CYBER DEFENSE MAGAZINE

eMAGAZINE

JANUARY 2024

In This Edition

3 New Risks That CISOs Will Face in 2024

Steps To Implement Cyber Controls and Processes

Closing the Gap: Safeguarding Critical Infrastructure's IT and OT Environments

...and much more...

MORE INSIDE!

CONTENTS

Welcome to CDM's January 2024 Issue ---------- 8

3 New Risks That CISOs Will Face in 2024 ---------- 20

By Daniel Barber, CEO, DataGrail

Steps To Implement Cyber Controls and Processes ---------- 23

By Juliana Spofford, General Counsel and Chief Privacy Officer, Aidentified

Closing the Gap: Safeguarding Critical Infrastructure's IT and OT Environments ---------- 26

By Victor Atkins, Director | Cybersecurity, 1898 & Co.

Addressing the Particular Cybersecurity Challenge of Discrete Manufacturing ---------- 30

By Dave Purdy, Regional Vice President of Sales, North America, TXOne Networks

AI in DevSecOps: Moving from A Co-Pilot to An Autopilot ---------- 34

By Stephen Chin, VP of Developer Relations, JFrog

AI-Enhanced Identity Fraud: A Mounting Threat to Organizations and Users ---------- 38

By Philipp Pointner, Chief of Digital Identity at Jumio

Why Cybersecurity Maturity Model Certification (CMMC) Matters for All Businesses, Not Just DoD Contractors ---------- 41

By John Funk, Creative Consultant, SevenAtoms

AI: The Human Touch in Cybersecurity Recruitment ---------- 45

By Darrin Straff, Senior Staffing Consultant, NinjaJobs

Beyond Traditional Cyber Defences: The Rise of Outcome-Based Security In Modern Business --------- 48

By Paul Brucciani, Cyber Security Advisor at WithSecure™

AI, Cybersecurity Awareness, And Communication ---------- 52

By John Trest, Chief Learning Officer, VIPRE Security Group

Addressing Bias in Insider Risk Monitoring ---------- 56

By Chris Denbigh-White, Chief Security Officer, Next

NIS 2: From Obligation to Opportunity ---------- 59

By Jacques de La Rivière, CEO, Gatewatcher

Top 6 Security Challenges of SMEs ---------- 62

By Michal Gil, Head of Product, CybeReady

Is 2024 the Year of Cloud Repatriation? ---------- 67

By Eyal Arazi, cloud security manager at Radware

How A Strong Digital Culture Is the Foundation For Successful Metaverse Exploration ---------- 70

By Jaime McMahon, CDO, LineZero

SolarWinds Lawsuit Reinforces the Need for Critical Communication Between CISOs and the C-Suite 73

By Jose Seara, Founder and CEO, Denexus

Combating Terrorism Using Information Protection ---------- 76

By Milica D. Djekic

Reshaping the Focus of Cybersecurity ---------- 82

By Todd Thorsen, Chief Information Security Officer, CrashPlan

MGM & Caesars Cyberattacks: Lessons Learned ---------- 85

By Tim Callan, Chief Experience Officer, Sectigo

Evolution and Escalation of Cybersecurity Threats ---------- 88

By Augusto Barros, Vice President Cyber Security Evangelist at Securonix

Cyber Insurance: A Smart Investment to Protect Your Business from Cyber Threats in 2023 ---------- 91

By Zia Muhammad, Cyber Risk Advisor, Onpoint Insurance Services

Cyber Resilience – Beyond Cyber Security ---------- 95

By James Gorman, Hard2hack.com

Cybersecurity Preparedness 2024 ---------- 99

By Chris Leach, Board Advisor for Judy Security

Digital Technologies Power Global Operations but Present Growing Risks ---------- 102

By Charlie Regan, CEO, Nerds on Site

Enhancing PCI DSS Compliance: The Urgent Need for Risk-Based Prioritization ---------- 105

By Ian Robinson, Chief Architect of Titania

How Businesses Can Manage Cryptocurrency Fraud ---------- *108*

By James Hunt, Subject Matter Expert Payments, Feedzai

It's Time to End the Myth of Untouchable Mainframe Security. ---------- *112*

By Al Saurette, CEO, MainTegrity

From the SIEM to the Lake: Bridging the Gap for Splunk Customers Post-Acquisition ---------- *115*

By Omer Singer, VP of Strategy, Anvilogic

From Virtual Visions to Tangible Profits: A Founder's Guide to Launching a vCISO Firm in 2024 ----- *118*

By Caroline McCaffrey, CEO and Co-founder, ClearOPS

Getting AI Right for Security: 5 Principles---------- *123*

By Kevin Kennedy, SVP Products, Vectra AI

VPNs in Times of War: Why a Rise in Global Conflicts Mean Citizens Now Need VPNs More Than Ever ---------- *126*

By Sebastian Schaub, CEO, hide.me

Hyperautomation: Revolutionizing the Security Market ---------- *130*

By Divakar Kolhe, Digital Marketer, Market Research Future (Part of Wantstats Research and Media Private Limited)

How The Security of The Cloud's Supply Chain Will Shift in 2024 ---------- *134*

By Jason Martin, Co-founder and Co-CEO at Permiso Security

Four Ways Genai Will Change the Contours Of The Corporate Landscape In 2024 ---------- *138*

By Neil Serebryany, CEO and Founder of CalypsoAI

New Year, New Consumer Demands in Cybersecurity: Navigating the Landscape of Consumer Expectations and App Developer Responsibility in Mobile App Security ---------- *141*

By Alan Bavosa, VP of Security Products, Appdome

Building a Better Perimeter Defense Strategy to Meet the Challenges of 2024 ---------- *144*

By Yiyi Miao, Chief Product Officer, OPSWAT

Ransom-War Escalation: The New Frontline in Cyber Warfare ---------- *148*

By Nissim Ben Saadon, Director of Innovation, CYREBRO

Reducing Burnout and Increasing SOC Retention: How Leaders Can Improve Their Employees' Lives and Improve Security ---------- 152

By Kayla Williams, CISO, Devo

Safeguarding Children in the Era of Big Data ---------- 155

By Ron Kerbs, CEO, Kidas

Securing Space Infrastructure for US And Allied Collaboration ---------- 159

By Kevin Kelly, CEO and Chairman, Arcfield

Understand Cyber Insurance: Rising Risks and How to Right-Size Policies ---------- 163

By John Reith, Partner Success Manager at DataStream Cyber Insurance

What You Need to Know About the Cybersecurity Market in 2024 ---------- 167

By Doug Saylors, Partner, Co-lead, Cybersecurity, Information Services Group (ISG)

Why Companies Are Still Investing in Tech During An Economic Slowdown ---------- 171

By Luke Wallace, VP of Engineering at Bottle Rocket

Why Higher Education Is So Vulnerable to Cyber Attacks — And What to Do ---------- 174

By Zac Amos, Features Editor, ReHack

With The World Distracted, China Stirs Trouble in The Asia Pacific ---------- 178

By Stan Vitek, Resident Geopolitical Analyst, Cyfirma

Wireless Peripheral Devices - Security Risk, Exploits and Remediation ---------- 182

By Prathibha Muraleedhara and Akhilesh Bhangepatil

@MILIEFSKY

From the

Publisher…

Dear Friends,

As we publish this first issue of Cyber Defense Magazine for 2024, celebrating delivering over 12,000 pages of content on our 12th year of operations, we would like to extend our appreciation to all participants in our publishing and promotional activities. As always, we are dedicated to bringing our contributors and readers the most up-to-date and actionable intelligence to conduct the most effective cyber security program to meet the challenges in our industry.

We take this occasion to remind our contributors and supporters that CyberDefenseCon 2024 has formally announced entries for Top Global CISOs for 2024, awards ceremony, networking with peers and speakers taking place October 31 - November 1, 2024 in The Ritz-Carlton, Orlando, Florida, USA.

More information about this invitation only five star conference is available at https://cyberdefenseconferences.com/

Let us also remind you of the CDMG Global Awards program at https://cyberdefenseawards.com/ , and the many participating professionals who have earned this important recognition for their contributions to the cybersecurity industry.

We continue to strive to be the best and most actionable set of resources for the CISO community in publishing Cyber Defense Magazine and providing the array of activities by Cyber Defense Media Group. With appreciation for the support of our contributors and readers, we continue to pursue our role as the premier provider of news, opinion, and forums in cybersecurity.

If you have any questions, ideas, or would like to learn about our advertising programs, or how to write for us please send an email to marketing@cyberdefensemagazine.com.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451
http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
https://www.cyberdefensemagazine.com/about-our-founder/

12 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense Magazine is your go-to-source for Information Security. We're a proud division. of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM
MAGAZINE TV RADIO AWARDS
PROFESSIONALS WIRE WEBINARS
CYBERDEFENSECONFERENCES

Welcome to CDM's January 2024 Issue

From the Editor-in-Chief

As we publish the first issue of the magazine for 2024, from my perspective as Editor-in-Chief, as well as our team of account executives and technical managers, we are gratified to receive important support from our contributors and readers.

In this issue, we bring you nearly 50 articles from a broad spectrum of technical experts, specialists in risk management, and others who share their experience and thoughts with other cyber security professionals.

It's a good reminder of the industry-wide community cooperation and support we enjoy to recognize that the vast majority of these articles come to us unsolicited. We do, of course, encourage submission and publication of topics we believe to be of most interest and applicability to our readers.

We continue to cover developments in artificial intelligence and regulatory actions, which together provide context for preparing cybersecurity protections for the present and the future. Recognition of challenges in the near term can help CISOs and their organizations and colleagues best prepare to overcome the ongoing threats in cyberspace.

As always, we are delighted to receive all 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 US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. 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


SPONSORS

RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

LEARNING.
NETWORKING.
INNOVATION.

THE TRIPLE THREAT FOR CYBERSECURITY SUCCESS.

RSA Conference 2024 will bring the cybersecurity community together again in San Francisco for four industry-shaping days, and you can be a part of that important conversation.

From May 6 – 9, you'll be able to:

- See what the future holds with the hottest industry topics and emerging trends
- Expand your knowledge and be inspired by forward-thinking Keynotes
- Demo the latest products to find real-world solutions from over 600 companies
- Enhance your career through valuable networking opportunities

Let's redefine The Art of Possible by shaping solutions, tackling challenges, and encouraging the collective strength of coming together as a community.

Act now for the biggest discount!

Visit www.rsaconference.com/cyberdefense24 to learn more and register.

#RSAC

FOLLOW US

THE ART OF POSSIBLE

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

• Deploy. • Manage. • Tune up. • Audit. • Defend. Report.

GET YOUR FREE eBook

Get https://cionsystems.com/

DAKOTA STATE UNIVERSITY

CYBER 27 INITIATIVE

< mission_BestCyberAnywhere />

The Cyber 27 Initiative is what's next for Dakota State University. Over the next five years, we're building new labs, forming new partnerships and pushing the limits of what a STEM university can do.

It's not just what's next for DSU.
It's the next chapter for cyber everywhere.

DSUcyber27.com

NIGHTDRAGON

***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

UNKNOWN
CYBER

"70% of Malware Infections Go Undetected by Antivirus..."

Not by us. We detect the unknowns.

www.unknowncyber.com

2001 2024

ALLEGIS CYBER CAPITAL

The first dedicated cybersecurity venture firm in the world.

AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.

For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.

BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER

Signifyd | SAFEGUARD CYBER | ELISITY | panaseer | Synack

SkyHive | cyber GRX | DRAGOS | CONCEAL | vArmour

ALLEGISCYBER CAPITAL

www.allegiscyber.com


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
quickcode
DRAGOS
ENVEIL
INERTIALSENSE
PREVAILION
the cyberwire
Ntrinsec
SIXMAP
STRIDER
CONTRAFORCE
BLACKCLOAK
SightGain
JOIN THE TRIBE
DATATRIBE.COM

CYDERES

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 **De**fense
& **Res**ponse.

It's what we do.

cyderes.com


ARTICLES

3 New Risks That CISOs Will Face in 2024

By Daniel Barber, CEO, DataGrail

Throughout 2023, data privacy has been front and center in conversations about cybersecurity. Consumers everywhere are increasingly vigilant about how their data is being gathered and used, especially with new technologies like AI creating fresh risks.

CISOs are leading the data privacy charge for their organizations. In a constantly changing environment, security leaders are always on the lookout for IT solutions that will shore up customer confidence and ensure regulatory compliance. And CISOs know best of all that failure to do so can have disastrous consequences.

In 2024, CISOs will need to adapt to a wave of new risks. Chief among these will be the challenges associated with AI, regulation and enforcement, and the very role of the CISO itself.

1. AI development and use will demand solutions.

AI poses new challenges for cybersecurity and regulators are taking notice. Just last week, EU lawmakers agreed on the core elements to regulate AI. It will require foundational AI models to comply with transparency obligations, and will ban several uses of AI, including the bulk scraping of facial images. It will also require businesses using "high-risk" AI to assess their systemic risks and report on them. The California Privacy Protection Agency (CPPA), the state's enforcement agency, also recently released its draft regulatory framework around "automated decision-making technology" (its description of AI), giving Californians the right to opt-out of their data being used in AI models.

No business can afford to simply ignore AI. Across sectors, the technology will be key to long-term innovation. How, then, can CISOs ward off the privacy risks that come with AI use internally and by vendors and other partners?

A first and necessary step is to recognize present limitations. Third-parties are likely to oversell solutions based on the promise of controlling AI, but we're not there yet. Before CISOs even think about control, they've got to get a handle on where AI is– and will be– used in their business. Discovering these points, and monitoring them, have to come before control because no one really knows how generative AI will evolve. For that reason, CISOs should be wary of any third-party solutions that claim to be able to harness this technology and its potential consequences.

Rather than buying into an illusion of control, CISOs should tap into their existing toolbox to further efforts at discovery and monitoring. Traditional tools still have value, even in the generative AI world. For instance, they can leverage ubiquitous network inspection to find calls to AI vendors unauthorized by the company's policies.Data mapping and detection can help cybersecurity teams know precisely where AI is being used in their organization and prevent shadow IT.

2. Data privacy regulation (and enforcement) will evolve.

When it comes to the data privacy market more generally, CISOs can expect one thing: change.

This is particularly true when it comes to regulation. While some agencies have kept pace with technological development, enforcement has been another issue entirely. As data privacy expert Anna Westfelt recently underlined, regulators around the globe currently face crippling personnel shortages and enormous backlogs.

While this was the case in 2023, other indicators give a better idea of what to expect in the months and years to come. In particular, data subject access requests (DSARs) continue to increase year over year. This reflects consumers' increasing concern with how their personal data is being handled; however, it also suggests that stricter DSAR enforcement is just around the corner.

For CISOs, this means that in addition to solutions for data mapping and AI discovery and monitoring, they need to begin thinking seriously about how they can efficiently respond to consumer demands for data transparency, be it through automated processes or other means. Doing so won't just protect their

organizations from fines stemming from regulatory violations—it will also increase consumer trust and buttress their brand.

3. CISOs will face greater scrutiny.

In 2023, CISOs faced considerable risks and challenges. Those tasked with this role often bear the brunt of data breaches and cyberattacks, a reality that often results in burnout, dismissal, and even legal consequences. As such, change is coming.

With so much weight on the CISOs shoulders, it stands to reason that CISOs of value will demand– and receive– higher compensation. They will also necessarily receive better indemnification guarantees, as well as an elevated profile within their organizations to break through the logjams created by corporate culture. Without a 'safe' space in which to perform their job, look for the truly qualified to take their talents elsewhere. Afterall, why should they remain in a position that holds them personally, legally responsible for outcomes in which other team members had a hand?

CISOs will solidify themselves as the torchbearers of risk in 2024 and beyond– but only if given the right mix of protection, compensation, and power.

About the Author

Daniel Barber is the Co-founder & CEO of DataGrail, the Privacy Control Center for modern brands to reduce risk and build trust. Prior to DataGrail, Daniel led revenue teams at DocuSign, Datanyze (acquired by ZoomInfo), ToutApp (acquired by Marketo) and Responsys (acquired by Oracle).

Spending much of his career working with data products and third-party apps, Daniel grew increasingly disturbed by the volume of personal information collected and how that data was used by the brands entrusted to keep it safe. He built DataGrail in response, believing that privacy is a human right.

Daniel has become a leading voice on data privacy, with his perspective regularly featured in outlets like TechCrunch, VentureBeat, USA Today, Fast Company, Fortune, and CNBC.

His insights in the field have also been distributed in security and privacy publications such as IAPP, CPO Magazine, Consumer Affairs, CIO Dive, and Dark Reading.

Daniel can be reached online at @gaijindan, https://www.linkedin.com/in/daniel-barber/ and at the company website: https://www.datagrail.io

How Small and Mid-Sized Businesses Can Achieve System and Organization Controls (SOC 2) Compliance

Steps To Implement Cyber Controls and Processes

By Juliana Spofford, General Counsel and Chief Privacy Officer, Aidentified

In today's tech world, it is often difficult to determine which businesses you can rely on to keep your data secure, and the matter continues to grow in importance as the cost of cybercrime is predicted to hit $8 trillions globally in 2023. Cybersecurity threats are on the rise, with ransomware, malware and threats from artificial intelligence and machine learning software foremost in our minds, and supply-chain threats are on the rise for all companies.

With growing security concerns, obtaining a System and Organization Controls (SOC 2) report, a gold standard for implementation of cybersecurity controls and processes, instills trust and attracts customers by proving that a company's security framework is reliable. Every business wants their customers and partners to rest assured knowing that security controls have been independently evaluated and rigorously tested in areas such as:

- Incident response
- Disaster recovery

- Access controls
- Vulnerability scanning and monitoring.

In 2021, Aidentified began our SOC 2 journey and obtained our SOC 2 Type 2 attestation. This accomplishment is a significant milestone for a small company, and you may be interested in how we achieved and continue to achieve SOC 2 compliance.

Here are key takeaways for small and mid-size companies with respect to the SOC 2 compliance process:

- Once your company has determined that it wants to pursue SOC2 compliance, it is important to pick your SOC2 partners and tools.

Not all tools are created equal, choose yours carefully. Aidentified partnered with Vanta as our Governance, Risk and Compliance ("GRC") SOC2 compliance tool. GRC tools are very helpful, especially for small and mid-size companies to assist with implementing and monitoring internal security programs with appropriate policies, security training, monitoring of devices, testing software vulnerabilities, vendor management and more. Aidentified also interviewed and selected independent SOC 2 auditors, Geels Norton, very early on in our SOC2 journey. Make sure your auditor aligns well with your team and tools and is willing to provide advisory services as you build out your SOC 2 program. Our auditors, for example, are adept at working with technology start-ups and are also a preferred assessor for Microsoft.

- Make sure you have buy-in for SOC 2 compliance at all levels of the company, including your Board of Directors.

Becoming SOC 2 compliant typically entails wide-spread changes to how you implement your internal company processes, and your company needs to understand this and should be committed at all levels and with all teams to prioritize SOC 2 requirements – from HR to customer service, to product and technology.

- Choose your SOC 2 team wisely.

You do not necessarily need to have employees with dedicated security information titles to be able to put a SOC 2 team together. You will need your Chief Technology Officer and designated security personnel on your technology team, and at a minimum, a program manager. This person can be an operations/legal operations dedicated resource, and one or two non-technology related back-end process resources. Aidentified also benefitted from the assistance of a compliance security consultant.

- Once you receive your first SOC 2 attestation, make sure you continue to monitor and improve your internal processes.

Do not make the mistake of becoming complacent once the first attestation is achieved. Continue to schedule your regular security review meetings, your access reviews, policy updates and SOC2 remediation check-ins based on the priorities included in your management letter to-do's.

Achieving SOC 2 Type 2 attestation is a sizeable undertaking for any company, but the designation is possible with the right plan and people in place. As cybercrime continues to grow in sophistication and frequency, we have a responsibility to ensure reliability of our security frameworks.

About the Author

Juliana is the General Counsel and Chief Privacy Officer for Aidentified, a leading AI-powered relationship-based prospecting and first-party data enrichment technology provider. She brings decades of legal experience and privacy expertise to her pointed in-house legal insights, having worked as counsel for both small data technology start-ups and powerhouse data services companies such as Dow Jones/Factiva and Dun & Bradstreet. She enjoys sharing her insights about compliance, privacy and security issues to help organizations do the right thing and understand the importance of these issues for their ultimate business success. Juliana can be reached at our company website https://www.aidentified.com/

Closing the Gap: Safeguarding Critical Infrastructure's IT and OT Environments

By Victor Atkins, Director | Cybersecurity, 1898 & Co.

The rise in the age of digitalization has provided numerous benefits for modern society, from the ability to conduct a telehealth doctor's meeting from the comfort of home to greater access to education for rural, isolated communities. Those who work in the critical infrastructure industry aren't strangers to the benefits — but also the downsides — of a more digitally connected world.

With an increase in streamlined, automated controls and the capability to work from remote locations, critical infrastructure decision-makers now have a greater ability to provide reliable services for the communities they serve. However, expanded access to critical infrastructure systems has led to information technology (IT) and operational technology (OT) systems becoming more vulnerable and susceptible to cybersecurity threats through a variety of attack vectors. These attack vectors can include any data communication pathways that hackers can exploit to illegally enter a network or system.

With critical infrastructure operations continuing to push toward more digitized solutions, IT and OT systems have become more integrated and dependent on each other. The increased connectivity between these two traditionally separated systems provides the opportunity for adversaries to gain access to either the IT or OT system, which if left unchecked by cybersecurity measures, can result in a major impact to the integrated environment. Quality of life and the stability that comes from knowing the

lights can be turned on at the flip of a switch or that the faucet at home never runs dry could be threatened without safeguarding attack vectors to prevent successful cyberattacks.

Feeling the Ripple Effect

While critical infrastructure may often be the target for malicious adversaries attempting to disrupt key services and day-to-day living, the ripple effect that comes from any organization facing a cyberattack can be widely felt. The initial target can often be just the starting point.

The recent conflict in Ukraine has become a case study example for how interdependent organizations that rely upon shared services have become. In a successful bid to render ViaSat's commercial satellite KA-SAT network inoperable to achieve military objectives, there was a ripple effect that spread into adjacent critical infrastructure domains causing a loss of critical public services in 2022. The same satellite services that supported Ukraine's military also supported European wind power generation, causing the shutdown of over 5,000 wind turbines in Germany that have total power output of 11 gigawatts.

The ransomware attack on Colonial Pipeline in 2021 was an example within the U.S. of what can happen when critical infrastructure operations are severely impacted. A ransomware attack resulted in the pipeline's digital systems being shut down for several days, halting a vital U.S. oil pipeline. Consumers and airlines alike were affected by the shutdown and resulted in President Joe Biden declaring a state of emergency. The attack was named the largest publicly disclosed cyberattack against critical infrastructure within the U.S. to date.

The purpose of the Colonial Pipeline attack was to collect a ransom but ultimately it led to a significant disruption to critical services that affected a large portion of the U.S. population. In both the Ukraine and Colonial Pipeline incidents, the effect of the cyberattacks extended well beyond the attacker's intentions. Given the many cyber interdependencies that exist, owners of critical infrastructure must prepare to be resilient to cyber incidents, even when not the intended target.

Another factor that is expanding the universe of attack vectors is the dramatic increase in remote work. Such work was required during the COVID-19 pandemic and launched a trend in decentralized workforces that is apparently here to stay. Owners and operators of critical infrastructure also had to adapt to these realities, enabling more remote access to operational control networks than ever before. Such an increase in access, especially for critical infrastructure assets, led to greater flexibility but also gaps in cybersecurity. With remote workers accessing crucial data, these individuals may have their own routers and configuration systems installed to complete work, resulting in unknown and unmonitored communications pathways to the OT environment. It's difficult to secure or monitor data communications pathways in and out of a critical system if the asset owner doesn't know these attack vectors exist.

In summary, cyber adversaries are leveraging these trends — the expanding number of vectors, including satellite and wireless communication networks, the growing shared dependence on third-party vendors, and the increasing number of network access points needed to accommodate remote workers — which is making critical infrastructure harder to defend from cyber incidents that result in downtime for key services.

Keeping Critical Infrastructure Secure

While it is unlikely to ever secure IT and OT environments 100%, risk reduction strategies can be put into place to prevent cyberattacks from becoming successful. Organizations should understand and prioritize the most critical operational functions that, if disrupted by a direct cyberattack or the loss of a key third-party service, would have a significant impact on the ability to operate. For instance, if a single facility accounts for 90% of a company's revenue or a single substation services a key national security site in a remote location, these assets are likely top priorities to keep operational and reduce downtime. Once these critical functions are identified, the organization can map the IT and OT network pathways that support these systems and implement security or engineering controls to reduce risks of downtime or failure.

Identifying and mitigating known vulnerabilities are also critical steps in the risk reduction process. Organizations can make significant gains by simply closing gaps that are widely known to exist. Installing cybersecurity sensors for 24/7 monitoring can also lead to faster mitigation action to limit damage from a cyberattack. Cyberattacks can occur at any time and having a dedicated team available on call to identify and respond to an incident can limit downtime and the potential for the event becoming a more widespread issue.

Closing vulnerabilities and implementing network monitoring are effective measures for reducing cyber risks in existing critical infrastructure but to really get ahead of the risks presented by a growing attack surface, cybersecurity and resilience should be addressed at the earliest design and planning phases of new projects. This kind of collaboration, commonly referred to as Cyber-Informed Engineering, consists of discussions among cybersecurity professionals, engineers and project designers to identify and address cyber risks in the control and safety of automated systems. When done at the front end, this approach can make the implementation of cybersecurity controls more effective, efficient and cost-effective rather than trying to add these measures on after the capital project is completed.

Adversaries often look for the path of least resistance when it comes to seeking an attack vector to take down a valuable asset. For critical infrastructure — or any organization — it's important to proactively safeguard systems to keep communities supplied with crucial services. Having a cybersecurity plan in place to identify potential vulnerabilities and putting a plan in place to respond to an attack are vital for maintaining the reliability and resiliency of critical infrastructure.

About the Author

Victor Atkins is a director of security and risk consulting at 1898 & Co., part of Burns & McDonnell. In his role, he develops and delivers industrial cybersecurity solutions and services to the critical infrastructure industry. He specializes in helping clients reduce risk in the critical infrastructure sectors. He is a nonresident senior fellow at the Atlantic Council, focusing on cybersecurity, hyperintelligence and nuclear security.

Victor can be reached online at victor.atkins@1898andco.com and at our company website https://1898andco.burnsmcd.com/about-us/our-people/victor-atkins

Addressing the Particular Cybersecurity Challenge of Discrete Manufacturing

By Dave Purdy, Regional Vice President of Sales, North America, TXOne Networks

Though it's often treated as a borrowed approach from the information technology (IT) world, cybersecurity for operational technology (OT) is best tackled as its own unique challenge. The pain points, protocols and tradeoffs to be balanced are fundamentally different in OT than in IT.

Perhaps in no industrial environment is this distinction more clear than in discrete manufacturing, where the pressure is most extreme to maintain unit volumes while, at the same time, protecting the safety of machines and the lives of the people who work with and near those machines. Discrete manufacturing offers an unusually delicate balance of factors and forces that OT managers must constantly maintain in cybersecurity.

What are the particular requirements and characteristics of OT cybersecurity in discrete manufacturing, and how do these weigh into decisions around implementing effective solutions for this environment?

The Distinct OT Cybersecurity Environment

OT cybersecurity is *not* IT cybersecurity applied in a plant-floor setting. The protocols and network languages that drive operational automation are totally different than what are common in IT environments. OT protocols are highly specialized, and there are hundreds of them.

Many of the technologies are several decades old. The electric grid, for example, is driven by technologies that were invented in the late 1940s and '50s. Modbus is a client/server protocol that is commonly relied upon for communication among industrial electronic devices in a tremendous range of domains, and it was originally published in 1979. These protocols were conceived and grew up in a climate without IT concepts of, for example, encryption and cybersecurity.

Plus, because today's high-speed manufacturing environment is so hypersensitive to networking latency, OT protocols cannot have the tremendous number of lines of code that are often found in sophisticated IT protocols.

The Distinct OT Needs in Discrete Manufacturing

Discrete manufacturers produce distinct unit volumes that can be disassembled, such as a car, a bicycle or a piece of furniture. Asset owners in this manufacturing sector are very focused on production volume, product quality, production uptime (availability) and, most importantly, human and asset safety. In the context of cybersecurity, the challenge for the asset operator is to implement solutions that impair none of these sometimes-competing priorities.

It's not uncommon for security solutions to be implemented in the OT space which err on the side of caution. The problem with such an approach is expensive overkill—they kick up alerts for relatively innocuous network events, and, in some cases, shut down production (and revenue streams) based on false positives.

The Growing Issue of OT Cyber Threats

Because adopting protective capabilities without jeopardizing revenues, operations and quality has proven so challenging, many discrete manufacturers have chosen and continue to simply "roll the dice" and do nothing to safeguard their OT environments. Or they might have a false belief that plants are "air gapped" from the threats found in IT and the internet. Or they rely on upstream IT security solutions with the false hope that threats will be blocked from reaching their production lines.

Until recently, they might've gotten by because the threat probability in OT historically has been low. There's very little debate, however, that the OT cyber threat landscape today is growing substantially—a fact borne out by the skyrocketing cyber insurance rates that many companies are confronting. In the wake of high-profile incidents like the May 2021 ransomware attack on the Colonial Pipeline, the cybersecurity insurance industry is increasingly asking very specific and tough questions around what cybersecurity mechanisms that a company has put into place in the OT space.

Driven by the cost to be insured or the ability to be insured at all, the cost of downtime because of attacks and the potential lasting brand damage in the wake of attacks, more and more discrete manufacturers are taking a fresh or even first look at OT cybersecurity.

What Can Be Done? What Must Be Taken into Account?

OT attacks are often missed by traditional IT cybersecurity tools, which fail to address risk vectors such as industrial control system (ICS) protocols, infected equipment getting installed into a production process or third parties entering a factory to perform maintenance.

Discrete manufacturers require OT-specific endpoint solutions. The endpoints to be protected in a production facility tend to be a human machine interface (HMI), a remote terminal unit (RTU), an engineering workstation (EWS) or supervisory control and data acquisition (SCADA) for overseeing machines and processes around critical and time-sensitive materials or events. IT cybersecurity tools typically are not predicated on the understanding of such endpoints and, therefore, fail to sufficiently safeguard them.

Because OT networks tend to be flat—all network elements connecting to and communicating with each other—OT cybersecurity demands a micro-segmentation capability so that attacks are isolated and unaffected manufacturing lines are kept open and firing. Plus, the system must be able to recognize OT protocols from other traffic that doesn't belong on the OT network through real-time inspection and act intelligently and swiftly to avert or mitigate the damage of attacks.

Insider threat is another important threat vector in OT cybersecurity. The individuals that come into a plant setting to perform maintenance can introduce malware in a non-malicious manner from a USB drive, for example. There have even been cases of brand-new equipment coming into a manufacturing setting that's been pre-infected. Repurposed IT tools are not built to recognize or act on these threats.

Finally, IT tools tend to be built to protect confidentiality, integrity and availability of assets and data in that order. OT cybersecurity demands the opposite approach. The individuals who run these plants are rewarded for how many widgets of a sufficient quality that their plants produce. The OT cybersecurity tools at their disposal must, consequently, emphasize availability over integrity and then confidentiality.

Conclusion

No company wants to be shut down because of a ransomware attack, but nor can a company afford to implement a complex security solution that hinders operations and generates false positives resulting in unnecessary interruptions. This is the vexing challenge in which OT managers for discrete manufacturers find themselves with regard to cybersecurity.

Simply extending IT security products and approaches into industrial settings, however, is insufficient for the emerging threat landscape. To safeguard assets, revenues, operations and revenues, discrete manufacturers require cybersecurity solutions built from the ground up for the unique requirements of OT.

About the Author

Dave Purdy is the Regional Vice President of Sales, North America at TXOne Networks. He is a veteran technology practitioner with a career-long focus on critical infrastructure protection and downtime avoidance. Dave's industry experience has had a central focus on business and operational resiliency spanning global financial services, power generation, utilities, defense contractors, and manufacturing. Prior to joining TXOne Networks he held various leadership positions at AWS, EMC Corporation, and IBM Corporation. Dave can be reached at Dave_Purdy@txone.com and https://www.txone.com/?utm_source=CyberDef.

AI in DevSecOps: Moving from A Co-Pilot to An Autopilot

By Stephen Chin, VP of Developer Relations, JFrog

What do autonomous driving and software (SW) development have in common? At first glance, not much. But when taking a closer look under the hood you'll begin to see some similarities, especially in the evolutionary path towards underlying targets. Development teams won't become "passengers" per se, but the traditional roles and responsibilities of the personas involved in designing, creating, securing, distributing, and operating SW will begin to shift. To connect the dots, let's begin by delving into the concept of autonomous driving and then relate it back to SW development.

The concept of autonomous driving has been around for years, and what once seemed like a futuristic concept is today's reality. At their core, autonomous vehicles (AVs) are aimed at minimizing human errors in traffic, accounting for ~90% of accidents today. The fundamental premise of AVs is that they should outperform an average human driver. Importantly, self-driving technology has the potential to free up an extremely valuable resource: time. This enables people to devote their focus to more gratifying pastimes instead of being tied up in traffic.

Two critical enablers for autonomous driving are Edge and AI: empowering vehicles to process IoT sensors' data within the vehicle itself and by doing so, enabling real-time operations. This capability is crucial for any mission-critical applications. Attempting to manually program the machine to handle every possible driving scenario becomes an impractical endeavor. Instead, the vehicle must dynamically learn from its environment. The intelligence of an AV hinges on the availability of various IoT sensor data, allowing the creation of a digital representation (a twin) of the physical world. The more diverse the data, the more sophisticated AI systems can be deployed.

When observing the evolution path of autonomous driving, we can notice a gradual reduction in human involvement at each stage. The AV framework includes 6 levels of automation ranging from 0 (fully manual) to 5 (fully autonomous).

- No automation: the driver retains complete control of all driving tasks.
- Driver assistance: the vehicle incorporates a single automated system that allows the driver to take their foot off the pedal.
- Partial automation: the vehicle becomes capable of handling steering and acceleration, allowing the driver to take their hands off the wheel.
- Conditional automation: the vehicle can control most driving tasks, enabling the driver to take their eyes off the road while still maintaining supervision.
- High automation: the vehicle performs all driving tasks under specific conditions, giving the driver the opportunity to take their mind off the road while remaining alert.
- Full automation: the vehicle can independently handle all driving tasks under any conditions. This transforms the driver into a passenger, completely freeing their mind from all driving responsibilities.

The benefits of AI in SW Development largely mirror those seen in autonomous driving:

Minimizing human errors and freeing-up time for more creativity-intensive work. Since human resources are often the costliest aspect of SW development, organizations are incentivized to adopt AI-based systems that can enable them to do more with less.

Closer examination of the SW development evolution paths reveals striking similarities to the advancements in autonomous driving: gradual reduction in human involvement at each stage of evolution:

- **In the early 2000s,** SW Development had little to no automation. Human control was required at every stage of the SW Development Lifecycle (SDLC), making the process largely manual. Issues were often identified by customers rather than internal teams.

- **Fast forward to the mid-2010s**, we witnessed the rise of Containerization, Cloud Computing, and DevOps, leading to increased automation and efficiency throughout the SDLC. Routine tasks and procedural decisions were automated based on predefined (hard-coded) policies and "if-then"

-rules in areas such as testing, code review and CI/CD. This allowed R&D teams to focus on creative aspects of their work with increased productivity - enabling “guided steering and acceleration”. Development cycles shortened based on agile principles, bridging Dev and Ops. Issue management and resolution started to shift from reactive to adaptive with more seamless coordination across teams. The majority of issues could be detected and fixed before customers even became aware.

- **Today,** Generative AI is taking SW development to new levels of efficiency and innovation. Automation extends far beyond routine tasks, as GenAI-based solutions enable the creation of new content through a seamless human-to-machine dialogue. Efficiency gains are only just beginning to unfold as AI can act as an inexhaustible assistant (Copilot) throughout the SDLC by providing suggestions, explaining issues, generating code, monitoring processes, scanning repositories, providing predictions, and augmenting quick decision-making. This will further accelerate and increase the overall code creation, translating into more SW builds, more SW to be secured, and more frequent updates to the runtime. As we add embedded AI models (MLOps) into the modern SW development equation, the aforementioned areas expand even further. The concept of "Liquid Software" is gradually becoming a reality, where small incremental improvements (binaries-based updates) automatically flow from development to runtime with minimal service downtime.

