSec Awards for 2023

As we go to press on this annual RSAC issue of Cyber Defense Magazine, on behalf of Cyber Defense Media Group, we celebrate our strong relationship with the RSA organization. Among the many valuable services and affiliations, we enjoy, the RSA connection is one of our most important.

It is with great pleasure that we dedicate this RSA/April 2023 issue of Cyber Defense Magazine to our support and participation in the RSA Conference set for April 24-27, 2023, in San Francisco.

We have worked diligently at our end to produce one of the largest and most comprehensive issues of Cyber Defense Magazine in our 11-year history. With 50 articles from cyber security professionals, many of them planning to attend RSAC 2023, we continue to grow in distribution and actionable intelligence for our contributors and readers. We continue to monitor closely and respond to the needs of our audience.

Accordingly, the scope of CDMG's activities has grown into many media endeavors to meet these growing needs. We offer Cyber Defense Awards; Cyber Defense Conferences; Cyber Defense Professionals (job postings); Cyber Defense TV, Radio, and Webinars; and Cyber Defense Ventures (partnering with investors). The full list, with links, can be accessed at:

<https://www.cyberdefensemagazine.com/cyber-defense-media-group-11-year-anniversary-daily-celebration-in-2023/>

Cybersecurity is on the front line of the ongoing protection of our economy and critical infrastructure. It's no surprise that there are now hundreds of thousands of career openings and unlimited opportunities for those who wish to make a positive impact on today's digital world. Cyber Defense Media Group is dedicated to providing information and tools for professionals to create resilient and sustainable cyber systems.

Congratulations to all our winners!

Gary S. Miliefsky, CEO

Cyber Defense Media Group

Publisher, Cyber Defense Magazine

Cyber Defense InfoSec Awards for 2023

Access Control

LenelS2 Best Product Portfolio Access Control

Account Takeover Protection

Keyless Technologies LTD Cutting Edge Account Takeover Protection

Advanced Persistent Threat (APT) Detection and Response

Acalvio Publisher's Choice Advanced Persistent Threat (APT) Detection and Response

BedRock Systems Inc. Most Comprehensive Advanced Persistent Threat (APT) Detection and Response

SECUINFRA GmbH Hot Company Advanced Persistent Threat (APT) Detection and Response

Adversarial ML Threat Mitigation

HiddenLayer Next Gen Adversarial ML Threat Mitigation

Anti-Malware

Microsoft Market Leader Anti-Malware

Cyber Defense InfoSec Awards for 2023

Anti-Phishing

Cofense Best Product Anti-Phishing
Hoxhunt Cutting Edge Anti-Phishing
Identity Digital Most Comprehensive Anti-Phishing
Inspired eLearning Best Solution Anti-Phishing
IRONSCALES Hot Company Anti-Phishing
SlashNext Next Gen Anti-Phishing
Vade Editor's Choice Anti-Phishing

Anti-Virus

Microsoft Best Product Anti-Virus

Anti-Vishing

Mutare Market Leader Anti-Vishing

API Security

Corsha Best Product API Security
Data Theorem Cutting Edge API Security
Impart Security Inc. Publisher's Choice API Security
Imperva Most Comprehensive API Security
Noname Security Editor's Choice API Security
Salt Security Hot Company API Security
StackHawk Next Gen API Security
ThreatX Market Leader API Security
Traceable AI Most Innovative API Security

Cyber Defense InfoSec Awards for 2023

Application Security

ArmorCode Hot Company Application Security
Backslash Security Editor's Choice Application Security
ImmuniWeb Best Product Application Security
Imperva Cutting Edge Application Security
Security Compass Most Comprehensive Application Security
Spin.AI Hot Company Application Security
Synopsys Next Gen Application Security
VMware Market Leader Application Security

Applied Artificial Intelligence in Cybersecurity

StrikeReady Most Innovative Applied Artificial Intelligence in Cybersecurity

Artificial Intelligence and Machine Learning

Deloitte Publisher's Choice Artificial Intelligence and Machine Learning
Flexxon Pte. Ltd Editor's Choice Artificial Intelligence and Machine Learning
Silobreaker Hot Company Artificial Intelligence and Machine Learning

Cyber Defense InfoSec Awards for 2023

Attack Surface Management

Armis Best Product Attack Surface Management
Cyble Most Comprehensive Attack Surface Management
CyCognito Hot Company Attack Surface Management
Cymulate Visionary Attack Surface Management
Deloitte Next Gen Attack Surface Management
Detectify Market Leader Attack Surface Management
Encore Most Innovative Attack Surface Management
ForeScout Technologies Editor's Choice Attack Surface Management
GitGuardian Publisher's Choice Attack Surface Management
ImmuniWeb Best Solution Attack Surface Management
IONIX Inc. Cutting Edge Attack Surface Management
NetSPI Next Gen Attack Surface Management
Noetic Cyber Next Gen Attack Surface Management
Noname Security Hot Company Attack Surface Management (RECON)

Automated Threat Mitigation & Prevention

Trinity Cyber Cutting Edge Automated Threat Mitigation & Prevention

Biometrics

Incode Technologies Most Comprehensive Biometrics
iProov Editor's Choice Biometrics
Keyless Technologies LTD Hot Company Biometrics

Cyber Defense InfoSec Awards for 2023

Bot Management

Imperva Next Gen Bot Management
Reblaze Market Leader Bot Management

Bot Mitigation

DataDome Most Innovative Bot Mitigation

Breach & Attack Simulation

Picus Security Cutting Edge Breach & Attack Simulation
SafeBreach Most Comprehensive Breach & Attack Simulation
SCYTHE Hot Company Breach & Attack Simulation
Cymulate Best Product Breach & Attack Simulation

Browser Isolation

Ericom Software Next Gen Browser Isolation

Browser Security

Talon Cyber Security Market Leader Browser Security

Certificate Lifecycle Management

AppViewX Most Innovative Certificate Lifecycle Management

Cyber Defense InfoSec Awards for 2023

Cloud Access Security Broker

ManageEngine Editor's Choice Cloud Access Security Broker

Cloud Backup

OpenText Cybersecurity Publisher's Choice Cloud Backup

Cloud Detection and Response

Gem Security Hot Company Cloud Detection and Response

Cloud Native Application Protection Platform (CNAPP)

Ermetic Ltd. Best Solution Cloud Native Application Protection Platform (CNAPP)

MoreSec Best Product Cloud Native Application Protection Platform (CNAPP)

Wiz Most Innovative Cloud Native Application Protection Platform (CNAPP)