- **In application security,** AI can significantly reduce the time to discover and remediate issues in a predictive manner, preventing malicious SW packages from ever entering an organization in the first place. This begins with automated vulnerability scanning and detection, utilizing AI-based severity and contextual analysis, and extends to automated remediation. Despite the aforementioned advancements, human intervention and approval are still necessary until AI-based solutions demonstrate a higher degree of trust and reliability.

- In recent years, we began transitioning towards a full automation paradigm, wherein we move from a Copilot (AI assistant) to an Autopilot (AI decision-maker). Machines can be directed to solve highly complex problems through a natural language UI (i.e. English), requiring new types of skills from the programmer to navigate the dialogue towards the intended state. Fundamentally, the AI system should outperform an average human developer or other persona involved in said processes. AI will further augment and automate decision-making processes, enabling organizations to select the best possible (data-driven) approach and tools to resolve any issues. Trust in AI systems will be paramount, necessitating vast contextual understanding and ethical decision-making, similar to the challenges experienced in autonomous driving today. Self-learning and self-healing capabilities will become essential in detecting, analyzing, isolating, and patching issues while maintaining service uptime. Meaning: software will be able to rewrite an update itself, as well as add new functionality to deal with new inputs. Similarly, to AVs, the AI system must learn from its operational environment and adapt accordingly.

In conclusion, while the parallels between autonomous driving and SW development may not be immediately apparent, both fields share the common objective of harnessing the power of AI to enhance their operations and to free time for individuals to focus on more gratifying pursuits. In the context of SW development, AI will continue to accelerate and improve the creation of new features and data, elevating the UX of various R&D personas and evolving gradually from a trusted advisor towards an elevated decision-making autonomy. AI-based Copilots will slowly start to become more mainstream throughout SDLC, starting from Intelligent Coding and Security and extending to cover the full DevOps stack. Businesses must adhere to responsible and secure AI principles and practices to ensure sustainable outcomes. This includes areas such as protecting their IP and avoiding potential security and license compliance issues in AI generated Software. Embracing progressive autonomy of AI systems will allow and ensure compatibility with existing infrastructures and regulatory environments.

As AI technologies continue to advance, we can anticipate even deeper integration and innovation in SW development. We are living in exciting times as AI continues to transform industries. The future of SW development is promising, and the degree of development responsibility we can entrust to machines may only be limited by our imagination.

About the Author

Stephen Chin is VP of Developer Relations at JFrog. Stephen can be reached at our company website: https://jfrog.com/

AI-Enhanced Identity Fraud: A Mounting Threat to Organizations and Users

Identifying the most common AI-enhanced cyber-attack methods and strategies to mitigate them

By Philipp Pointner, Chief of Digital Identity at Jumio

While AI-driven automation brings benefits, it also gives hackers advanced tools to develop more sophisticated methods for a wide range of malicious activities like fraud, disinformation and cyberattacks. To combat these threats, enterprises must implement robust risk management strategies.

In this article, we'll walk through today's AI-enhanced cyberattack methods, and steps for security leaders to prevent these threats. These steps include leveraging advanced strategies, such as comprehensive identity verification, biometric authentication and liveness detection, to ensure the safety and security of their enterprise.

Advanced AI-Powered Attack Methods

With generative AI frameworks at their fingertips, hackers are crafting increasingly convincing scams that bypass traditional cybersecurity measures. This is exemplified in the evolution of phishing scams. As fake emails were once underdeveloped and easy to detect, generative AI has enabled fraudsters to craft much more sophisticated, professional-looking messages that are harder to identify as fraud.

Some of the other prominent attack methods raising concern among businesses include:

1. **FraudGPT:** Hackers are exploiting a new product being sold on the dark web called FraudGPT, which was built solely for the purpose of enhancing fraud and scamming techniques. FraudGPT is an LLM without the same filters and limitations as ChatGPT, enabling users to generate information such as the curation of malicious code, locating vulnerabilities, identifying vulnerable targets and more - making it a powerful weapon for cybercriminals, and a danger to organizations and their users.

2. **Password guessing:** The deployment of AI-supported password guessing — also known as AI-assisted password cracking — is a tactic that uses AI techniques to guess or identify passwords. Similar to phishing, this technique uses machine learning algorithms to enhance password matching, accelerating and optimizing traditional password stealing processes. In fact, hackers can steal passwords with up to 95% accuracy when leveraging AI.

3. **Deepfakes:** These synthetic creations, crafted with AI and featuring eerily realistic faces, are evolving at an alarming pace. A recent study revealed a worrying trend: 52% of people believe they can identify a deepfake video. This overconfidence is dangerous, considering these digital doppelgangers can fool even the most discerning eye.

   The corporate world is now becoming a prime target for deepfake fraud, as high-level executives are falling victim to AI-powered scams. For example, voice cloning is now being used to impersonate C-suite individuals, which allows hackers to mimic the victim's voice and orchestrate elaborate fraud schemes within the company. The CEO of a major security enterprise recently learned this the hard way when a cloned voice impersonated him, attempting to pull off a corporate heist.

As AI-supercharged cyberattacks increasingly wreak havoc, security leaders must ramp up their defenses to shield themselves and their users.

Turning the Tables: Make AI a Cybersecurity Shield

As organizations are bombarded with AI-powered attack methods, how do they fight back? To stay one step ahead of the next threat, security leaders can fight fire with fire, leveraging AI-powered security tools including:

Adaptive learning: Modern solutions are equipped with adaptive learning capabilities, which provide continuous refinement in authentication precision over time, learning from every individual user interaction. As generative AI-powered attacks evolve each day, this function is critical to keeping pace with threats. Today's tools also enable user-friendly interactions across multiple devices and adhere to compliance and regulatory practices within industries including finance.

Biometric authentication: This is another critical tool capable of deterring identity scams and fraudulent attacks, introducing an additional layer of security that outperforms traditional methods.

Advanced liveness detection: This is an AI-enabled offering that can deter fraudsters attempting to deploy deceptive impersonations. This tool is comprised of algorithms that leverage neural networks to assist in defending against fraudsters, identity spoofing and theft attempts to bolster fraud prevention.

Keeping Pace in an Evolving Digital Landscape

AI-powered identity fraud tactics will only continue to evolve, making it crucial for businesses to adopt robust, modern defense strategies to protect their ecosystems. By deploying strategies including the integration of solutions equipped with advanced liveness detection, biometric authentication and adaptive learning capabilities, security leaders will bolster the security of their infrastructure and the safety of their users' sensitive data amid a continuously evolving digital threat landscape.

About the Author

Philipp Pointner is a seasoned security and identity expert with over 20 years of industry experience and currently spearheads Jumio's strategic vision in advancing digital identity solutions. He is a frequent speaker and panelist at international conferences and for various media formats. Before joining Jumio, Philipp was responsible for paysafecard, Europe's most popular prepaid solution for online purchases. Philipp has a BSc in International Business Engineering from the University of Applied Sciences Technikum in Vienna and in his spare time enjoys teaching scuba diving to adults and children. Philipp can be reached online at our company website https://www.jumio.com/

Why Cybersecurity Maturity Model Certification (CMMC) Matters for All Businesses, Not Just DoD Contractors

A Vital Set of Cybersecurity Best Practices

By John Funk, Creative Consultant, SevenAtoms

A new cybersecurity mandate being rolled out by the Pentagon has implications that reach beyond the military industrial base. Business leaders who adopt Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) have an opportunity to upgrade their organization's security posture from low-hanging fruit to a hardened attack surface.

The U.S. Department of Defense (DoD) has been working on unifying the way military contractors and supply chain organizations protect sensitive information linked to national security dating back to 2010. Prior to developing the CMMC concept (and the follow-up CMMC 2.0), companies followed a variety of security protocols. Inconsistency and failures to maintain adequate cybersecurity measures resulted in

unnecessary data breaches. Security officials at the DoD found themselves handing out penalties and fines after hostile nation-state actors had already pilfered off critical data.

"Here's the bottom-line challenge we all face. If we get this wrong, and we do too little, there is a vulnerable supply system that is compromised and weighed down when we need it," CEO of the National Defense Industrial Association David Norquist said. "For national security, we need to protect against both disruption as well as tampering. But what makes a market so powerful is exactly what makes this challenge so hard."

CMMC 2.0 brings more than 100,000 contractors and subcontractors under one policy, requiring ongoing certification. These same protocols required by the DoD can deliver the heightened cybersecurity every operation needs to defend against the relentless stream of cyberattacks.

How CMMC 2.0 Works

This cybersecurity policy evolved from standards published by the National Institute of Standards and Technology (NIST). An initial model included five cyber hygiene levels that applied to outfits based on the type of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) the enterprise stored and transferred. The five tiers were revised down to the following three in the CMMC 2.0 version, which is gradually being implemented.

- **Level 1:** Considered "Foundational" cyber hygiene, supply chain organizations that store or transmit FCI are required to follow 17 practices to meet 59 objectives. Companies that fall under Level 1 are tasked with self-assessments and reporting the findings to the federal government.
- **Level 2:** Protecting CUI, this "Advanced" cyber hygiene standard tasks companies with adhering to 110 NIST practices to achieve more than 300 objectives. Depending on the type of digital assets, companies can report annual self-assessments or be vetted by a CMMC Third Party Assessor Organization, also known as a C3PAO.
- **Level 3:** Recognized as "Expert" cyber hygiene, military contractors and enterprises with critical CUI must meet more than 110 NIST measures, as well as other related defenses. Companies undergo an audit every three years by a C3PAO, with the outcome reported to the Pentagon.

Businesses that fail to meet the CMMC 2.0 mandate will likely find themselves sidelined. Losing revenue streams from lucrative DoD contracts tends to be more whip than carrot in the push to secure sensitive military defense secrets. But that does not necessarily mean businesses should implement CMMC 2.0 solely to gain DoD approval. The cybersecurity policy proves equally effective at repelling hackers trying to infiltrate networks out of greed.

What CMMC Accomplishes

It's essential for business leaders to understand that cybersecurity measures are not necessarily industry specific. Anti-virus software packages, enterprise-level firewalls, virtual private networks, and other commonly used data protection strategies are deployed across the healthcare, financial, manufacturing, and military industrial base. Cybersecurity professionals and software developers continue to find new ways to protect sensitive and valuable digital assets, including those in the military supply chain, to respond to newly minted hacking schemes. The point is that the following controls, embedded in CMMC 2.0, can deliver a determined cybersecurity posture that benefits any business.

Access Control

The DoD mandate requires outfits to impose network access limits on legitimate users, including internal and remote access to information on a network. The concept of limited data access mirrors that of the "zero-trust" profiles cybersecurity experts recommend companies utilize. This essentially prevents any user from gaining access to sensitive and valuable information that isn't necessary to complete their respective tasks. Should a hacker learn someone's login credentials, the criminal runs into the same restrictions.

Awareness and Training

Providing cybersecurity awareness training to employees is not restricted to the military industrial base. Studies indicate that human error accounts for 88 to 95 percent of all data breaches. When companies integrate awareness training into their security plan, employees are far less vulnerable to phishing schemes and social engineering. Instead of being a weakness, staff members become a front line of defense. That's precisely why CMMC 2.0 insists workforces know the telltale signs of a hacking threat.

Risk Management

Commonly referred to as "cybersecurity risk management," this concept speaks to how industry leaders invest in data security. A third-party managed IT firm with cybersecurity expertise typically runs a risk assessment to determine a system's strength and vulnerabilities. Then, business leaders review the risk assessment report to make informed decisions about how to deploy their resources. The conventional wisdom is that critical data and vital systems enjoy the greatest protection and security investment. Only by understanding risk can strategic policies and best practices be established in any organization.

Incident Response

Organizations that operate within the military industrial base face advanced persistent threats from America's adversaries. These threat actors possess the funding, tools, technologies, and sophisticated

hacking skills to penetrate networks with robust defenses. The DoD understands these cybercriminals can drill down and find a way into critical systems. That's why CMMC 2.0 tasks companies with crafting an incident response plan. Each company requires a nuanced incident response plan that fits its processes, goals, and secures its digital assets. However, the fundamental idea of having an up-to-date strategy to respond to emerging threats and protect digital assets remains ubiquitous across sectors.

Why CMMC 2.0 Makes Sense for Wide-Reaching Businesses

Foreign threat actors typically attack U.S. military supply chain businesses to gather bits of information to better clarify America's national security plans. This may entail stealing CUI and FCI or infecting a subcontractor's system with malware in hopes it will spread to high-value targets. Similar supply chain attacks are taking place across the private sector, leaving no organization safe from ransomware, spyware, or other malicious applications. By adopting CMMC 2.0 as a comprehensive data protection strategy, businesses have the ability to deter, detect, and expel garden variety hackers and sophisticated cybercriminals alike.

About the Author

John Funk is a Creative Consultant at SevenAtoms. A lifelong writer and storyteller, he has a passion for tech and cybersecurity. When he's not found enjoying craft beer or playing Dungeons & Dragons, John can be often found spending time with his cats. John can be reached online at johnfunk@sevenatoms.com or at www.sevenatoms.com

AI: The Human Touch in Cybersecurity Recruitment

Harnessing the Digital Scout for Cybersecurity's Future

By Darrin Straff, Senior Staffing Consultant, NinjaJobs

Introduction:

In the digital age, where cybersecurity threats are ever-evolving, AI's role in strengthening our defenses has become invaluable. But its potential doesn't end there; AI is also reshaping how we identify and nurture the next wave of cybersecurity talent. For CISOs, AI is a powerful tool, offering innovative ways to build robust teams equipped for the future.

AI as a Cyber Scout and Mentor:

AI shines as a talent scout – pinpointing promising candidates by analyzing their digital interactions and contributions. It can tailor individual development plans, providing a personalized approach to upskilling team members, ensuring they possess the most current and in-demand cybersecurity skills.

Embracing Challenges:

While AI's capabilities are impressive, it's essential to acknowledge the challenges. AI may not fully grasp the subtleties of human interaction or the importance of a cultural fit, and there's a risk of over-reliance on technology in making hiring decisions. CISOs must balance AI's efficiency with human judgment to maintain a personal touch in the recruitment process.

Actionable Steps for CISOs:

Here are some steps CISOs can take to integrate AI into their hiring and development processes effectively:

- Start small with a well-defined AI pilot program.
- Maintain transparency in the AI-driven recruitment process.
- Regularly review AI tools to ensure they remain aligned with the organization's evolving needs.

Staying Informed with Research:

Emerging studies have started to underscore the significant role of AI in enhancing recruitment processes. For instance, research suggests that AI can extend beyond the capabilities of traditional recruitment methods by analyzing large datasets to predict candidate success and job performance with greater precision. These AI systems can assess a candidate's fit based on their digital footprint, work samples, and even subtle cues in their communications.

Further, AI's ability to learn and adapt over time means that it can continually refine its selection criteria. However, it's critical to stay updated on the most recent advances and discussions in this space. Journals like 'Journal of Applied Psychology' and conferences such as the 'International Conference on Machine Learning' regularly publish insights that can shape future AI strategies. By leveraging these resources, CISOs can ensure that their use of AI in recruitment is grounded in proven research, aligning cutting-edge technology with the nuanced needs of their organizations.

Conclusion:

AI is reshaping the cybersecurity landscape, offering CISOs an innovative pathway to build teams that are not only technologically adept but also diverse and adaptive. This blend of AI's analytical capabilities

with human intuition creates a powerful synergy. By utilizing AI, CISOs can foster a workplace where talent is nurtured based on a deep understanding of both data-driven insights and the invaluable nuances of human judgment. It's a partnership that doesn't just fill positions but cultivates a cybersecurity force equipped for the evolving challenges of the digital world. The future of cybersecurity is not only about the threats we face but also about the teams we build to counter them, and AI is becoming a pivotal ally in this mission.

About the Author

Darrin Straff is the Senior Staffing Consultant of the NinjaJobs. He blends insight into human behavior rooted in a bachelor's degree in psychology with 14+ years of recruiting experience to navigate the complex landscape of cybersecurity talent acquisition. Darrin excels not just in aligning technical skills with business needs but also at understanding the critical human elements that underpin strong candidate-client relationships. His comprehensive approach extends beyond mere placements, advocating for secure and synergistic connections in our digitalized professional world. Darrin can be reached online at dstraff@ninjajobs.org or www.linkedin.com/in/darrinstraff and at our company website http://www.ninjajobs.com

Beyond Traditional Cyber Defences: The Rise of Outcome-Based Security In Modern Business

By Paul Brucciani, Cyber Security Advisor at WithSecure™

Cyber security is no longer just about keeping systems and devices safe, it's also become central in enabling business to achieve their strategic objectives.

Paul Brucciani, Cyber Security Advisor at WithSecure™, has important information about helping organisations overcome challenging times, and shedding light on how the outcome-based security mindset can be a game changer.

He offers this Q&A format presentation on Outcome-based Security in Modern Business.

How does shifting from a reactive approach to an outcome-based security approach enhance an organisation's security posture?

Organisations are finding it increasingly tough to manage cyber threats. According to a study by Forrester, commissioned by WithSecure, 75% of organisations have placed cyber security on their priority list, influenced by a combination of global events, digital transformation and tightening regulations. However, adversaries constantly evolve their methods, catching many off-guard.

Even with budget hikes, 90% of global IT decision-makers are in a constant scramble to counteract these ongoing threats. Many companies are on the defensive, reacting to threats as they come. The study found that 60% of companies operate in this 'fire-fighting' mode, leading to a mismatch in team efforts, processes, and tech tools.

One way to get beyond this cycle is by embracing an outcome-based approach to security, which provides a clear direction for cyber security measures. This emphasises the outcome of cyber strategies, rather than security activity itself. Also known as ‘servitisation’, the outcome-based approach has been around for many years in fields like manufacturing. But with cyber security being a relatively young industry, it’s a new concept in this field.

The idea is to seamlessly weave cyber security into the business fabric, positioning it as an enabler through which organisations can achieve their strategic objectives. Companies are turning to an outcome-driven cyber security strategy to enhance business results, bolster resilience, and elevate productivity and competitiveness, all while safeguarding their operations.

It's a strategy that places the focus on tangible outcomes a strategy which not only helps in fending off unforeseen challenges but also positions cyber security as a catalyst for business growth.

How does proactively prioritising and safeguarding critical business assets lead to a higher ROI?

Imagine driving with an outdated map and suddenly finding infrastructural advancements that have left you feeling lost. Transitioning to an outcome-based security model is much like changing your navigation method from traditional maps to modern GPS. The starting point is to establish clear goals that resonate with business ambitions, such as enhancing risk management, optimising customer experience, or strengthening operational agility. One useful approach here is the ‘security canvas’, mapping out key initiatives, resources, and costs, and balancing them against opportunities, risks, and business outcomes.

As Forrester outlines, outcome-based security is all about harnessing capabilities that help to achieve these set objectives. This means that your risk management plans need to be in harmony with these organisational aims. It's not just about building walls but strategically placing watchtowers to see and counter potential threats.

Most importantly, this transformation calls for a fresh viewpoint. Instead of seeing cyber security as a cost centre, businesses should recognise its potential as a key driver of growth, helping the organisation achieve key objectives such as securely rolling out new services or helping teams collaborate safely. By

doing so, not only can companies propel their development, but they can also elevate their stature in the marketplace, which leads to higher ROI.

What are some of the challenges organisations face when trying to align cyber security strategies with business outcomes?

One significant roadblock organisations grapple with is the need for clear visibility into cyber threats. There's minimal margin for error in cyber risk management, and stakeholders – from boards and investors to customers – demand a crystal-clear view of a company's cyber security strategy. Yet, in our study, 41% of professionals have expressed difficulties in achieving this visibility.

Additionally, there's the pressing issue of talent acquisition. Just over a third of businesses, 35%, find it challenging to hire skilled cyber security professionals without breaking the bank.

Alongside this, most cyber threats are time-sensitive, and organisations find themselves in a tricky spot, often unable to respond promptly due to this limited visibility. This has further hindered the synchronisation of cyber security efforts with broader business objectives.

Cyberspace can be likened to a rapidly growing city, with new constructions popping up every day, making the landscape more intricate. 37% of professionals have pointed out how this expanding digital territory makes even the most fundamental cyber security tasks challenging. So, how do we navigate this bustling cityscape?

Organisations must adopt a well-structured cyber security roadmap, offering a bird's-eye view of their entire IT territory, pinpointing potential hazards, delivering business benefits, and enhancing operational efficiency. Investing in cutting-edge tools is key. These digital watchdogs, powered by machine learning such as artificial intelligence, keep an eye on your network in real-time and foresee potential threats. With such tools at their disposal, organisations can take the front foot, intercepting cyber threats before they snowball into larger crises, ensuring a smoother journey in the digital domain.

One other challenge to consider is dealing with radical uncertainty – unexpected events that cannot be anticipated. In a cyber context, this usually means the appearance of totally new technology or attack techniques. It is impossible to plan ahead for these 'unknown-unknowns'. However, businesses that have a well-established security canvas will be better positioned to cope with radical uncertainty, while those still struggling to align business and security objectives will be more wrong-footed by the unexpected.

About the Author

Paul Brucianni, Cyber Security Advisor at WithSecure™

"My cyber security career began shortly after the World Wide Web was invented. I am a cyber security advisor at WithSecure, one of Europe's largest cyber security companies, headquartered in Helsinki.

I have an eclectic, largely unplanned early-career working as a gold-prospecting geologist, satellite imaging specialist, system engineering consultant, barista, baker and a teacher. I am a Fellow of the Chartered Institute of Information Security and a regular blogger on topics related to cyber security risk and uncertainty."

Paul can be reached online at LinkedIn and at our company website www.withsecure.com

Ai, Cybersecurity Awareness, And Communication

Moving beyond the hype, are AI cybersecurity solutions as advanced as they claim?

By John Trest, Chief Learning Officer, VIPRE Security Group

The emergence of numerous AI-driven cybersecurity products emphasizes the significance of AI in the field. However, it is essential to move beyond the hype and take a realistic look at AI's capabilities, considering its vast scope and varying levels of sophistication. Are the solutions offered truly as advanced as they claim?

Current AI technologies operate above automation, utilizing algorithms, machine learning, and natural language processing. As a result, many of the products may not be as sophisticated as customers perceive them to be. It's important to clarify that the primary purpose of AI products is to streamline and automate repetitive tasks, provide quick access to information, and facilitate faster decision-making. Essentially, they complement human intelligence with technology, enabling more rapid processing of complex data that would pose challenges for humans.

AI-powered programs assist developers in creating personalized outlines and templates for their code, similar to predictive coding or chat functionality. While these benefit organizational efficiency, it is also essential to acknowledge the adversarial impact of AI.

AI and cybersecurity

Cybercriminals also leverage AI technologies to their advantage. For example, malicious applications can collect and process personal data much faster than humans, enabling cybercriminals to engineer more sophisticated phishing emails and create malware more efficiently.

These threats have been extensively highlighted in discussions on dangerous attack techniques. We're only beginning to see the scope of these attacks and the approaches attackers are developing because of this technology. The rapid advancements in AI technology have opened up new avenues for attackers to exploit vulnerabilities and launch sophisticated attacks. As AI algorithms become more powerful and capable, cybercriminals are leveraging these advancements to amplify the scale and effectiveness of their operations.

The true scope of AI-driven attacks is still unfolding as attackers continuously evolve their tactics and techniques. The integration of AI enables them to gather and process vast amounts of data with remarkable speed and precision. This newfound capability empowers cybercriminals to develop more sophisticated and convincing phishing emails, making it increasingly challenging for individuals to discern between genuine and fraudulent communications.

Moreover, AI enables attackers to create malware that adapts and evolves in response to changing security measures. By leveraging machine learning algorithms, malicious actors can analyze the behavior of security systems, identify weaknesses, and craft tailored attacks that evade detection. These AI-powered attacks can potentially infiltrate organizations, compromise sensitive data, and inflict substantial damage before detection.

Furthermore, as AI advances, we are only beginning to scratch the surface of the scope and scale of these AI-driven attacks. The rapidly evolving nature of AI technology means that attackers constantly refine their techniques and develop new approaches to exploit vulnerabilities. As a result, the cybersecurity landscape is in a perpetual race to keep pace with the ever-growing sophistication of AI-powered threats.

Cybersecurity professionals must stay abreast of the latest developments in AI-driven attacks to counter these emerging challenges effectively. By closely monitoring threat intelligence, collaborating with industry peers, and investing in robust defensive measures, organizations can better prepare to mitigate the risks posed by AI-enabled cyberattacks.

As the cybersecurity community gains a deeper understanding of the potential impact of AI, it becomes increasingly evident that proactive measures are essential. This includes investing in advanced threat detection systems that leverage AI algorithms to analyze patterns, behaviors, and anomalies in network traffic and email communications. Additionally, fostering a cybersecurity awareness and education culture within organizations can empower individuals to recognize and respond to AI-powered attacks effectively.

To truly understand the capabilities of AI, must we first identify the problems it aims to solve and ask relevant questions to develop solutions to these emerging challenges. By doing so, we can determine whether a particular product genuinely addresses organizational needs or is only another automation solution that solves problems we don't encounter.

AI and email security

Let's shift gears, bringing one real-world issue into the conversation. Email is the most widely used communication asset in businesses across the globe, transcending borders and languages. It is crucial to recognize that cybersecurity, including email security, should be part of determining how actors can and will use AI and email to make their jobs easier and more challenging to detect phishing and other attacks.

As cybersecurity evolves, professionals must anticipate how malicious actors could leverage AI to strengthen their attacks and evade detection. By understanding these potential threats, we can better develop proactive measures to safeguard our digital infrastructure.

One area where AI can bolster cyberattacks is in the realm of social engineering, specifically phishing attacks. Phishing involves tricking individuals into revealing sensitive information or performing actions that compromise their security. Attackers can employ AI algorithms to create highly convincing phishing emails by analyzing vast amounts of data, including personal details, social media profiles, and online behaviors. This information can be used to craft customized emails that appear legitimate, making them more likely to deceive unsuspecting recipients.

AI-powered phishing attacks could employ advanced natural language processing (NLP) algorithms to generate persuasive email content that mimics trusted sources' writing style and tone. These sophisticated messages might bypass traditional spam filters and raise fewer suspicions among recipients. Furthermore, AI algorithms can analyze patterns in email responses, enabling attackers to automate and refine their techniques based on real-time feedback.

Another aspect of email-based attacks that AI could enhance is email spoofing. Email spoofing involves forging the sender's address to make an email appear to come from a trusted source. AI algorithms can analyze legitimate senders' communication patterns and linguistic styles to generate highly convincing spoofed emails. This technique could impersonate high-ranking executives, reputable organizations, or even friends and family members, increasing the chances of luring victims into providing sensitive information or executing malicious actions.

Furthermore, AI can aid cybercriminals in evading detection by improving the stealth and persistence of their attacks. Machine learning algorithms can analyze security systems, identify vulnerabilities, and adapt attack techniques accordingly. By constantly evolving and adapting, AI-powered attacks can stay one step ahead of traditional security measures, making them more difficult to detect and mitigate.

To combat these emerging threats, the cybersecurity community must also harness the power of AI. By leveraging machine learning and AI algorithms, security professionals can develop robust email security solutions to detect and block sophisticated phishing attempts. AI-powered email security systems can analyze email content, attachments, and sender behavior to identify indicators of malicious activity. Furthermore, AI algorithms can learn from vast datasets of known attacks to proactively identify new attack patterns and rapidly respond to emerging threats.

Conclusion

In conclusion, combining AI and email-based attacks presents new challenges for cybersecurity professionals. AI can enhance the sophistication and effectiveness of phishing attacks, making them more challenging to detect and increasing the potential for successful compromises. However, we must approach AI-driven cybersecurity solutions with a realistic perspective, acknowledging their capabilities and limitations.

While AI excels in automating repetitive tasks, facilitating faster decision-making, and processing complex data, we must also recognize that AI technologies are not immune to adversarial exploitation. Cybercriminals quickly leverage AI for their malicious intents, using it to expedite the creation of sophisticated phishing emails and more efficient malware. These AI-powered attacks' true extent and impact are still being realized as attackers continue to innovate.

To fully harness the potential of AI in cybersecurity, we must identify the specific challenges AI aims to address and ask relevant questions to develop tailored solutions. By scrutinizing whether a particular product genuinely addresses organizational needs or merely offers automated functionalities, we can discern the value and effectiveness of AI tools.

As the cybersecurity landscape evolves, organizations and security professionals must remain vigilant and adapt their defenses to the ever-evolving cyber threats. Collaborating with AI technology while leveraging human expertise is critical to staying ahead in this complex and interconnected world. By continually assessing the capabilities and limitations of AI-driven solutions, we can enhance our security posture and safeguard our digital assets effectively.

In summary, the emergence of AI-driven cybersecurity products highlights the significance of AI in the field. However, a balanced perspective is crucial to separate the hype from reality. By understanding the capabilities of AI, acknowledging its adversarial impact, and adopting a proactive approach, we can leverage AI to bolster our defenses and protect against evolving cyber threats.

About the Author

John Trest is the Chief Learning Officer at VIPRE Security Group. John is highly skilled in driving product and curriculum strategy for diverse compliance training courses, implementing innovative learning initiatives, and fostering inclusive and motivating training environments for long-term information retention. Adept at stakeholder engagement, technology integration, and client relationship management, including Fortune 500 businesses, he values his ability to stay abreast of adult learning and instructional design best practices and cutting-edge technologies. You can find more about John at https://vipre.com/.

Addressing Bias in Insider Risk Monitoring

By Chris Denbigh-White, Chief Security Officer, Next

Preventing the loss of sensitive information can be difficult for organizations. Enterprises often take similar steps to protect data from internal and outside threats, where teams analyze activities to identify potential risks. Security operations centers (SOCs) defending against these threats must look at employees, partners, and threat actors through a similar lens to pinpoint potential data leaks. However, when surveilling for insider threats, there is the added concern of potential bias.

Defining Monitoring Bias

Monitoring bias is the unfounded, often discriminatory observation of specific employees or departments irrespective of their conduct. This can generate unsupported, negative conclusions about the credibility and trust an organization should have about an employee or department, resulting in intrusive monitoring. Conversely, it can lead to data leaks if biases prevent other employees from being adequately monitored.

Monitoring bias affects how businesses analyze insider risks, resulting in errors that can prevent identifying potential threats. This type of discrimination comes in many forms:

1. **Unequal Monitoring**: Monitoring specific members of your organization without holding others to the same standard can result in low visibility of vulnerabilities that, when spotted, can prevent insider threats.

2. **Selective Attention:** Concentrating on specific actions or behaviors instead of considering other risk indicators.
3. **Attribution Bias**: Judging specific employees or departments as presenting a heightened or lowered risk for an organization without considering their behaviors is attribution bias. This leads to inaccuracies when developing risk profiles.
4. **Group Identity Bias:** Stereotyping employees and assuming they present a higher risk based on their backgrounds can generate inaccurate assessments of their level of risk.
5. **Confirmation Bias:** Monitoring bias can cause organizations to believe data that supports preconceived assumptions is far more trustworthy than it is, resulting in a lack of focus on contradictory information.

These biases can inadvertently make security teams fail to see risky activities from other employees, partners, or threat actors. The Intelligence and National Security Alliance finds that unfounded monitoring of individuals due to biases can lead to issues like:

- Increased risk from unfounded confidence due to threat hunters and SOC teams concentrating on the wrong issues and individuals.
- Wasted resources from spending too much time observing the wrong users due to biases.
- Legal liability if protected groups are wrongfully monitored due to biases or privacy laws are violated.
- Reputational damage due to unfavorable news reports because of biased investigations.

Legacy Approaches Don't Address Bias

Older, legacy Data Loss Prevention and Insider Risk Management solutions use dated blueprints to run locally within organizational firewalls. These solutions often only utilize keystroke logging, screen recording, or web monitoring for users individually, therefore losing sight of the "bigger picture" and promoting bias.

Eliminate Bias and Improve Data Protection

It is best practice to reduce bias when monitoring employees by pinpointing activities involving sensitive data that can jeopardize sensitive information. Using technology that anonymizes employees while monitoring activities to maintain organizational security is crucial for eliminating bias. This monitoring technology still allows teams to unveil users displaying suspicious activity by providing 'scoped investigations,' giving audited data access to investigators with limited access to maintain privacy regulations.

Protecting and identifying employee information helps security teams detect risks without the interference of bias. This form of anonymity in monitoring provides teams with a holistic view of organizational activities that help detect threats and reduce monitoring bias, supporting an impartial management program that employees can trust.

About the Author

Chris Denbigh-White is the Chief Security Officer for Next. He has over 14 years of experience in the cyber security space including in the office of the CISO at Deutsche Bank as well as cyber intelligence for the Metropolitan Police. Chris can be reached online at https://www.linkedin.com/in/chris-dw/?originalSubdomain=uk and at our company website https://www.nextdlp.com/

NIS 2: From Obligation to Opportunity

By Jacques de La Rivière, CEO, Gatewatcher

The world of cybersecurity is constantly evolving; not only in talent, products, and technologies, but also in regulatory requirements. As cyber threats evolve and advance, the spotlight has fallen on the European Commission to focus on regulatory issues, to address this threat. Consequently, we have seen the Cyber Resilience Act (CRA); the AI Act; the Digital Operational Resilience Act (DORA), and most pressing, the second Network and Information Security framework – NIS 2.

NIS 2: a necessary evolution of the regulatory framework

Going well beyond the objectives of NIS 1, which provided a minimum of adequate security conditions for entities and sectors targeted by cyber attacks, the objective of NIS is to strengthen resilience by addressing new sectors and entities.

This is a necessary development in view of the growing threats, targeting local authorities, public health establishments, higher education establishments and all parties in the supply chain, not included in NIS 1.

For EU Member states, NIS2 will also address the lack of coherence and fragmentation in the treatment of cyber attacks for sensitive sectors on a European scale.

The new regulatory framework, will also deliver:

- Harmonisation of the implementation of the Directive across Europe, with more precise regulations.
- Stronger overall security, with strict and proportional criteria depending on the categorisation of the given organisation, between essential or important entities.
- Increased responsibility and powers of supervision, control, and sanction for the Member States to ensure proper implementation of these measures.
- A delegation of this responsibility to businesses, who must manage their own risks.

The question businesses therefore now face is how to meet these compliance challenges quickly and with minimal disruption.

This is frustrated by the fact that currently, no binding measures have yet been taken (other than notification of contact persons, incident reporting procedures and the potential sharing of information). The Member States are currently in the process of transposing the directive at national level.

However, there are elements that must be considered, based on NIS 1.

- A governance policy must be in place to ensure adequate risk management. This needs to include audit, risk analysis, security indicators, accreditation, and mapping.
- The consideration of key protection elements in relation to security policies linked to the architecture itself: this needs to account for administration, access, and maintenance.
- Appropriate and reinforced detection measures, as well as incident response and management measures, must be in place to maintain business continuity in a crisis should a cyber attack occur.

NIS 2 considers these areas, but there is a delay for details at European and national level, particularly in terms of integration with other legislation.

However, it is possible to translate these demands into a workable strategy to begin now. There are five pillars to consider:

- Identifying and protecting the risks
- Protecting data and sensitive information
- Investing in or strengthening cybersecurity technologies
- Implementing incident management and CSIRT notification measures
- Training and awareness-raising for employees

Primarily, it is essential to develop, enhance or maintain complete visibility of the information system. This means an inventory and mapping of all assets and user behaviours on the network.

Once the risks and challenges are identified, especially those around sensitive data, it is important to control access and comply with security policies, especially on restricted and confidential networks.

This has made NDR a core of successful strategies, integrated with a comprehensive cybersecurity ecosystem. The goal here is proactive research; easy, rapid qualification and remediation of incidents by experts.

Compliance, an ongoing journey

Today, compliance must be a strategic opportunity for companies, not an additional constraint or tick box exercise to merely meet new regulatory standards.

We need to take a long-term view. Achieving compliance is not only reactive, enabling a business to establish a comprehensive, up-to-date response to compliance needs, but also to anticipate future regulatory developments.

Beyond compliance, NDR enables organisations to raise overall levels of cybersecurity and optimise investments for the most effective detection of and response to threats. Building a cybersecurity strategy with NDR as a cornerstone means choosing a long-term cyber path, with anticipation as the keystone. For cyber-attackers and defenders alike, time is of the essence. The aim is to be able to respond effectively to potential future threats, thanks to an adapted and responsive defence system.

Think of NIS 2 as a guide to identifying and prioritizing the risks and areas of weakness, as well as cybersecurity strengths, to draw up a dynamic strategy to combat attacks. When approached strategically, compliance transforms from a necessity into a real opportunity and competitive advantage.

About the Author

Jacques de la Riviere is CEO of Gatewatcher. Gatewatcher is a leader in the detection of cyber threats, and has been protecting the critical networks of worldwide large companies and public institutions since 2015. Combining Network Detection and Response (NDR) and Cyber Threats Intelligence (CTI) solutions, with AI-powered, dynamic analysis techniques, Gatewatcher delivers a real-time 360-degree view of threats, covering both cloud and on-premise infrastructures.

Jacques can be reached online via LinkedIn and at the company website https://www.gatewatcher.com/en/

Top 6 Security Challenges of SMEs

By Michal Gil, Head of Product, CybeReady

Small to Medium Enterprises (SMEs) are vital for innovation and economic growth, and their role in larger supply chains makes them an attractive gateway for hackers. After all, you're never too small to be a target for cyberattacks.

Over 50% of cyberattacks target SMEs. These attacks lead to consequences like data loss, reputational damage, fines, or a complete system shutdown—and within six months of experiencing a data breach or hacking incident, 60% of these businesses cease operations. For hackers, it's not about headline-grabbing attacks that'll earn them millions in illicit fortunes. It's about taking the path of least resistance to an organization's finances, data, and systems, and unfortunately, SMEs offer easier entry points.

Almost every business experienced turbulent digital transformation thanks to the hurried transition to remote working and cloud infrastructure when the pandemic hit. Although a few years have passed, the lack of dedicated security teams and budget, plus less sophisticated tech stacks, continue to put SMEs on the firing line.

Let's review the security challenges that are making IT teams nervous this year and discuss the essential remediation strategies you need to know.

Top 6 Security Challenges of SMEs

Balancing the speed of growth with the quality of security is extremely difficult, but SMEs must find a way to prioritize both. Otherwise, you could open your doors to the following risks and challenges.

1. Outdated Technology

Reliance on basic security strategies like firewalls and antivirus software is rife among SMEs. Who can blame them? New cybersecurity technology is either too complex, expensive, or requires deep knowledge to maintain. Providers' pricing and packaging options are often not appealing to SMEs and their specific and complex requirements, which makes purchasing and maintaining a security tech stack overwhelming.

2. Overworked Teams

SMEs' IT teams often turn the cogs with limited budgets and resources, meaning every business decision requires careful prioritization. But this leanness leaves IT teams siloed from the rest of the business and juggling multiple plates. For this reason, 90% of IT staff say they are paying *less* attention to security alerts than last year.

3. Supply Chain Risks

SMEs are the stepping stone to larger organizations and third-party vendors that are more valuable to hackers. Compliance regulations force SMEs to establish policies and processes between themselves and third parties, but most businesses don't realize that these regulations often define minimum acceptable requirements. That means you must do more, such as investing in employee training and continuous monitoring solutions.

4. Rapidly Evolving Cyber Threats

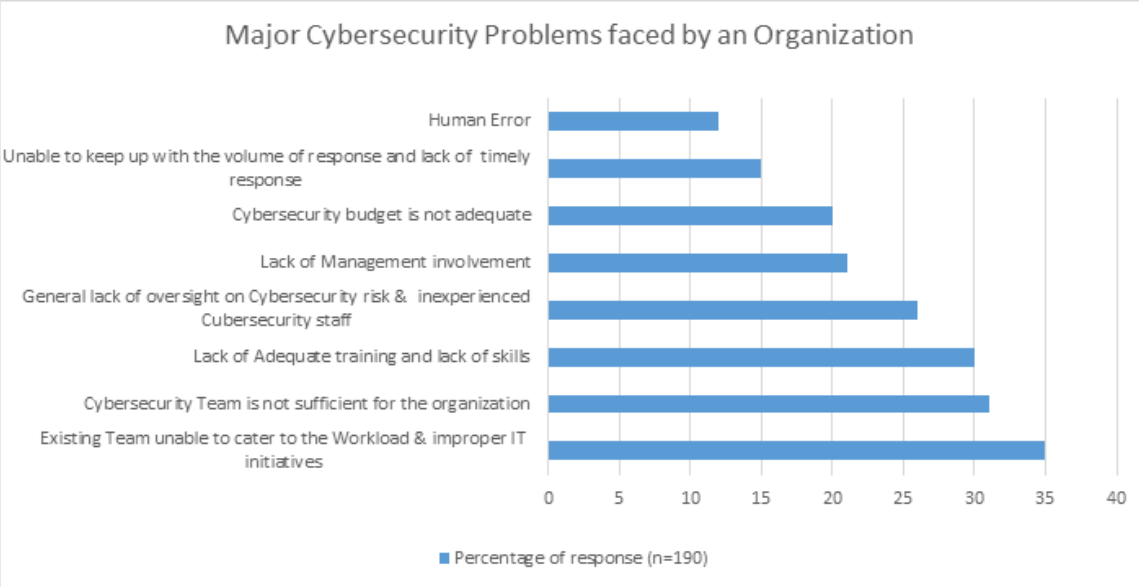
Cloud services are essential for improving efficiency and cost savings, especially in the era of remote working and agility. Without an advanced understanding of cloud security requirements and the context of the evolving threat landscape, SMEs risk falling victim to attacks like malware, ransomware, and phishing. 42% of SME leaders have difficulty visualizing the full scope of an attack, highlighting that they are unprepared for disruptive crisis events.

5. Lack of Cybersecurity Training for Employees

40% of SMEs say that a lack of skilled security personnel is a barrier to maintaining a security posture. Knowledge and experience gaps mean employees won't feel confident and competent in identifying dangerous threats like social engineering attacks and phishing. Cybersecurity training helps foster a culture of security, making it an everyday, long-term consideration rather than a cause for panic.

6. Internal Threats and Human Error

While IT professionals are focused on external threats like hackers, the danger might be lurking closer to home. Common mistakes like easy-to-guess passwords, a lack of multi-factor authentication, and little understanding of access control for ex-employees can put your organization at risk. Only half of SME leaders are confident that ex-employees can no longer access systems—let's hope there's no bad blood!



Proactive Remediation is the Way Forward

Adopting new technology is one piece of the puzzle, but it's not the only prevention and remediation strategy SMEs should implement. Here are some effective short- and long-term solutions to help your business build a solid cyber-safe foundation:

Establish an Incident Response Plan

What should you do in the event of a cyberattack? Hopefully, this crisis never happens, but preparing for the unknown is essential. An incident response plan (IRP) defines the exact procedures and recovery strategies your SME will follow in the event of an attack, ensuring you respond swiftly and minimize financial, legal, and reputational damage.

Conduct Periodic Risk Assessments and Vulnerability Testing

Like an incident response plan, you should regularly review risk assessments and vulnerability testing strategies. This task involves assessing your organization's technology, people, and processes, defining your security posture, identifying areas of concern, and implementing automated monitoring and testing tools to keep you safe 24/7.

Invest in Up-to-date Security Software

We've already discussed that SMEs need simple yet effective solutions to make up their cybersecurity tech stack. For example, out-of-the-box solutions are often much easier to deploy and require less technical expertise, which makes life easier for lean IT teams. Other essential software solutions include cloud-based applications (so your data is constantly backed up to prevent data loss), threat detection, and auto-remediation.

Implement Cybersecurity Awareness Employee Training

Finally, regular cybersecurity awareness training like phishing simulations equips employees with the skills needed for secure and confident online working experiences, helping reduce human error, improve security awareness, and protect your organization. You can also consult external experts that tailor award-winning security

training to the exclusive needs of SMEs with 25 - 150 employees.

Software security training solutions are used by leading banks, hospitals, and tech companies worldwide. They offer continuous and automated training and advanced analytics features to keep on top of your employees' progress and knowledge gaps.

Regular employee cybersecurity awareness training is a reliable and high ROI strategy to help SMEs like yours strengthen security measures, and it's one that doesn't pull your resources and teams away from other critical tasks.

About the Author

Michal Gil is an accomplished product leader with a passion for developing innovative solutions that meet the needs of modern users. Currently serving as the Head of Product at CybeReady, Michal leverages her extensive experience in product development to drive the company's vision forward. Michal is driven by a deep commitment to delivering exceptional user experiences and loves the challenge of taking complex problems and turning them into elegant, simple solutions. These include Employee Readiness Solutions for SMEs. She is a firm believer in the power of teamwork and collaboration, and strives to create an environment that is inclusive, supportive, and empowering for everyone.

Is 2024 the Year of Cloud Repatriation?

By Eyal Arazi, cloud security manager at Radware

Eyal Arazi, cloud security manager at Radware, looks at why organizations once committed to cloud-first and cloud-only strategies are now reevaluating their approach. Learn how two hundred organizations are thinking about a shift back to on-premise and the motivations behind this reversal.

"Cloud migration is over; everyone is in the cloud. And this trend is irreversible. “

But is it really?

In recent years, the business landscape has witnessed a remarkable transformation with the rapid adoption of cloud computing. Companies have moved en masse to the cloud, changing the way they manage and deploy their workloads to take advantage of the promises of unparalleled flexibility, scalability, and cost-efficiency. And while organizations have reaped the benefits, they are also starting to reevaluate their cloud-first and cloud-only strategies and migrate some workloads back on-premise. This u-turn in thinking and events is a process called cloud repatriation.

According to Radware's 2023 Application Security in a Multi-Cloud World report, two hundred organizations weighed in on this trend, confirming a shift in their security strategies. According to the 2023 data, only 24% of them said they deployed applications on multiple cloud environments. This is down from the 58% of organizations that said they deployed applications across two or more public cloud environments in our 2022 survey. And while 21% of organizations were using three or more cloud environments in 2022, only a negligible percentage seem to be doing so in 2023.

Why companies are making a u-turn

So why are companies making this shift? There are several compelling factors.

Security is one of them. At the same time that multi-cloud deployments are showing signs of decline, concerns about security threats are on the rise. The inability to achieve consistent security policies across multi-clouds topped the list as a problem or extreme problem for 56% of the organizations surveyed in 2023 compared to just 26% in 2022. And security mistakes are costly. According to the survey, downtime due to a successful application DDoS attack costs organizations an average of $6,130 per minute.

Other security areas respondents ranked as problems or extreme problems included protection between platforms (61% in 2023 vs. 38% in 2022), unified visibility (58% in 2023 vs. 41% in 2022) and centralized management (46% in 2023 vs. 34% in 2022).

Security is not, however, the only factor causing companies to rethink their security strategies and move applications and data back on-premise. Other considerations include:

Cost management: While the cloud's pay-as-you-go model can be cost-effective for variable workloads, it can lead to unexpected expenses when usage spikes. Where predictable workloads are concerned, it can be more cost-efficient to invest in on-premise infrastructure over the long term, rather than paying ongoing cloud service fees.

Performance and latency: Applications requiring low-latency responses or intense computational power can encounter performance bottlenecks in a cloud environment. Running such workloads on-premise can offer more consistent performance and responsiveness.

Data sovereignty and security: Industries with strict regulatory requirements often need to ensure that sensitive data is stored and processed within specific geographic regions to comply with data sovereignty laws. Maintaining control over that data and having physical access to it offers a level of security and compliance that cloud solutions cannot always guarantee.

Complexity and vendor lock-in: Adopting multiple cloud services and platforms can create technical and security complexities. Additionally, concerns about vendor lock-in and potential difficulties in migrating between cloud providers can cause some organizations to consider bringing workloads back in-house.

Changing priorities: As strategic priorities evolve and shift, some workloads can end up being better suited for an on-premise environment. This could be driven by an organizational desire for tighter control, specific performance requirements, or changing business needs.

Resource optimization: Workloads that have stable resource requirements may not fully leverage the cloud's elasticity. In such cases, dedicated on-premise hardware can have better resource utilization and cost savings profile.

A cloud-also approach

While repatriation to the cloud will continue in 2024, it is not a wholesale withdrawal from the cloud. Instead, companies are weighing a cloud-also approach against a cloud-first or cloud-only approach.

According to our survey, most organizations still deploy applications in a hybrid architecture made up of private and public clouds and on-premise environments. In 2023, nearly three quarters of survey respondents reported still using their on-premises data centers, and 70% are using a private cloud environment. Nearly nine out 10 organizations use a combination of two or three types of environments (on-prem, public cloud, or private cloud), with 46% reporting they use all three in tandem.

When deciding on the optimal deployment strategy for their workloads, the key for organizations going forward is finding the right balance based on their unique business needs. This means carefully defining which workloads go where. While cost is often a motivating factor, it should be weighed along with other important considerations, including operational efficiencies, regulatory requirements, speed and delivering a quality user experience.

About the Author

Eyal Arazi, Cloud Security Manager at Radware

Eyal is a Cloud Security Manager at Radware, where he is responsible for market strategy for Radware's line of cloud security products. He is originally from Israel, where he served in Unit 8200 of Israeli military intelligence, which is the Israeli equivalent of the NSA. Following his military service, Eyal worked at a number of startups in the areas of information security, computing and big data, and marketing. Eyal has now been with Radware for almost 4 years. He holds a Bachelor's degree in Management from the Interdisciplinary Center (IDC) Herzliya, and a MBA from the UCLA Anderson School of Management.

Eyal can be reached online at

LinkedIn: https://www.linkedin.com/company/radware/

Company website http://www.radware.com

How A Strong Digital Culture Is the Foundation For Successful Metaverse Exploration

Businesses must become digital-first to understand the emerging realm of the metaverse and develop the innovations that will drive success there.

By Jaime McMahon, CDO, LineZero

The metaverse is open for business. A growing number of companies are shifting their strategies (albeit slowly) to include engaging with consumers in the evolving virtual world, and a growing number of consumers — more than half according to a recent survey — say they are ready to connect in the metaverse as well.

For businesses preparing to enter the metaverse, developing a strong digital culture is a critical step. The metaverse is more than simply a new digital venue where businesses can deploy traditional methods of promotion, sales, and customer support. It is a new world of digital-first engagement that requires a digital-first mindset.

What to expect in the metaverse

The metaverse is often described as revolutionary. Some experts, however, refer to it as an evolution rather than a revolution, citing that the metaverse is still an emerging technology. There is a long list of promises about what the metaverse can become, but the vast majority of those promises have yet to be realized.

As long as the metaverse remains an emerging technology, identifying effective business models will be challenging. It remains to be seen whether strategies that succeed in e-commerce will be applicable in the metaverse, as achieving profitability with emerging technologies can take years — if not decades.

Businesses should also expect that metaverse success will require the development of new skills. Brands that want to establish a metaverse presence will need to navigate the world of virtual design, blockchain, AI, and spatial computing. In addition, the social component of the metaverse will require businesses to be ready to excel at community management and other human-centered skills.

Even in its emergent state, the metaverse has already been labeled a high risk for fraud and cybersecurity attacks. Metaverse scams could target digital identities — stealing avatars or online profiles to use for malicious purposes — and intellectual property such as music or 3D models developed by businesses. Cyberattacks could target user data or metaverse assets such as cryptocurrency or non-fungible tokens. Ransomware attacks that seek to gain control of metaverse operations are another threat.

How to engage in the metaverse

Building the type of strong digital culture needed for metaverse exploration starts with becoming a digital-first business. IT can no longer be strictly a department within a business, but instead must be at the core of the business, driving the worldview of the workplace.

Businesses must also prioritize innovation to effectively explore the metaverse. Users expect an immersive experience, which means businesses will need to develop innovative approaches to engagement and interaction. Businesses will also need to develop innovative approaches to connecting the metaverse to other business channels to drive mainstream consumer adoption.

Curiosity is key to innovating, so businesses should explore the metaverse with a desire to learn, an open mind, and a willingness to listen to those they encounter there. Resilience is also key to innovating, and the metaverse's digital landscape is the perfect laboratory for experimenting, failing fast, learning from mistakes, and trying again.

Prioritizing data-driven decision-making is another key to building a strong digital culture. The metaverse will provide businesses with data-rich consumer interactions, but until strong patterns of behavior emerge, businesses will need to engage in an ongoing process of data analysis and experimentation to identify insights that can drive effective decision-making.

Businesses should also plan to invest heavily in cybersecurity as they set up shop in the metaverse. Multi-factor authentication and digital rights management will be critical for protecting the digital identities and assets used to populate the metaverse. Vulnerability testing and patch management should also be prioritized due to the emerging nature of metaverse technologies.

Essentially, a strong digital culture evolves as businesses and their employees begin to see “digital” as a value instead of a format. Building a metaverse-ready workforce requires moving in that direction. As businesses become more comfortable in the metaverse environment, they will be better equipped to identify and take advantage of the opportunities it will bring to the business world.

About the Author

– Jaime McMahon, Chief Digital Officer of LineZero, has a passion for helping organizations unlock their digital potential. He has extensive experience in the technology industry, working with businesses of all sizes to drive growth through digital transformation. Jaime is a sought-after speaker on a range of technology solutions, delivering talks hosted by industry leaders throughout North America. He is committed to democratizing technology and shifting its role in business from a cost-centric focus to a strategic enabler of positive outcomes. At LineZero, Jaime leverages his expertise to help businesses achieve their goals and optimize their operations.

SolarWinds Lawsuit Reinforces the Need for Critical Communication Between CISOs and the C-Suite

By Jose Seara, Founder and CEO, Denexus

As demonstrated by recent developments in the legal matter between SolarWinds and the SEC, the landscape of CISO liability is expanding. After the announcement that SolarWinds' CISO Timothy Brown would face charges for failing to disclose the severity of certain cybersecurity risks, the CISO community has realized that the potential cost of managing cyber risk is more severe than ever.

Beyond the legal and financial liability demonstrated by the SEC's charges for fraud and internal control failures against Brown, this incident also reinforces that cybersecurity breaches pose a significant risk of hefty compliance fines and a negative image in the public eye. With heightened consequences across the board, it is imperative that security leaders are doing more than just ensuring organizational compliance – they must go above and beyond to secure critical systems and data. Compliance usually drives behavior, but rarely is the end point.

However, CISOs can't tackle this challenge entirely on their own. To effectively protect an organization from security breaches, lawsuits, fines, and potential reputation damage, CISOs must collaborate with C-suite benches (and CFOs in particular) to ensure that priorities are aligned. And the C-suite must also work with the Board, which holds the ultimate governance responsibility.

Communication Within the C-Suite

Due to the specific nature of their respective roles, CISOs and other C-suite executives often find themselves focusing their time and attention on separate, distinct parts of business. However, the siloed nature of these individual priorities can prevent organizations from establishing and maintaining complete awareness of the severity of potential cyber risks. To effectively prevent a situation like what happened at SolarWinds, clear and consistent communication between CISOs and C-suite executives like CFOs is essential.

Without the presence of constant communication between CISOs and C-suite leaders, there is no way to ensure that everyone is on the same page. The challenge is that they usually speak with different jargon, and more often than not they deal with conflicting topics. But that should not be the case. The implications of cyber risks are not limited exclusively to security-related concerns; we've now seen how these risks can rapidly develop into massive legal and financial issues. As a result, it is imperative to foster open dialogue on a continuous basis so that security concerns are explicitly disclosed to all members of an organization's C-suite, ensuring that they are fully aware of the presence and severity of cyber risks, and how these risks can snowball into situations that directly impact the operations of each executive's respective role and detrimentally impact the organization's bottom line.

Speaking the Same Language

One of the biggest barriers to communication between CISOs and C-suite executives is the complexity of communicating cyber risks and potential implications in a way that makes sense to individuals from non-security backgrounds. This is particularly important for CISOs and CFOs, who must collaborate on a continuous basis to analyze and evaluate the relationships between potential cybersecurity incidents, the associated legal and financial implications and the prioritization of cybersecurity investments based on ROI and positive impact on risk mitigation.

To facilitate this process, organizations can leverage cyber risk quantification and management tools (CRQM) that congregate data to calculate, quantify, and translate information about threats and vulnerabilities into more digestible language and data. This simplifies the ability to have critical conversations between CISOs and other C-suite members, which ensures organizational alignment.

Once CISOs and other business leaders like CFOs can speak the same language and relate to one another and their priorities, it facilitates the ability to align their priorities and goals to support the organization as a whole, providing them with the comprehension necessary to implement risk mitigation strategies that are based on data, evidence, and outcomes that are relevant to each respective leader and sector of business. Not everything is about vulnerabilities and firewalls, and not everything is just about return on a specific investment in stand-alone basis. A targeted investment in an expensive firewall upgrade can protect you from a massive lawsuit post incident and yield immeasurable ROI in terms of risk mitigation.

Inviting Others to the Table

By incorporating other leaders into security-focused conversations, CISOs can dissolve silos and establish cybersecurity as a shared business priority that impacts and involves the entire organization. Making space for executives from other areas of business to participate in dialogue about cyber risks ensures that everyone is aware of potential threats and how they will impact all parts of the organization if left unaddressed. At the executive level, this also bodes well for cyber teams by increasing the chance of receiving funding for additional resources needed to mitigate potential risks – when the board is more aware of the prevalence of certain cyber risks and the need to mitigate them to preserve smooth operations for all branches or departments of an organization, they are more likely to approve capital to uphold cyber risk management efforts.

This is true beyond the C-suite as well, both upstream and downstream; inviting other employee teams into conversations, trainings, and educational sessions about cyber risk management sends the message that cybersecurity operations and strategy is key to the success of the entire organization. Expanding the narrative to encompass a wider scope encourages more people to care and be involved in the practices and efforts necessary to mitigate cyber risk.

Proactivity as a Priority for Prevention

In collaboration with CFOs and other C-suite executives, CISOs can prevent catastrophic events like the SEC/SolarWinds lawsuit by taking a proactive approach to cyber risk management. By fostering clear, ongoing, and comprehensive conversations about security-related topics and investments, organizations can ensure they are operating offensively instead of defensively and stay several steps ahead of any potential risks. When security infrastructure is being continuously monitored and the proper defenses are in place to catch and prevent a breach before it becomes a problem, organizations can develop a clear picture of their risk exposure and make data-driven decisions on where to make meaningful cyber security investments.

About the Author

Jose M. Seara is the founder and CEO of DeNexus, a leader in cyber risk quantification and management for operational technology (OT) and industrial control systems (ICS). Jose can be reached online at https://www.linkedin.com/in/jmseara/ and at our company website https://www.denexus.io/

Combating Terrorism Using Information Protection

By Milica D. Djekic

The global landscape has changed significantly since a beginning of the new millennium as a threat to everyday life and work is arising day by day causing a technological, physical, financial and health danger to many. The security challenges of nowadays mainly choose an asymmetric tactic to attack and in such a sense it is clear why their operations are such an impactful and fatal to the majority of people. In such a case, it's needed to make a focus on high-tech campaigns as a cyberspace is also an asymmetric platform giving chance to assault using a minimum of the resources and getting in position to make harm to the entire nations and their countries. The cases of the bioterrorism through the last two decades have taught everyone the bio-weapon can kill many only give them an illness which can be treated, but in some cases, it can lead to death. Also, the recent events in the Gaza Strip have shown that if intelligently coordinated the physical offenses can lead to catastrophic consequences as the Hamas strategy has demonstrated that the small spatial areas can be applied to threaten many simply making from such a place the terrorist base which has dealt with a certain range and coverage in a fashion of the armed force's strikes. On the other hand, it is very well known that the cyberspace is a true technological field of the asymmetric threats and in that case, there must be taken some steps in preventing, monitoring and responding to those incidents as such technical advancements are in need for a better cyber defense that should include a highly sophisticated cryptosystem solution. It's easy to say, but extremely difficult to obtain as any cryptosystem is supposed to cope with the good encryption and decryption which is not always easy to produce. Some current experiences suggest the humankind is very close to make its first steps in developing, designing and deploying the pioneering perfect secrecy crypto-algorithms that can

be used for an information protection either being with a device or any transmission of the data via a communication asset, so far. In other words, this effort is going to stress out some terror challenges, as well as explain why a serious cyber security like a cryptology must be applied in a case of the combating terrorism that as any crime area must rely on a cutting-edge technology.

The terrorism by itself is not a product of the modern time as throughout history, there have always existed groups, movements and organizations which aim has been to shake ongoing law and order and take control over some approved countries territory. For instance, there are some findings which might suggest that even in the Middle Age in Europe there had been the entire chords of the arson terrorists that could literally burn the entire villages in order to frighten common people and attempt to ruin that state's governance over such a geographical area. Those villages had been a collection of the poor people and in other words, there had been nothing to get robbed, but more likely those attacks had been done in order to intimidate the folks and cause an unrest within such a country. The system of the past had so many difficulties to smash those groups as in that time, the world had not been at a today's stage of the development and the barbarism had been a usual thing in even the most progressive societies of such an era. Even nowadays the situation is not a bit better as anyone being with barbarian approach can attempt to intimidate anyone literally putting the entire super-forces and forces worldwide under a quite unpleasant condition. The mission of any country is to protect their innocent civilians from being hurt and the terror-makers would know that well enough, so for such a reason they will push hard to exploit the gravest vulnerability any nation has and those are the lives and wellbeing of the innocent civilians, so far.

From a current point of view, it seems the history will always give some lessons and as there is a defense system of today, there was something similar within the past epochs. To clarify, in the past the human communities had also dealt with the well-trained worriers who could then ride a horse and be skilled with a wide range of the weaponry of such a time. Those soldiers had needed to cope with the spots where they could adopt such a skill and from a modern perspective, those were the very first terrorist campuses being used to train men getting a combating capacity, as well as dealing with that time logistics, arms and secret communication which had been delivered through the land. Also, if that sort of the bandits could cut anyone's correspondence, they truly had done so. The majority of their curriers had used a cryptography of that age and even if such authorities could catch their message delivery, they could not figure out their plans as the entire communication had been ciphered. For such a purpose, the terror groups had applied a piece of the paper and sometimes some animal skin in order to camouflage what they really want to do. Apparently, the state authorities had also needed to use some kind of data protection as then it had been necessary to bridge long distances in order to let know anyone being such a far away what is all about. Further, those were the very first days of the escort as not only the important persons of that time had gotten their personal security, but most likely an official information transfer had coped with cryptography, as well as with physical assurance. With a very beginning of the country governance, there had appeared the very first laws enforcing people to deal by rules. If anyone through the history has been disobeying about such limitations, that person would suffer restrictions and consequently some punishments. Those things have been introduced in order to show everyone the state rulership over some territory must be accepted and anyone not being willing to cope with those requirements has gotten in touch with extremely serious implications. The very first legal regulations in Europe had been that strict to prolong a methodology eye-for-eye and tooth-for-tooth to those who would even believe to commit crime and remain unsanctioned. The main reason why the human beings have

agreed upon the laws or in other words, live by rules is there have always been predatory groups which could severely threaten anyone's life and for avoiding to be under chase and danger the ancient countries needed to invoke such a way of the society control protecting everyone who was admitting their rulership and eliminating those who had to make conspiracies against those states. Indeed, a good community has undoubtedly protected those being obeying about the rules and punished those who were daring to challenge the system.

In the modern times, a way of thinking and judging is more or less pretty the same as the global landscape is yet building up using the previous experiences as a base for the entire construction. The ongoing logistics is much better than in the past as the current civilization can travel through land, air and water applying the new methods of transportation, while the digital revolution has brought a plenty of the advantages in communication and data assurance. Next, with this novel time the defense systems across the globe can realize what the asymmetry means and why it is important to manage a risk from being attacked in a truly terrorist manner. The cryptography with cryptanalysis being the building blocks of the cryptology must count on more innovative and better ingenious angles in science and technology as even in the past times someone had been that clever to send an escort with such a correspondence also protecting the both – a sender and receiver of that message. The similar logics is followed even nowadays as those who are exchanging information, as well as the overall communication channel are supposed to be well secured. It appears if looking back to the past can bring an inspiration for a future as once the mankind accurately masters all historical lessons the world will honestly be on a track of the progress, while on the other hand if the historical findings are not well-studied the wheel of the time will always pull back those who select to go froward. Probably there is some word about taking a responsibility for being a good leader as those who can lead need to have the both – well-educated mind and heart in order to avoid the flaws from the past that put under risk a wellbeing of the entire humankind, so far.

By a novel understanding, the security is about a risk management as it is a process of maintaining the risk at an acceptable level providing in such a term some methods of protection to many. As it is well known, an accurate and timing information might mean an advantage in any sense of the people's activities as in such a case those two or more who are exchanging data can make a plan what to do relying on such pluses. If it is considered how such a communication works and if it could be followed with the information leakage and any way of the weak findings management, it could be clear that being capable to cut such a contact could take that confidential content directly making a conflict of the interest with such a group preparing a deal about some business. The golden rule in an information assurance is the confidential findings should remain confidential as if not protected adequately those data could put many on a risk offering to opponents to get a step or two ahead the communicators. On the other hand, many defense organizations are with a demanding task to uncover the bad actors and their actions in order to prevent some of the possible security anomalies among those communities. The main imperative at present is there is a need for a strong international collaboration across the world and as there are a plenty of the services which protect some of their national interests there must be more international security and policing associations such as the Interpol, Europol and much more that can coordinate any sort of the investigations at a global scale, so far. With an advanced technological development and growth, many of the ongoing activities over the globe can be quantified and get measurable with a certain degree of the accuracy as it is well known, those technical solutions operate in compliance with the rules of nature or in an engineering sense, they strongly cope with the laws of the math and science otherwise they would not function at all. The engineering is existing nearly within any aspect of the modern life and

work and not only the good guys can apply those technologies to progress and deal with the precision, but more likely the bad actors are also dependable on such an outcome of the civilization's progress. From that point of view, it is obvious as an accuracy of those technical improvements rises and moreover, those who are using a technology can count on a better accuracy which means a more accurate security to many of such associations. Some beliefs suggest that in the nature everything is about a cause and effect, so if anyone has created any kind of technological, biological, physical and the other weapons in order to accomplish something it is more than appealing to design a counter-weapon as things could get returned into balance. In other words, someone will challenge and consequently, someone will respond, so far.

Next, there will be discussed some alarming stuffs in regards to ever evolving threats and their actions about the entire nations and their countries which indeed, can be uncovered and spied by some transnational crime or terrorist organizations. If it is gone back to a quite recent past, it can be clear that the ISIL terrorist group has been beaten through the air strikes in Iraq and Syria about a decade ago, but such a challenge is yet active in the world as that military intervention did not smash the entire terror units. The cause to such an intervention was those terror members have dared to challenge the United States and the other societies across the world just using the advantages of the cyberspace to track any kind of an unprotected communication between very important persons and institutions at a global level. On the other hand, the effect is well-known, but it does not mean no one in the world will be that rude in the future to make a new criminal scheme trying to challenge the authorities anywhere and in order to break into that scenario it could be needed decades as with a good capacity to cope with technology something new can be innovated and the good guys could figure out a lot of so sooner or later, but there will always be some methods to avoid being confirmed following some case management procedures and policies as those who are making a criminal scheme could be very smart and create something which can take a lot of time from the authorities remaining some of the past cases in a policing practice being unresolved for an entire time.

The fact with a current cryptography is the networking devices use a communication channel in order to deliver data via a grid and in order to prevent anyone from external to make a breach to such a communication it is needed to develop a strong cryptosystem which can stop an opponent from reading such exchanged information. In the practice, many armies' cryptographic solutions are capable to transfer data relying on an end-to-end, link and combined encryption and the majority of those systems are yet struggling with a key distribution, but there are some indications that the world is getting on a race for the perfect secrecy as some of the founders of the information theory have so wisely predicted a couple of decades back. As it is well known, the ongoing time is a chapter of the industrial revolutions and maybe some people will talk about those endeavors suggesting that the planet is going to a cyborg epoch, while the overall global situation is very far away from those forecasts, because at this degree the security is something being such a desperately needed. From a today's perspective, the entire planet is facing up a time of the emergency and the ongoing indicators show there will be still a plenty of the routine tasks getting tackled and some results must come with such an effort. The theory of information is an achievement being accomplished during the World War 2 and the engineers of that time contributed to such a victory serving hard to produce something reliable and very intelligent for their era. Indeed, the similar situation is manly present nowadays as the entire teams of the engineers, scientists and researchers need to pull up their sleeves in order to develop a technology which will make a world becoming a more safe and secure place to the majority of its residents. No time in the history was easy

and maybe the current situation worldwide might appear as tough, but if it is made a look back it could be feasible to understand those brave men and women who has built up the world and made it as it is today no matter if the majority of their days have not been shiny at all.

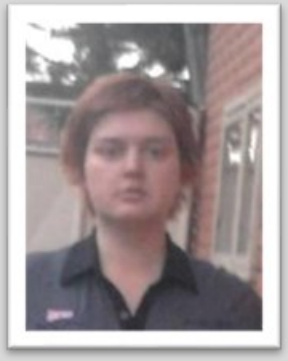
In the modern time, a terrorism is escalating nearly everywhere in the world either being biological, high-tech or physical by its nature it is going to show a tendency to become the real nightmare to the humankind of nowadays, so far. In comparation with the past, the ongoing terror has kept dealing with more or less same rules, but with an outstandingly better technological background as a technological development is a true engine of the today's progress, as well as current human's activities. The terrorism is something that has evolved as the entire civilization and it deeply takes advantages of the emerging technical systems bringing with itself all the concerns and better saying, challenges of the new historical chapter. As it is well known, the terrorist organizations at present can plan their actions with a high precision as the technological landscape lets them do so, but on the other hand, anyone dealing with the high-tech environment must leave a trace and in such a sense, there is a good portion of the confidence to authorities those threats will be uncovered, located and caught sooner or later and today many will talk with a full assurance that no matter what the bad actors do the good guys will get that and come to bring them to the justice. In other words, that's how the modern world has progressed and that's how brilliantly the good officers and their cooperators can tackle anything appearing within a field of the security. Indeed, it's not easy at all preparing a terror attack and the other operations and the majority of those plans get accomplished, because the terror actors know a lot about the cutting-edge technologies as they cope with an advanced user experience skill, as well as with some hardware design and software coding capacities making them a truly clever predators which instinct can support them in avoiding all the traps and obstacles the experienced hunters could apply in order to get them. In other words, it's all about an accurate and timing information which can be obtained through many approaches and that's why the ISIL was spying on the critical US asset in order to gather some findings and consequently push them into an entire analytical process which has offered them completely collected intelligence suggesting to their strategists how to formulate a very dangerous strategy being resolved in both – tactical and operational manner which gave them some sort of the awareness about what those who are working over their head do and which details have remained unprotected opening them a chance to attack to the most critical, but yet inadequately saved spots across the globe. That's why the world has gotten to deal with an asymmetric warfare and that's why the minority could threaten the majority causing truly severe impacts to the world as it is well known nowadays.

The main challenge with the terrorism of today is an awareness as those who are in an everyday search for a terror grid need to adjust their approaches to their mission coping with a great situational awareness in order to uncover the threat and make some serious and far reaching geostrategic predictions always getting in mind the troubles can come, but literally not from nowhere as there must exist some source and once those origins are identified it can be possible to make some grouping that can put the authorities and their investigations getting on the right track. Apparently, it's not handy at all resolving such cases and it seems the security undoubtedly needs a multidisciplinary and, say, more scientific approach in tackling crime as it is known today. The existing trends and tendencies in criminology suggest that the ongoing criminalities can be resolved in a less time-consuming and better cost-effective fashion as those combating any area of the criminality relying on a plenty of the innovations within a defense can make a significant step froward in order to smash the majority of the transnational crime and terrorist organizations as it is well known that the transnational organized crime is the biggest sponsor to a

terrorism. The criminal groups mostly have a rational approach to their business as the majority of the professional criminals work for a profit and if a legal system is pressed by terrorism, armed conflicts, social unrests and much more those governments must take into a consideration some kind of the negotiation or making a favor to those who are in position to dictate the rules literally forcing the entire areas to collapse in front of their pressure obviously frightening anyone to get a barbarian if that person or institution is not willing to make their list of wishes getting satisfied, so far.