Cloud Security

Deloitte Publisher's Choice Cloud Security

Dig Security Most Comprehensive Cloud Security

Forward Networks Hot Company Cloud Security

Gem Security Editor's Choice Cloud Security

Imperva Next Gen Cloud Security

ShardSecure, Inc. Hot Company Cloud Security

Wiz Most Innovative Cloud Security

Cyber Defense InfoSec Awards for 2023

Cloud Security Automation

CoreStack Market Leader Cloud Security Automation

Cloud Security Monitoring

CoreStack Most Innovative Cloud Security Monitoring
ManageEngine Editor's Choice Cloud Security Monitoring
Proficio Publisher's Choice Cloud Security Monitoring

Cloud Security Posture Management (CSPM)

CoreStack Best Solution Cloud Security Posture Management (CSPM)
Data Theorem Next Gen Cloud Security Posture Management (CSPM)

Cloud Workload Protection

Hillstone Networks Next Gen Cloud Workload Protection
HYAS Infosec Inc. Hot Company Cloud Workload Protection
Ridge Security Technology Inc. Most Innovative Cloud Workload Protection

Cloud Native Security

Skyhigh Security Most Innovative Cloud Native Security

Cyber Defense InfoSec Awards for 2023

Compliance

A-LIGN Hot Company Compliance

Compliance Automation

CoreStack Best Product Compliance Automation
Vanta Cutting Edge Compliance Automation

Configuration Risk Intelligence

Evolgen Software Hot Company Configuration Risk Intelligence

Container Security

ColorTokens Best Product Container Security
Tigera Hot Company Container Security

Content Disarm and Reconstruction (CDR)

Resec Hot Company Content Disarm and Reconstruction (CDR)
Votiro Most Comprehensive Content Disarm and Reconstruction (CDR)

Continuous Controls Monitoring Platform

Noetic Cyber Hot Company Continuous Controls Monitoring Platform

Cyber Defense InfoSec Awards for 2023

Continuous Detection Posture Management

CardinalOps Next Gen Continuous Detection Posture Management

Credential Service Provider

1Kosmos Market Leader Credential Service Provider

Critical Infrastructure Protection

BedRock Systems Inc. Most Innovative Critical Infrastructure Protection

Dedrone Editor's Choice Critical Infrastructure Protection

HYAS Infosec Inc. Hot Company Critical Infrastructure Protection

Resecurity, Inc. Publisher's Choice Critical Infrastructure Protection

Crypto Security

Kroll Cutting Edge Crypto Security

Cyber Defense Readiness Platform

RangeForce Most Comprehensive Cyber Defense Readiness Platform

Cyber Insurance

Cowbell Cyber Hot Company Cyber Insurance

Safe Security Next Gen Cyber Insurance

Cyber Defense InfoSec Awards for 2023

Cyber InsureTech

IronSDN, Corp. Best Product Cyber InsureTech

Cyber Recovery Solution

Optiv Security Market Leader Cyber Recovery Solution

Cyber Resilience

Absolute Software Next Gen Cyber Resilience

OpenText Cybersecurity Most Innovative Cyber Resilience

Cyber Security Research

ULTRA-RED Publisher's Choice Cyber Security Research

Cyber Defense InfoSec Awards for 2023

Cybersecurity Artificial Intelligence

Coro Cutting Edge Cybersecurity Artificial Intelligence
Deep Instinct Most Comprehensive Cybersecurity Artificial Intelligence
Deloitte Hot Company Cybersecurity Artificial Intelligence

Cybersecurity Blog

BlackBerry Next Gen Cybersecurity Blog

Cybersecurity Company

Noname Security Next Gen Cybersecurity Company
Wing Security Market Leader Cybersecurity Company
Sangfor Technologies Visionary Cybersecurity Company

Cybersecurity Content

Inspired eLearning Publisher's Choice Cybersecurity Content
Noname Security Most Innovative Cybersecurity Content – Noname Academy

Cyber Defense InfoSec Awards for 2023

CyberSecurity Discovery

Noname Security Most Innovative CyberSecurity Discovery

Cybersecurity Education - for Enterprises

Bank of America Most Innovative Cybersecurity Education - for Enterprises

INE Editor's Choice Cybersecurity Education - for Enterprises

Inspired eLearning Most Comprehensive Cybersecurity Education - for Enterprises

Cybersecurity Education - for Small to Medium Size Businesses (SMBs)

Bank of America Most Innovative Cybersecurity Education - for Small to Medium Size Businesses (SMBs)

ConnectWise Market Leader Cybersecurity Education - for Small to Medium Size Businesses (SMBs)

INE Publisher's Choice Cybersecurity Education - for Small to Medium Size Businesses (SMBs)

Cybersecurity Healthcare Practices

Atlantic.Net Best Solution Cybersecurity Healthcare Practices

Cyber Defense InfoSec Awards for 2023

Cybersecurity Internet of Things (IoT)

CUJO LLC Next Gen Cybersecurity Internet of Things (IoT)

Cybersecurity Investor

AllegisCyber Capital Visionary Cybersecurity Investor
In-Q-Tel Most Innovative Cybersecurity Investor
VentureScope Hot Company Cybersecurity Investor

Cybersecurity Performance Management

SeeMetrics Next Gen Cybersecurity Performance Management

Cybersecurity Product Engineering Services

Sacumen Best Solution Cybersecurity Product Engineering Services

Cybersecurity Research

Bank of America Publisher's Choice Cybersecurity Research
BlackBerry Cutting Edge Cybersecurity Research
Cyble Most Comprehensive Cybersecurity Research
Forescout Technologies Hot Company Cybersecurity Research
Microsoft Editor's Choice Cybersecurity Research
MITRE Next Gen Cybersecurity Research
Trellix Market Leader Cybersecurity Research
WatchGuard Technologies Most Innovative Cybersecurity Research

Cyber Defense InfoSec Awards for 2023

Cybersecurity Service Provider

ConnectWise Market Leader Cybersecurity Service Provider
Digital Silence Most Innovative Cybersecurity Service Provider
Nisos Editor's Choice Cybersecurity Service Provider
NuData Security Cutting Edge Cybersecurity Service Provider

Cybersecurity Service Provider of the Year

Deloitte Editor's Choice Cybersecurity Service Provider of the Year
Ntirety Most Innovative Cybersecurity Service Provider of the Year
Immersive Labs Publisher's Choice Cybersecurity Service Provider of the Year

Cybersecurity Startup

BedRock Systems Inc. Cutting Edge Cybersecurity Startup
Cyble Editor's Choice Cybersecurity Startup
Dig Security Most Comprehensive Cybersecurity Startup
HolistiCyber Hot Company Cybersecurity Startup
Noetic Cyber Next Gen Cybersecurity Startup
Astrix Security Most Innovative Cybersecurity Startup of the Year

Cyber Defense InfoSec Awards for 2023

Cybersecurity Training

CybeReady Editor's Choice Cybersecurity Training
CyberVista Publisher's Choice Cybersecurity Training
Fortinet Best Solution Cybersecurity Training
Global Learning Systems Editor's Choice Cybersecurity Training
Immersive Labs Most Innovative Cybersecurity Training
INE Next Gen Cybersecurity Training
Inspired eLearning Most Comprehensive Cybersecurity Training
NowSecure Publisher's Choice Cybersecurity Training
PECB Hot Company Cybersecurity Training
Noname Security Most Innovative Cybersecurity Training - API Security Workshop
Deloitte Best Solution Cybersecurity Training
EC-Council Cybersecurity Training Company of the Year

Cybersecurity Training Videos

INE Best Product Cybersecurity Training Videos
ITPro by ACI Learning Cutting Edge Cybersecurity Training Videos
NINJIO Most Comprehensive Cybersecurity Training Videos

Cybersecurity Visionary

Centripetal Hot Company Cybersecurity Visionary
Intelligent Waves Next Gen Cybersecurity Visionary
NightDragon Market Leader Cybersecurity Visionary
RackTop Systems Editor's Choice Cybersecurity Visionary

Cyber Defense InfoSec Awards for 2023

Cybersecurity-as-a-Service (CaaS)

Allot Most Innovative Cybersecurity-as-a-Service (CaaS)
Critical Insight Editor's Choice Cybersecurity-as-a-Service (CaaS)
SharkStriker Publisher's Choice Cybersecurity-as-a-Service (CaaS)
Deloitte Editor's Choice Cybersecurity-as-a-Service (CaaS)

Data Governance

Egnyte Best Solution Data Governance
Imperva Market Leader Data Governance

Data Loss Prevention (DLP)

DTEX Systems Best Product Data Loss Prevention (DLP)
Endpoint Protector by CoSoSys Cutting Edge Data Loss Prevention (DLP)
Next DLP Most Comprehensive Data Loss Prevention (DLP)
Spin.AI Hot Company Data Loss Prevention (DLP)

Data Security

Cloudrise Best Product Data Security
Cyera Cutting Edge Data Security
Dig Security Most Comprehensive Data Security
Egnyte Hot Company Data Security
Fortanix Next Gen Data Security
Guangdong Yizhi Security Technology Co. Ltd. Hot Company Data Security
Imperva Market Leader Data Security
Rubrik Inc. Most Innovative Data Security
Satori Next Gen Data Security
Sentra Editor's Choice Data Security

Cyber Defense InfoSec Awards for 2023

Data Security Posture Management (DSPM)

BigID Market Leader Data Security Posture Management (DSPM)

Concentric.ai Publisher's Choice Data Security Posture Management (DSPM)

Laminar Next Gen Data Security Posture Management (DSPM)

DDoS Protection for Data Centers

A10 Networks Market Leader DDoS Protection for Data Centers

Deception-Based Security

MITRE Market Leader Deception-Based Security

Deep Sea Phishing Email Security

Ericom Software Next Gen Deep Sea Phishing Email Security

DevSecOps

Arnica Best Product DevSecOps

Evolver Software Publisher's Choice DevSecOps

Graylog Cutting Edge DevSecOps

JFrog Most Comprehensive DevSecOps

Kroll Hot Company DevSecOps

MoreSec Next Gen DevSecOps

NowSecure Market Leader DevSecOps

Security Compass Most Innovative DevSecOps

Wabbi Editor's Choice DevSecOps

Cyber Defense InfoSec Awards for 2023

Digital Executive Protection

BlackCloak Market Leader Digital Executive Protection
Nisos Hot Company Digital Executive Protection

Digital Footprint Security

DigiCert Best Solution Digital Footprint Security
Resecurity, Inc. Next Gen Digital Footprint Security

Digital Intelligence

UnknownCyber Next Gen Digital Intelligence

Digital Risk Protection

Cyble Best Product Digital Risk Protection
Nisos Cutting Edge Digital Risk Protection
ZeroFox Most Comprehensive Digital Risk Protection

Distributed Digital Identity Platform

1Kosmos Hot Company Distributed Digital Identity Platform

DNS Security

HYAS Infosec Inc. Hot Company DNS Security

Cyber Defense InfoSec Awards for 2023

Email Security

Hornetsecurity Next Gen Email Security

Microsoft Editor's Choice Email Security

Email Security and Management

Armorblox Market Leader Email Security and Management

OpenText Cybersecurity Most Innovative Email Security and Management

Red Sift Editor's Choice Email Security and Management

SlashNext Publisher's Choice Email Security and Management

Trellix Best Solution Email Security and Management

Embedded Security

BedRock Systems Inc. Next Gen Embedded Security

Enea Best Product Embedded Security

GammaTech Cutting Edge Embedded Security

Encryption Expert

Vaulttree Editor's Choice Encryption Expert

Endpoint Detection and Response (EDR)

QAX Technology Group Inc. Hot Company Endpoint Detection and Response (EDR)

Cyber Defense InfoSec Awards for 2023

Endpoint Security

Cynet Inc. Best Product Endpoint Security
Microsoft Market Leader Endpoint Security
PKWARE, Inc. Hot Company Endpoint Security
Syxsense Next Gen Endpoint Security
Trellix Most Innovative Endpoint Security
TXOne Networks Inc. Editor's Choice Endpoint Security
VMware Publisher's Choice Endpoint Security
WatchGuard Technologies Best Solution Endpoint Security
Konica Minolta Business Solutions USA, Inc. Cutting Edge Endpoint Security
VIPRE Security Group Hot Company Endpoint Security
Tanium Market Leader Endpoint Security
Lattice Semiconductor Most Comprehensive Endpoint Security

Enterprise Security

Armis Best Solution Enterprise Security
Sectigo Limited Next Gen Enterprise Security
WithSecure Cutting Edge Enterprise Security
SpyCloud Hot Company Enterprise Security

Executive Protection

ZeroFox Cutting Edge Executive Protection

Cyber Defense InfoSec Awards for 2023

Extended Detection and Response (XDR)

Cynet Inc. Most Comprehensive Extended Detection and Response (XDR)
Deloitte Publisher's Choice Extended Detection and Response (XDR)
Microsoft Best Solution Extended Detection and Response (XDR)
Netsurion Hot Company Extended Detection and Response (XDR)
Stellar Cyber Most Innovative Extended Detection and Response (XDR)
Trellix Editor's Choice Extended Detection and Response (XDR)
Sangfor Technologies Hot Company Extended Detection and Response (XDR)
ThreatQuotient Market Leader Extended Detection and Response (XDR)
Red Piranha Next Gen Extended Detection and Response (XDR)