In addition, the modern terrorism is strongly correlated with the roads of drug smuggling, human trafficking, firearms distribution and the entire spectrum of the heavy case criminalities which appear to take control over the global landscape as those criminal networks frequently operate transnationally supporting terror groups, because of a plenty of the benefits and interests they can get if they obtain a rulership over some territory. Therefore, those criminal organizations are getting very sophisticated for a reason they use a service of the cybercrime underworld, as well as they look for an economic power over some country as they put a lot of money into a legal flow doing a money laundering which can give them a capacity to create a political and social situation within some area. Indeed, those lawbreakers show a tendency to get untouched in any sense as they need their safe place where no one will recognized them as criminals, but more likely as highly successful businessmen who have a heap of the amazing business ideas which have made them rich and powerful in the eyes of public. On the other hand, the majority of jihadist groups seek to be with a dominance, but in order to intimidate a community they have to work hard in preparing a terror operation and if they are mostly occupied with such an activity, they would obviously get no time to make a profit as professional criminals do and that's why they will accept a financial help from, say, drug lords and their trafficking group, so far. Above all, all those actors are desperately dependable on the novel technologies and even if they could get many benefits from so, they will literally cope with a sword with two edges as the modern authorities can cut their communications and totally uncover their information exchange in a cyberspace which can be assumed as their greatest weakness for a reason there are some methods to get their spot of grouping which gives confidence to the good guys the lawful communities might stay at least a step in front of the arising threat.

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 disability.

Reshaping the Focus of Cybersecurity

Key Insights from the International Counter Ransomware Initiative Statement

By Todd Thorsen, Chief Information Security Officer, CrashPlan

Earlier in November, media outlets widely reported the contents of a remarkable joint statement. The International Counter Ransomware Initiative (CRI), comprising 40 countries, declared that they would no longer pay ransom to bad actors. In the same policy statement, CRI also agreed to create a shared blacklist of wallets used by ransomware actors and help any of their members respond in the event of a ransomware attack. In addition to these strong stances against ransomware, the coalition also welcomed 13 new members this year. All this signals that ransomware is looming large as a global concern for several states — and that there is a genuine interest in developing strong, consistent international policy responses to a growing problem.

The problem is real. From 2019 to 2022, the number of ransomware attempts worldwide went from 187 million to 493 million, according to Statista. Moreover, Corvus' Q3 2023 Global Ransomware Report noted that global ransomware attack frequency went up 95% in the last year. Against this backdrop, CRI's

statement, and the other actions it's taken, are a step in the right direction. Somebody needs to do something.

The silver bullet

But an international pledge is unlikely to be the silver bullet CISOs are still looking for. Or, at least, not this particular international pledge as it currently stands. While symbolically powerful with some good initial steps in the agreement aimed at monitoring and sharing at the nation-state level, it does not include actionable guidelines for the organizations on the front lines. At the very least this serves as a barometer highlighting the level of global concern around ransomware, but it remains to be seen how effective this pledge will be at disrupting payments mechanisms for ransomware actors and whether these actions will reduce the number of ransomware attacks. The pledges' challenges are common to anyone who follows international policy: these things move slowly with too many caveats and exceptions. The pledge of course only covers the National level, and even then, it allows for exceptions to the refusal to pay ransoms in the event of emergency situations. And when is ransomware ever not an emergency situation?

The main utility of CRI's statement is that it's opened once again, on a global scale, a conversation around data security and resiliency. This is helpful because it invites us to consider our current practices and fundamental assumptions around how we protect our data. We desperately need this conversation, because in my view we're thinking about it all wrong.

Prevention itself isn't enough

Most organizations tend to think about ransomware attacks in terms of prevention — how to stop them from happening in the first place. Huge swathes of cybersecurity budgets are spent trying to build digital walls high enough that no bad actor can ever get across. This isn't a bad practice — preventive measures are important — but they are not infallible. What happens when ransomware is successful? Response time is important, but no matter how fast you respond to a successful ransomware attack or breach, you still must work to undo the damage caused and this is why having resiliency and recovery capabilities comes into play.

It's time for more conversation on this point. Not because the answer is particularly elusive, or profound, but rather because it's right under our nose, and insufficiently discussed: Backup and recovery strategy. It's frustrating that this is often seen as a nice-to-have when, in fact, it is really a fundamental aspect of your defense-in-depth strategy. More than anything else, including legislation, international agreements, policy positions, a sound backup and recovery strategy has the greatest potential to greatly reduce the impact of ransomware and bad actors.

The power is within backup and recovery

Ransomware is a problem, but there is a solution. Did you know that just over 50% of businesses have a backup and recovery plan? Having a sound backup and recovery strategy with purpose built backup

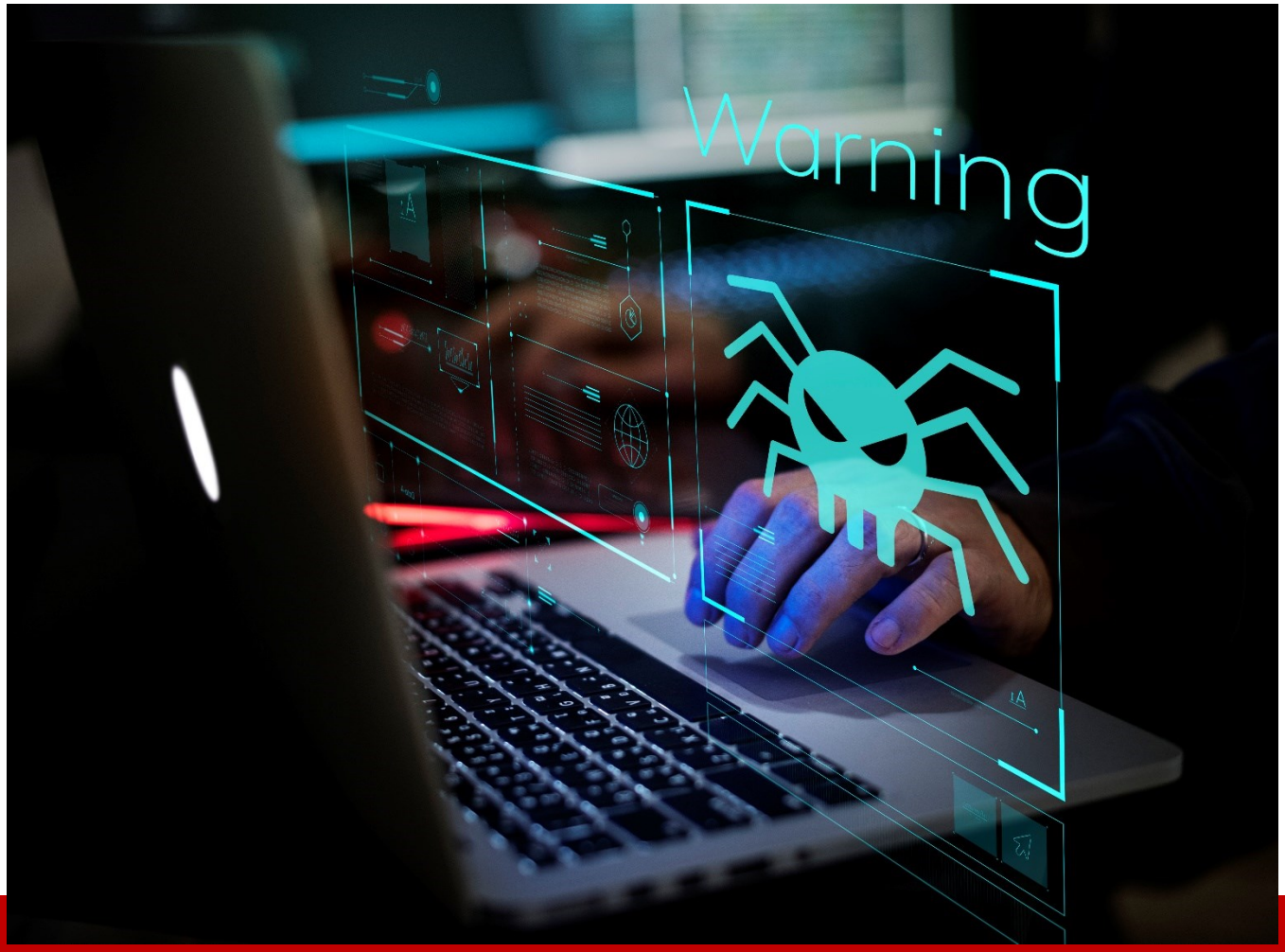
and recovery tools for your critical data and systems can take all the power away from ransomware actors — if you are impacted by a ransomware attack, you don't have to think through whether or not you need to pay to get your data back, you already have the ability to recover it from your encrypted, immutable and isolated backups.

Every CISO and security practitioner should take the CRI's pledge as an opportunity to reinforce the seriousness and impact of ransomware with their boards and leadership within their organization and have a risk discussion based on the organization's control environment highlighting any gaps in your data resilience and recovery posture. Simply having a working backup and recovery can greatly reduce the risk associated with ransomware, not to mention non-malicious and accidental data loss scenarios. Like I said, having preventative measures in place is important as we all know, but it is equally important to have data resilience and recovery capabilities in place to protect your sensitive data when bad things happen. So, my ask is this…do yourself and your organizations a favor and take a fresh look at your data resilience and recovery capabilities, if you don't have a plan, create one; if you don't have the capabilities to recovery critical data implement them or share this information with your leaders and Board members and initiate risk-based discussions and options to address gaps in your capabilities.

While the CRI's pledge is a positive step, I'm certainly not waiting for them to solve the ransomware problem. But I'm hopeful that all the energy and attention it's generated will compel companies to take a hard and objective look at their data resilience and recovery capabilities and plans and take action to address any gaps. In doing so, you are taking control and changing the narrative around the impact of a ransomware attack on your organization.

About the Author

Todd Thorsen is the Chief Information Security Officer of CrashPlan. He brings more than 15 years of information security experience across various disciplines. Todd has a proven track record of building and leading security programs focused on global security operations, risk and compliance, incident response, resilience, and data protection. He can be reached online on LinkedIn and through the company website at www.crashplan.com.



MGM & Caesars Cyberattacks: Lessons Learned

By Tim Callan, Chief Experience Officer, Sectigo

In the aftermath of the MGM and Caesars cyberattacks, many IT professionals are probably asking themselves, am I next? What lessons can businesses learn from these attacks and what can you do to make sure you are not next?

One thing to keep top of mind is the fact that everybody is a potential target. Many people say, “I'm not a major casino, bank, or business. Why would anyone go after me?” The answer is, why not?

If you are running digital systems necessary for your business to operate, you are a target. If your business comes to a stop, that is damaging to you, your customers, and your reputation. Therefore,

anybody who has digital processes at the core of their business is a potential ransomware target. Thus, point number one is to get over the line of thinking that “I’m not a target” because you most certainly are.

Second, social engineering is and will always be an attack vector. By their very nature, our digital systems demand that human beings interact with them. And as long as there are places where human beings can interact with systems, human beings can be tricked into providing access to the system. Social engineering has been going on since before the internet, and the reason it has persisted for decades and decades is because it consistently works.

How then do we deal with social engineering? For many years, the approach has been training. We do recommend training, but training is not even remotely sufficient to solve the problem. If it were, these attacks would not continue to succeed. And no matter how much training people receive, they invariably make mistakes. They forget, they get distracted, they get taken in by a different flavor of attack that they are not used to and fall for it.

So, what do you need to do? Your best defense is to take the decision making out of the human being's hands. If I am supposed to click on a window and put in a username and password, then there are ways for me to be tricked. There are ways for someone to trick me into putting my username and password in the wrong place. There are ways for someone to trick me into giving my username and password out to somebody else.

In a recent published attack, bad actors defeated one-time passwords using deep voice fakes spoofing the identity of the victim’s internal IT help desk team. When asked for a one-time password the employee readily gave an OTP to this “internal help desk.” The bad actors then used that one-time password in conjunction with a stolen credential to steal access to the company’s systems.

To the degree that you can remove the decision making from human beings, you take away the social engineering angle. Fortunately, such a mechanism has been used for 40 years and has never been defeated. That mechanism is Public Key Infrastructure, or “PKI.” Employees using known devices—laptops or mobile devices or workstations that remain at an office—can authenticate their identities automatically through the use of digital certificates on these devices. No known attack can defeat the cryptographically unassailable mechanisms that assure these certificates are real and true. And social engineering attacks to gain access are defeated.

So why would network administrators fail to employ PKI-based authentication? The main reason is ignorance. They think that username-password is secure, or they erroneously think that multi-factor authentication (MFA) is a bullet-proof addition. However, every major multi-factor authentication mechanism can be defeated by a determined, educated, and well-resourced attacker.

Multi-factor authentication leads users to a false sense of security. When you have MFA, you begin to think that you are beyond attack. In reality, you are beyond attack solely by “spray and pray attackers,” but you are not beyond attack by an Advanced Persistent Threat (APT). That is a mistake many people make. They put MFA in place, and they think they have checked a box that they need not think about again. In reality, well-resourced professional attackers can and do frequently get around it. Taking the decision making out of human hands as much as you can is what is most needed because the oddities of how the human brain works are not something that you and I are going to solve in our lifetime.

Companies must also adopt a zero-trust security mentality wherein no one trying to gain access to your site can or should be trusted. One of the core tenets of this paradigm is that it requires users to be verified regardless of whether or not they have been previously authenticated. The zero-trust framework institutes stringent access controls, continuous validation and yet another layer of security and protection from bad actors.

Another cyberattack like those at MGM and Caesars is not a matter of if but when. Taking the decisions out of the user's hands and implementing critical, proven protocols like certificate management, PKI and zero trust, will ensure you are not the next victim of a cyber attack.

About the Author

Tim Callan serves as Chief Experience Officer at Sectigo, the leading provider of automated certificate lifecycle management and digital certificates, spearheading efforts to optimize the customer journey across all aspects of the business. Tim has more than 20 years of experience as a strategic marketing and product leader for successful B2B software and SaaS companies, with 15 years of experience in the SSL and PKI technology spaces. For more information on Sectigo, please visit www.sectigo.com. To reach Tim Callan direct, please email tim.callan@sectigo.com.

Evolution and Escalation of Cybersecurity Threats

The Darwinian Effect in the Threat Community

By Augusto Barros, Vice President Cyber Security Evangelist at Securonix

Among the typical predictions for the upcoming new year, we often see something like “threats will keep growing.” A prediction like this is like saying there will be some rainy days next year, or that some place in the world will suffer from drought. But with all the investment we do in security, why do we keep seeing threats growing?

First, it is important to understand the nature of threats. Threat existence and intensity is mostly independent from an organization’s security effort. Those efforts can reduce the risk from a threat causing harm, but they won’t reduce the threat itself. Sometimes, if a large portion of the potential targets implement a certain control, that “herd immunity” can affect the overall threat intensity: If there are no chances to be successful with a certain approach, threat actors are likely to abandon that approach to try something else.

Another reason why threats keep growing is related to how threat actors evolve their capabilities. Threat actors are good at advancing their capabilities because they operate as a syndicate. The level of information sharing in the "threat community" is far higher than what we have on the defense side. Why? Threat actors do not have concerns about legal implications, mandates, privacy or IP protection. If sharing information makes sense for them to achieve their goal, they will do it, regardless of the implications.

Threat actors also advance their capabilities to counteract the evolution of defense practices, but they don't necessarily need to produce more advanced attack techniques. They need to produce more effective techniques. If there's low hanging fruit, they will go for it; no need for a high tech alternative when simple and manual will do it. They optimize towards their final objective, not towards a specific path to it. If they want to make money, they can move from trying to steal it directly from bank accounts to simple extortion when that produces more money at a lower cost. They don't need to evolve to break all the barriers put up by defenders around those bank accounts if there is a cheaper and more efficient manner to get money.

Because of all points above, the threat community acquires a certain evolutionary, Darwinian aspect. Just as species will not necessarily evolve towards better, advanced eyesight, speed and strength to survive, threat actors may not produce more advanced TTPs either: They just need to survive - or, in their context, achieve their objectives. While objectives are easily reachable, no evolution is necessary.

Finally, the potential outcome of threat activity is also something that grows continually. Cyber-attacks are one of the ways criminals can perform financial fraud, for example. If there is more money circulating, it will attract more criminal activity, and criminal activity these days is one of the major drivers behind cyberthreats. There are more potential targets, as the world becomes increasingly connected. It is natural to see more attempts to cause harm online when there are more things that can be harmed that way.

The ability of threat actors to evolve their practices, more and bigger targets available, combined with how limited the target organizations are in affecting threat presence or intensity are clear explanations about why it is so easy to predict that threats will keep growing. So don’t be surprised if you see it, but also there is no need for defeatism. Common criminal activity has been around for years, but it doesn’t mean that our law enforcement does not work. Threats, just like crime, are part of our existence in the connected world. We must do as much as possible to keep the risk of suffering from those threats under control, but at the same time, keep in mind that it will be a continuous effort that will never reach a point where the problem is “solved”.

About the Author

Augusto Barros is an established security professional, currently serving as VP Cyber Security Evangelist at Securonix. In this role, Barros works to strategically deliver the best threat cloud native detection and response solutions. He helps customers around the globe leverage the latest SIEM advancements with best-in-class analytics to avoid cyber threats and optimize ROI. Before coming to Securonix, he spent five years as a research analyst at Gartner talking to thousands of clients and vendors about their challenges and solutions on security operations. This role led him to Securonix, as he watched the company grow and evolve as a visionary and leader in the space. Previous positions held include security roles at CIBC and Davis and Henderson, Credit Solutions Group. Augusto can be reached online at: https://www.linkedin.com/in/apbarros/ and at our company website: https://www.securonix.com/

Cyber Insurance: A Smart Investment to Protect Your Business from Cyber Threats in 2023

Don't wait until it's too late - get cyber insurance today and secure your business for tomorrow.

By Zia Muhammad, Cyber Risk Advisor, Onpoint Insurance Services

In the current era of technological advancements, businesses are increasingly reliant on technology that opens up a new world of increasing volume and sophistication of cyber threats. Cyberattacks severely impact businesses and cause significant financial losses, damage to their reputation, and compromise sensitive data. Therefore, it is crucial for businesses to prepare for the inevitability of cyber-attacks, mitigate risks, and secure their infrastructure. This can be done by implementing proactive defensive security controls and implementing cyber insurance to have your back in case something goes wrong. This article covers Cyber Insurance and Why it Can Be a Smart Investment for Your Business.

What is Cyber Insurance?

According to the U.S. Federal Trade Commission (FTC), cyber insurance is a particular type of insurance that helps businesses mitigate financial losses resulting from cyberattacks. Consider it as a contract between the insured business and the insurer company where the insured is obligated to pay a premium, and the Insurer is obligated to provide coverage for various aspects of cyber attacks, such as data breaches, ransomware, network interruption, cyber extortion, identity theft, and other cyber threats.

Cyber insurance covers the damage that a business suffers because of a cyberattack. The coverage usually covers the costs for breach recovery, notification costs, business interruption costs, ransom costs, investigative services, data recovery, and legal fees, among others. As per U.S. Government Accountability Office (GAO) guidelines, every business that handles customer data or stores information online should consider cyber insurance.

Scope and Coverages Offered in the Cyber Insurance Market

The cyber insurance market has experienced significant growth in recent years, with premiums reaching $10 billion in 2021. However, the market still faces challenges in accurately assessing and pricing cyber risk. Therefore, it's really important to note that the scope and coverage offered in the cyber insurance market are constantly evolving to keep up with the changing landscape of cyber threats. On a broader level, cyber insurance can be divided into two major categories: first-party coverages and third-party coverages.

First-party coverage protects the insured business data and resources, including employee and customer information. This coverage primarily covers incidents that directly impact your business and underlined operations. For example, business interruption costs, legal counsel, regulatory obligations, recovery and replacement of lost or stolen data, customer notification, lost income, crisis management, public relations, cyber extortion, forensic services to investigate the breach, and penalties related to the cyber incident, among others.

On the other hand, third-party cyber coverage usually protects businesses from legal liability if a third party brings claims. This coverage typically includes payments to consumers affected by the breach, claims, and settlement expenses relating to disputes or lawsuits, losses related to defamation and copyright or trademark infringement, and costs of responding to regulatory inquiries, among others. These coverages are not universally standard or consistently adopted by all providers. Instead, these are general categorizations that average out the offerings of major providers. The underlined breakdown information is here to provide you with an overview and a broader level of knowledge and does not explicitly feature any carrier or insurance provider.

Recommendations for businesses

The convergence of cyber insurance is creating opportunities for organizations to make smarter investments. Historically, cyber insurance focused on financial protection while cybersecurity focused on

data protection. However, the two are now merging as cyber insurers have started incorporating data-driven risk assessments and requirements into their policies. This has led to a closer alignment between cybersecurity teams and insurance buyers, resulting in improved cyber resilience. Organizations that invest in cybersecurity not only protect themselves but also receive better rates and terms upon policy renewal. Insurers are also offering more sophisticated services and partnerships to help policyholders achieve compliance and best practices. Despite challenges in obtaining and renewing policies, the convergence of cybersecurity and cyber insurance offers a win-win situation for organizations and their security staff.

Cyber insurance should not be viewed as the first line of defense but instead as a component of a broader risk management strategy that includes identifying, defending, and residue risk transfer. The first step should be to access the current state of security of your organization. For instance, The Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (CAT) to help financial institutions, banks, and credit unions identify cybersecurity risks and determine their preparedness. The CAT is also useful for non-depository institutions and other small companies. The second step should be to implement defensive measures, such as installing antivirus software, updating systems and applications, encrypting data, using strong passwords, and educating employees on cybersecurity best practices. Finally, the third step should be to buy cyber insurance that can cover the costs and damages of cyber incidents that may still occur despite your best efforts.

Choosing the Right Cyber Insurance Policy

Cyber insurance is essential for businesses to cover the costs and damages of cyber incidents, but it is not easy to obtain. Different policies have different terms and conditions, such as coverages, exclusions, limits, deductibles, and premiums. These can make buying cyber insurance a complex and challenging process. When choosing a policy, it is important to review existing business policies, understand the volume of sensitive data, reduce risk where possible, and carefully read the policy to ensure adequate coverage. That is why you need a cyber expert on your side while buying cyber insurance.

A cyber expert can help you understand the contract language, compare different policies and options, and choose optimal coverage tailored to your needs. You don't want to end up with an insurance agent who only cares about lowering the budget and selling you a cheap insurance policy that you keep paying for, but when there is a cyberattack, the insurance proves useless due to policy exclusion or other conditions that you or your agent were not aware of. You want to buy cyber insurance that gives you the best value for your money and the best protection for your business.

That is why you should trust OnPoint Insurance Services, a trusted and reputable consultation company that provides outstanding service and has a team of experienced insurance professionals. OnPoint Insurance Group is an independent agency that works with over 150 insurance companies to provide customized and affordable solutions for first-party cyber insurance and cyber liability insurance. Its mission is to deliver quality and honesty to its customers and to help them protect their assets. OnPoint Insurance Group also offers 24/7 service, online quotes, and easy switching options for its customers. For your free business evaluation and quotes, visit their website and get a free quote today.

Ending Remarks

Cyber insurance is not a luxury, but a necessity for any business that relies on technology. Cyber threats are constantly evolving and becoming more sophisticated, posing serious risks to your data, reputation, and bottom line. By investing in cyber insurance, you can protect your business from the financial and legal consequences of a cyberattack, and gain access to valuable resources and support to help you recover and resume your operations. Cyber insurance is a smart investment that can give you peace of mind and a competitive edge in the digital age. To find the best cyber insurance policy for your business, compare online quotes from different insurers with OnPoint Insurance Services and choose the one that meets your specific needs and budget. Don't wait until it's too late - get cyber insurance today and secure your business for tomorrow.

About the Author

Zia Muhammad is a Cyber Risk Advisor at OnPoint Insurance Services. He has a master's and a Ph.D. in cybersecurity. He helps clients assess and manage their cyber risks through cyber insurance. He advises them on how to select the best insurance coverage for their needs, compare different policies, and negotiate favorable terms. He also ensures that their insurance program aligns with their risk profile and business goals. His goal is to help clients make smart decisions and optimize their risk strategies in the face of evolving cyber threats. Zia can be reached online at (zia@onpointins.com, and on LinkedIn) and at our company website https://onpointins.com/

Cyber Resilience – Beyond Cyber Security

In a world where 100% security is not possible, we need to be resilient as we strive to be secure.

By James Gorman, Hard2hack.com

The evolving landscape of cyber threats in our increasingly digital world calls for a strategic shift from traditional cybersecurity to a more encompassing and proactive approach: cyber resilience. This transition is not just a change in technology or tactics but a fundamental shift in mindset and organizational culture. Let's delve deeper into each of the critical steps to achieve this crucial transition:

1. Assess and Understand Risks

Understanding the unique risk profile of your organization is the bedrock of cyber resilience. This involves:

- **Comprehensive Risk Assessments**: These should cover all aspects of the organization, including IT infrastructure, data, personnel, and third-party interactions. A thorough assessment identifies potential vulnerabilities and threats, both internal and external.
- **Regular Reviews and Updates**: Cyber threats are dynamic, so regular reviews and updates to the risk assessment are essential. This ensures that the organization's understanding of its risk profile evolves with the changing threat landscape.

2. Develop an Incident Response Plan

An effective incident response plan is a cornerstone of cyber resilience. Key components include:

- **Clear Procedures and Protocols**: The plan should outline specific steps during a cyber incident. This includes identifying the breach, containing it, and initiating recovery processes.
- **Designated Response Team**: A dedicated team, well-versed in the response plan, is crucial. This team should have clearly defined roles and responsibilities and be equipped to act swiftly in the event of an incident.
- **Communication Strategy**: A well-thought-out communication strategy is vital, both for internal coordination and for managing external communications with stakeholders, customers, and potentially the public.

3. Foster a Security Culture

Building a culture of security is about more than rules and regulations; it's about creating an environment where cyber resilience is everyone's responsibility.

- **Employee Training and Awareness**: Regular training and awareness programs help employees understand the importance of cybersecurity and their role in maintaining it. This includes recognizing potential threats like phishing attacks and practicing safe online behaviors.
- **Empowering Employees**: Employees should feel empowered to voice concerns and report suspicious activities. A culture of openness and vigilance can be one of the strongest defenses against cyber threats.

4. Regularly Test and Update Systems

Keeping your defenses up-to-date is critical in the face of constantly evolving cyber threats.

- **Continuous Monitoring and Testing**: Regular penetration testing and vulnerability scans help identify weaknesses in the system before they can be exploited. Continuous monitoring allows for the early detection of unusual activities that could signify a breach.
- **Software and System Updates**: Ensuring that all software and systems are up-to-date with the latest security patches is crucial. Outdated systems are often the weakest links in cybersecurity.

5. Collaborate with Industry Experts

Collaboration and knowledge sharing are essential in staying ahead of cyber threats.

- **Partnerships and Networks**: Engaging with industry experts, attending cybersecurity conferences, and participating in knowledge-sharing platforms can provide valuable insights into emerging threats and best practices.

- **Leveraging External Expertise**: Sometimes, the best approach is to seek external expertise. Cybersecurity firms and consultants can provide specialized knowledge and resources that might be beyond an organization's internal capabilities.

Beyond the Basics: Advanced Steps Towards Cyber Resilience

1. Implement Advanced Technologies

Leveraging advanced technologies like AI and machine learning can enhance an organization's ability to detect and respond to cyber threats more effectively.

- **Predictive Analytics**: Using AI to analyze patterns and predict potential threats can provide a significant advantage in preemptive defense.
- **Automated Response Mechanisms**: Automating certain aspects of the cyber defense can speed up the response time and reduce the impact of human error.

2. Create Redundancy and Backup Systems

Ensuring that critical data and systems have redundancy and are regularly backed up can mitigate the impact of data loss or system compromise.

- **Regular Data Backups**: Regular and secure backups of critical data ensure that essential information is not permanently lost in the event of a cyberattack.
- **Disaster Recovery Plans**: These plans ensure the organization can quickly restore its critical functions after a significant cyber incident.

3. Legal and Regulatory Compliance

Staying compliant with legal and regulatory requirements is not just about avoiding penalties; it also forms an integral part of a robust cyber resilience strategy.

- **Understanding Compliance Requirements**: Different industries often have specific cybersecurity regulations. Understanding and adhering to these is crucial.
- **Regular Compliance Audits**: Regular audits can help ensure that the organization remains compliant and identify potential areas of improvement in cybersecurity practices.

4. Engaging Stakeholders

Ensuring that all stakeholders, from employees to board members, understand and are committed to the organization’s cyber resilience strategies is crucial.

- **Board-Level Engagement**: Ensuring cyber resilience is a board-level issue guarantees the necessary attention and resources.
- **Customer Education**: Educating customers about cybersecurity practices related to your products or services can extend your cyber resilience efforts beyond the confines of the organization.

Conclusion: Embracing Cyber Resilience for a Safer Future

The transition from cybersecurity to cyber resilience is more than a tactical shift; it's a strategic imperative. In today's digital world, the question is not if a cyber incident will occur but when. By embracing cyber resilience, organizations can prepare themselves for these challenges, ensuring they can respond, recover, and thrive in the face of cyber threats. This proactive approach safeguards against immediate threats and strengthens the overall organizational resilience, ensuring a safer and more secure future in the digital age.

Join the Hard2hack Mailing list today:

https://hard2hack.com/join-the-hard2hack-mailing-list/

About the Author

James Gorman, Hard2hack.com. With over 35 years of experience in cybersecurity, network engineering, and IT operations, James is a trusted advisor and consultant for startups, enterprises, and government agencies. As a Fractional CISO and CTO at Hard2Hack.com, James helps clients secure, design, build, and maintain their cloud and network infrastructure while achieving compliance with various standards and regulations, such as HITRUST, FedRAMP, PCI, and ISO.

His aim is to enable digital transformation and innovation through robust, reliable cybersecurity solutions and strategies. He has successfully led teams through multiple audits, certifications, and migrations, delivering scalable, resilient, and cost-effective outcomes. James' notable projects include providing security assessments and certifications for Business Associates in Health Care, payment gateways, building the data center and platform infrastructure for a SaaS provider in the identity space, and developing universal security technologies for 5G networks. He is passionate about staying ahead of the curve and leveraging his diverse and extensive expertise to solve complex and challenging problems.

James can be reached online at (jg@hard2hack.com, https://www.linkedin.com/in/jamesgorman/) and at our company website https://hard2hack.com.

Cybersecurity Preparedness 2024

By Chris Leach, Board Advisor for Judy Security

The new year is just around the corner. We have had a great Thanksgiving meal and soon our thoughts will turn to what is to be accomplished in 2024. Many businesses will start the year off with optimism while many new businesses will be looking for a way to get a leg up on the competition.

In an increasingly digital world, small and medium-size businesses (SMBs) have become prime targets for cybercriminals. With the rapid advancement of technology and the growing reliance on digital infrastructure, the need for robust cybersecurity measures has never been more critical. As we enter a new year, SMBs must prioritize cybersecurity to safeguard their sensitive data, protect their customers, and ensure the continuity of their operations. This presents you, the Managed Service Provider (MSP), an ideal opportunity the onboard new customers or strengthen your relationship with your current customers – perhaps you are a small or medium sized business yourself!

So, what should the MSP be aware of in 2024 as it relates to cybersecurity, so you are better prepared to work with your current and future customers? First let's look at the overall cybersecurity space. There is a tremendous lack of expertise.

According to a report issued by (ISC)[2], there is a global shortage of cybersecurity professionals of over 3.12 million and this number is growing. Most of the available processionals come at a high price often out of reach of the typical business. The turnover of these professionals is high as they are often lured into moving to another company for higher pay and benefits.

Next, is the cost element of solutions, platforms, and software. Unlike their larger customers, the large enterprise, the SMB owner cannot afford the high costs that are a part of a robust solution. Providers of these solutions have a difficult time working with the SMB community due to their cost structures. Therefore, the SMB customer must either deploy a solution that does not provide a strong protection to their company or simply hope that they are not subject to a cyber attack.

In addition to offering an integrated solution, the MSP should also prioritize continuous training and education for their own technical teams and the employees of their SMB customers. Staying up to date with the latest threats and technologies is crucial in the ever-evolving cybersecurity landscape. By providing ongoing training, the MSP can ensure that their customers have the expertise and knowledge necessary to maintain good cybersecurity hygiene.

Finally, there has been a tremendous amount of legislation globally around the topic of privacy. Starting in Europe with GDPR the need for strong privacy policies and controls has been moving across the globe. In the United States there is currently no Federal mandate. Instead, many states have created their own requirement. Among those states with a current privacy requirement are New York, California, Colorado and Utah and Virginia – this list is growing. Some of these laws overlap while others contradict each other. These laws require a breach response, notification requirement and customer rights. It is important for SMBs to have a robust cybersecurity program in place to protect sensitive customer data and comply with legal requirements. The MSP can assist their customers in executing and responding to privacy laws, further solidifying their role as a trusted cybersecurity partner.

To summarize the issues that an SMB must deal with:

- Lack of available cybersecurity expertise with the corresponding budget
- Access to state-of-the-art solutions and software due to cost constraints
- Inadequate and current training and education
- Added business requirement of complying with the various privacy laws

You, the MSP, can assist your customer by offering a cybersecurity solution that is an “easy button” for them. This may be an additional revenue stream for you and will strengthen your relationship with them.

Let’s take a few moments to call out the elements of a strong solution provider for a robust and current cybersecurity that should be considered.

When selecting an MSSP provider, the MSP should look for one that offers an all-in-one solution and can demonstrate how they keep their solutions and platforms up to date in response to the rapidly changing threat landscape. The provider should also offer various levels or packages of services to cater to the specific needs of different businesses. Seamless installation and self-service options for changes should be provided to make the transition to the MSSP platform as smooth as possible.

By offering a comprehensive cybersecurity solution and addressing the specific challenges faced by SMBs, the MSP can position themselves as a valuable partner in safeguarding sensitive data, protecting customers, and ensuring the continuity of operations. This not only presents an opportunity for additional revenue but also strengthens the relationship between the MSP and their customers. With the right

approach and a focus on providing effective cybersecurity solutions, the MSP can become the hero for SMBs in the digital age.

All these things will make you the hero and take away some of your operating frustrations and concerns.

As always – Good Luck and Good Computing

About the Author

Chris Leach is a Board Advisor for Judy Security. His career spans over 30 years in risk analysis, operations, strategy and financial controls and has included senior management, consulting and entrepreneurial experiences. He has held positions at HP, HPE and DXC. Chris is the founder of CISO Tool Box where he works with CISOs, CTOs, CIOs on security strategies, security mega trends and emerging threats. Follow Chris can be reached online at LinkedIn and at the Judy Security website: https://www.judysecurity.ai/

Digital Technologies Power Global Operations but Present Growing Risks

By Charlie Regan, CEO, Nerds on Site

As more and more industries and businesses turn to digital technologies in order to power their operations, cyber-attacks present a larger and more widespread threat for organizations and enterprises all over the world. The frequency and severity of these attacks have grown exponentially in recent years, causing major disruptions in services and costing companies enormous sums of money and time. This growing risk affects every level of industry, from critical services and infrastructure down to small-to-medium enterprises. In fact, for every high-profile attack, there are hundreds that affect smaller companies and networks, such as small businesses, city and town municipalities, local medical facilities, legal offices, and non-profit organizations. Cyber security is not just a concern for critical infrastructure and major corporations, but for any organization that means safeguarding the networks and systems vital to maintaining their operations.

The rise in cyber attacks has coincided with the number of companies and services that are now hosted on digital networks. While these technologies have made countless processes easier to execute, they also come with inherent vulnerabilities. This growing pool of potential targets has attracted more and more hackers and ransomware gangs that endlessly seek to exploit weaknesses in any system. Advancements in these digital technologies, such as artificial intelligence, may have improved operational efficiency and allowed companies to become more streamlined and sustainable, but they have also

enabled hacker groups to increase the severity and sophistication of these cyber-attacks and made it easier to gain access to systems and sensitive information. Hackers are casting wider nets, probing deeper for network vulnerabilities, and breaching companies at higher rates, all at greater and greater speeds afforded to them by the continued advancement of digital technologies.

Cyber attacks are largely a financially-motivated crime. A hacker or ransomware gang is able to gain access to a company's servers and threaten to either release sensitive customer data or cripple their operations unless payment of ransom is made. While critical infrastructure and high-profile companies with billion-dollar valuations would seem the logical preferred target of these groups, small-to-medium enterprises actually account for almost 70% of reported attacks. The reason being is quite simple. These companies, by and large, lack the resources and security protocols to repel cyber attacks, and hackers will always gravitate towards the path of least resistance.