Firewall

VMware Best Solution Firewall

Firmware

Eclypsium Best Product Firmware
NetRise, Inc. Cutting Edge Firmware

Forensics

Regula Most Comprehensive Forensics

Fraud Prevention

Resecurity, Inc. Hot Company Fraud Prevention
nSure.ai Editor's Choice Fraud Prevention

Cyber Defense InfoSec Awards for 2023

Future Day Malware Protection

UnknownCyber Next Gen Future Day Malware Protection

Governance, Risk and Compliance (GRC)

Imprivata Market Leader Governance, Risk and Compliance

Lynx Technology Partners LLC Most Innovative Governance, Risk and Compliance

Healthcare IoT Security

Armis Editor's Choice Healthcare IoT Security

Asimily Publisher's Choice Healthcare IoT Security

Claroty Best Solution Healthcare IoT Security

Imprivata Next Gen Healthcare IoT Security

Hybrid Cloud Application Security

A10 Networks Market Leader Hybrid Cloud Application Security

Hybrid Work Security

Red Access Next Gen Hybrid Work Security

ICS/SCADA Security

SynSaber Cutting Edge ICS/SCADA Security

TXOne Networks Inc. Most Comprehensive ICS/SCADA Security

SIGA OT Solutions Best Product ICS/SCADA Security

SCADAfence Market Leader ICS/SCADA Security

Cyber Defense InfoSec Awards for 2023

Identity & Access Management

AppViewX Hot Company Identity & Access Management
Enzoic Next Gen Identity & Access Management
ManageEngine Editor's Choice Identity & Access Management
Microsoft Market Leader Identity & Access Management
SecureAuth Corporation Next Gen Identity & Access Management
Ping Identity Best Solution Identity & Access Management
Grip Security Cutting Edge Identity & Access Management
Frontegg Hot Company Identity & Access Management
Imprivata Market Leader Identity & Access Management
Simeio NextGen Identity & Access Management
Omada Publisher's Choice Identity & Access Management

Identity Access Management (IAM)

Cyderes Hot Company Identity Access Management (IAM)
Cyolo Cutting Edge Identity Access Management (IAM)
SPHERE Editor's Choice Identity Access Management (IAM)

Identity Data

Radiant Logic Best Product Identity Data

Identity Orchestration

Strata Identity Most Comprehensive Identity Orchestration
Simeio Cutting Edge Identity Orchestration

Cyber Defense InfoSec Awards for 2023

Identity Protection

IDShield Hot Company Identity Protection

Identity Security

CyberArk Next Gen Identity Security
ManageEngine Cutting Edge Identity Security
Oort Editor's Choice Identity Security
Saviynt Publisher's Choice Identity Security
Semperis Best Solution Identity Security
AuthMind Inc. Hot Company Identity Security
Silverfort Hot Company Identity Security
Grip Security Most Innovative Identity Security

Identity Verification

Telesign Publisher's Choice Identity Verification
Regula Cutting Edge Identity Verification
Persona Editor's Choice Identity Verification
Incode Technologies Next Gen Identity Verification

Incident Response

Cyble Editor's Choice Incident Response
Deloitte Best Solution Incident Response
Kroll Most Comprehensive Incident Response
Sygnia Hot Company Incident Response
ConnectWise Market Leader Incident Response

Cyber Defense InfoSec Awards for 2023

Industrial Cybersecurity

Forescout Technologies Next Gen Industrial Cybersecurity
Resecurity, Inc. Market Leader Industrial Cybersecurity
Dragos Most Comprehensive Industrial Cybersecurity

InfoSec Startup

BedRock Systems Inc. Cutting Edge InfoSec Startup
Valence Security Editor's Choice InfoSec Startup of the Year

Insider Threat Detection

Code42 Publisher's Choice Insider Threat Detection
innerActiv Best Solution Insider Threat Detection
Racktop Systems Hot Company Insider Threat Detection

Insider Threat Prevention

Deloitte Cutting Edge Insider Threat Prevention
Imperva Hot Company Insider Threat Prevention
Microsoft Editor's Choice Insider Threat Prevention
DTEX Systems Most Comprehensive Insider Threat Prevention
Advance Onion, Inc. Next Gen Insider Threat Prevention

Cyber Defense InfoSec Awards for 2023

Threat Protection

Deloitte Next Gen Insider Threat Protection

Internet Filtering

DNSFilter Market Leader Internet Filtering

Internet Intelligence

DomainTools Cutting Edge Internet Intelligence

Internet of Things (IoT) Security

Armis Publisher's Choice Internet of Things (IoT) Security
ForeScout Technologies Best Solution Internet of Things (IoT) Security
SAM Seamless Network Editor's Choice Internet of Things (IoT) Security
Viakoo Next Gen Internet of Things (IoT) Security

Low-Code/No-Code Security

Zenity Most Innovative Low-Code/No-Code Security

Machine Identity Management

Venafi Best Product Machine Identity Management

Malware Analysis

Cyble Cutting Edge Malware Analysis

Cyber Defense InfoSec Awards for 2023

Managed Compliance

GhostWatch Next Gen Managed Compliance

Managed Detection and Response (MDR)

BlackBerry Hot Company Managed Detection and Response (MDR)

CRITICALSTART Next Gen Managed Detection and Response (MDR)

Cyberes Market Leader Managed Detection and Response (MDR)

Deloitte Cutting Edge Managed Detection and Response (MDR)

eSentire Publisher's Choice Managed Detection and Response (MDR)

Netsurion Best Solution Managed Detection and Response (MDR)

WithSecure Most Comprehensive Managed Detection and Response (MDR)

Adlumin Editor's Choice Managed Detection and Response (MDR)

Managed Detection and Response (MDR) Service Provider

Kroll Hot Company Managed Detection and Response (MDR) Service Provider

Netsurion Next Gen Managed Detection and Response (MDR) Service Provider

Trustwave Editor's Choice Managed Detection and Response (MDR) Service Provider

Ontinue Publisher's Choice Managed Detection and Response (MDR) Service Provider

Vercara Best Solution Managed Detection and Response (MDR) Service Provider

Avertium Cutting Edge Managed Detection and Response (MDR) Service Provider

Proficio Cutting Edge Managed Detection and Response (MDR) Service Provider

ConnectWise Market Leader Managed Detection and Response (MDR) Service Provider

CyberProof Most Comprehensive Managed Detection and Response (MDR) Service Provider

Cyber Defense InfoSec Awards for 2023

Managed Extended Detection and Response (MxDR)

Difenda Editor's Choice Managed Extended Detection and Response (MxDR)

Managed Security Service Provider (MSSP)

Deloitte Market Leader Managed Security Service Provider (MSSP)

ClearDATA Best Solution Managed Security Service Provider (MSSP)

SCADAfence Hot Company Managed Security Service Provider (MSSP)

Vercara Best Solution Managed Security Service Provider (MSSP)

Proficio Most Innovative Managed Security Service Provider (MSSP)

GhostWatch Next Gen Managed Security Service Provider (MSSP)

Avertium Publisher's Choice Managed Security Service Provider (MSSP)

GM Sectec Hot Company Managed Security Service Provider (MSSP)

MDR Service Provider

GM Sectec Hot Company MDR Service Provider

Messaging Security

SafeGuard Cyber Cutting Edge Messaging Security

Micro-Segmentation

Airgap Networks Most Comprehensive Micro-Segmentation

BedRock Systems Inc. Hot Company Micro-Segmentation

ColorTokens Editor's Choice Micro-Segmentation

TrueFort Next Gen Micro-Segmentation

Cyber Defense InfoSec Awards for 2023

Microsoft Security Professional Service

Difenda Market Leader Microsoft Security Professional Service

Mobile App Security

Data Theorem Best Product Mobile App Security
Verimatrix Hot Company Mobile App Security
Zimperium Best Solution Mobile App Security
Qoukka Publisher's Choice Mobile App Security
LastPass Most Innovative Mobile App Security
Now Secure Editor's Choice Mobile App Security
Guardsquare Cutting Edge Mobile App Security

Mobile Device Security

BedRock Systems Inc. Most Comprehensive Mobile Device Security
SlashNext Hot Company Mobile Device Security

Mobile Endpoint Security

Zimperium Next Gen Mobile Endpoint Security

Multifactor Authentication

WatchGuard Technologies Market Leader Multifactor Authentication

Network Access Control (NAC)

Beijing ThreatBook Technology Co., Ltd Cutting Edge Network Access Control (NAC)

Forescout Technologies Editor's Choice Network Access Control (NAC)

Cyber Defense InfoSec Awards for 2023

Network Detection and Response

Armis Publisher's Choice Network Detection and Response
Beijing ThreatBook Technology Co., Ltd Best Solution Network Detection and Response
Corelight Next Gen Network Detection and Response
LiveAction Most Innovative Network Detection and Response
TXOne Networks Inc. Most Comprehensive Network Detection and Response
Vercara Cutting Edge Network Detection and Response

Network Security and Management

Endace Next Gen Network Security and Response
Vercara Market Leader Network Security and Response
Calix Hot Company Network Security and Response
WatchGuard Technologies Editor's Choice Network Security and Response
Timus Networks, Inc. Cutting Edge Network Security and Response

Next Generation Firewall

TXOne Networks Inc. Editor's Choice Next Generation Firewall

Operational Technology (OT) Security

TXOne Networks Inc. Editor's Choice Operational Technology (OT) Security

OT and IoT Endpoint Security

Nozomi Networks Publisher's Choice OT and IoT Endpoint Security

Cyber Defense InfoSec Awards for 2023

OT Asset Visibility

OPSWAT Best Solution OT Asset Visibility
SCADAfence Market Leader OT Asset Visibility

OT Security

Airgap Networks Next Gen OT Security
Armis Most Innovative OT Security
Radiflow Most Comprehensive OT Security
Dragos Market Leader OT Security
HYAS Infosec Inc. Hot Company OT Security
Difenda Cutting Edge OT Security

Outcome-Based Security Solutions

Inspira Enterprise, Inc. Hot Company Outcome-Based Security Solutions

PAM for Cloud

Delinea Next Gen PAM for Cloud

PAM for Cloud Infrastructure

Saviynt Market Leader PAM for Cloud Infrastructure

Cyber Defense InfoSec Awards for 2023

Passwordless Authentication

Keeper Security Publisher's Choice Passwordless Authentication
Microsoft Editor's Choice Passwordless Authentication
SecureAuth Corporation Next Gen Passwordless Authentication
Keyless Technologies LTD Best Solution Passwordless Authentication
Imprivata Editor's Choice Passwordless Authentication
Axiad Most Innovative Passwordless Authentication

Penetration Testing

Bugcrowd Hot Company Penetration Testing
NetSPI Most Comprehensive Penetration Testing
Trustwave Market Leader Penetration Testing
Bishop Fox Next Gen Penetration Testing
Now Secure Hot Company Penetration Testing
Coalfire Editor's Choice Penetration Testing
Konica Minolta Business Solutions USA, Inc. Cutting Edge Penetration Testing

Pentesting

Cobalt Next Gen Pentesting
Cymulate Most Innovative Pentesting

Phishing-Resistant MFA

Axiad Most Innovative Phishing-Resistant MFA

Cyber Defense InfoSec Awards for 2023

PKI-as-a-Service

AppViewX Editor's Choice PKI-as-a-Service
Keyfactor Publisher's Choice PKI-as-a-Service

PR Firm for InfoSec

Madison Alexander PR Best Solution PR Firm for InfoSec

Privilege Access Management (PAM)

Delinea Cutting Edge Privilege Access Management (PAM)
Keeper Security Most Comprehensive Privilege Access Management (PAM)
StrongDM Market Leader Privilege Access Management (PAM)
SENHASEGURA USA LLC Hot Company Privilege Access Management (PAM)