While money may be the principal motivation for these ransomware groups, it is not the only one. Many of these hacker groups are actually using these tactics in order to advance some politically or ideologically motivated agenda. This can be domestic, as we have seen a rise in 'hacktivism', the practice of using cyber attacks and breaches as exercises in civil disobedience and a means to strike out at political parties, industries, and businesses. This can also be global, however, as these groups militarize. As international conflicts continue to erupt and escalate in every corner of the world, cyber terrorists join ranks in these wars in order to strike out at the economic and social structure of their enemies. Whether this is Russian efforts to destabilize Ukraine or Hamas attacking United States organizations that use Israeli-made technologies and industrial devices, these hacker groups fight their own war on digital battlefields. When mobilized, these groups can cause untold damage and disruption to a nation's economic and military capabilities.

For many companies, the threat of cyber attacks looms large. Not only do these attacks cause loss of revenue and disruption of services, but they also come at the risk of the personal data and information entrusted to them by their valued customers and clients. These incidents are not just minor threats to a company's continued viability. Many do not last six months following a reported breach. Then there is the toll that these attacks take on the very fabric of our society. Hospitals and health centers have to turn patients away and prioritize the urgency of one surgery over another due to massive operational outages. Municipalities and critical infrastructure are unable to respond effectively to emergencies and provide vital services to constituents and customers.

As these attacks increase in frequency and scope, cybersecurity protocols must be implemented and adhered to in order to thwart hackers and ransomware groups. There needs to be a better understanding of security risks and appropriate cyber attack strategies among all levels of business and industry. There must be a concerted effort to become more proactive. The traditional approach to cyber security is not enough. Cyber criminals are able to gain access to and set up network surveillance and data drips for months before businesses are even made aware of a breach. By implementing safeguards that can monitor all outbound traffic on a network and install egress controls to deny any connections that are unknown and/or connecting to highly suspicious countries, organizations can identify threats and prevent breaches with greater speed and efficacy. The deployment of these protocols would allow businesses and IT providers the foresight to know about any activity taking place on their network and over their

network connection and offer them the tools and resources to effectively handle any potential threat that may arise. Until this has been achieved, cyber-attacks will continue to rise, and, given our world's increasing reliance on digital technologies, so will the stakes.

About the Author

Charlie Regan, CEO at Nerds On Site.

Charlie can be reached online at ronnie@vewpr.com and at our company website https://www.nerdsonsite.com

Enhancing PCI DSS Compliance: The Urgent Need for Risk-Based Prioritization

By Ian Robinson, Chief Architect of Titania

Keeping U.S. commercial critical national infrastructure (CNI) organizations safe is vital to national security, and it's never been more top of mind as international conflicts and cyberattacks increase and create tensions for businesses, governments, and citizens. These 16 critical sectors - communications, energy, financial services to name a few - with their assets, systems and networks are considered so crucial that their breakdown or destruction would cripple the operations of the country and put public health or safety at serious risk.

Payment card data and payment systems within CNI networks are a natural target for cybercriminals thanks to the riches they hold. And the deadline for organizations to meet the latest data security standards (PCI DSS 4.0) is looming. By March 2024, compliance goals must be hit, and the harsh reality is that according to recent research only 37% of these organizations possess the capability to effectively categorize and prioritize compliance risks within their networks. In the face of ever-evolving cybersecurity threats, this deficiency poses a significant threat to the security posture of critical national infrastructure and emphasizes the need for a robust and prioritized approach to compliance.

The Imperative of Risk-Based Prioritization

Recognizing the urgency of this challenge, it's time for organizations to adopt a risk-based prioritization approach to CDE network hardening; also known as risk-based vulnerability management (RBVM). Key to this is a detailed risk analysis of misconfigurations which leverages networking expertise to determine the ease of exploit, potential impact to security, and ease of fix. This capability has been automated and is available at network scale and on a continuous basis, if required. Using risk-focused solutions, organizations are able to identify compliance risk trends and proactively address their most critical vulnerabilities to strengthen their defense against evolving cyber threats - efficiently and strategically.

Automation Revolutionizes Compliance

Historically, achieving PCI DSS compliance involved laborious manual mapping of network infrastructure device checks to specific requirements. A time-consuming process that was prone to error proliferation. However, new solutions allow for automating ready-mapped network device checks with drill-down access to testing procedures to provide evidence to QSAs. Compliance reports demonstrate whether routers, switches, and firewalls either pass or fail to meet PCI DSS 4.0 requirements. Non-compliances are also prioritized by risk, so organizations can identify gaps. This allows internal security teams to quickly and efficiently categorize and prioritize mitigating action, which is a fundamental aspect of enhancing PCI DSS compliance posture.

Selecting the Right Tools

A certified NSA cryptanalyst and PCI expert with over twenty years in the payment card industry recently shared that most products on the market don't truly understand PCI and vendors rarely have a deep understanding of data security requirements, so it is essential that companies investigate this when selecting a solution. It's crucial that solutions measure how well an entity meets the PCI DSS 4.0 requirements.

Choosing automated risk-based prioritization solutions can guide a business towards a more secure and resilient future by determining exactly how and where configurations do not comply with the desired state. And by reporting what needs to be done to fix the issues identified, the analysis can reduce the time to remediate.

After all, reducing the time to remediate an issue is equally as essential as knowing that a configuration doesn't comply and how it can be mitigated.

Proactive Measures for a Secure Future

Proactive security approaches are the glue that will ultimately protect cardholder data environments (CDE).

Understanding how adversaries operate is key to this, and essential to assessing risk, exposure to attack, and therefore, the priority with which networking devices should be remediated to protect critical areas of the network, such as the CDE.

This is essential for targeting remediation efforts and resources where they are most needed – using attack surface vulnerability assessments and threat intelligence to inform risk prioritization and remediation allows organizations to view what is most critical but also what is most likely to be exploited. Viewing the organization's risk through an attacker's lens takes RBVM to the next level - going way beyond just discovering a vulnerability, it helps understand the risk in the context of real-world threat and insight into the potential impact on a business.

With next year's deadline on the horizon, the time is ripe for organizations to embrace evidence-based reporting to elevate their PCI DSS compliance posture to new heights. But it's also an ideal opportunity to find solutions that support RBVM and provide a risk analysis of each non-compliance leverages networking expertise to determine exploit ease, potential security impact, and fix feasibility. This will ensure organizations achieve security from compliance.

A proactive security approach underpinned with RBVM and coupled with strategies such as Zero Trust network segmentation empowers organizations to address vulnerabilities strategically, reinforcing their defense against evolving cyber threats and safeguarding operations and potentially national security.

About the Author

Ian Robinson, Chief Architect of Titania

Chief Architect, Ian Robinson, works closely with Titania's customers and partners to continuously hone the unique capabilities of its configuration assessment solutions Nipper Enterprise and Nipper; ensuring each product roadmap strategically builds customer value by providing organizations with the insight needed to mitigate their most critical network security and compliance risks, first. With a strong record in full stack development, he is fluent in an array of different languages and versed in the wide range of platforms, frameworks, libraries and integrations needed to build elegant, well-designed, and innovative cybersecurity solutions.

Ian can be reached online at ian.robinson@titania.com and at our company website https://www.titania.com/

How Businesses Can Manage Cryptocurrency Fraud

With cryptocurrency payments on the rise, businesses must learn how to safeguard against potential risks.

By James Hunt, Subject Matter Expert Payments, Feedzai

Businesses across the US are seeking innovative payment methods, with an estimated 75% of retailers looking to embrace cryptocurrency payment options in 2024. However, with cryptocurrency becoming increasingly synonymous with fraud, businesses must continue to take the right steps to protect themselves and their customers.

Weighing up the risk and benefits

Approximately 2,352 US businesses have embraced cryptocurrencies such as Bitcoin for transactions. However, it's crucial for business owners to weigh the pros and cons before diving in. A significant concern is the reputational risk associated with cryptocurrency acceptance. Not all customers view

cryptocurrency favorably, and there are valid concerns to consider. For example, the Federal Trade Commission warns that cryptocurrency payments lack the legal protections that accompany credit or debit card purchases, particularly when disputing transactions. Traditional financial institutions and card issuers offer mechanisms to recover funds, whereas cryptocurrency transactions are not reversible, even in the case of fraud.

However, the finality of cryptocurrency transactions can offer a safeguard against chargeback fraud. This type of fraud occurs when a customer falsely claims a transaction was unauthorized or defective before seeking a refund from their bank or card provider. With the average cost per chargeback costing retailers $128, the adoption of cryptocurrency could ease some of the financial burden stemming from these fraudulent chargeback claims.

Nonetheless, while cryptocurrency may offer a deterrent to certain types of fraud, it does not eliminate the risk of fraud. The digital wallets used to store and manage cryptocurrency are not immune to cyber threats. Businesses can face the peril of their funds vanishing into the ether if these wallets fall prey to hacking, sophisticated phishing attacks, or even flaws within the wallet software itself. Furthermore, the decision to accept cryptocurrency payments could inadvertently lead customers to let down their defenses, making them more susceptible to impersonation scams. In such scenarios, fraudsters might masquerade as your business through text, emails, or phone calls, attempting to swindle cryptocurrency from your customers. This tactic mirrors the deceptive practices seen in Amazon scams, where customers are tricked into sharing their credit card information.

Cryptocurrency – like any innovation – is not a one size fits but it can offer great opportunities. For some businesses, it could open the doors to previously inaccessible markets and offer a more inclusive financial gateway for global customers. For others, the lower transaction fees associated with cryptocurrency could translate into cost savings for the business. And for some, it may not be the right fit at all. Overall, it's important that businesses have the right defenses in place to prevent fraud and misuse of cryptocurrency, and the following tips could help in that effort.

Protecting your business and customers

If you do choose to accept cryptocurrency payments, there are a few steps you can take to protect your business and customers from fraud. It's also crucial to consult with financial experts to fully understand the implications for your business and any specific regulation in your area.

1. **Be mindful about the coins you accept.**

Being selective in the currencies you choose to accept can help you balance innovation with reputational integrity. For instance, choosing to accept widely recognized and established currencies such as Bitcoin or Ethereum, rather than more volatile or meme-driven coins like Dogecoin can align you with the more stable end of the crypto spectrum. Although no digital currency is immune to the fluctuations inherent in these markets, the broader market acceptance of leading cryptocurrencies may offer a semblance of stability to your customers.

2. **Find the right payment processing method for your business**

The method you choose to accept cryptocurrency payments should be tailored to the unique demands of your business. For instance, physical stores might benefit from implementing QR code payments. This system enables customers to quickly scan a QR code at the checkout, which is linked to the store's cryptocurrency wallet. Vigilance is key in securely displaying this code to prevent fraudulent replacements by scammers. When managed correctly, QR code payments offer a swift, secure, and contactless payment option suitable for bustling retail environments.

Additionally, there are various cryptocurrency Point of Sale (PoS) systems designed to facilitate the acceptance of crypto and its conversion into traditional currency. It's crucial to partner with a reliable crypto payment processor that can efficiently convert your cryptocurrency earnings into fiat currency. The choice of platform can range from specialized services like Coinbase to versatile processors such as PayPal.

3. **Set limits for cryptocurrency payments**

Setting transaction limits or payment thresholds for customers is a great risk management strategy when it comes to accepting cryptocurrency payments. By setting the maximum amount that can be transacted within a specified time frame, it gives you as a business more control over how funds flow and helps mitigate the impact of fraudulent activities and large losses.

4. **Educate your staff and consumers on cryptocurrency fraud**

Educating both your staff and customers about the risks of cryptocurrency fraud is a vital step in safeguarding your business against fraud. One effective method to raise awareness among customers is through your existing marketing channels. For example, incorporating reminders in your email communications warning customers not to click on links from unexpected texts, emails, or social media messages, even if they appear to originate from your business. For your staff, it's important to add awareness about cryptocurrency to their training and keep this up to date in line with the latest developments.

5. **Stay updated on the cryptocurrency landscape**

It's important to stay up to date on the latest regulations – especially when it comes to accepting cryptocurrency payments. Failure to do so can land your business in hot water. It's also valuable to monitor recommendations from bodies like the Federal Trade Commission on how to manage fraud risk.

While blockchain technology can enhance payment security by reducing fraud risk, protecting customer information, and ensuring transaction integrity, it is not a panacea for all types of fraud. Businesses must, therefore, carefully assess and manage the risks associated with accepting cryptocurrency to make an informed decision.

About the Author

James Hunt holds over 20 years of experience across fraud, risk, and payments. He is currently the Subject Matter Expert, Payments at Feedzai. Prior to joining Feedzai – a financial fraud detection software company – James worked at GoCardless where he was a Senior Manager, Risk Operations. He was also previously a Senior Director at CyberSource – a leading payment management company, owned by Visa Inc.

You can learn more about Feedzai by visiting our website: https://feedzai.com/

It's Time to End the Myth of Untouchable Mainframe Security.

By Al Saurette, CEO, MainTegrity,

Most large organizations, including 70% of Fortune 500 companies, rely extensively on mainframes for managing their business and IT infrastructure.

However, despite the significant role mainframes play, the conversation of how to best secure mainframes security does gets relatively little attention. Considering today's cyberthreat landscape mainframes have never been more vulnerable to attacks. Cyberattackers are becoming bolder, stronger and more innovative by the day.

The timing couldn't be worse. A large cohort of senior, experienced security professionals are set to retire in the coming years, further exacerbating the ongoing skills shortage and exerting more pressure on remaining professionals. As the complexity of threats increases, their jobs become tougher. Short-staffed security teams will tend to prioritize their time and mobilize their efforts to reactively address the most obvious issues, which often means mainframe security falls to the bottom of the priority list.

It is critical for mainframe security to re-enter the cybersecurity conversation, and that starts with doing away with commonly held misconceptions. First is the mistaken belief that due to their mature or

streamlined architecture with fewer vulnerabilities, mainframes are virtually impervious to hackers. There is the misconception that they exist in isolation within the enterprise IT framework, disconnected from the external world where genuine threats lurk. And then there's the age factor. People newer to the profession have relatively little experience with mainframe systems when compared to their more experienced counterparts and will tend to not question their viewpoints or approaches of their leaders or senior team members.

This state of affairs can't continue. In the contemporary landscape, modern mainframes are routinely accessed by employees and are intricately linked to applications that encompass a wide array of functions, ranging from processing e-commerce transactions to facilitating personal banking services.

The implications of a breach can't be overstated. Given the substantial financial toll of a data breach, estimated to be USD $9.48 million on average, it's imperative to swiftly detect any potential threat to the mainframe.

To counter this threat to mainframes, security teams must look at two key areas: encryption and early warning.

Encryption is now a weapon, and must be treated accordingly

Encryption is a double-edged sword in today's IT environment. On one hand it serves as a crucial defense mechanism against cyberattacks targeting sensitive data. On the other, encryption can be manipulated by unscrupulous individuals, disgruntled employees, or even rogue state actors. It has emerged as a favored attack vector among hackers due to its remarkable speed on modern mainframes and its susceptibility to reversal. Consequently, malicious actors often follow a straightforward modus operandi: infiltrate a system, initiate malicious encryption, and then attempt to sell the decryption key back to the victim.

It is paramount to proactively halt encryption before it causes substantial harm. The primary challenge lies in establishing a reliable method for detecting encryption in progress, while preventing the support staff from being overwhelmed with an avalanche of alerts. This is especially important in large business and government settings, where the routine exchange of encrypted files is common. A glut of alerts can lead to a desensitized response, ultimately leaving the system no more secure than it was.

To address this, an immediate response, ideally within seconds, is imperative. Unfortunately, relying solely on human intervention falls short of achieving the required speed. The solution lies in the deployment of a specialized tool capable of swiftly detecting the initiation of encryption and promptly initiating corrective measures.

Achieving near real-time encryption monitoring

IBM Security's 2023 Cost of a Data Breach Report highlights a troubling reality: it takes an average of 204 days to detect a breach, followed by an additional 73 days to recover. During this prolonged period,

malicious actors are free to infiltrate systems, discreetly establish backdoors for future access, compromise backup systems, encrypt data, and potentially issue a ransom demand.

For numerous mainframe operators, a significant portion of these nefarious activities occur behind the scenes, escaping detection until it's too late. It's not only a matter of prudence but also a fundamental aspect of business and security strategy for these sites to mitigate risk and attendant damage with early detection.

To address this, a method for identifying malicious encryption as soon as it starts and providing instantaneous reaction is required. One approach involves having the system compile a whitelist of authorized encryption processes. Whenever a new process emerges, updating the whitelist becomes a logical step. However, relying on human intervention for whitelist updates can be risky.

An emerging and more efficient approach - one that our team is pioneering - involves triggering a real-time alert when software detects a rogue process. Whitelist processing can be invoked to determine if the actions are malicious or desired. If it is desired the process is simply resumed, eliminating unnecessary alerts. Otherwise, it's understood to be a malicious attack.

To remove the dependance on human reaction time, the offending process must be suspended, so that no further damage occurs, while support staff investigate the situation. As a result, ensuing damage can be dramatically mitigated, often by several orders of magnitude.

Our very way of life is dependent on the smooth and continuous operation of this critical piece of business and government infrastructure. The lesson for mainframe operators is clear. What may have worked in the past can't be relied on for the future. Now's the time to ask hard questions, break out of a culture of complacency, and embrace innovative new monitoring technologies

About the Author

Al Saurette, the CEO of MainTegrity. With deep experience in mainframes, hybrid cloud platforms, open systems and mobile computing, Al Saurette is recognized as a thought leader in cyber security, compliance and cyber resilience solutions for banks, insurers, transport and government clients in North America, Europe and around the world. Currently, Al is CEO of mainframe cyber security provider MainTegrity Inc. providing next-generation threat detection, advanced file integrity monitoring, automated forensics, and recovery solutions.

Al can be reached online at Al@MainTegrity.com and LinkedIn https://www.linkedin.com/in/al-saurette/

and at our company website https://maintegrity.com/

From the SIEM to the Lake: Bridging the Gap for Splunk Customers Post-Acquisition

By Omer Singer, VP of Strategy, Anvilogic

The smoke has cleared on Cisco's largest acquisition ever: that of Splunk for $28 billion in September. This acquisition has added a new layer of uncertainty for users, many of which were already wondering what the future holds for threat detection and response in the cloud.

The steep buyout premium (31% over the market price) reflects an expectation that customers will stick around and gain a preference for additional Cisco security products. Organizations that spent years investing in Splunk infrastructure and content have good reasons to stay on. They fear that severing ties with Splunk would wreak havoc on workflows that Security Operations Centers (SOC) rely on to assess and mitigate security threats to the business.

But years of delays in their cloud transition, along with leadership shuffles and recent layoffs, have sparked interest in potential alternatives. Improved offerings from the cloud hyperscalers and advanced data lake offerings have kicked off a wave of SOC modernization initiatives.

Over the last few months since the acquisition of Splunk, we've been waiting for the other shoe to drop, and it finally has.

Solving for What the SOC Needs Now: Flexibility and Optionality

The cybersecurity ecosystem is reshaping itself. The technology, the leaders, everything now is shifting so that security teams can have a more open future – a future where they're not locked into a single SIEM, one with freedom for detections, and freedom for response.

From data pipelines to threat detection platforms, an unbundling is taking place. Security organizations increasingly prioritize flexibility and optionality, driving demand for decoupled solutions. Analytics separate from data storage, stand schemas and open table formats are all gaining mindshare.

Interest in decoupling threat detection from log storage is fueled by the huge difference in cost between data platform options. Where tightly coupled SIEM solutions impose a steep ingest tax, cloud data lake options charge by usage and don't limit retention. Use cases whose data can be analyzed outside the SIEM often see cost savings upwards of 80%. The combination of improved visibility and lower spend makes new data platforms appealing. As a result, CISOs have started demanding the flexibility to explore cost-effective alternatives on a per-use case basis.

A New Era of Freedom for Splunk + Snowflake Users

Enterprises are being pushed by lock-in fears and pulled by opportunities for better scale. They are looking for ways to augment Splunk with data platforms that deliver efficiencies and support the latest machine learning. But "rip and replace" is not an option for most, so a bridge is needed for the transition from monolithic SIEMs to a security data lake architecture.

In my experiences working with customers at Snowflake, I saw the immediate impact when they could start using Snowflake alongside Splunk. **They no longer only had one option for their security data. They had more choices, they had freedom.**

Splunk isn't disappearing. Beyond its continued relevance in cybersecurity, Cisco will invest heavily in bolstering Observability and application monitoring. At the same time, the "all in one" approach is being replaced by a SOC architecture that utilizes the most suitable home for each data source and use case.

Security teams demand the liberty of choosing where their data lives and the flexibility to detect threats equally well across their SIEM and data lake of choice. I look forward to helping organizations do just that in my new role at Anvilogic.

About the Author

Omer Singer is the VP of Strategy at Anvilogic where he helps customers break free from SIEM lock-in. With an extensive background as the former Head of Cybersecurity Strategy at Snowflake and VP of Security Operations at a global MSSP, Omer brings over 15 years of experience and a belief in the power of better data to drive better security.

Omer can be reached on LinkedIn: https://www.linkedin.com/in/omer-singer and you can learn more about Anvilogic here: https://www.anvilogic.com/.

From Virtual Visions to Tangible Profits: A Founder's Guide to Launching a vCISO Firm in 2024

By Caroline McCaffrey, CEO and Co-founder, ClearOPS

Most people find themselves in cybersecurity because they find its ever-changing landscape interesting. 2023 did not disappoint with new concerns over liability in the CISO role coupled with greater restrictions from the SEC and various state privacy laws. These concerns and, frankly, opportunities for more work are why security experts are turning their focus from corporate employment to starting their own firm.

This year, I've had the privilege of interviewing nearly 40 vCISOs and security entrepreneurs, and I want to share my findings, offering a roadmap for those who dream of building their own vCISO firm in 2024.

The Hardest Part: Marketing and Sales

My favorite question from the interviews is “What is the hardest part about running your own virtual CISO firm?” I think it is a tough question, but the responses seem to come pretty easily. 80% of the time the answer is “sales.”

Why is sales so hard? Focusing on what I have learned from the consultants versus my own experience with this problem, there is no magic bullet and almost everyone has their own unique approach. I will address a few of them.

The first approach to sales is to focus on marketing. I have spoken to several vCISOs who have a podcast, teach through LinkedIn learning or other teaching platforms, write books or contribute to a specific publication. What was most interesting about this approach was the focus on how their expertise is discovered by their potential client. They have really focused on identifying that ideal client profile for their services and then targeting their marketing towards that client. For example, if they find that they are most suited to startups in the $1M to $10M revenue range, they will target their marketing to the CEO or CTO of that startup and figure out how they do their research for service providers.

The second approach is to solely rely on their network. Often, the reason a vCISO launches their own firm in the first place is because a former employer, boss or colleague asks them to provide fractional security services to a business that is in a growth or established phase. This is a lucrative consulting position that sets the vCISO up financially to make the leap. Once they do quality work for this one company client, they use it aa a reference to build a network of other potential customers through word of mouth.

The third approach I will mention here is the direct sales route. In my discussions, I find that this is the one that vCISOs consider the hardest path to take. Whether it is cold outreach or using a staffing firm, the time a vCISO must commit is significant and takes them away from providing the client services. It can also be relatively expensive as both paths require buying tools or paying fees. Also, vCISOs are generally uncomfortable doing sales. My suspicion is that part of that comes from having been on the other side of the sales pitch so many times that they are hesitant to fall into sleazy practices.

Fractional vs. Virtual: Demystifying the Divide

When I interview a vCISO, I like to ask them what they think about the use of the term “vCISO” versus “fractional CISO” when referring to their practice. Interestingly, several interviewees refuse to label themselves as “vCISOs” or they used to label themselves as “fractional CISOs” only to now focus on “vCISO.” Ignoring the SEO of either term, these two words "fractional CISO" and "virtual CISO" seem to be awkwardly used and confused.

In speaking to an industry expert, I enjoyed her perspective on the difference. She stated that because the term “fractional” is a mathematical term, those who tend to be more math thinkers may prefer to use it. Following that logic, it defines the role as someone who offers some of their time, a fraction, to companies and CISO departments.

Virtual CISO, on the other hand, is a bit more ephemeral and implies someone who can work full-time, but remotely. The implication being that this virtual person is the only security expert working for that company which in turn means the company is relatively small or has an immature security program.

I like this distinction that she made but I am not convinced that the industry has adopted it. In my more recent conversations with vCISOs, some of them expressed an opinion that they originally called themselves vCISO only to now switch to fractional CISO. I picked up that the term vCISO has been degraded. I see on social media posts that "anyone can call themselves a vCISO" without requiring the corresponding experience or credentials, which further gives evidence that the community is becoming skeptical of the term.

And that list bit is an interesting point because even though there are several certifications and credentials in the cybersecurity space, most of them are younger than the cybersecurity professionals. Therefore, not everyone is credentialed. Regardless of that debate, I see the movement to "fractional CISO" more and more, so if you are launching your own firm, choose which term you want to use on your website with full knowledge that the line, while still fuzzy, is getting drawn.

Mapping Your Path: Finding Your Niche

The vCISO market is diverse, offering a range of client needs and engagement models. Identify your sweet spot. Will you specialize in specific industries? Focus on project-based work? Or do you charge hourly? Or maybe you prefer to cater to long-term engagements for larger enterprises? Choose your path wisely, honing your expertise and value proposition to become the go-to vCISO for your chosen niche.

As I explained in the previous section, vCISO has varying meaning. Some vCISOs I have spoken to only focus on pre-audit readiness. These are limited engagements, varying from 6 months to a year, where the vCISO builds the security program for the client, maintains it during the audit period and coordinates with the auditor during the audit. This type of vCISO then terminates their contract at the audit conclusion.

Another practice focus for vCISOs is the fractional cybersecurity professional who charges a flat fee, monthly, to their clients for building and maintaining a security program. With this work, the vCISO conducts a gap analysis, builds an action plan for the client that is customized and mapped to a specific framework and then works with the client on implementation, all the while helping with responses to security questionnaires and insurance assessments on the client's behalf. Sometimes the vCISO charges an hourly fee instead of a flat fee and I usually see this type of billing when the vCISO is early in the life of the firm and trying to establish that initial client base (because hourly earns them less money). These services are usually referred to as "Advisory Services" and MSPs and MSSPs are also offering them.

Finally, the third most common vCISO offering is what I refer to as a secondment. The vCISO works full-time, but for a temporary period of time, within the client's business. In this work, either the client lost their in-house CISO and needs someone to cover for a period, or they have never hired a CISO and need coverage while they conduct their search. With the dearth of high level, c-suite talent (and the fears over liability since Joe Sullivan of Uber was prosecuted), a CISO search can take up to a year, so these vCISOs cover the gap. Usually, these vCISOs also have a whole separate engine built for discovering and training new talent so that when they receive the client call, they have a pool of aspiring CISOs to

call upon. I find this fascinating because the vCISO is part cybersecurity advisor, part strategist, part practitioner and part recruiter.

I am sure more niches will evolve, but, based on my interviews, these are the most common. One consistency I have noted is the initial due diligence required with each client, usually called a gap analysis or gap assessment. My takeaway is that if you are offering vCISO services, you have to be offering gap analyses.

Go It Alone or Build a Scaling Business

It is exciting to start your own business working for yourself. While consulting businesses are often considered "lifestyle" businesses, they still can grow and scale like a startup. I personally like to analogize cybersecurity consulting firms to law firms and I think the model works well. The most highly experienced partner starts the firm and starts to grow enough client work such that they need help due to bandwidth constraints. At first, they have a few vCISO friends who can pitch in and consult when needed. Eventually, they need to hire someone to take over the client work so they can focus more on marketing and sales. Eventually, the founding partner is managing several other vCISOs and also associates who are earlier in their career. In this model, a vCISO partners with the associate. The associate has a cheaper hourly rate than the vCISO and works on more of the heavy lifting, like conducting the due diligence for gap assessments, reviewing vendor evidence of security and responding to security questionnaires on the client's behalf. The vCISO partners focus more of their time on high-level tasks, training the associates and keeping abreast of changes to any standards or regulations (like NIST CSF 2.0 or CMMC).

Meanwhile, the founding partner now spends almost all of his/ her or their time managing the business, hiring and firing and marketing and sales. It is worth taking the time to understand what you want. Do you want to run a business or do you like doing the work for the clients? Your decision will determine whether you stay a one-person firm or grow into something much larger.

Back to the law firm analogy, I see vCISO firms eventually having specialties like law firms do now. One firm may have an entire practice area that focuses on audit readiness while another practice area that focuses on secondments within companies. Basically, those choices you made to start your firm, which niche to offer, becomes one division of your much larger firm.

2023 was the year of the explosion of the vCISO market and I do not anticipate that it slows down in 2024. If anything, we will start to see larger and larger firms emerge as top-tier with reputations for being best in class. If you have been thinking of starting your own firm, I say the time is now before the price of entry gets too high.

As you dive deeper into running your own firm, you'll discover even more insights and nuances. Stay curious, adapt to the changing landscape, and never stop learning. With dedication and the right strategies, you can build a vCISO firm that brings you challenges that are worth experiencing and enjoyment in your work that you never thought possible.

About the Author

Caroline McCaffery is the CEO & a Co-founder of ClearOPS, Inc., a security program management platform for security experts, powered by Generative AI. Prior to ClearOPS, Caroline spent the last 23 years as an attorney, both as in-house counsel and outside counsel, representing technology start-up companies in Silicon Valley and the tri-state area. Most recently, Caroline was the General Counsel & VP of Business Affairs at an A.I. company performing image recognition, where she was also responsible for ethics, finance, information security, people operations and business operations. Caroline is a frequent speaker on topics such as privacy, ethics in A.I. and women in business and law. Caroline received her B.A. in International Relations from the University of Pennsylvania and her JD from New York University School of Law. Caroline is a member of the bar in both NY and CA and she is a Certified Privacy Professional (CIPP/US).

Caroline can be reached online at (ronnie@vewpr.com) and at our company website https://www.clearops.io

Getting AI Right for Security: 5 Principles

By Kevin Kennedy, SVP Products, Vectra AI

Now more than ever, companies need effective security solutions. The cost of global cybercrime is projected to grow by seventeen percent each year, reaching a staggering $12 trillion USD, cumulatively, by 2025.Thankfully, fire can be used to fight fire: AI can help organizations better protect their data, thwart attackers, and quickly identify and remediate threats. But with the buzz around "AI" dwarfing even "crypto" at its peak, it's nearly impossible to cut through the marketing to find truth. Based on a decade of building applied cybersecurity AI, here are the five principles we've identified for maximizing value:

Start with a clear problem statement.

If you've played with ChatGPT, you know that small tweaks to the query can make huge differences in the output. The same is true in building any AI model. So, nailing the problem statement is critical. When we started, we built a model with the problem statement: "Find unusual use of any account." Our customers begged us to turn it off because it was too noisy. Turns out, unusual is the usual in the modern enterprise.

We went back to the drawing board, thought through the threat model, and got more precise: "Identity any privileged account operating in the gap between observed and granted privilege". Why? Attackers inevitably escalate through privileged accounts, and they take advantage of overly broad privilege. So, if we can effectively define the zero-trust policy and then flag violations, we can accurately identify attacker activity. This required an entirely different approach to building the models, but the difference is profound.

Privileged Access Analytics (PAA) is now one of the most valued capabilities in our entire portfolio—because we started with a more precise problem statement.

Collect the right data

No AI model can be better than the data it's trained and operates on. The PAA models referenced could not operate without knowledge of every Kerberos transaction and/or Azure AD action in the relevant domain. That data trains its view of privilege and relationships, as well as gives the right insight to evaluate account usage in real-time for detection. Similarly, reliably identifying network command and control requires very granular time-series data on packet flow, along with a massive corpus of labeled data for both bad and good traffic.

It may be tempting to use the data that's most readily available. For networks, that may be flow or firewall logs rather than detailed network metadata. But if you take shortcuts like that, it will dramatically impact the value delivered.

Choose the best AI approach for each problem

You have the right problem statement and the right data; now it's time to select an AI approach tailored to the problem you're trying to solve. There are a plethora of machine learning (ML) techniques available—from neural networks and deep learning, to K-means clustering, novelties, and (the current rage) transformer and large language models

As the "No free lunch" theorem dictates, just as with the data, there are no shortcuts to success when it comes to working with AI algorithms. Data scientists and machine learning engineers (MLEs) need to understand the data they're working with and the problem at hand in order to select a specialized algorithm that will achieve the desired results—and general-purpose algorithms won't cut it. In fact, choosing the wrong algorithm may give results that aren't just suboptimal, but flat-out wrong.

Oh, and if you think that LLMs/transformers make this theorem obsolete, you'd be wrong: we've evaluated state of the art for detection use cases and found that they underperform specialized models today. LLMs are good at predicting what's next (e.g. how many bytes will be in the next packet), but not so good at categorizing things (e.g. is this connection malicious or benign).

Run at speed and scale (and cost-effectively!)

Cyberattacks happen fast. This is especially true in the cloud, but even in-network, ransomware attacks can occur seemingly in the blink of an eye. Every minute counts for defenders. According to one study, the vast majority of organizations—90 percent—can't detect, contain, and resolve cyber threats within an hour.

Against this backdrop, it's critical that AI not just get the right answers, but also that it works fast and is affordable in your environment. The speed requirements rule out batch analytics, as it's not helpful to detect today that you were ransomwared yesterday. That means it's critical to have a real-time, streaming architecture that still meets the requirements above to run the best AI approach against your organizations data to answer all of the security problem statements you need coverage on…at an affordable price point. Platform matters.

Getting the most from AI requires continuous validation and improvement

Security is a hyper-dynamic space: Attack surfaces are ever-expanding, and threats are becoming increasingly difficult to detect. At the same time, security operations center (SOC) analysts are being inundated with alerts. According to The 2023 State of Threat Detection Research Report, "97 percent of SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts."

Thus, it's important even for AI that vendors validate and improve products on an ongoing basis to ensure that AI models are continuing to accomplish what they're designed to do. In the jargon, this is done by precision and recall. Precision is a measure of the false-positive rates and recall is a measure of false-negative rates, and they generally operate in tension with each other. Essentially, vendors need to know whether their models are catching the threats they're intended to detect without burying analysts in alerts. No ML model is perfect, but with the right focus they can be an amazingly powerful weapon for defenders.

With 92 percent of companies either using or planning to use AI and ML to enhance cybersecurity, a significant opportunity exists for vendors to create groundbreaking products that bolster security. By practicing the principles outlined above, vendors can maximize their AI-powered security offerings and bring more value to their customers than ever before.

About the Author

Kevin Kennedy is senior vice president of products at Vectra AI. With more than 27 years in technology product management, more than half of those years in security, Kevin has seen it all. From Threat Intel, Encryption and Secure Web Gateways to Content, Email, Firewall, and Network security to today leading the Threat Detection and Response product vision and strategy for Vectra. Not afraid to challenge the status quo, but respectful of the challenges security teams face, Kevin approaches product with a healthy dose of empathy - staying true to the problem to be solved - and effectively balancing innovation and practicality. Prior to Vectra, Kevin launched his career in threat intel at IronPort. He continued to hone his security product management skills with stints at Juniper, Cisco, and Agari Data. Kevin bleeds maize and blue graduating from the University of Michigan with a BSE in computer engineering.

Kevin can be reached on LinkedIn at https://www.linkedin.com/in/kevinkennedysf/ and at the Vectra AI company website https://www.vectra.ai/.

VPNs in Times of War: Why a Rise in Global Conflicts Mean Citizens Now Need VPNs More Than Ever

A NEW era of global instability is dawning.

By Sebastian Schaub, CEO, hide.me

Russia's ongoing invasion of Ukraine continues to fan the flames of war in Europe. American and Chinese global interests appear increasingly incompatible, threatening a second Cold War. And now that Israel's long-standing conflict with Palestine has escalated all the way to a ground invasion of Gaza, there are fears that regional powers may be sucked into a wider war in the Middle East.

Between armed conflicts and increasing tensions between global superpowers, it is clear that global volatility is becoming the new normal. But there is one aspect of this new era of instability which is not given enough attention: online freedom.

History tells us that in times of war, citizens are often subject to exceptional restrictions in their daily lives, with the 'war effort' demanding sacrifices from everyone in the name of national security. Online, this trade-off may take the form of increased censorship of foreign websites, repression of domestic

opposition, and even complete internet blackouts in contested territories. We are already seeing this today, in conflict zones from Russia to Gaza, and in the pre-emptive steps which superpowers like China and America are taking to control an evolving digital battlefield.