Protective DNS

HYAS Infosec Inc. Hot Company Protective DNS

Quantum Computing

QuSecure, Inc. Next Gen Quantum Computing

Quantum Encryption

SandboxAQ Most Innovative Quantum Encryption

Cyber Defense InfoSec Awards for 2023

Quantum Resilient Encryption

Aliro Quantum Hot Company Quantum Resilient Encryption

Rail Cybersecurity

Cylus Cybersecurity Ltd Editor's Choice Rail Cybersecurity

Railway Cybersecurity

Cervello Publisher's Choice Railway Cybersecurity

Ransomless Ransomware Protection

Ericom Software Best Solution Ransomless Ransomware Protection

Ransomware Data Security Solution

Calamu Next Gen Ransomware Data Security Solution

Flexxon Pte. Ltd Best Product Ransomware Data Security Solution

RackTop Systems Publisher's Choice Ransomware Data Security Solution

ThreatBlockr Hot Company Ransomware Data Security Solution

Absolute Software Editor's Choice Ransomware Data Security Solution

Ransomware Protection of SaaS Data

Spin.AI Cutting Edge Ransomware Protection of SaaS Data

Cyber Defense InfoSec Awards for 2023

Remote Work Security

Airgap Networks Most Comprehensive Remote Work Security

Venn Hot Company Remote Work Security

Risk Management

Cyble Market Leader Risk Management

Safe Security Publisher's Choice Risk Management

Radiflow Most Innovative Risk Management

RiskLens Editor's Choice Risk Management

Risk-based Vulnerability Management

Brinqa Publisher's Choice Risk-based Vulnerability Management

Forescout Technologies Best Solution Risk-based Vulnerability Management

FortifyData Editor's Choice Risk-based Vulnerability Management

Nucleus Security Next Gen Risk-based Vulnerability Management

SaaS Security

BetterCloud Cutting Edge SaaS Security

Cyber Defense InfoSec Awards for 2023

SaaS/Cloud Security

Adaptive Shield Ltd Most Comprehensive SaaS/Cloud Security
Armis Next Gen SaaS/Cloud Security
DoControl Most Innovative SaaS/Cloud Security
Infoblox Publisher's Choice SaaS/Cloud Security
Obsidian Security Best Solution SaaS/Cloud Security
Spin.AI Next Gen SaaS/Cloud Security
Valence Security Hot Company SaaS/Cloud security
Wing Security Hot Company SaaS/Cloud Security
Grip Security Editor's Choice SaaS/Cloud Security
AppOmni Hot Company SaaS/Cloud Security
Rhymetec Hot Company SaaS/Cloud Security
Astrix Security Market Leader SaaS/Cloud Security
Suridata Next Gen SaaS/Cloud Security

SecOps-as-a-Service

CoreStack Most Innovative SecOps-as-a-Service

Secure Access Service Edge (SASE)

Netskope Cutting Edge Secure Access Service Edge (SASE)
VMware Most Comprehensive Secure Access Service Edge (SASE)
Open Systems Publisher's Choice Secure Access Service Edge (SASE)
Ericom Software Best Product Secure Access Service Edge (SASE)

Secure Coding Tools

GitGuardian Next Gen Secure Coding Tools
Noname Security Hot Company Secure Coding Tools

Cyber Defense InfoSec Awards for 2023

Secure Low Code/No Code Process Automation

Coviant Software Market Leader Secure Low Code/No Code Process Automation

Secure Managed File Transfer

Coviant Software Most Innovative Secure Managed File Transfer

Secure SaaS Backups

Spin.AI Editor's Choice Secure SaaS Backups

Secure Web Gateway (SWG)

Dope.Security Publisher's Choice Secure Web Gateway (SWG)

Security Abstraction

MITRE Best Solution Security Abstraction

Security Awareness Training

Deloitte Service LLP Editor's Choice Security Awareness Training

Fortinet Cutting Edge Security Awareness Training

Hornetsecurity Most Comprehensive Security Awareness Training

NINJIO Hot Company Security Awareness Training

Inspired eLearning Publisher's Choice Security Awareness Training

Cyber Defense InfoSec Awards for 2023

Security Company

BlackBerry Market Leader Security Company
ForeScout Technologies Most Innovative Security Company
Imperva Editor's Choice Security Company
Syxsense Publisher's Choice Security Company
Bishop Fox Next Gen Security Company

Security Company of the Year

Cyderes Most Innovative Security Company of the Year
Raytheon Intelligence & Space Next Gen Security Company of the Year
Sectigo Limited Cutting Edge Security Company of the Year
WatchGuard Technologies Market Leader Security Company of the Year

Security Information and Event Management (SIEM)

Devo Technology Inc. Most Comprehensive Security Information and Event Management (SIEM)
Graylog Best Solution Security Information and Event Management (SIEM)
Gurukul Cutting Edge Security Information and Event Management (SIEM)
ManageEngine Hot Company Security Information and Event Management (SIEM)
Panther Labs Next Gen Security Information and Event Management (SIEM)
QAX Technology Group Inc. Hot Company Security Information and Event Management (SIEM)
SECUINFRA GmbH Market Leader Security Information and Event Management (SIEM)

Security Investigation Platform

HYAS Infosec Inc. Hot Company Security Investigation Platform
Endace Most Innovative Security Investigation Platform

Cyber Defense InfoSec Awards for 2023

Security Investor

NightDragon Market Leader Security Investor

Security Orchestration, Automation & Response (SOAR)

Deloitte Publisher's Choice Security Orchestration, Automation & Response (SOAR)

ManageEngine Cutting Edge Security Orchestration, Automation & Response (SOAR)

StrikeReady Hot Company Security Orchestration, Automation & Response (SOAR)

SIRP Labs Limited Editor's Choice Security Orchestration, Automation & Response (SOAR)

Revelstoke Security Most Comprehensive Security Orchestration, Automation & Response (SOAR)

Security Penetration Testing

Viettel Cyber Security Company Next Gen Security Penetration Testing

Security Software

SCYTHE Most Innovative Security Software

Security Solutions

DFIN Cutting Edge Security Solutions

Cyber Defense InfoSec Awards for 2023

Security Team

SecurityMetrics Most Comprehensive Security Team
Breakthru Beverage Group Top Security Team
Zoom Video Communications, Inc. Next Gen Security Team
Bank of America Most Innovative Security Team
Sygnia Hot Company Security Team

Security Training

Bank of America Most Innovative Security Training

Service Account Protection

TrueFort Market Leader Service Account Protection

Service Provider Infrastructure Security

A10 Networks Market Leader Service Provider Infrastructure Security

Smart City Cybersecurity

Resecurity, Inc. Most Innovative Smart City Cybersecurity

Cyber Defense InfoSec Awards for 2023

SMB Cybersecurity

Defendify Best Solution SMB Cybersecurity
Coro Editor's Choice SMB Cybersecurity
SAM Seamless Network Hot Company SMB Cybersecurity
TPx Hot Company SMB Cybersecurity
WatchGuard Technologies Market Leader SMB Cybersecurity
A-LIGN Most Innovative SMB Cybersecurity
JumpCloud Next Gen SMB Cybersecurity
Timus Networks, Inc Next Gen SMB Cybersecurity
CYREBRO Publisher's Choice SMB Cybersecurity