But although the fog of war can seem impenetrable, citizens can still stand up for their online freedoms in times of global conflict. And as we continue to advocate for a free and open internet, we must remember the promise of the internet as an emancipatory tool – a means of lifting that fog, rather than just another battlefield liable to become lost in it.

Freedom Under Fire

The first casualty of war, as the saying goes, is truth. This has certainly been the case in Russia, where the state continues to take extensive steps to prevent its own citizens from learning the truth about its ongoing war in Ukraine.

Since the invasion, Russian regulators have censored social media and blocked access to any news websites which refused to follow the Kremlin's official lines on the 'special military operation.' Online freedom campaigners at Citizen Lab have estimated that social media censorship increased thirtyfold in Russia in the wake of the invasion. Among countless others, Facebook, Instagram, and the BBC News website have all been restricted in the name of security. This amounts to the imposition of a digital Iron Curtain, making it difficult for citizens in Russia and occupied Ukraine to get a clear and unbiased picture of the war which is supposedly being carried out in their name.

In response, thousands of Russian citizens have turned to VPNs to circumvent local internet restrictions and inform themselves about the ongoing war. Yet this situation is sadly not unique to Russia. In authoritarian states across the globe, the imposition of online restrictions is a common and growing danger. And as global tensions escalate, restrictions could become more sweeping and more widespread, further threatening the promise of a free and open internet.

The Digital Battlefield

Wars are no longer contested merely on land, at sea, and in the skies. Modern warfare has evolved to view the contested spaces of the internet as a new front, and conflicts between nation states are as likely to take place in foreign cyberspace as on foreign soil.

Under the auspices of national security – or even existential self-preservation – warring states are liable to weaponise the internet by enforcing restrictions both at home and overseas. This may take the form of increased internet surveillance, which threatens freedom of speech and privacy, or else states may try to throttle internet speeds or cut off access altogether in a contested or hostile territory. Since Russia's invasion, Ukraine has been the victim of cyberattacks targeting its digital and physical infrastructure – and many of Ukraine's allies, including the UK, have raised the alarm about the possibility of Russian cyberattacks elsewhere.

A similar story is playing out in the Middle East. Israel controls much of the physical infrastructure which powers the internet in Gaza, and this has allowed Israel to impose strategic communications blackouts to aid its invasion. By severely slowing internet speeds – if not cutting connectivity altogether – Israel has been able to control cyberspace, preventing the spread of information and hampering its enemies' ability to communicate at the war's most critical early junctures. The problem, as ever, is that non-combatants are inevitably caught in the crossfire. In this case, citizens have been left without internet access at a time when online connectivity – which allows the spread of news about evacuations, aid supplies, and medical access – can be lifesaving.

The Second Cold War

If war can be said to have a second casualty, after truth, it is probably freedom. In addition to conflicts in Europe and the Middle East, some observers believe the world is also heading for a new Cold War. The old battle lines have been redrawn, however, so that it is now China – and not Russia – who can be thought of as the United States' main adversary. There are many potential flashpoints between China and the US, but disagreements over the governance and independence of Taiwan is the one which has been in the news lately. The two superpowers are also major economic competitors, and China is currently in the process of expanding and modernising its nuclear arsenal – a move which has set some US observers on edge.

The two powers are also competing in cyberspace (as everywhere else) and their rivalry has manifested in internet restrictions on both sides. The Chinese state is famous for its regime of total control of the internet, with its 'Great Firewall of China' blocking citizens from viewing any and all content which the authoritarian government doesn't want them to see. As tensions with America rise, it is possible that the Chinese government will further tighten its stranglehold on the internet in the name of national security. This represents another clear instance where the usefulness and importance of VPNs cannot be overstated.

The internet in America may be much freer, but there are still prominent voices in the US calling for greater online restrictions in response the perceived Chinese threat. Lawmakers have recently debated banning TikTok – owned by Chinese firm ByteDance – over fears around espionage and dodgy data practices, and the attitude of suspicion towards Chinese technology is only growing. Perhaps this suspicion is justified, but ultimately, the American people are the ones who will suffer if their government pulls up the online drawbridge by banning Chinese apps and software.

Preserving Online Freedoms

Against this backdrop of volatility and conflict, it would be easy to simply surrender our claim to a free and open internet. National security is important, of course, and many of the justifications for wartime restrictions on internet usage may sound reasonable – especially at first, in the heat of battle. But law-abiding citizens are the ones who stand the lose the most if we allow the dream of a free internet to become another casualty of war.

As we have seen in Russia, VPNs offer hope for citizens in territories where the internet is heavily restricted or censored. VPNs allow internet users to browse with greater security and privacy while circumventing local restrictions – and in most states and territories, they're completely legal. VPNs are indispensable for truth-seeking citizens, and those of us who believe in internet freedom must advocate for their continued use.

And in times of war, VPNs are more important than ever. As the world becomes more volatile, we have an even greater duty to safeguard the right to information. This is especially vital for citizens whose internet is under siege and for those living under authoritarian regimes, where war aims and justifications may be hidden from the public.

The power of VPNs lies in lifting the fog of war and safeguarding truth. When war spreads to the internet, and civilians are caught in the crossfire, VPNs remain the free internet's last line of defence.

About the Author

Sebastian is the founder of hide.me VPN and he has been working in the internet security industry for over a decade. He started hide.me VPN to make internet security and privacy accessible to everybody.

Hyperautomation: Revolutionizing the Security Market

By Divakar Kolhe, Digital Marketer, Market Research Future (Part of Wantstats Research and Media Private Limited)

Hyperautomation: Revolutionizing the Security Market

In today's digital age, the security landscape is constantly evolving, presenting new challenges and threats that require innovative solutions. With the growing complexity of cyber threats and the increasing reliance on technology, organizations are seeking ways to enhance their security measures. One approach that has gained considerable attention is hyperautomation, a concept that promises to transform the security market. In this article, we will explore the role of hyperautomation in the security market and how it is revolutionizing the way organizations defend against cyber threats.

Understanding Hyperautomation

Hyperautomation is an advanced approach to automation that leverages a combination of technologies, including artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), and advanced analytics. Its primary goal is to streamline and optimize business processes by automating repetitive tasks, making decisions based on data, and enhancing overall operational efficiency. In the security market, hyperautomation is a game-changer because it not only automates routine security tasks but also enhances threat detection, response, and remediation.

Enhanced Threat Detection

One of the primary applications of hyperautomation in the security market is its ability to enhance threat detection. Traditional security tools often struggle to keep up with the rapid evolution of cyber threats. Hackers use sophisticated techniques to breach security defences, making it essential for organizations to stay one step ahead. Hyperautomation leverages AI and ML to analyze massive datasets and identify patterns and anomalies that may indicate a security threat. It can detect unusual user behaviour, identify potential vulnerabilities, and spot zero-day exploits that may go unnoticed by traditional security tools.

Automation in Threat Response

Automating threat detection is only the first step. Hyperautomation goes a step further by automating threat response. When a potential security threat is detected, hyperautomation can take immediate action to contain and mitigate the risk. For example, it can quarantine infected devices, block malicious IP addresses, and disable compromised user accounts, all without human intervention. This not only speeds up the response time but also reduces the risk of human error in the process. The ability to automate response actions is particularly crucial in the ever-evolving landscape of cyber threats.

Dynamic Risk Assessment

Hyperautomation also plays a pivotal role in dynamic risk assessment. Traditional security approaches often rely on static security policies and rules, which may not adapt well to rapidly changing threats. Hyperautomation uses AI and ML algorithms to continuously assess the risk profile of an organization's network, applications, and data. This dynamic risk assessment allows security teams to allocate resources and focus their efforts on the most critical areas, increasing the overall resilience of the organization's security posture.

Security Orchestration and Incident Response

Hyperautomation can be a game-changer in the field of incident response. When a security incident occurs, time is of the essence, and a well-coordinated response is essential to minimize damage.

Hyperautomation provides the means to orchestrate incident response by automating the coordination of various security tools and teams. It can gather information from multiple sources, correlate data, and initiate predefined response actions. This not only reduces response times but also ensures that incident response is consistent and efficient, even in high-stress situations.

Improved Compliance and Reporting

Compliance with regulatory standards and the ability to provide accurate reporting are vital in the security market. Hyperautomation helps organizations maintain compliance by automating the monitoring and enforcement of security policies. It can generate detailed reports on security events and incidents, making it easier for organizations to demonstrate their commitment to security and regulatory compliance. This is especially important for organizations in highly regulated industries, such as finance and healthcare.

Challenges and Considerations

While hyperautomation offers significant benefits to the security market, there are challenges and considerations that organizations must address:

Data Privacy: As hyperautomation relies heavily on data, organizations must ensure the privacy and security of sensitive information. Complying with data protection regulations, such as GDPR, is essential.

Integration: Implementing hyperautomation in the security market often requires integrating various existing security tools and systems. Compatibility and interoperability must be carefully considered.

Human Oversight: While automation can enhance security, it should not replace human expertise entirely. Organizations must strike a balance between automation and human oversight to ensure that critical decisions are made by experienced security professionals.

Training and Skill Development: As hyperautomation relies on advanced technologies, organizations may need to invest in training and skill development for their security teams to effectively manage and utilize these tools.

In conclusion, we can say that hyperautomation is reshaping the security market by providing organizations with the tools and capabilities needed to stay ahead of the constantly evolving cyber threat landscape. Its ability to enhance threat detection, automate response actions, and optimize security processes makes it a valuable asset for any organization looking to bolster its security measures. However, organizations need to address challenges such as data privacy, integration, and the need for human oversight to fully realize the benefits of hyperautomation in the security market. As technology continues to advance, hyperautomation will remain a key element in the ongoing battle against cyber threats, providing organizations with the agility and resilience required to protect their digital assets.

According to Market Research Future's latest research report on Hyperautomation in the security market By Offering (Solutions, Services {Professional Services, Security Consulting Services, Integration & Deployment Services}, Managed Security Services), By Technology (Artificial Intelligence (AI), Machine

Learning (ML), Robotic Process Automation (RPA), Process Analytics, Ingestion Engines, and Others), By Region (North America, Europe, Asia-Pacific, Middle East and Africa and South America) - Forecast Till 2032

Reference - Market Research Future

About the Author

Divakar Kolhe is a highly skilled and experienced digital marketer who has dedicated his career to driving online success for businesses. With a strong passion for data-driven strategies and a deep understanding of consumer behavior, Divakar has become an invaluable asset in the field of digital marketing.

Divakar Kolhe - divakar.kolhe@marketresearchfuture.in
Market Research Future (Part of Wantstats Research and Media Private Limited)
99 Hudson Street, 5Th Floor
New York, NY 10013
United States of America
+1 628 258 0071 (US)
Website: https://www.marketresearchfuture.com

How The Security of The Cloud's Supply Chain Will Shift in 2024

What we can expect from advanced threat actor groups in the new year.

By Jason Martin, Co-founder and Co-CEO at Permiso Security

In 2023, we started to witness a change in the way both attackers and defenders thought about cloud security. The days when attackers target a single service and steal data from an S3 bucket are almost a long gone memory at this point - simpler times. Attackers got smart about who and what they targeted. Through initial recon, the help of credentials for purchase, and some masterful reconnaissance in SaaS environments, groups like LUCR-3 (Scattered Spider) were able to breach the environments of companies like MGM, Caesars, Clorox and others.

While advanced cloud threat actors showcased their skill at being able to gain access to cloud environments and move laterally, they also tipped their hand at what cloud supply chain attacks might look like in 2024.

Identity Providers Are Still the Bullseye for Cloud Attacks

Okta, Microsoft Entra ID (Azure AD) and JumpCloud all experienced breaches in 2023, with Okta perhaps suffering the brunt of customer exposure. Identity providers, while offering convenience of centralized authentication, have proven to be a security risk to many organizations. If a threat actor gains access to a victim's IdP instance, the impact is multi-casted because of the access they now have to all of the applications that SSO through that IdP. If Okta themselves get breached, this multi-cast is magnified exponentially as the threat actor can now potentially access all of Okta's customer environments. Adding to this risk is the increasing reliance on third-parties and outsourced technical support teams for core help desk services. Threat actors have found these organizations as prime targets to attack their downstream customer base and play a significant role in the increased risk associated with the cloud supply chain.

SaaS Providers Are Going to be Heavily Targeted in 2024

SaaS providers that have delegated access into customer environments via role assumption or persistent keys will see an increase in targeted attacks. Threat actors will continue to focus on cloud supply chain compromise to target downstream customers of those vendors. Similar to what we witnessed in Okta, other, non-IdP SaaS vendors present similar risks in the cloud's supply chain. By compromising the vendor itself, threat actors can access all of the customer tenants they are managing in the environment. If a threat actor were able to gain access to Github's platform, for instance, they could have access to code signing certificates for the millions of customers that use it. If they were to compromise Jira, this could lead to the compromise of sensitive data of hundreds of thousands of companies. Many SaaS infrastructure tools rely on access delegation, where the vendor is provided a credential within the customer environment which they can assume externally. In an instance where a threat actor was able to compromise one of these SaaS providers, they would gain access to those credentials, in the SaaS providers' customer environments. These cloud SaaS vendors not only have tens of thousands of customers that would be impacted downstream, but they are historically overprivileged. The P0 labs team has found that more than 90% of the privileges granted to these vendors go unused, and attackers love nothing more than overprivileged accounts and identities. The stakes are high in SaaS.

Could A Major Cloud Service Provider Get Compromised?

If we think about the supply chain in the cloud, there are perhaps no greater stakes than the cloud service providers like AWS, Azure and GCP. While these providers invest heavily in staff and tooling to secure their platforms, they can be just as vulnerable to the risk that lies in support entities and third-party contractors. It's clear that threat groups are no longer interested in the diminishing returns of activities like crypto mining. Compromising a victim's identity provider, SaaS applications or CI/CD instances allow threat actors to gain access to sensitive, valuable data in as little time as possible. If they're able to compromise cloud vendors themselves, the supply chain impact would be disastrous. If they can compromise the cloud service providers themselves, the downstream impact would be catastrophic.

Enterprises Will Start to Seriously Rethink Their MFA

If advanced threat actor groups like LUCR-3 taught us anything in their attacks on cloud environments, it's that MFA doesn't provide the security guarantees we'd like to think it does. Through SIM swapping, phishing, and push fatigue, MFA has been something advanced threat actors have found ways around over the last few years, especially with those victim organizations that allow SMS as a second factor. We're likely to see more companies move away from SMS based authentication and accelerate movement toward solutions that rely on biometrics or hardware keys as MFA bypass techniques will continue to innovate. Facial biometric technology and hardware keys such as Yubikeys, for example, offer better security guarantees and make it significantly more difficult to bypass. So how will threat actors adapt?

Threat Actor Groups Will Continue to Leverage AI for Evil

With the increase in the adoption of biometric security for MFA, there will be a growth in the availability of toolkits to create deepfakes for purposes of voice or video-based verification and in social engineering personnel involved in credential reset workflows. These toolkits, like many others today, will be easily available in underground markets for purchase. These deepfake assets will be critical to help the threat actors orchestrate sophisticated impersonation in social engineering attacks as part of their larger campaigns. Groups continue to be bolder and more sophisticated with their social engineering attacks and driven by the success in exploiting the human factor in enterprises they will continue to do so. Many commercial platforms have gone to great lengths to prohibit the abuse of LLM models; however, this will create high demand by threat actors for nefarious Chat-GPT equivalent solutions without such safeguards. With the release of powerful open-source models and the acceleration in public domain research the barrier to creating, training, and maintaining bad actor LLMs has never been lower.

In short, the attack patterns we saw in 2023 are most likely to continue into 2024. Modern cloud threat actors are moving away from activities like cryptomining that have proven to be less profitable in the last year or so and are gravitating toward more lucrative endeavors such as ransomware and extortion. Because MFA bypass has been a critical piece to gaining access into an environment, expect threat actors TTPs to keep up with the measures put in place for more secure MFA such as hardware keys and biometrics. It would appear that many advanced threat actor groups are starting to understand cloud and the resources available to them that can be leveraged for their own gain. They will continue to orchestrate more elaborate campaigns against SaaS and Cloud Service Providers that will yield larger gains than typical attacks against a single victim or tenant. As always, it's the responsibility of security teams to account for how threat actors' TTPs are evolving and construct policies and plans that will better address those threats.

About the Author

Jason Martin and I am the Co-founder and Co-CEO at Permiso Security. 25+ years in cybersecurity. Conference organizer (Shakacon), author, investor, and formerly EVP, Products & Engineering at FireEye/Mandiant. I can be reached on LinkedIn and at our company website permiso.io.

Four Ways Genai Will Change the Contours of The Corporate Landscape In 2024

By Neil Serebryany, CEO and Founder of CalypsoAI

Generative artificial intelligence (GenAI) models, including large language models (LLMs) have been the focal point of the business world's attention since ChatGPT made its debut just a year ago. They have revolutionized operational practices across sectors, from streamlining supply chains to enabling unique, detailed customer interactions. While not quite ubiquitous yet, this technology is getting closer to that milestone every day, and its potential for innovation is boundless. It's clear these models and their other GenAI cousins are poised to reshape the corporate landscape even further. Here are some ways I anticipate they will do so in the upcoming year.

- **The first large-scale breach of a foundation model provider, such as OpenAI, Microsoft, Google, etc., will happen in the upcoming year and will lead to a large-scale security incident.** The scope and scale of the attack itself will be on par with recent incidents, such as Microsoft's "accidental" disclosure of 38 terabytes of private data and Google Fi's hack that exposed the data of 38 million customers. With the amount of sensitive information that has been sent to LLMs like ChatGPT, the fallout would be profound and could easily exceed either of those

in terms of reputational, operational, and financial damage. The damage inflicted by such a breach would not stop at the company boundaries, but would create a ripple effect across the AI ecosystem as organizations that had relied on the model(s) would need to immediately go into damage control mode. Abruptly ceasing to use the model(s) would affect applications that require it and security teams would have to investigate, reassess, and possibly recreate or replace elements of the organizational security infrastructure. Explaining their accountability to their own shareholders and customers would be a painful exercise for executives, and come with its own set of consequences.

- **An enterprise embracing GenAI is going to have a permissioning breach due to multiple models at play and a lack of access controls.** As a company layers in external base models, such as ChatGPT, as well as models embedded in SaaS applications, and retrieval-augmented generation (RAG) models, the organizational attack surface expands, the security team's ability to know what's going on (observability) decreases, and the intense, perhaps even giddy, focus on increased productivity overshadows security concerns. Until, that is, a disgruntled project manager is given the access to the new proprietary accounting model that the payroll manager with a similar name requested. Depending on the level of disgruntlement and the personality involved, company payroll information could be shared in the next *sotto voce* rant at the coffee machine, in an ill-considered all-hands email, or as breaking news on a business news website. Or nothing will be shared and no one will notice the error until the payroll manager makes a second request for access. Whatever the channel or audience, or lack thereof, the company has experienced a serious breach of private, confidential, and highly personal data, and must address it rapidly and thoroughly. The AI security team's days or weeks will be spent reviewing and likely overhauling the organization's AI security infrastructure, at the very least, and the term "trust layer" will become a feature of their vocabulary.

- **Data science will become increasingly democratized thanks to foundation models (LLM usage).** The speed and power of LLMs to analyze and extract important insights from huge amounts of data, to simplify complex, time-consuming processes, and to develop scenarios and predict future trends has already begun to bring big-data analytics into the workflow of teams and departments in all business functions. That will continue to scale up dramatically. Across an organization, teams will increasingly be able to rapidly generate data streams tailored to their specific needs, which will streamline productivity and expand the institutional knowledge base. Humans will not be out of the loop, however, as I do not foresee models' propensity to make stuff up being resolved any time soon, although fine-tuning is showing some benefits in that area.

- **Increasingly new and novel cyberattacks created by offensive fine-tuned LLMs like WormGPT and FraudGPT will occur.** The ability to fine-tune specialized models quickly and with relative ease has been a boon to developers, including the criminal variety. Just as models can be trained on a specific collection of financial data, for instance, models can also be trained on a corpus of malware-focused data and be built with no guardrails, ethical boundaries, or limitations on criminal activity or intent. As natural language processing (NLP) models, these tools function as ChatGPT's evil cousins, possessing the same capabilities for generating malicious

code, as well as sophisticated content that easily passes for human-generated communication, such as phishing emails, social engineering attacks, and prompt injections or “jailbreak” attacks.

LLMs are nothing short of revolutionary tools with diverse applications and unlimited utility across industry sectors. As their adoption becomes more widespread, they stand to eclipse currently held notions of innovation and efficiency, and push the boundaries of the business ecosystem. The upcoming year could be just as interesting as this year has been.

About the Author

Neil Serebryany is the CEO and Founder of CalypsoAI. My Name is the My Title of the My Company. He has led industry-defining innovations throughout his career. Before founding CalypsoAI, Neil was one of the world’s youngest venture capital investors at Jump Investors. Neil has started and successfully managed several previous ventures and conducted reinforcement learning research at the University of South California. Neil has been awarded multiple patents in adversarial machine learning. Neil can be reached online at https://www.linkedin.com/in/neil-serebryany/ and at our company website https://calypsoai.com/.

New Year, New Consumer Demands in Cybersecurity: Navigating the Landscape of Consumer Expectations and App Developer Responsibility in Mobile App Security

By Alan Bavosa, VP of Security Products, Appdome

The significant growth and mass adoption of mobile applications has completely transformed the way users engage with brands today. From managing finances to indulging in leisurely pursuits, mobile apps have become an integral and expected part of our daily lives.

In fact, consumers globally are not merely embracing mobile apps; they are fully migrating to the mobile app channel for personal and professional objectives, creating a digital-only marketplace for brands. According to a survey conducted by Appdome spanning 25,000 consumers across 12 countries, nearly 52% of global consumers today prefer engaging with mobile applications over web channels.

With over half of the global population choosing mobile apps, there is now an increased and inherent risk of cybersecurity issues. 41.8% of the survey respondents reported experiencing or knowing someone close to them who had fallen victim to a cyber-attack. This alarming statistic highlights the sophisticated and deep-seated fears individuals harbor regarding cyber threats, data theft, and fraud in the mobile app landscape, underscoring the need for robust security measures that has never been more pronounced.

Emerging Threats and Consumer Fears

The problem? Attackers are ahead of most consumers and mobile developers alike and are quickly evolving thanks to breakthrough technologies like artificial intelligence and mobile bot adoption across the globe. The landscape of threats has evolved so much, in fact, that more sophisticated challenges are emerging including accessibility service malware, screen overlay attacks, and credential stuffing – all of which are taking center stage in 2024. The fear of unprotected or compromised mobile apps leading to unauthorized data access, account takeovers or fraudulent transactions has become a prevalent concern with few brands taking it seriously outside of traditionally regulated spaces, such as healthcare and finance.

Consumer Awareness and Responsibility Hierarchy

Additionally, consumers are becoming more aware of the potential misuse of on-device or over-the-wire exploits, raising questions about the security of their personal data directly with brands, and when those same questions go unanswered, they abandon brand loyalty altogether in search of a competitor who can offer mobile app protection. Beyond this, consumers are not only aware of the threats but are educating themselves enough to establish a clear hierarchy of responsibility when it comes to mobile app defense. Nearly 60% of global consumers believe that the primary responsibility lies with the mobile brand or developer, according to the survey results. This insight indicates a growing cyber-savviness among consumers who evaluate the risk associated with using mobile apps. Additionally, the fastest-growing concern among consumers is that brands may not care enough, indicating that more needs to be done between brands and developers.

Developers' Dilemma: Balancing Features and Security

While consumers prioritize security, developers find themselves in an ongoing debate about balancing features and security. The survey reveals that nearly 90% of all surveyed believe that security is equally or more important than features. This shows an emerging pattern for consumers, and a nuanced understanding and recognition that only robust security measures in mobile applications can be effective in protecting their personal data and information.

The Developer's Action Plan

Considering these insights, developers face the imperative task of revamping their mobile business protection strategy. Traditional methods like network protections and client-side compliance are deemed inadequate in the face of diverse devices and evolving threats. The action plan for developers involves:

1. Proactive prevention over reactive recovery: Acknowledge the inadequacy of network-level protections and prioritize investments in meeting user expectations for security, anti-fraud measures and malware prevention in mobile apps. Focus on proactive prevention rather than reactive recovery.

2. Transparent communication: Highlight security, anti-fraud and anti-malware features in release notes and app store descriptions to enhance the perceived value of mobile services. Incorporate threat awareness and intelligent response into the app experience to instill consumer confidence.

3. Continuous updates via DevOps CI/CD pipeline: Implement security, anti-fraud and anti-malware updates in every app release within the DevOps CI/CD pipeline. Utilize real-time threat intelligence to guide data-driven decisions on the most effective protections for consumers.

4. Real-time threat monitoring: Track real-time threats to mobile apps and environments to validate deployed protections, empower consumers to proactively counteract attacks and swiftly identify and respond to emerging threats.

5. No-code, no-SDK mobile platform integration: Enhance DevSecOps processes by incorporating a no-code, no-SDK mobile platform for increased agility and control. Certify that security, anti-fraud and anti-malware protections are seamlessly included in every Android and iOS release without burdening the development team with additional work.

The landscape of mobile app security is rapidly evolving and mirroring the growing reliance on mobile applications. Consumer expectations are clear – they demand comprehensive protection against cyber threats, fraud and malware. Developers, in turn, bear the responsibility of fortifying these digital gateways to ensure a secure and seamless user experience. By adopting a proactive approach, transparent communication and integrating advanced security measures into their development processes, developers can not only meet but exceed consumer expectations, thereby ensuring the sustained success and trust of their mobile applications in an increasingly interconnected digital world.

About the Author

Alan Bavosa is the VP of Security Products at Appdome, the leading pioneer in no-code, automated mobile app defense. He is passionate about helping mobile developers build secure mobile apps rapidly as part of the DevOps CI/CD pipeline. Prior to Appdome, Alan held numerous executive and entrepreneurial roles at leading cybersecurity firms including ArcSight, NetScreen, and Palerra as well their respective acquirers HP, Juniper, and Oracle. Alan can be reached online on LinkedIn, Twitter, and at our company website https://www.appdome.com.

Building a Better Perimeter Defense Strategy to Meet the Challenges of 2024

By Yiyi Miao, Chief Product Officer, OPSWAT

In the ever-changing domain of cybersecurity, organizations continue to face multifaceted challenges with protecting their digital assets and infrastructure. A new report, written by MIT professor Stuart Madnic and funded by Apple, showed 20 percent more data breaches in the first nine months of 2023 than the entire year prior. As people increasingly conduct their lives online, more personal data is collected — creating an ever-more appealing target for cyber criminals.

Among these breaches are ransomware attacks, which have increased in volume, sophistication, and aggression. The U.S. and U.K. governments have together accused Russian intelligence of a global hacking campaign over the past eight years. They assert that these attackers have targeted British lawmakers, journalists, and civil society organizations in an attempt to interfere in British elections. In the U.S., cyberattackers allegedly aimed their efforts at U.S. energy networks and American spies. These are just a few of the pervasive attacks that show a clear need for businesses to re-examine their cybersecurity strategies and prepare for the evolving tactics of threat actors in 2024. As we head into the new year, several key trends and emerging threats highlight the need to review and strengthen overall cybersecurity and perimeter defense strategies.

Key Trends in Cybersecurity

Evolving Tactics

The cyber threat landscape continues to evolve in tandem with technological advancements, making it increasingly difficult for organizations to effectively protect themselves from cyber threats. Cybercriminals are leveraging artificial intelligence (AI) and machine learning (ML) to launch more sophisticated attacks. This requires defense strategies to evolve at the same pace, using AI and ML to enhance threat detection and response capabilities.

Supply Chain – The Critical Role of SBOMs

Supply chain attacks continue to be an appealing attack vector for threat actors. By compromising trusted vendors, it becomes simple for attackers to infiltrate numerous organizations at once, as the MOVEit vulnerability continues to prove. To prepare for such attacks, organizations must implement strict vendor risk management practices, perform security audits regularly, and analyze the integrity of all software in use. A software bill of materials (SBOMs) provides detailed inventories of software components, which can help organizations identify vulnerabilities and dependencies within their supply chain.

IoT Expansion

Internet of Things (IoT) devices continue to introduce new attack vectors, expanding the potential attack surface. The Office of Management and Budget (OMB) recently announced it will establish an enterprise-wide inventory of the agency's covered IoT assets "to enhance the U.S. Government's overall cybersecurity posture and to help ensure integrity of systems." In any organization, such an inventory is key to securing IoT networks and devices effectively and helping to prevent unauthorized access and potential breaches in this interconnected world.

LLM-Based Threat Detection Startups

The rapid rise and evolution of Language Learning Models (LLMs) creates a new way to detect threats, offering new methodologies for quickly identifying and responding to cyber threats. However, as LLM-based startups emerge in the cybersecurity sector, it is important to evaluate these innovative technologies carefully as well as ensure that they integrate effectively into the existing security infrastructure.

Human Error

Despite many advancements in technology, humans remain a significant risk factor. Indeed, Verizon's 2023 Data Breach Investigations Report attributed 74 percent of security breaches to human error. While technology is essential and should be used to shield people from as many attacks as possible, comprehensive security awareness programs remain vital. Educating employees about the newest threats, teaching them how to identify phishing attempts, and ensuring responsible behavior online can help them both at work and in their personal lives.

People, Process, and Technologies

Together, people, processes, and technology all combine to help you build a more robust cybersecurity strategy. **People** are the first pillar of such a strategy. To support this, security awareness programs must include simulated cyberattacks and phishing simulations. This provides employees with firsthand experience in identifying, thwarting, and mitigating potential risks. Regular penetration testing, vulnerability assessments, and personalized security training all contribute to increasing an organization's defense systems.

Processes are the second pillar to the strategy, because they define how an organization manages and mitigates risks. Organizations must adopt consistent policies for both information technology (IT) and operational technology (OT) security. Policies going forward will require SBOMs, the analysis of those SBOMs, and how that may impact other software and systems. Policies may also require a deeper understanding of security tools to ensure that they are being used effectively. As regulatory bodies increasingly become involved in OT cybersecurity, processes must include the review of compliance with relevant regulations. And as leadership teams and boards of directors require more cybersecurity expertise, processes help increase cybersecurity maturity and effectiveness.

The third pillar, **technology**, will play a crucial role in the rapid identification and neutralization of potential threats as organizations adopt advanced technologies. By leveraging the power of AI and ML, organizations can more rapidly discern patterns, anomalies, and potential risks in real-time, allowing for proactive threat mitigation. Organizations must stay up to date with evolving tactics and defenses to mitigate risks effectively.

Looking Ahead

Increased Partnerships and Mergers

The OT security sector is undergoing a transformation driven by increased partnerships and acquisitions. This reflects the need for specialized expertise in securing the operational technologies that are critical in manufacturing, energy, and utilities. Partnerships and mergers bring together diverse expertise and enable organizations to develop more comprehensive security solutions for OT environments. Cybersecurity firms and OT experts must address the complex threats faced by critical infrastructure systems.

Firewalls, Intrusion Detection Systems, and Secure Gateways

Traditional cybersecurity measures, such as firewalls, intrusion detection systems (IDS), and secure gateways continue to be critical in perimeter defense strategies. These technologies are evolving to provide more sophisticated and integrated solutions. Advanced firewalls now provide deeper insights into network traffic, enabling more effective detection and prevention of malicious activities. Similarly, IDS can identify complex attack patterns using AI and ML. Secure gateways now offer deep packet inspection and threat intelligence integration to improve security.

Better and Faster Sandboxes

Traditional sandboxes may be considered obsolete to be applied to combat evolving threat landscape, however, with newer technologies and implementation, sandboxes are still highly effective to provide a safe and isolated environment to test and analyze untrusted programs and code, preventing potential threats from impacting the primary network or system. This enables security teams to conduct dynamic analysis and identify critical indicators of compromise (IoCs), such as network IPs, URLs, and domains. The increased use of sandboxes enables a shift towards more proactive cybersecurity strategies.

Proactive Threat Detection

Proactive threat detection is a key component of perimeter defense strategies. Rather than responding to threats after they emerge, proactive threat detection aims to predict and prevent attacks before they occur. By leveraging predictive analytics, AI, and ML to analyze patterns and anomalies that could indicate impending attacks, organizations can respond proactively to reduce the likelihood of and fallout from security breaches.

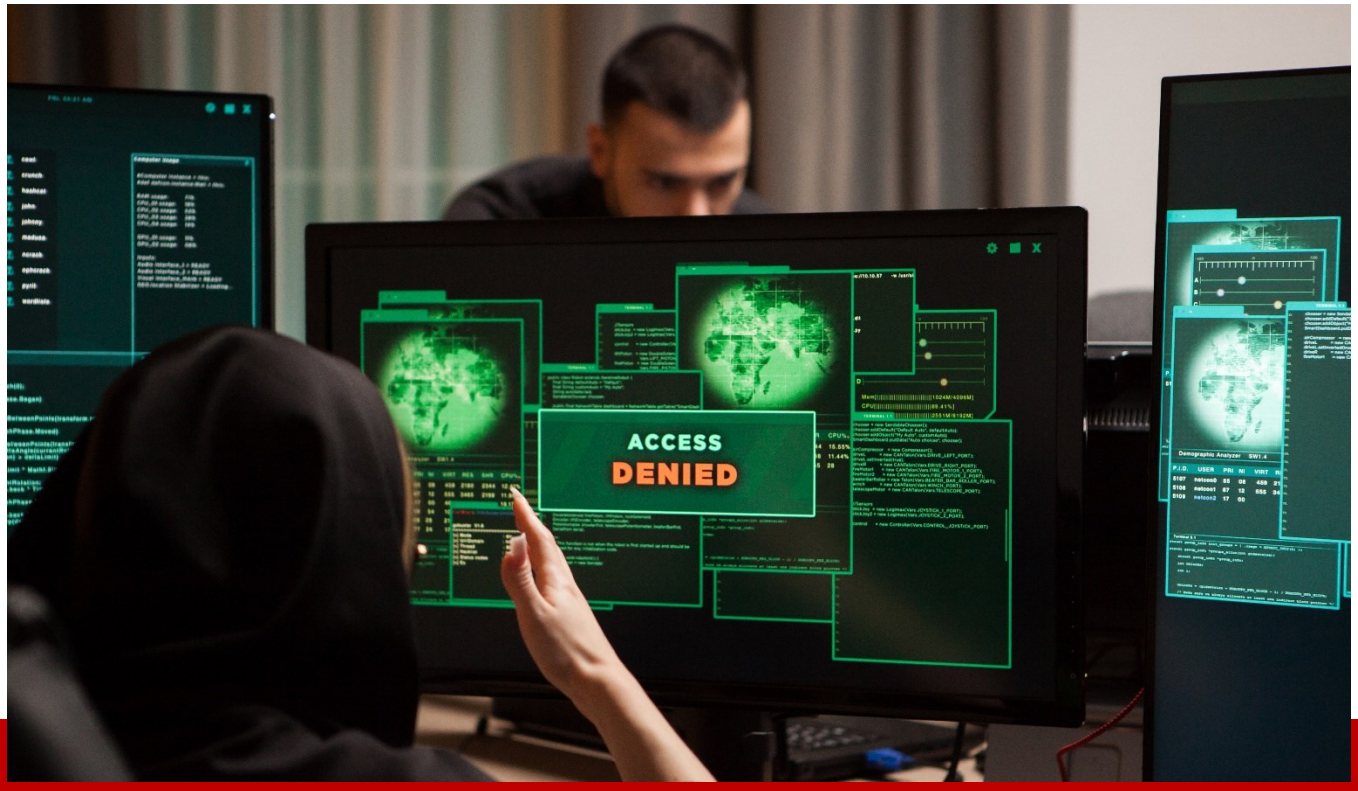
Prepare for New Challenges

In the years ahead, cybersecurity must move beyond defense and adopt an evolving strategy to stay ahead of new threats and challenges. Comprehensive employee training, automated threat detection and mitigation, and consistent policies for IT and OT security can help organizations build a cybersecurity system that is responsive to changing technologies and regulations. The cyber landscape is unpredictable, but as society becomes increasingly digitalized, organizations must invest in cybersecurity, starting with perimeter defense, in order to achieve and sustain success.

About the Author

Yiyi Miao, Chief Product Officer, OPSWAT. Yiyi Miao is the Chief Product Officer at OPSWAT, a global leader in critical infrastructure cybersecurity solutions. He joined OPSWAT in 2009 as a Software Engineer in the company's Research and Development Engineering Team. Yiyi started managing the Product Engineering and Product Management teams in 2017 and is responsible for the overall product design, engineering, and delivery processes. Yiyi earned a Bachelor's degree in Biomedical Engineering from Shanghai University in China and a Master's degree in Computer Science from San Francisco State University.

Yiyi can be reached online on LinkedIn: https://www.linkedin.com/in/yiyi-m-4362096/ and at our company website https://www.opswat.com/



Ransom-War Escalation: The New Frontline in Cyber Warfare

By Nissim Ben Saadon, Director of Innovation, CYREBRO

High-profile ransomware attacks against government targets in Costa Rica and Peru last year brought a new twist to the concept of cyberwar: Ransom-War. With the rise of ransomware-as-a-service (RaaS) and the relative impotence of government agencies to counter attacks, for-profit ransomware wars conducted by private or state-sanctioned hacking groups against local and national government targets are increasing in severity and intensity. In this article, we'll take a deep dive into why this is happening and discuss possible mitigation options.

The Rise and Fall of Conti

The now-defunct ransomware group known as Conti set the standard for Ransom-War attacks. Prior to announcing its public support for the Russian invasion of Ukraine, the group – together with its sister group REvil – rampaged across the digital world.

Over an 18-month period, Conti accumulated over $180 million in payouts, leading the US Department of State to offer a $15 million reward for information leading to the identification or conviction of its members.

Notably, Conti was responsible for the state of national emergency declared by Costa Rica in 2022, after that country refused to pay a $10 million ransom and suffered a 672GB leak of sensitive data from various Costa Rican government agencies. Costa Rica's then newly-elected president, Rodrigo Chaves, declared the country "at war" with cybercriminals.

Similarly, Conti hacked Peru's premier intelligence agency, which is responsible for national, military and police intelligence, as well as counterintelligence. They succeeded in exfiltrating 9.1GB of sensitive intelligence data.

The group apparently disbanded after a crackdown precipitated by their public support for the Russian invasion of Ukraine. Yet the bar they set for sheer audacity and efficacy in their attacks against government targets remains high.

Most Recent Ransom-War Targets

In recent months, other ransomware hacking groups seem to be targeting government entities worldwide with increasing frequency. Most notably:

- In July 2023, the city of Hayward, California declared a state of emergency, after a ransomware attack breached the city's computer systems and networks.

- Also in July, Barts Health NHS Trust – an entity within the UK's national healthcare system – suffered a ransomware attack, potentially leaving data from 2.5 million people at risk.

- In February 2023, the city of Oakland, California was hit by a ransomware attack, forcing it to take all systems offline.

- That same month, the U.S. Marshals Service – a federal government agency - suffered a ransomware attack that exposed sensitive law enforcement information.

- In January of 2023, also in the UK, a ransomware attack shut down the Royal Mail, the country's largest mail delivery service.

- Also in January, a ransomware attack on San Francicso's Bay Area Rapid Transit Authority (BART) led to the release of sensitive files after the authority refused to pay the ransom.

Drill Down: Why Target Governments?

Ransomware groups target governments for several reasons. First, governments collect and store valuable data on their citizens and have large budgets. This makes them potentially lucrative targets for financial gain. Second, they own and run sensitive critical infrastructure. Attacking governments allows ransomware groups to disrupt critical services with the resulting chaos potentially exerting political pressure to pay ransoms. And of course, some threat actors have political or ideological agendas, and governments represent easy and symbolic targets for local or regional vendettas.

To better understand the motives of Ransom-War threat actors, we analyzed the above-mentioned Costa Rica attack more in-depth. Costa Rica is, after all, a popular tourist destination and not generally considered a country with overbearing or extended political reach. So why would Conti have chosen to launch an attack against such an unassuming country?

- Theory 1 – The attack was simply a crime of opportunity. Attackers were looking for vulnerabilities or weaknesses and struck when they found them in the Costa Rican government's systems.
- Theory 2 - Owing to the sensitive timing of the attack (immediately following the transition of power following a national election), it was an attempt to destabilize the country or overthrow it altogether.
- Theory 3 - Based on internal Conti communications, the attack may have been a smokescreen created to remind the public of the group's prominence and lucrative attack prowess.
- Theory 4 - Since Costa Rica publicly rejected the Russian invasion of Ukraine and Conti was aligned with Russia, the motivation was political.

Understanding the motives of ransomware groups that target governments is crucial for devising effective strategies to combat and mitigate the impact of ransomware attacks on governments.

What Can Governments and Their IT Service Providers Do?

It is common for attackers to target companies providing IT services to governments, as they may be less secure.

While having backups in place can mitigate the need to pay for a decryption key, it does not prevent ransomware attacks from occurring against government agencies or entities. To establish robust government cybersecurity, it is crucial to implement preventive measures and proactively counter threats. Some actions companies providing services to governments can offer:

- Limit publicity over governmental projects - this is particularly important in foreign media outlets in foreign languages.

- Decentralize public and external digital assets so that if attackers are familiar with one IP/domain, they can't know everything within the public domain

- During wartime, reduce the attack surface by temporarily taking down unnecessary public assets such as old websites

- Review and prioritize publicly accessible vulnerabilities, and address their urgency according to risk

- Continuously monitor networks and proactively hunt for threats to identify and intercept intrusions early on

The Bottom Line

Ransom-War is on the rise. High-profile attacks against strategic government targets are becoming increasingly severe and intense. Governments are attractive targets due to their valuable data, large budgets, and critical infrastructure. To combat this menace, governments must implement effective preventive measures. It's time for governments to take a stand and protect their digital fortresses from acts of Ransom-War.

About the Author

Nissim has over 10 years' experience serving in a variety of cybersecurity functions including being a CISO, and providing DFIR, malware analysis and SIEM professional services for private companies, military organizations and government. He also occasionally creates and teaches cybersecurity courses for professionals. He currently serves as CYREBRO's Director of Innovation. Nissim can be reach via LinkedIn at https://www.linkedin.com/in/nissim-ben-saadon-0ba173bb/ and at CYREBRO via www.cyrebro.io.

Reducing Burnout and Increasing SOC Retention: How Leaders Can Improve Their Employees' Lives and Improve Security

By Kayla Williams, CISO, Devo

The significant skills gap and burnout of current personnel are two of the most frequent challenges cybersecurity leaders must solve. ISC(2) estimates there's still a 3.4 million-person deficit in cybersecurity worldwide. And this problem might soon grow worse. A new Wakefield Research study found that 85% of participating IT security professionals think they'll need to leave at least their job, if not their organization, because of the severity of their burnout issues. It's gotten so bad that 24% of the survey respondents saidthey may switch to a different career altogether.

We can't afford to widen the security skills gap by letting burnout run rampant. Overcoming these two issues is crucial for security leaders, but doing so will require a grasp of how serious a threat burnout is and the technologies/procedures needed to address it.

What's happening in the SOC

Burnout and the cyber skills shortage affect virtually every function in cybersecurity, but they're particularly severe in the SOC. The Wakefield Research survey also found that 76% of respondents believe their IT leaders couldn't make it through one day of trying to manage the massive alert workload.

SOC roles aren't for the faint of heart. At every level of the SOC, employees are under almost continual pressure because failure might have catastrophic consequences for the business. SOC work is challenging and demanding. A staggering 71% of security leaders and non-management personnel rate the pain of SOC staffers at 6 through 9 on a scale of 10.

The good news is that we are seeing more organizations turn to automation to augment the work of their SOC analysts by shifting some of the more monotonous tasks and enabling analysts to focus more on the threats most important to their organization. However, this shift takes time, and threats continuously evolve, which means SOC roles also continue to change. To be effective today, Tier 3 analysts must be more skilled and aligned to business objectives.

Deep disconnects remain between SOC leaders and staff, and teams don't feel heard or taken seriously about burnout-related issues. 45% of SOC analysts surveyed said their leadership hadn't responded proactively to burnout.

Time to assess your technology stack.

The issues of SOC hiring and retention must be addressed in part by assessing an organization's technology stack. Having comprehensive visibility is the foundation of this. Fortunately, there are security solutions today that are easily implemented and can provide visibility into all parts of an organization's operations, gathering logs and insights in one place.

It's not just visibility that matters; it's also about what's done with the data, which means it must be usable. The dynamic scalability of cloud-based security analytics tools allows them to take in all of the data and then process it in real time. Organizations are investing appropriately to ensure they can switch to a real-time alert detection, investigation and response framework now that the capability exists.

Adopting a wider application of artificial intelligence and machine learning is the third move toward upending outdated methods. The AI/ML tools available now are excellent, and they'll only get better. Specifically, new capabilities include autonomous alert triage, where AI-driven systems rapidly assess and prioritize alerts, and proactive threat hunting, where machine learning algorithms uncover hidden threats. This is advantageous for SOC teams and CISOs who are able and willing to adopt these technologies, transforming their SOC teams from front-line gatekeepers into guardians and instructors of rapid automated response systems.

Implementing more automation will be key. According to the survey, 55% of SOC practitioners want their leaders to invest in automation, among other solutions/resources they said they desired.

Attending to the SOC team

Burnout is impacting organizations' security posture in a real way. 83% of IT security professionals in the Wakefield Research study reported that they or a member of their department have made mistakes due to burnout that led to a network breach; 39% have experienced this more than once. Ensuring that SOC analysts find meaning in their work is another key component to addressing the burnout challenge. By

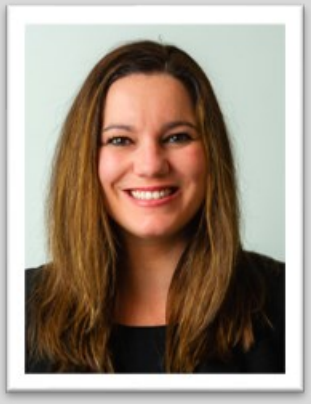
having the right tools, for example, SOC teams can lower the number of false alarms and reduce alert fatigue, enabling analysts to concentrate more on delivering business value and reducing risk.

SOC staff also want their leaders to offer additional training, mentorship and development (59%) to help with burnout. If managers allocate time each week for staff training for both personal and professional development, this promotes a culture of company commitment to work-life balance and mental well-being. All these factors increase retention and job satisfaction

Act now for future success

The shortage of cybersecurity professionals and SOC analyst burnout require immediate action. It's crucial to strengthen your technology stack for real-time response. Additionally, boosting job happiness through meaningful work, reducing false alarms, and promoting personal development are necessary to address today's challenges in the long term. To retain qualified employees and successfully manage industry challenges, IT leaders must adopt cutting-edge tools and foster a SOC culture that prioritizes well-being.

About the Author

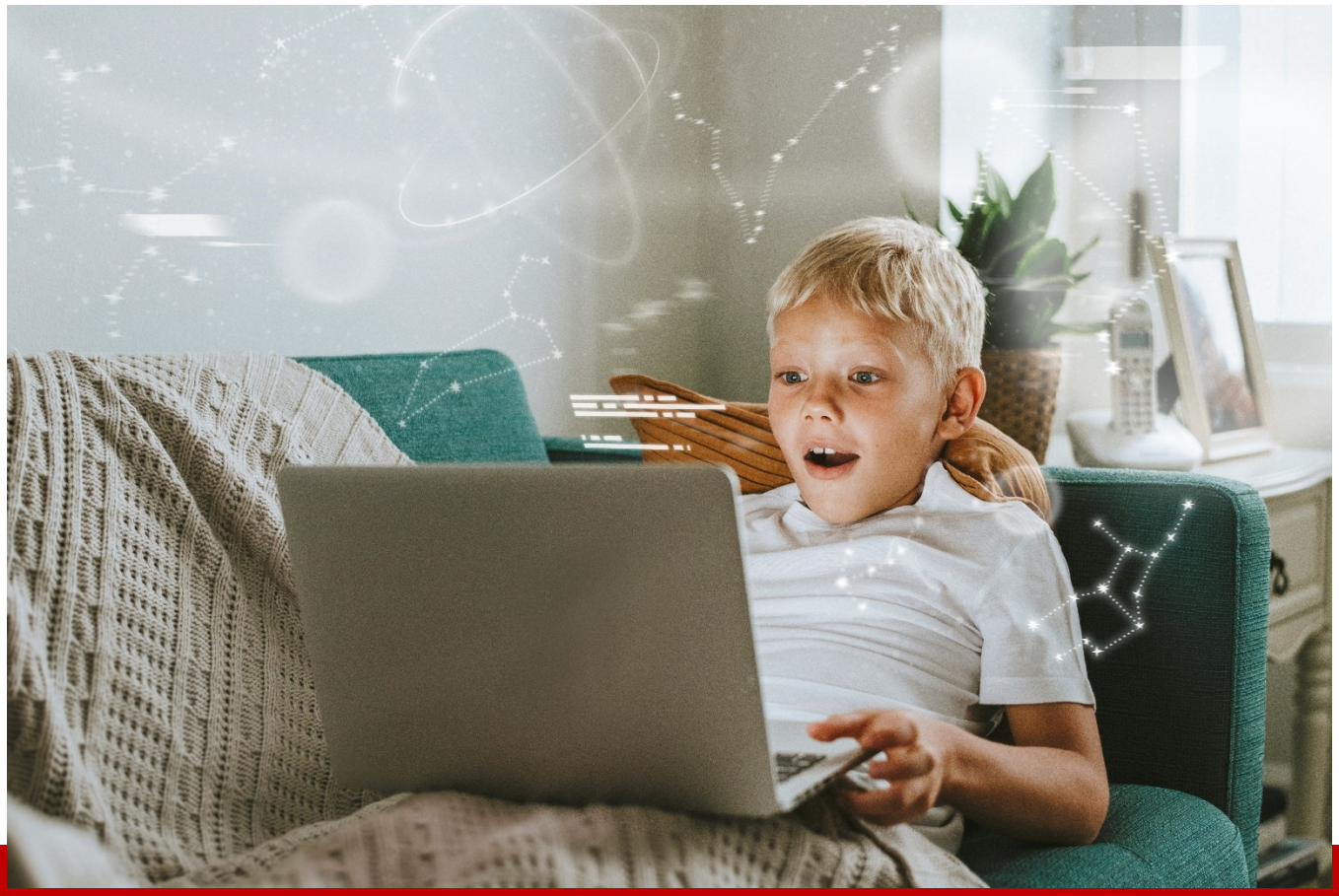


Kayla Williams is the CISO and VP, governance, risk, and compliance (GRC) at Devo, a cloud-native logging and security analytics platform with a $2B valuation.

She is an analytical and results-driven professional with experience in management of cybersecurity incidents, compliance management, corporate risks, information security, project and program management, and organizational controls surrounding many different aspects of business. Kayla also is accomplished in the development of key methods for organizations to strengthen productivity, enhance operational performance, and improve financial and operational controls. Prior to this role, Kayla was the director of GRC at LogMeIn, a $1b global SaaS company, and the senior risk manager for Computershare US, a global financial services company, where she was responsible for supporting the development, implementation, and monitoring of operational, financial, compliance, and IT risk. Additionally, she worked directly with executive management to identify, assess, and establish mitigation strategies for any risk that arose from inadequate or failed processes, people, systems, or external events, while maintaining a balance between risk mitigation and operational efficiency. This enabled executive management to make informed decisions about the risk posture of the organization and dedicate resources to key areas to minimize critical and high risk to business operations.

Kayla currently resides in Boston, Massachusetts and Alfreton, Derbyshire, UK.

Kayla can be reached at our company website https://www.devo.com/.



Safeguarding Children in the Era of Big Data

By Ron Kerbs, CEO, Kidas

In the ever-evolving landscape of cyberspace, 2023 unveiled a concerning trend: major players in the tech industry, including giants like Meta and Discord, were found either misusing or inadequately handling data — particularly data belonging to children. As we stride into 2024, legislative and regulatory efforts are underway to address these data privacy concerns. However, it is crucial for parents, guardians, schools and anyone responsible for the well-being of children to remain vigilant. Rather than solely relying on regulatory measures, proactive steps must be taken to educate and empower the younger generation with proper online etiquette and safety guidelines.

The Big Data Dilemma

The past year has highlighted instances where big data companies and social media platforms, entrusted with the sensitive information of millions, fell short in safeguarding the privacy of their youngest users. From targeted advertising to data breaches, vulnerabilities in existing systems became apparent, raising serious questions about the ethics of data collection and usage.

In response to these concerns, legislators and policymakers are racing to establish frameworks that hold tech companies accountable for their handling of user data, especially that of our youngest users. While these initiatives are commendable, the pace of technological advancements often outstrips the speed at which regulations can be implemented and enforced.

Be Cautious

As we await the implementation of stricter data protection measures, it is imperative for parents to exercise caution when allowing children access to the digital realm. This is not a call for technophobia - a fear of technology, but rather a plea for prudence. Parents should take an active role in familiarizing themselves with the privacy policies of the platforms their children engage with, understanding how data is handled and staying informed about any changes in those policies. Once decisions have been made on what social media networks, video game platforms and other online access children have, parents should put boundaries in place to keep their children safe.

Shaping Digital Citizens

Instead of relying solely on external regulations, the onus is on parents, guardians and educators to instill in children a foundational understanding of responsible digital citizenship. This involves teaching them not only about the potential dangers lurking online but also about the importance of respectful communication, empathy, and adherence to ethical guidelines.

Kidas, a software company specializing in monitoring in-game voice and text communication in PC video games, discovered a troubling trend between October and December 2023. Among gamers aged 8 to 15, 23% experienced privacy violations, including the sharing of sensitive information such as credit card details, social security numbers and passwords during their gaming activities.

Despite most social media platforms and games setting a minimum usage age of 13, an alarming 31% of identified threats were directed at children between 8 and 12 years old during the same timeframe. More unsettling is the fact that 35% of 13-year-olds, the age at which many platforms require account creation, faced privacy violation threats. This suggests that even at the age of 13, children may not possess the necessary technological savvy to ensure their online safety.

To safeguard children online, it is imperative to focus on education and protection measures. Providing guidance on the potential dangers of the internet, emphasizing the types of information to avoid sharing online and fostering an understanding of the anonymity inherent in online interactions are crucial steps in ensuring the safety of children in the digital realm.

Earlier Intervention

In an era where children gain digital literacy at an increasingly young age, the importance of early intervention cannot be overstated. Waiting for regulatory frameworks to fully catch up is not a viable

strategy. Parents should seize the opportunity to educate their children about the intricacies of the digital world and empower them to make informed decisions regarding their online presence. Education about monitoring and the importance of a shield online will help keep the lines of communication between parents and children which allows for early intervention. When both parents and children are in the loop on what's happening online, early intervention becomes possible.

The Role of Monitoring Software

Recognizing the challenges parents face in monitoring their children's online activities, technology provides a solution. Software solutions offer parents a valuable tool to keep tabs on in-game voice and text communication. By leveraging such monitoring tools, parents can strike a balance between fostering independence and ensuring their children's safety in the virtual space.

Monitoring software serves as a bridge between cautious parenting and the ever-expanding digital landscape. It allows parents to understand their children's online interactions, identify potential risks and intervene when necessary, promoting a safer and more secure online experience.

As children are exposed to the internet at increasingly younger ages, they lack the emotional and mental maturity to know how to deal with many of the real dangers they may be exposed to on the internet. A child's innocence blindsides them when an online predator tells them that they are the same age and begins to form a friendship with them. The same innocence is what gets them taken advantage of when another gamer suggests they will give them free gaming currency and then steals their gaming accounts with a simple click.

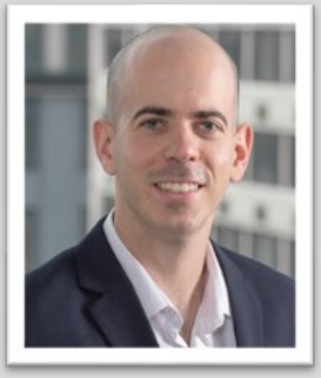
With a monitoring software on board, parents are given a birds eye view into any threats their children are exposed to enabling them to be proactive in dealing with threats as soon as they are detected. Parents can't completely rely on their children to have the maturity to come to them when they are exposed to a threat online, or to be aware of all threat exposures. Instead, parents need to work in partnership with their child by communicating about monitoring softwares as well as educating them on dangers online.

Conclusion

As we confront the challenges posed by the misuse of children's data, the emphasis should not solely be on reactive regulatory measures. Parents, guardians and educators must proactively engage in the digital education of children, empowering them to navigate the online landscape responsibly. By combining vigilance with technological solutions, we can foster a generation of digital citizens who are not only aware of the potential risks but are also equipped with the skills to navigate the digital playground safely. In doing so, we pave the way for a future where the digital world becomes a secure and enriching space for all.

About the Author

Ron Kerbs is the founder and CEO of Kidas. He holds an MSc in information systems engineering and machine learning from Technion, Israel Institute of Technology, an MBA from the Wharton School of Business and an MA in global studies from the Lauder Institute at the University of Pennsylvania. Ron was an early-venture capital investor, and prior to that, he was an R&D manager who led teams to create big data and machine learning-based solutions for national security. First Name can be reached online at Ron@getkidas.com and at our website at www.getkidas.com.



Securing Space Infrastructure for US And Allied Collaboration

By Kevin Kelly, CEO and Chairman, Arcfield

As the role of satellite communication systems in geopolitical conflicts and critical infrastructure sectors continues to expand, concern regarding the security of satellite communications (SATCOM) systems is growing. These concerns are valid, as evidenced by the February 2022 cyberattack against satellite company Viasat, which the European Union dubbed one of the most significant hacks of space equipment to date.

There's no doubt that space is one of the fastest growing sectors, for federal and commercial markets alike. According to the United Nations Office for Outer Space Affairs, there are more than 16,700 satellites orbiting Earth, with 2,748 launched just last year. Additionally, Euroconsult estimates that an average of 1,700 satellites will be launched per year by 2030. Starlink's mega-constellation had over 5,000 satellites launched earlier this year and is projected to have as many as 42,000 total satellites when fully deployed.

Amid the rapid growth of the space domain, the U.S. Space Force is developing a next-generation, resilient SATCOM system known as the Protected Anti-Jam Tactical Satellite Communications (PATS) family of systems. For the program to be successful, it must address numerous challenges to promote

increased bandwidth, cybersecurity, resilience, and interoperability among the U.S. and its international partners.

Why SATCOM cybersecurity is critical

Satellite operations are built on memory, compute and communications infrastructures. These systems rely on microelectronics and circuitry and are increasingly connected to the internet. As a result, both in-orbit satellites and their ground operations may contain network vulnerabilities that bad actors can exploit.

If a malicious actor successfully deployed a phishing or ransomware attack to gain control of a network of terrestrial-based stations that are communicating commands to a satellite constellation, the attackers could issue commands to alter a satellite's telemetry, control, memory and content. From there, the attackers could use their own wireless uplink to mimic command and control signals to targeted satellites completely taking over a target satellite.

With satellites now responsible for critical functions such as military communications, national defense systems, missile launch detection, aircraft navigation services and much more, such an attack could have seismic consequences. It's imperative that the U.S. government continue to invest in a system such as PATS and prioritize international cooperation with our allies to improve global SATCOM security.

Bolstering satellite and ground system cybersecurity postures

Comprehensive SATCOM security requires diligence and dedication to ensure systems are kept up to date; however, this investment is well worth it to avoid the potentially severe outcome of a cyberattack.

Legacy systems are a primary hurdle that engineers and IT professionals must overcome when striving to secure satellite constellations and ground systems. Many satellites that were engineered decades ago are still in-orbit and being used today, however, the notion of a cyberattack against a satellite was considered impossible when those systems were developed and launched. Therefore, few safeguards were put in place to defend against cyberattacks.

While the ability to push upgrades via software is inherent to each spacecraft's operating system, it is important to realize that comprehensive security is more than just a piece of software and should include an architecture that involves authentication layers and encryption. Even the ground control data link to the satellite can potentially be compromised with the limited encryption used in legacy SATCOM systems.

However, the ability to provide a software upgrade and add layers of security to the legacy satellite itself is often limited when the satellite utilizes a first or second-generation microprocessor, whereas modern, advanced cybersecurity software systems require a fifth or sixth generation processor. As such, it's imperative to invest in and protect the numerous servers and command controls on the ground. To defend the ground base network and provide a more sophisticated level of security, it's critical to ensure the entire architecture has the authentication, encryption and different layers of protection necessary to deter and defend against bad actors. With each of those security layers receiving updates against emerging threats.

For new satellite constellations, protection begins in the architecture and engineering phase. Irrespective of cost, it's imperative to build security inside all the different subsystems within the satellite—doing so initially is much more efficient than attempting to retroactively patch vulnerabilities.

As mentioned earlier, adequate defense requires multiple layers of protection. These layers include a range of encryption and monitoring systems which can detect nefarious activity. It's also important to prioritize architectural resiliency. If a system is compromised, the first step is to take it offline. Engineers should also consider implementing multiple safe/recovery modes that allow the compromised satellite to be recovered from an attack and re-initialized.

Another defense tactic is to create a cost imposing strategy for adversaries. By making the defense systems exceedingly difficult and expensive to penetrate, the target becomes less attractive and therefore less likely to be attacked.

All hands on deck — the role of legislation, regulation and cooperation

In addition to technical enhancements, securing our space infrastructure and maintaining a strong foothold in the domain will require international cooperation, as well as domestic legislative and regulatory updates.

As such, the September 2023 release of NIST's Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) is well timed. This framework provides guidance for improving infrastructure security, hardening security for assets, data and systems, and reducing the risks to HSNs, which is an aggregation of independently owned and operated terminals, antennas, satellites, payloads, or other components that comprise a satellite system.

In addition to NIST's guidance, legislation is now being proposed to have space added to the list of critical infrastructures. The Space Infrastructure Act would direct the Department of Homeland Security secretary to designate space systems, services and technology as a sector of critical infrastructure.

It's evident now more than ever, that the U.S. federal government has a large role to play in helping to shape and secure the future of the space domain by hardening our SATCOM defenses, strengthening collaboration with international allies, and implementing necessary security guidance and legislation.

Given the exponentially increasing role of SATCOM in both the commercial and military landscapes, public and private sector collaboration will be integral to satellite cybersecurity initiatives. Luckily, some of the best minds in the nation are dedicated to these efforts. With continued, comprehensive, and committed work, the U.S. and its allies can reap the many benefits that SATCOM has to offer without compromising on security.

About the Author

As chairman and chief executive officer (CEO) of Arcfield, Kevin Kelly oversees the development and implementation of the company's strategy while ensuring the company delivers technology-differentiated solutions to missions that are critical in protecting the United States and its allies. As CEO, Kevin is responsible for establishing a corporate culture, building and managing an expert leadership team, launching an innovation incubator that will ensure the company is developing solutions ahead of mission needs, and the overall growth of the company.

Kevin has been an active leader in the defense and intelligence industry for more than 30 years with proven success leading and managing companies through growth activities. He is passionate about innovation and ensuring that a company leverages its people, processes and technologies to its maximum potential to deliver for its customers.

Prior to Arcfield, Kevin was the CEO of LGS Innovations, a privately held independent technology company that was eventually acquired by CACI International in March of 2019. After its acquisition, Kevin oversaw the company's integration into CACI through the company's creation of a new high-tech sector (National Security and Innovation Solutions Sector), where Kevin would ultimately serve as president. In this role, Kevin oversaw the operations of a $2B business consisting of the technology and products portions of several key acquisitions; namely LGS Innovations, SIX3 Systems, TICOM Geomatics, and L3 NSS.

Prior to his appointment as CEO at LGS Innovations, Kevin served as the company's chief operating officer and senior vice president of strategy. Earlier in his career, he held senior positions within General Dynamics and Lockheed Martin.

Kevin holds a bachelor's degree in electrical engineering from Penn State University and a master's degree in engineering management from George Washington University (GWU). He has held board and advisory positions with the LGS Innovations board of directors, Innovative Technologies Council of the Intelligence and National Security Alliance (INSA), Armed Forces Communications and Electronics Association (AFCEA), Institute of Electrical and Electronics Engineers (IEEE), the National Advisory Council for the GW School of Engineering and Applied Science (SEAS), and several other firms. Kevin is also a proud member of the Engineering Hall of Fame at GWU SEAS.

Kevin can be reached online at https://www.linkedin.com/in/kevin-l-kelly/ and at our company website https://www.arcfield.com/

Understand Cyber Insurance: Rising Risks and How to Right-Size Policies

Cyber insurance can be a tricky part of cybersecurity strategy — here's what to know in today's security climate

By John Reith, Partner Success Manager at DataStream Cyber Insurance

Cyber insurance is an increasingly crucial backstop to cybersecurity practices. While enlisting comprehensive protections and preventing data breaches is always the best-case scenario, a sufficient cyber insurance policy can mitigate the sizable expenses that arrive in a breach's aftermath—from the investigation, to public relations and legal costs, to regulatory fines. Because cyber insurance often requires policyholders to adhere to prescribed cybersecurity practices based on established compliance mandates, cyber insurance can also help businesses adopt safeguards to get their houses in order and stay on regulators' good sides.

As I see it, the day is fast arriving when most businesses will be required to hold cyber insurance—maybe even every business. Mortgage lenders require borrowers to carry homeowners insurance, and the law

requires every car owner to carry auto insurance. This forces owners to take responsibility and mitigate the costs of a disaster themselves. Cyber insurance fills a similar role, enabling organizations to both take financial responsibility and protect themselves from data breach costs that could otherwise put them out of business.

In the same way, some lenders now require organizations to carry cyber insurance to make sure they can repay their business loans. Some businesses now require cyber insurance in contracts with supply chain partners to ensure their security and stability. The government has a similar interest in making sure organizations representing key infrastructure can survive a cybersecurity event. Some managed service providers (MSPs) even now require that their clients carry cyber insurance, declining the risk of working with businesses that don't.

However, many SMBs—and even the MSPs they rely on for expert guidance in cybersecurity matters—still don't fully grasp the importance of adequate cyber insurance and the tremendous risks they face without it. These organizations and their partners may similarly have inaccurate notions of what size of a cyber insurance policy is appropriate, the lengths they must go to demonstrate effective cybersecurity practices, and how to vet cyber insurance providers to ensure trust.

Let's set these misconceptions straight.

SMBs, look out

In general, small- and medium-sized businesses require a wake-up call to shatter their false sense of security. Although cyberattacks on SMBs don't make media headlines like major enterprises, the fact is that cyber attackers actually prefer to go after SMBs, because they're usually soft targets.

SMBs often falsely believe they're not on attackers' hit lists, or that an incident such as a ransomware attack will only impact their systems for a few hours. In reality, they are attackers' prime targets, and most ransomware attacks lock up systems for days or weeks. The bottom line: 75% of SMBs would go out of business if struck with ransomware. Effective cyber security and cyber insurance mitigate that extinction-level risk for SMBs.

How much cyber insurance does an organization need?

Cyber insurance policies are broad, and choosing the right coverage is essential to an organization's survival in the aftermath of an incident. MSPs and cybersecurity experts can offer crucial guidance in selecting effective policies and making sure that organizations meet all policy requirements.

As a best practice, businesses should carry coverage equaling at least 15% of their annual revenue, or $1 million minimum. Policies may include first-party coverage for the company's costs caused by an incident, and third-party coverage for costs relating to their customers or other parties. Policies may include sub-limits and exclusions as well. A policy with $1 million dollars in coverage might have a sub-limit of just $50,000 for ransomware incidents. A policy with an exclusion for social engineering-based attacks—an exceptionally effective method for attackers today—would leave a business covering its own

costs for such an incident. This is why thorough attention to policy terms and conditions can make or break an organization when it's time to put in a claim.

Cyber insurance (still) requires robust and compliant cybersecurity

Trust me, cyber insurance providers don't stay in business by insuring organizations with bad security. Businesses must pass a risk assessment and security questionnaire to complete the underwriting process. Such risk assessments are usually based on established regulatory frameworks such as the NIST Framework and others. Therefore, effective cybersecurity is a requisite for cyber insurance. Businesses must implement comprehensive tooling, such as data encryption, access control, multifactor authentication (MFA), automated threat monitoring and mitigation, logging and reporting, and more. For this reason, I recommend multi-faceted security tools to organizations, such as BeachheadSecure, which meets 76% of NIST requirements, and Acronis in order to start checking a lot of boxes and set the table for a successful cyber insurance partnership.

All that said, having effective cyber security isn't enough: organizations must carefully document protections to ensure approval of cyber insurance claims. For instance, a business required to implement MFA on all endpoint devices needs to have screenshots and documentation ready to prove that even newly added devices have those contractually necessary safeguards in place, and that they were active as an incident occurred.

Be wary of traditional insurers

Cyber insurance is a specialized product requiring expertise on the insurer's part as well. Unfortunately, some traditional insurers began to offer cyber insurance in recent years without acquiring the knowledge to do so correctly. The result has been horror stories, as these providers fail to correctly explain policy requirements to customers and then deny their claims for failure to meet those unclear requisites. Just as cyber insurers vet potential customers, organizations should carefully vet their insurers as well, and stick to trustworthy proven cyber insurance providers.

Protect your organization before and after an attack

Comprehensive cyber security and cyber insurance play an overlapping role in protecting organizations from the potentially devastating impacts of a cyberattack. Cyber insurance providers require organizations to implement robust security processes, and insulate them from the consequences if those measures nevertheless fail. By selecting the right cyber insurance strategy and policy, businesses can take peace of mind that they will survive anything attackers throw their way.

About the Author

John Reith is a Partner Success Manager at DataStream Cyber Insurance. He joined the company in 2021 from Forecastable, and has also held channel roles at Time to Reply and Seynd. John lives outside of Austin, Texas. He can be reached via LinkedIn https://www.linkedin.com/in/john-reith-vii/ and at https://datastreaminsurance.com/

What You Need to Know About the Cybersecurity Market in 2024

By Doug Saylors, Partner, Co-lead, Cybersecurity, Information Services Group (ISG)

The cybersecurity market offers promising opportunities for real-time threat intelligence through advanced technologies such as AI and ML. It's also characterized by formidable challenges: the complexity of modern systems, deepfakes, synthetic identities and other emerging tech-related developments.

Heading into 2024, organizations are investing heavily and proactively in cybersecurity to safeguard their digital assets, recognizing that prevention is more effective and cost-efficient than recovery. This includes implementing robust security protocols, deploying cutting-edge threat detection systems, conducting regular vulnerability assessments and promoting a culture of cybersecurity awareness among employees. Additionally, organizations are embracing the concept of "defense in depth," deploying multiple layers of security to create a resilient and robust security posture.

The importance of cybersecurity at the board level cannot be over-emphasized. Executives and board members understand the ramifications of security breaches and are actively exploring strategies and investments to protect the organization's reputation and financial well-being and foster customer trust and loyalty. To do this, they need comprehensive insights into the organization's cybersecurity posture,

including threat intelligence, incident response capabilities, risk quantification and ongoing security assessments.

Regulatory bodies and governments are shaping the cybersecurity agenda with regulatory frameworks that shift accountability to and incentivize enterprises to ensure they have appropriate defenses for critical vulnerabilities. New U.S. Securities and Exchange Commission (SEC) measures will require cyber organizations in large, public corporations to disclose cyber incidents that hit a materiality threshold to the SEC and in financial reports. This is causing an uptick in new financial frameworks and processes, which in turn will have to be auditable and defensible.

Key Trends and Developments in the Cybersecurity Market

Increased dependence on digital infrastructure and connected systems, the expanded attack surface created by connected devices, cloud computing and IoT, and the increasingly distributed workforce and applications work model have accelerated demand for security architecture guidance on cloud, edge, virtualized implementations, zero trust and endpoint detection and response (EDR).

At the same time, cybercriminals and hacktivists are constantly devising new ways to breach security defenses. Human-centric security is now a top CISO concern as techniques such as social engineering and phishing manipulate individuals into revealing sensitive data or granting access to protected systems. Behavioral psychology can provide insight into employees' relationships with risk and ensure cybersecurity awareness education and training is as effective as possible.

These factors reinforce the need for a holistic approach to risk management, harnessing the convergence of disaster recovery, business continuity and cybersecurity to minimize the impact of security incidents and ensure critical systems and services are not interrupted.

Other top cybersecurity trends for 2024 will include:

1. Increased adoption of extended detection and response (XDR)

Extended detection and response (XDR) is an architectural approach that facilitates integrated detection and response capabilities for all internal data sources. Ideally, an XDR approach consolidates multiple security tools to provide a unified solution that automatically monitors, analyzes, detects and mitigates threats. This AI-powered approach uses automation to improve the efficiency of security operations, enabling a cohesive view of threat signals and data across a security environment. XDR vendors use two main approaches in their offering: open and native.