SMB MSSP

SEI Cutting Edge SMB MSSP

SMB Zero Trust

Timus Networks, Inc Most Comprehensive SMB Zero Trust

SOC-as-a-Service

ConnectWise Market Leader SOC-as-a-Service

Cyber Defense InfoSec Awards for 2023

Software Supply Chain Security

Scribe Security Best Solution Software Supply Chain Security

MoreSec Editor's Choice Software Supply Chain Security

Arnica Hot Company Software Supply Chain Security

Legit Security Market Leader Software Supply Chain Security

Lineaje Most Innovative Software Supply Chain Security

GammaTech Next Gen Software Supply Chain Security

Sonatype Next Gen Software Supply Chain Security

ReversingLabs Publisher's Choice Software Supply Chain Security

Strategic Advisor

Momentum Cybersecurity Group Visionary Strategic Advisor

Supply Chain Risk

Advanced Onion, Inc. Most Innovative Supply Chain Risk

Cyber Defense InfoSec Awards for 2023

Third-Party Cyber Risk

Jscrambler Most Comprehensive Third-Party Cyber Risk

Black Kite Hot Company Third-Party Cyber Risk

Astrix Security Cutting Edge Third-Party Cyber Risk

Third-Party Cyber Risk Management (TPCRM)

CyberGRX Hot Company Third-Party Cyber Risk Management (TPCRM)

FortifyData Next Gen Third-Party Cyber Risk Management (TPCRM)

Resecurity, Inc. Market Leader Third-Party Cyber Risk Management (TPCRM)

Third-Party Risk

Imprivata Most Innovative Third-Party Risk

Third-Party Risk Management (TPRM)

CyberGRX Editor's Choice Third-Party Risk Management (TPRM)

AuditBoard Hot Company Third-Party Risk Management (TPRM)

Resecurity, Inc. Publisher's Choice Third-Party Risk Management (TPRM)

Threat Actor Infrastructure Mapping

HYAS Infosec Inc. Hot Company Threat Actor Infrastructure Mapping

Threat Detection

Hoxhunt Best Solution Threat Detection

Cyber Defense InfoSec Awards for 2023

Threat Detection, Incident Response, Hunting and Triage Platform

Anomali Cutting Edge Threat Detection, Incident Response, Hunting and Triage Platform

Anvilogic Most Comprehensive Threat Detection, Incident Response, Hunting and Triage Platform

Cyble Hot Company Threat Detection, Incident Response, Hunting and Triage Platform

Microsoft Editor's Choice Threat Detection, Incident Response, Hunting and Triage Platform

Resecurity, Inc. Market Leader Threat Detection, Incident Response, Hunting and Triage Platform

Endace Next Gen Threat Detection, Incident Response, Hunting and Triage Platform

Threat Exposure Management

Anomali Most Innovative Threat Exposure Management
Noetic Cyber Editor's Choice Threat Exposure Management

Threat Hunting

Deloitte Publisher's Choice Threat Hunting

Cyber Defense InfoSec Awards for 2023

Threat Intelligence

Cybersixgill Most Comprehensive Threat Intelligence
Cyble Hot Company Threat Intelligence
Deloitte Market Leader Threat Intelligence
Forescout Technologies Most Innovative Threat Intelligence
Intel 471 Editor's Choice Threat Intelligence
Microsoft Hot Company Threat Intelligence
OpenText Security Solutions Best Solution Threat Intelligence
Panther Labs Next Gen Threat Intelligence
Resecurity, Inc. Cutting Edge Threat Intelligence
SCYTHE Most Comprehensive Threat Intelligence
ThreatConnect Next Gen Threat Intelligence
Trellix Most Innovative Threat Intelligence
VMware Best Solution Threat Intelligence
ZeroFox Next Gen Threat Intelligence
SEI Hot Company Threat Intelligence
Cobwebs Technologies Cutting Edge Threat Intelligence
HYAS Infosec Inc. Hot Company Threat Intelligence
Silobreaker Hot Company Threat Intelligence
ThreatQuotient Market Leader Threat Intelligence
CYFIRMA Next Gen Threat Intelligence
Nisos Publisher's Choice Threat Intelligence

Threat Intelligence Management

StrikeReady Publisher's Choice Threat Intelligence Management

Threat Modeling

Resecurity, Inc. Best Product Threat Modeling
ThreatModeler Cutting Edge Threat Modeling

Cyber Defense InfoSec Awards for 2023

Transportation Cybersecurity

Cervello Most Comprehensive Transportation Cybersecurity

Unified Data Controls

Securiti Hot Company Unified Data Controls

Unified Threat Management

Deloitte Editor's Choice Unified Threat Management

User Behavior Analytics

ManageEngine Most Innovative User Behavior Analytics
XTN Cognitive Security Market Leader User Behavior Analytics

Virtual Assistant for Cybersecurity

StrikeReady Editor's Choice Virtual Assistant for Cybersecurity

Virtual Directory Services

DFIN Publisher's Choice Virtual Directory Services

Virtual Private Network (VPN)

ClearVPN Editor's Choice Virtual Private Network (VPN)
Intelligent Waves Best Solution Virtual Private Network (VPN)

Cyber Defense InfoSec Awards for 2023

Vulnerability Assessment, Remediation and Management

Coalfire Most Innovative Vulnerability Assessment, Remediation and Management
Autobahn Security Next Gen Vulnerability Assessment, Remediation and Management

Vulnerability Intelligence

Silobreaker Hot Company Vulnerability Intelligence

Vulnerability Management

Onapsis Editor's Choice Vulnerability Management
Coalfire Hot Company Vulnerability Management

Vulnerability Management as a Service

TuxCare Market Leader Vulnerability Management as a Service
Difenda Next Gen Vulnerability Management as a Service

Web Application Security

Imperva Most Innovative Web Application Security
Jscrambler Editor's Choice Web Application Security
Edgio Hot Company Web Application Security
Reblaze Publisher's Choice Web Application Security

Web Penetration Testing

Ridge Security Technology Inc. Best Solution Web Penetration Testing

Cyber Defense InfoSec Awards for 2023

Zero Trust

BedRock Systems Inc. Market Leader Zero Trust
ColorTokens Hot Company Zero Trust
Cyolo Most Innovative Zero Trust
ForeScout Technologies Publisher's Choice Zero Trust
iboss Best Solution Zero Trust
Keeper Security Cutting Edge Zero Trust
ManageEngine Most Comprehensive Zero Trust
Syxsense Hot Company Zero Trust
Tresorit Next Gen Zero Trust
Votiro Next Gen Zero Trust
Xage Security Hot Company Zero Trust
Ericom Software Editor's Choice Zero Trust

Zero Trust Application Protection

BedRock Systems Inc. Hot Company Zero Trust Application Protection
Corsha Next Gen Zero Trust Application Protection

Zero Trust BYOD

Hypori Editor's Choice Zero Trust BYOD
Venn Publisher's Choice Zero Trust BYOD

Zero Trust ETM (Encrypted Traffic Management)

A10 Networks Market Leader Zero Trust ETM (Encrypted Traffic Management)

Cyber Defense InfoSec Awards for 2023

Zero Trust Platform

ColorTokens Editor's Choice Zero Trust Platform
RackTop Systems Hot Company Zero Trust Platform
Axis Security Publisher's Choice Zero Trust Platform

ZTNA Solution

Hillstone Networks Best Solution ZTNA Solution

Top Chief Executive Officer

Tony Crescenzo Intelligent Waves
Kevin Lynch Optiv Security
Gee Rittenhouse Skyhigh Security
Camellia Chan Flexxon Pte. Ltd
Nikhil Gupta ArmorCode
Yevgeny Dibrov Armis
Geoff Haydon Ontinue

Top Chief Information Officer

Jeff Buss Nordic Consulting

Cyber Defense InfoSec Awards for 2023

Top Chief Information Security Officer

Oleg Khudiakov Miratech
Christopher Porter Fannie Mae
Bret Arsenault Microsoft
Samir Sherif Absolute Software
Chris Lanzilotta Home Depot
Cory Brasel Nordic Consulting
Charles Blauner Team8

Top Chief Product Officer

Yiyi Miao OPSWAT
Aparna Rayasam Trellix

Top Chief Security & Trust Officer

Malcolm Harkins Epiphany Systems

Top Chief Security Officer

George Gerchow Sumo Logic

Top Chief Technology Officer

Osman Ismael BedRock Systems
Pat McGarry ThreatBlockr
Anthony Pierce Splunk

Top Cybersecurity Author

Thomas Kranz Making *Sense of Cybersecurity*

Cyber Defense InfoSec Awards for 2023

Top Cybersecurity Product Expert

Dana Torgerson Sumo Logic

Top Security Expert

Joseph Carson Delinea
Anuj Gargeya Malkapuram Salesforce

Top Women in Cybersecurity

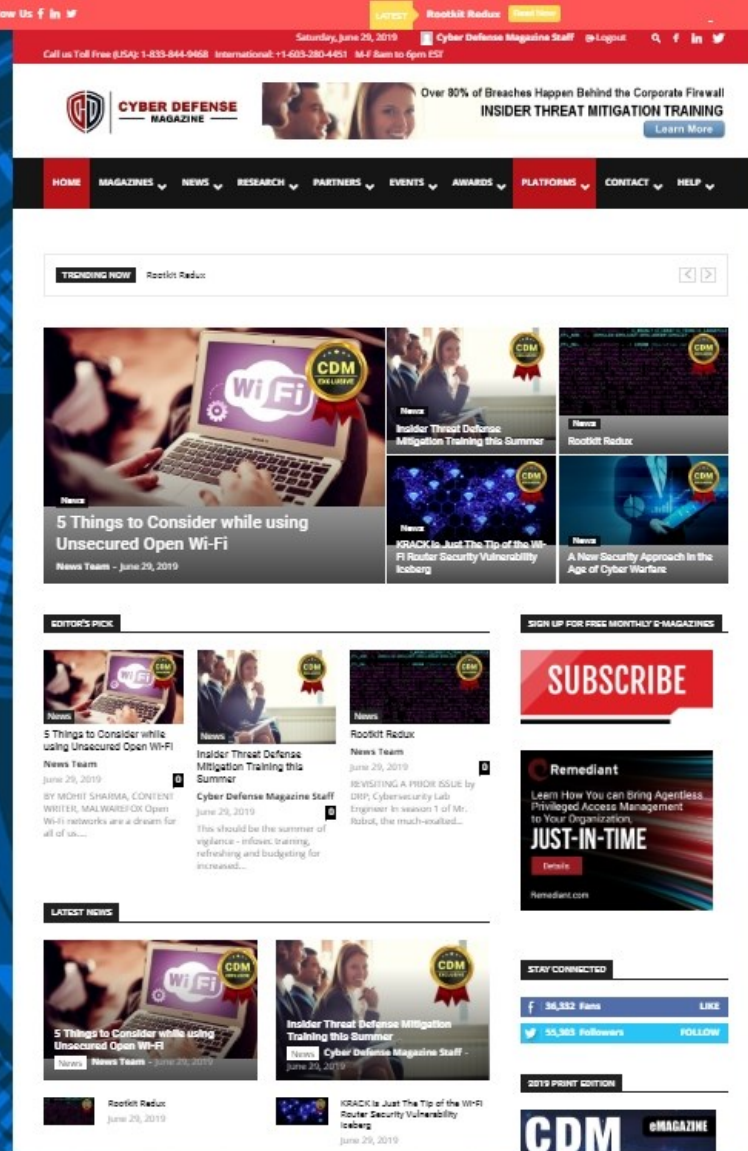
Jennifer Eiben CyberWire
Simone Petrella CyberVista
Julie Giannini Egnite
Ellen Sundra Forescout Technologies
Robyn Yaniero Marsi Lynx Technology Partners LLC.
Anne Genge Myla Training Co.
Amy De Salvatore NightDragon
Carolyn Crandall Cymulate
Camellia Chan Flexxon Pte. Ltd
Eva Chen TrendMicro
Hila Zigman Zinshtein Noname Security
Larissa Schneider Noname Security
Jen Easterly Cybersecurity and Infrastructure Security Agency (CISA)
Michelle Welch WatchGuard Technologies
Erin Cassell Bank of America

Visionary Cybersecurity Leader

Dave Burg EY Americas

Young Women in Cybersecurity Scholarship

Kylie Amison Winner



Books by our Publisher: <https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH> (with others coming soon...)

11 Years in The Making...

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched <http://www.cyberdefenseconferences.com> and have another amazing platform coming soon.

CyberDefenseCon

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefenseemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert



**ALWAYS FREE
NO STRINGS ATTACHED**



UNKNOWN
CYBER

**"70% of Malware Infections Go
Undetected by Antivirus..."**

Not by us. We detect the unknowns.

www.unknowncyber.com



CYBER DEFENSE

MAGAZINE



www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensenewswire.com
www.cyberdefensewebinars.com
www.cyberdefenseemagazine.com
www.cyberdefenseconferences.com



Cyber & Strategic Risk

What does it take to lead through disruption?

Hear from thought leaders and change agents on transforming challenges into opportunities to outpace and outperform.

Co-hosted by Deloitte and Fast Company

Visit RSA Conference booth N-6078 or explore online



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved.



*** with help from writers
and friends all over the Globe.**