- An open XDR approach uses an enterprise's security tools to provide a layer of integration across silos. Open XDR vendors are required to have extensive integration capabilities. Large organizations with a comprehensive security stack prefer open XDR to create a single management platform, regardless of the vendor ecosystem and pre-existing security environment.
- A native XDR approach involves a single-vendor outlook as an all-in-one platform for security intelligence, in which the vendor takes responsibility for the set up and integrations, enabling rapid

deployment and time to value. Typically, native XDR solutions can be integrated with other security products of the same vendor and have limited interoperability with other vendor security products.

2. **Growth of attribute- or context-based access control and the decline of pure, role-based access control**

Passwordless authentication is becoming a component of a zero-trust architecture. Some enterprises eliminate passwords whenever possible, but to attain the actual state of zero trust architecture, it is imperative to consider other options.

- Security solutions that offer passwordless authentication are gaining prominence among enterprises as they reduce user log-in friction and strengthen system resilience by adding an AI-powered layer of security.
- Some identity and access management (IAM) vendors have acquired start-ups and technology companies to launch AI-driven passwordless authentication platforms that use behavioral data to interpret suspicious activities.

3. **Acceleration of managed security services (MSS) and managed detection and response (MDR) services**

MSS and MDR services empower enterprises to strengthen their cybersecurity frameworks, mitigate risks and respond effectively to security incidents. Outsourcing these services to experts frees organizations to focus on their core competencies.

MSS: Large enterprises need a full range of MSS, including data security, threat intelligence and analytics, incident response, security risk and compliance services and rapid response and recovery to cyberthreats. MSS providers help these enterprises develop and implement a comprehensive security strategy and roadmap.

MDR: Phishing and ransomware attacks are the most common security breaches for small and medium businesses. These businesses need end-to-end threat detection and response capabilities to protect sensitive corporate data and assets, but they lack the budget and expertise to implement robust security measures. MDR service providers offer network and endpoint monitoring, incident analysis and response and proactive threat hunting.

4. **Incident response assessments and virtual CISO services are gaining momentum**

The shortage of skilled experts is a challenge in the industry, and enterprises of all sizes are struggling to hire well-qualified and experienced CISOs. As an alternative, some enterprises are choosing virtual CISO or CISO on-demand services from cybersecurity consulting firms, MSSPs and independent

consultants. These providers offer well-defined and comprehensive virtual CSO (vCISO) services that focus more on small and medium businesses.

For large enterprises, incident response assessments improve understanding of cyber resilience maturity and determine detection, response and recovery capabilities across their security operations.

5. Cybersecurity risk quantification gains traction

Enterprise boards and senior leadership teams are starting to ask how their cybersecurity investments address evolving threats to the business and how to quantify the reduction in risk they deliver. Enter cyber risk quantification methods that use actuarial models to provide tangible, practical and easy-to-understand estimates of cybersecurity value.

In this area, organizations will be hyper-focused on risk analysis from the perspective of AI-driven cyber threats, risks that stem from the organization's use of AI and the cyber implications of the internal use of AI. This will lead to a reactive flurry of policies and guidelines, such as acceptable use policies for ChatGPT, Grok, Copilot and others.

In 2024, more IT and cyber leaders will add cyber risk quantification to their portfolio of tools to communicate cybersecurity value. Solutions range from those that are highly customized and require significant training for cyber and risk teams working with actuarial and risk modelling experts, to risk-quantification-as-a-service leveraging available market and organization data on platforms with proprietary actuarial models.

Investments in advanced security tools and solutions alone will not ensure business continuity. The multitude of challenges enterprises face, including cyber risks, threats and cyberattacks, compliance obligations and more, require them to double down on achieving cyber resilience in 2024.

About the Author

Doug Saylors leads the ISG Cybersecurity business in the Americas, ANZ and Asia Pacific. He offers expertise in cybersecurity strategy, administrative and operational models, large-scale transformation projects, infrastructure, digital enablement, relationship management and service delivery, and a strong focus on minimizing the risk of loss. He has helped dozens of the firm's most prominent global clients in multiple industries, including Aerospace & Defense, Life Sciences, Financial Services, Healthcare and Manufacturing, with operational assessments and strategy development to select optimal delivery alternatives and achieve the client's overall business objectives. Doug can be reached on LinkedIn and at our company website https://isg-one.com/.

Why Companies Are Still Investing in Tech During an Economic Slowdown

By Luke Wallace, VP of Engineering at Bottle Rocket

With rising oil prices, higher interest rates, and an economic downturn plaguing Europe and China throughout 2023, recession is looming in the United States. However, according to a recent Forrester report, American businesses are still increasing their spending on technology despite the threat of an economic downturn. In fact, the study showed that 67% of participants reported an expansion of technology budgets over 2023, specifically increasing spending on security and privacy tools along with digital experience software and backend optimization. With cyber-attacks becoming more sophisticated and complex, especially with the emergence of AI, it has never been more important for companies to invest in cybersecurity to protect employees, customers and the business. Companies are taking advantage of the downturn period to get their ship in order. This involves concentrating on customer value and making sure they aren't wasting money by optimizing current tech investments. Additionally, keeping up to date with the latest tech allows businesses to retain valuable customers while remaining one step ahead of their competitors, putting them at the forefront of the market when the economy comes out of recession.

As budgets begin to shrink, companies need to find innovative ways to continue investing in the best possible security tools to keep up with modernizing cybercriminals. Carefully choosing top-rate security tools and reviewing existing underutilized software contracts may help businesses cut down budgets while securing themselves from cyber threats.

Why investing in your company's security is crucial during a recession

While making budget cuts may seem like the natural reaction to an economic slowdown, tech leaders actually plan to increase spending in IT and security departments to promote resilience through the recession.

Data breaches don't stop during a recession and in fact, cybercriminals are more likely to attack during periods of economic uncertainty. Not only does this leave a company at risk of an attack, but may also impact their client's data if top-rate security is swapped out with an underfunded department. To ensure client retention, tech leaders are prioritizing their customer service by increasing their funding in high-quality security tools.

What is worth the investment, and what isn't worth the hype?

Companies need to prioritize their investments in customers, resilience, and revenue when planning their recession budget. Despite economic turbulence, 70% of respondents in the Forrester study reported planned budget increases in customer experience in 2023. To retain valuable customers during a period of instability, businesses will have to continue putting them first and exceeding their expectations. Baseline expectations of consumers continue to rise, and without proper investment there is a risk of driving customers away.

With client data more and more at risk, client-facing security solutions are a sustainable investment for businesses. By prioritizing customer's data as well as their digital experience, companies can simultaneously protect their reputation and their clients. Maintaining focus on data security even when times are tough will also lead to better understanding throughout the company of the latest cyber threats. This will also help prevent accidental internal data breaches, which can sometimes be more costly for companies than attacks from cybercriminals.

Companies should invest in resilient security tools to optimize their budgets. Though initially more costly, high-quality solutions will be more sustainable than lower-cost solutions, which could potentially be more liable to security breaches, leading to expensive crisis management. Forrester suggests businesses should invest in support for modernizing the cloud, a complete transition to Zero Trust, or in the event that a security breach does occur, training on crisis management and purple team exercises.

How do you test out the latest security while also making sure that your solutions are resilient? Approach new tech with caution, Forrester research recommends. For example, while AI is clearly an extremely powerful tool that can help optimize business, it also comes with multiple risks. Privacy preserving

technologies (PPT) could be an AI alternative, as it promises to act like most models while maintaining privacy, ethics, and regulatory requirements.

Optimizing your security tech.

There are multiple ways to optimize existing security tools to perform at their best, which can help relieve tight budgets. Existing software contracts should be reviewed to make sure that they still work for the company. This may be done by validating any new terms and conditions, renegotiating pricing, and ensuring that only those employees who need it have a license. It may also be time to have a look at your prior investments and make sure they are still relevant to the company. Cut out legacy contracts or underutilized tech that no longer aligns with your business, and consolidate to fewer tools if possible, as some may have integrated a solution that previously required a separate tool.

With economic recession looming over the US economy once again, the majority of companies still recognize how important it is that customers, employees, and stakeholders feel like their needs are being met. That's why it is so important to invest in technology that protects businesses from cyber threats as a company necessity, not a luxury.

About the Author

Luke Wallace, VP of Engineering at Bottle Rocket, unpacks why companies are expected to increase their budgets in tech, including privacy tools and cloud security, despite a looming recession.

https://www.bottlerocketstudios.com/

Why Higher Education Is So Vulnerable to Cyber Attacks — And What to Do

By Zac Amos, Features Editor, ReHack

Cyberattacks are a growing problem worldwide as they can cause significant damage to any organization, big or small. Higher education institutions are especially vulnerable, exposing students and employees to various attacks that can put their personal information and welfare at risk.

Why Is Higher Education a Prime Target?

Cybercrimes are rising in all industries, but higher education institutions remain prime targets for hackers looking for a fat paycheck. The sector experienced 44% more cyberattacks in 2022 than the previous year. Why are criminals targeting schools? Here are a few reasons:

- **Abundance of sensitive information:** The size of higher education institutions makes them prime targets for hackers looking to cash in on stealing and selling sensitive data. Student and employee Social Security numbers, bank accounts and other private information motivate bad actors to infiltrate systems using various attack patterns.
- **Valuable research data:** Many universities pride themselves in having the best and most brilliant minds working on valuable research projects and groundbreaking technologies. Cybercriminals look for opportunities wherever possible. They know intellectual property can be worth millions if sold to the highest bidder.
- **Lack of cyber preparedness:** Many higher-ed institutions prioritize improving facilities and education standards over other factors like cybersecurity. Organizations' complacency and feelings of false security make them prime targets for bad actors.

How Vulnerable Are Universities and Colleges to Data Breaches?

In 2023, the University of Michigan had to shut down systems and IT services after a cybersecurity incident occurred just before the start of a new academic year. The university has over 30,000 faculty and administrative staff and 51,000 students. Some common cyberthreats plaguing higher-ed institutions are SQL injections, phishing and ransomware attacks.

Cybercriminals are scaling their attacks to expose vulnerabilities in higher-ed institutions. They won't stop there. Here are several reasons why schools are more vulnerable to cyberattacks:

- **Lack of funding:** Many colleges and universities fail to prepare for imminent attacks due to a lack of funding for critical cybersecurity systems. As a result, these institutions are forced to pay steep ransoms that only encourage hackers to launch more attacks in the future.
- **Outdated systems:** Higher-ed institutions prioritize large-scale adoption without proper preparation for associated risks as online learning becomes more prevalent. Many universities still use old and outdated systems that are more vulnerable to high-tech cyberthreats.
- **Cybersecurity labor shortage:** According to a 2022 study, over 700,000 unfilled cybersecurity roles exist in the U.S. alone. The lack of qualified professionals headlining cybersecurity departments in higher-ed institutions leads to more vulnerabilities due to lax security standards.

Strategies to Strengthen Cybersecurity in Higher Education

In the U.K., 92% of higher education institutions were affected by cybersecurity compromises in 2022 — significantly higher than the 39% average rate for all businesses. While attacks keep mounting, only 13% of global industries will protect their data in 2023. It's time to start proactively changing cybersecurity awareness by adopting a security mindset.

Here's how universities and colleges can adopt a cybersecurity stance and bolster their defenses against bad actors.

1. Test and Assess Existing Systems for Vulnerability

Many universities and colleges have outdated systems and minimal security safeguards. Bad actors can exploit this situation, force their way into supposedly secure networks and access sensitive information.

Higher education institutions must examine their systems, test existing security measures and address vulnerabilities. Acknowledging areas for improvement and staying open to adopting possible solutions are the first steps to defending against cyberthreats.

2. Implement Rigorous Cybersecurity Measures

Cybercriminals are leveling up their game by adopting new technologies and strategies to steal valuable information. If they are ramping up their methods to infiltrate secure systems, higher education institutions must also recognize relevant trends and take steps to bolster their defenses.

Enabling newer cybersecurity protocols and adopting modern technologies like access control and multifactor authentication can help universities improve their defenses against data breaches. Security teams must monitor critical networks for suspicious activity and patterns outside normal user behavior.

3. Leverage Digital Literacy to Defend Against Cyberthreats

Cybersecurity is a collective responsibility. The quicker education institutions recognize this, the better. University and college leaders should address security issues at every level — from students and administrators to faculty and stakeholders. Digital literacy can be a powerful tool to reduce human errors and prevent data breaches.

Higher education institutions must leverage their educational background to promote cyber hygiene in the school community. Launching cybersecurity campaigns is a viable solution to addressing existing issues. Universities and colleges must inform users of existing cyberthreats and train them to use systems responsibly.

4. Allocate Resources for Cybersecurity

While funding can be a delicate topic for many universities and colleges, it's high time they adapt to the changing digital landscape. Gone are the days when passwords, firewalls and antivirus software are enough to protect against malware and other cyberthreats. Leaders in the higher education sector must recognize the growing risk of cyberattacks.

Universities must allocate ample resources to hire qualified professionals and implement updated cybersecurity strategies to protect sensitive data and secure critical networks. Massive adoption of online learning and the rise in connected devices open a new attack vector for bad actors. As learning methods change for the better, security standards must also keep up to protect everyone's valuable data and sensitive information.

5. Upgrade to Newer, More Secure Systems

Old universities and colleges are traditional institutions and most likely use legacy systems to process and store data. As the education sector faces new challenges, it must transition into updated methods to help shield its users from cyberthreats.

Moving away from outdated systems and establishing attack-resistant ones will give higher education institutions more peace of mind. Although budget constraints can be a significant obstacle, upgrading systems is still a more financially logical alternative to paying expensive ransoms to cybercriminals.

Future-Proofing Higher Education With Cybersecurity

Higher education institutions should be safe spaces for students, staff and faculty — both physically and digitally. Improvements in education and cybersecurity standards must go hand in hand to prepare for a future with evolving technology and threats. Leaders in academia must acknowledge the need for more robust systems and strategies and implement them to ensure everyone's safety.

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.

With The World Distracted, China Stirs Trouble in The Asia Pacific

By Stan Vitek, Resident Geopolitical Analyst, Cyfirma

Introduction – Thrilla in Manilla

President Biden warned that "conflict and chaos could spread to the Indo-Pacific" from late October, and, amidst the wars in Ukraine and Israel, little attention has been paid to China's ongoing coercion, in what Beijing calls the South China Sea, and Manila, the West Philippine Sea (or simply, the Philippine Sea).

China's latest actions involve a Coast Guard vessel nudging a tiny Philippines government-contracted resupply boat, and a Chinese armed militia vessel similarly knocking a smaller Philippines Coast Guard vessel. This is the first time the Philippines has reported Chinese ships deliberately hitting Philippine government vessels, however, it's not unexpected.

The Philippines has a derelict vessel called Sierra Madre beached on Second Thomas Shoal on which live a number of military personnel who would fall under the U.S.-Philippines Mutual Defense Treaty, if

they came under armed attack. However, that vessel is disintegrating, and the Philippine government aims to reinforce the structure using construction materials brought to the site by ship.

China appears determined to prevent these efforts and Beijing is using a combination of fishing vessels, maritime militia, coast guard, and People's Liberation Army Navy ships to intercept the Philippines' resupply manoevres, steadily escalating tensions. More than 100 militia ships and numerous Chinese Coast Guard ships have been witnessed in the area, allegedly almost colliding with Philippine Coast Guard ships at times. This recent incident described above is just the latest in a string of intimidating actions by Beijing, who arguably sees this as an effort to uphold the status quo.

Both Beijing and Manila appear determined to press ahead at Second Thomas Shoal, which means that the U.S. – due to the Mutual Defense Treaty with the Philippines – are increasingly more likely to get embroiled in the conflict. Thus far, Washington has been supportive of Manila, but has largely stayed in the background, offering mostly political assistance. The U.S. State Department asserted its stance after the latest incident, stating that the mutual defense treaty extends to "armed attacks on Philippine armed forces, public vessels, and aircraft." Therefore, it stands to reason that a if a more serious clash occurs, the South China Sea could become the next major global flashpoint.

The Biden – Xi Meeting

Presidents Biden and Xi Jinping met in Silicon Valley in mid-November in an attempt to reduce tensions in the world's most precarious bilateral relationship, but many questions remain unanswered.

The formalized meeting adjacent to the APEC summit – rather than a bilateral summit or state visit – which in itself is arguably indicative of how low relations between the two countries have sunk.

After a year of almost no recorded communication, the meeting itself was presented as an important deliverable, with both leaders announcing a set of measures, including the partial resumption of military communication, following the Chinese withdrawal from military talking channels last year as 'punishment' for US Speaker Pelosi's visit to Taiwan. The resumption of military communications will include operational contact between senior commanders and ship captains, and a meeting between Defense Secretary Lloyd Austin and his Chinese counterpart.

Despite signs of renewed engagement, both Beijing and Washington (and Manila, for that matter) appear committed to their current confrontational course, which means the prospects for stabilization remain distant at best, and foolhardy at worst. It was during the conference in California that Chinese ships were provoking Philippine vessels in the exclusive economic zone, and Chinese hackers were infiltrating the Filipino government.

It could be asserted that Beijing's skepticism around dialogue is because this situation is seen as an avenue for the United States to try to contain China's actions in regions that China feels are sovereign (i.e. the fault lines inside China's so-called ‚ten dash line'), claims on territory in internationally-recognized waters belonging to other Asia–Pacific states like Vietnam, Indonesia or the Philippines. China argues it's Coast Guard and the militia are simply enforcing China's domestic laws, which the country has unilaterally decided to apply to the 90% of the sea it claims. In terms of area, China's contested take-

over of this expanse dwarfs Russia's attempted annexation of Ukraine – to a tune of five times – but was rejected by the Permanent Court of Arbitration at The Hague in 2016.

From the People's Liberation Army's perspective, the United States has no business being anywhere near the Taiwan Strait, Thomas Shoal, or anywhere within region of the ten dash line, where China claims territory. For that reason, we should restrain our expectations as to the real beneft of the recent talks. Given Chinese actions, we can rest assured that this will be tested soon. However, we should not expect either the US-China Defense Policy Coordination Talks or the US-China Military Maritime Consultative Agreement to fundamentally alter the trajectory of events in the second Thomas Shoal.

The Cyber Perspective

The Asia–Pacific region is host to the most prolific users of cyber as a tool of statecraft, with China being the undisputed largest state sponsor of cyber attacks in the world. Many tensions in the region (exacerbated by extra-regional powers like the U.S.) have the potential to escalate into conflict, and most likely take place in cyberspace.

While Beijing was stirring up trouble in the Philippine Sea, the China-affiliated APT; Mustang Panda, has been attacking governmental organizations in Manila. Researchers have also attributed three other campaigns from this summer, primarily singling out organizations in the South Pacific to the same Chinese APT. The campaigns leveraged legitimate software including Solid PDF Creator to sideload malicious files which cleverly impersonated legitimate Microsoft traffic for command-and-control connections.

Mustang Panda, also tracked under the name Bronze President, has been active since at least 2012, orchestrating cyber espionage campaigns targeting both non-governmental organizations and government bodies across North America, Europe, and Asia. This year, Mustang Panda and other APTs have been focused on countries surrounding the South China Sea, where China presses territorial claims on countries like the Philippines, Vietnam or Indonesia, as well as on the United States, with which China is in conflict over primacy in the region and global affairs as a whole. Guam; a US territory in the Western Pacific that is home to significant US military bases, has allegedly been targeted.

A joint advisory from all Five Eyes countries (Australia, Canada, New Zealand, the United Kingdom, and the United States) reported a major Chinese cyberespionage operation that has reportedly succeeded in penetrating a range of US critical infrastructure sectors earlier this year. The attack is attributed to a Chinese APT known as Volt Typhoon, a group that has been active for at least two years. The industries of communications, manufacturing, utilities, transportation, construction, maritime industries, government, information technology, and education have all become targets of the observed campaign. The threat actor has likely been trying to conduct espionage and keep access without being discovered for as long as feasible, according to the observed behavior.

Just recently, the Five Eyes issued another warning against, use of artificial intelligence in large scale Chinese hacking campaigns, given AI's potential to amplify and augment the threat. Chinese hackers have been mainly focusing on the defense industrial base, successfully compromising the networks of contractors to the Pentagon's U.S. Transportation Command 20 times in a single year, while many other

incursions have probably never been found. Some researchers are also worried China is trying to position itself in a way it could try to paralyze U.S. critical infrastructure in case of an eruption of conflict between the two countries over the issue of Taiwanese or Philippine waters.

External Threat Landscape Management (ETLM)

The meeting between Joe Biden and Xi Jinping in San Francisco produced an agreement to partially restore previous channels of military-to-military communication, suspended by Beijing in August 2022. While resumption of some military-to-military dialogues is welcome, the agreement does not restore pre-2020 levels of defense communication between the U.S. and China. More senior strategic defense policy dialogues, such as those previously held at the undersecretary or assistant secretary level, do not appear to have been restored.

US officials blame China's increasingly aggressive stance for more unsafe intercepts. Communication gaps amid tensions will hinder crisis de-escalation. Crisis prevention progress is elusive as both sides use military and cyber posturing, reflecting an intractable disagreement over Western Pacific operational rights. As Taiwan and the US approach presidential elections, the political climate will likely remain fraught with risks and tensions.

China's longstanding strategy of escalating actions appears poised for further intensification. The Chinese Communist Party backed Global Times has already predicted "more severe collisions," and in the immediate future, there is a high probability that China will damage or sink a Philippine Coast Guard vessel or one of the smaller Philippine government-chartered vessels. Additionally, the heavily armed Chinese ships could fire warning shots to further demonstrate their growing determination, with other actions also possible. In such a tense environment, large state-sponsored cyberattacks remain a very real threat.

About the Author

Resident International Relations Analyst at Cyfirma, working for technology companies in Southeast Asia and the US since graduation from International Security Studies at Charles University in Prague in 2019. He focuses on international relations and security issues, especially on those revolving around West-East

Stan can be reached online at (stan.vitek@cyfirma.com, https://twitter.com/FogOfWarCZ, etc..) and at our company website https://www.cyfirma.com

Wireless Peripheral Devices - Security Risk, Exploits and Remediation

This article covers the importance of Wireless Peripheral Device Security, the risks involved, and ways to remediate the security exploits.

By Prathibha Muraleedhara and Akhilesh Bhangepatil

Abstract

The advancement of technology has led to an increase in cybercrimes. Any potential threat to user computers is worth investigating. One such threat could be through peripheral devices like mice and keyboards that are connected to the computers. Cybercriminals can capture keystrokes by intercepting the traffic between these peripheral devices and the computer. Just by using a $20 USB dongle, they can inject keystrokes and remotely type in malicious commands on the victim's laptop. Using specially crafted commands the attackers can potentially take over full control of the target laptop. This article intends to create awareness about security exploits through peripheral devices and ways to prevent these attacks.

Keywords - Wireless peripheral devices, radio frequency, MouseJack, Crazyradio, wireless keyboards, USB Dongle, keystrokes, vulnerability, threat.

1. Introduction

Wired mouse and keyboards are no longer used as they are very messy. Today, wireless peripheral devices are widely preferred as they provide a convenient cable-free connection. However, unlike other USB devices like memory card readers, MFA authentication devices, USB storage drives, and fingerprint sensors, wireless mice and keyboards hardly include any security features. Many of these peripherals are affected by security vulnerabilities which can lead to complete compromise of the computers they are connected to. As more organizations are supporting remote work, it's very important to understand the security risks involved when choosing the type of accessories that the employees are allowed to connect to the workstations.

Wireless peripheral devices like mice and keyboards use proprietary protocols operating in the 2.4GHz ISM band (Marc Newlin, 2016). They do not follow the Bluetooth protocol which has well-defined industry-standard security schemas. Thus, the manufacturers end up implementing their own security schemas which often include weaknesses that can be exploited by malicious users. Wireless mice and keyboards are paired with a USB dongle that is connected to the computer. The wireless mouse or keyboard communicates by transmitting radio frequency packets to the USB dongle. When a key is typed on the keyboard or when the mouse is moved, the packet describing the action performed is transmitted to the dongle. The dongle listens to these packets and notifies the computer to process and perform the required actions like moving the cursor or typing the text/commands. To prevent sniffing or eavesdropping, some manufacturers encrypt the radio frequency packets that are transmitted to the dongle. The decryption key is stored in the USB dongle using which it can decrypt the data and process the packets. This prevents attackers from intercepting the data and analyzing the keystrokes transmitted. Also, encryption lets the wireless devices authenticate to the connected dongle, thus preventing a rouge wireless device from connecting to the dongle and sending maliciously crafted keystrokes to the computer. However, most of the wireless peripheral device manufacturers do not encrypt their connection which has allowed attackers to capture the mouse clicks and keystrokes transmitted. Due to the lack of authentication, the dongle will not be able to differentiate if the packets are coming from a legitimate peripheral device or from the attacker. This allows hackers to send malicious keystrokes and mouse clicks to the target computer. Thus, it is important to evaluate if wireless connections are encrypted and how the dongle listens to and processes the received commands. Also, if sensitive information is handled it is recommended not to use wireless peripheral devices regardless of the manufacturers.

2. Wireless Peripheral Devices Security Threats

Wireless peripheral devices like mice and keyboards are affected by various classes of vulnerabilities. Some of them are described below (Niklas Tomsic, 2022):

2.1 Promiscuous mode nRF24L01+

The Nordic Semiconductor nRF24L01+ can be used to promiscuously sniff radio frequency packets transmitted between the wireless peripheral devices and the dongle connected to the computer. This attack does not require any specially crafted hardware. Also, this can be used to reverse engineer manufacturer proprietary protocols like Nike+ and study lower levels of ANT+ protocol.

In this exploit the sniffing of the radio packets is achieved by reducing the MAC address to 2 bytes by disabling checksums, setting the MAC address to the same as the preamble, and forcing the dongle to accept the noise as a valid MAC address (T. Goodspeed, 2011). The trick used here is to make a few illegal register settings, disable the checksum, and generate background noise that is consumed as a valid MAC address.

Once the MAC address is spoofed, the next step is to break the packet encryption. Usually, the packet header is in cleartext and only the payload is XOR encrypted using the MAC address. Just by applying XOR to the right regions, it is possible to decrypt the USB HID events and derive the key positions. Thus, this technique can be successfully used to sniff keystrokes and mouse clicks promiscuously.

2.2 NATO Tempest

TEMPEST is a United States National Security Agency specification and a North Atlantic Treaty Organization (NATO) certification. This specification refers to spying on information systems by listening to electrical or radio signals, vibrations, sounds, and other leaking emanations. TEMPEST does cover some methods that can be used to spy on wireless equipment like logging user keystrokes. It classifies the emitted signals as sensitive because if these signals are sniffed and analyzed, they may disclose all the data that is transmitted and processed by the wireless device. Along with covering details on how to spy on other information systems, it also defines ways to prevent/protect devices from such spying. The protection efforts are also known as emission security (EMSEC), which is a subset of communications security (COMSEC). Prevention of spying can be achieved by shielding, masking, monitoring, filtering, and defining the distance an attacker can get without being able to sniff the leaked signals. The standards defined go from level A to C, with level A being the strictest for critical devices that operate in NATO zone 0.

2.3 SATAn: Air-Gap Exfiltration Attack

Air-gapped systems usually do not have any public internet connection and are used in critical environments like industrial OT networks, government, military, nuclear plants, and other industrial networks. They are isolated from other less secure networks that have access to the internet. It was discovered that it is possible to exfiltrate data from air-gapped systems through Serial ATA (SATA) cables that are in the form of wireless antennae inside the computers.

To perform this attack, the hacker must first gain physical access to the air-gapped system and install the malware software. The software then prepares the sensitive data to be exfiltrated through modulation and encoding. The SATA cables can deliver over a radio channel between 5.9995 and 5.9996 GHz electromagnetic signals that correspond to specific characters (Mordechai Guri, 2022). Thus, this malware can be used to hijack legitimate processes on air-gapped systems and emit radio signals during specific read-and-write operations. In real real-world scenario, the receiver will be embedded in a piece of hardware equipment placed close to the air-gapped system or realized as a process in a computer

nearby. The best way to prevent such attacks is to use SATA jammers, which detect suspicious read and write operations initiated from legitimate software and distort that signal.

2.4 Far Field Electromagnetic Side-Channel Attack

It was proved that it is possible to break AES-128 encryption through electromagnetic side-channel attack. The attacker must be within a 15-meter radius to perform this attack. This was accomplished by using a deep neural network and a convolution neural network with an input size of 110 (R. Wang, H. Wang, and E. Dubrova, 2020). If sensitive information like the AES key can be retrieved from about 15 meters away just by sniffing the electromagnetic side-channel signals, it provides enough evidence that any information can be intercepted and stolen by being in proximity to an unaware victim.

2.5 Bastille Research

The Bastille Research team has conducted several research regarding wireless security threats. Some of their discoveries include rouge Wi-Fi hotspots, eavesdropping/surveillance devices, wireless camera exploits, home security systems, IoT device exploits, and rogue cell towers that can be used to hijack mobile phone connections to eavesdrop and listen to other's phone calls, read text messages, break 2-factor authentication and push malware to victim phones (Bastille Research Team, 2017). Also, they have discovered several exploits that affect wireless peripheral devices like mice and keyboards.

KeySniffer is an exploit that targets non-Bluetooth wireless devices that do not encrypt their radio communication. This allows hackers to intercept all keystrokes entered by the victim from several hundred feet away (Marc Newlin, 2016a). All personal information including usernames, passwords, credit card details, sensitive transactions, and all information can be intercepted and stolen. KeyJack is another exploit discovered by the Bastille Research team that allows malicious users to inject encrypted keystrokes into the vulnerable USB dongle without access to the encryption key (Marc Newlin, 2016b).

3. Mousejack Exploit Technical Details

Mousejack is a class of vulnerability that affects non-Bluetooth wireless peripheral devices like mice and keyboards connected through USB dongles. This section will cover in-depth technical details on how to sniff mouse clicks, keystrokes and inject maliciously crafted keystrokes to compromise a victim machine. An attacker can take complete control over the target computer without any physical access by launching this attack using a dongle which costs less than 15$.

Mousejack attack includes three methods that can be used to sniff transmitted radio traffic or to inject keystrokes to compromise the victim's device. The three methods include:

3.1 Injecting keystrokes as a spoofed mouse.

Most of the peripheral wireless device manufacturers only encrypt the connection between keyboards and dongles. They do not encrypt the connection between the mouse and the dongle as they only transmit mouse movement and right or left click signals. It is assumed that these signals are not sensitive. Due to a lack of encryption and authentication, the USB dongle directly accepts and processes data packets from any rouge-spoofed mouse.

Additionally, the USB dongle does not validate if the type of signal it received matches the type of the device that generated it. It blindly accepts keystroke signals even if it is generated from a mouse. This allows attackers to send out maliciously crafted keystroke signals from a spoofed mouse and remotely execute commands on victim machines.

3.2 Injecting keystrokes as a spoofed keyboard.

Most wireless device manufacturers encrypt the communication between the USB dongle and keyboards to prevent sniffing of keystrokes. However, a vulnerable dongle sometimes does accept unencrypted signals and successfully process them. This allows attackers to send malicious commands to the victim's laptop and take control of it.

3.3 Force pairing an illegitimate mouse or keyboard.

Earlier the keyboard and mouse were paired before they left the factory. It means the dongle wireless address and encryption key were hardcoded in the keyboard firmware and the decryption key was stored in the dongle firmware. But lately, manufacturers have provided features where users can pair wireless devices to new dongles or even pair multiple devices to a single dongle. Pairing can be done by physically enabling pairing mode for a few seconds using a button on the device. But sometimes it is possible to bypass this pairing process without any user interactions. For example, the user may be using only a mouse but paired with a vulnerable dongle that accepts keystrokes from rouge devices. This way an attacker can send malicious commands to the victim's laptop.

The nRF24L transceivers are used to transmit data packets between the wireless devices and the dongle connected to the laptop. To create a rouge peripheral device, a Crazyradio PA dongle is used. This is an amplified nRF24L-based USB dongle that is used to control Crazyfile open-source drones. By modifying the Crazyradio PA firmware and enabling pseudo-promiscuous mode it is possible to convert the dongle into a fuzzer. The USB dongle connected to the computer sends instructions to the operating system in the form of USB HID packets (Marc Newlin, 2016). These packets can be sniffed by enabling the usbmon kernel module on Linux. The Crazyradio PA fuzzer takes advantage of this by sending radio frequency signals to the victim's USB dongle and monitoring the generated USB HID packets. By analyzing the radio frequency signal and the HID events the packet format and behaviors are derived.

The first step to launch this attack is to purchase a CrazyRadio PA USB dongle and flash the dongle with the Bastille network's Mousejack firmware (Marc Newlin, 2016c). The next step is to install the Jackit toolkit (Marc Newlin, 2016d). This toolkit includes a set of ducky scripts that will be used to transmit a sequence of keystrokes to compromise the target computer. The attacker scans the surroundings by listening to the radio frequency signals transmitted by nearby wireless devices to find a vulnerable target. Once the target is identified the hacker force pairs the victim's dongle with the Crazyradio dongle. Then a ducky script payload is created and the jackit tool is executed to send out a sequence of unencrypted keystrokes to the vulnerable dongle. The dongle trusts the signals to be coming from legitimate wireless devices and processes them. Through this attack, a hacker can install rootkits, viruses, exfiltrate data and do everything possible if he has physical access to the victim's laptop.

Remediation - The nRF24L transceiver chip used in wireless peripheral devices like mouse, keyboard, and USB dongles includes either one-time programmable or flash memory. If one-time programmable

devices are found vulnerable, they must be discarded as their firmware cannot be updated once they leave the factory. Devices with flash memory can be fixed if updated firmware is available from the manufacturers. It is recommended to upgrade to the latest firmware before continuing to use the affected wireless devices.

4. Conclusion

The various exploits like Mousejack, KeyJack, and electromagnetic side-channel attacks prove that wireless products even from trusted manufacturers may be vulnerable to serious security exploits. Also, this shows how creative hackers can get to compromise computer networks. Before the pandemic, organizations had to only worry about physical security in company onsite locations. But now the threat landscape is changing as the workforce moves from traditional onsite spaces to home offices. Organizations must perform due diligence to make sure the peripheral devices that they have issued are not vulnerable to these exploits. The IT department must frequently check the list of affected devices published by researchers and take appropriate measures. If updated firmware is available from the manufacturers, it must be pushed to all the devices. All vulnerable devices with no firmware updates must be discarded. Organizations must maintain a thorough inventory of all devices used to keep track of vulnerable and end-of-life systems. It is important to create awareness among users about these exploits so that they can take simple measures like locking their laptops before stepping away from their desks or removing the USB dongle when not in use. This also helps them identify irregular unexpected behaviors in their workstations.

Reference:

Bastille Research Team (2017). Rogue Cell Towers. Bastille Wireless Threat Intelligence. Retrieved from https://www.bastille.net/vulnerabilities/rogue-cell-towers

Marc Newlin (2016). MouseJack Technical Details. Bastille Wireless Threat Intelligence. Retrieved from https://www.bastille.net/research/vulnerabilities/mousejack/technical-details

Marc Newlin (2016a). Keysniffer. GitHub - Bastille Wireless Threat Intelligence. Retrieved from https://github.com/BastilleResearch/keysniffer

Marc Newlin (2016b). Keyjack. GitHub - Bastille Wireless Threat Intelligence. Retrieved from https://github.com/BastilleResearch/keyjack

Marc Newlin (2016c). BastilleResearch/mousejack. Github. Retrieved from https://github.com/BastilleResearch/mousejack

Marc Newlin (2016d). BastilleResearch/nrf-research-firmware. Github. Retrieved from https://github.com/BastilleResearch/nrf-research-firmware

Mordechai Guri (2022). SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables. Retrieved from https://browse.arxiv.org/pdf/2207.07413.pdf

Niklas Tomsic (2022). Penetration testing wireless keyboards. KTH Royal Institute of Technology. Retrieved from https://kth.diva-portal.org/smash/get/diva2:1701492/FULLTEXT01.pdf

R. Wang, H. Wang, and E. Dubrova, (2020). Far-field em side-channel attack on aes using deep learning. Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security. Retrieved from https://dl.acm.org/doi/abs/10.1145/3411504.3421214?sid=SCITRUS

T. Goodspeed (2011). Promiscuity is the nRF24L01+'s Duty. Retrieved from http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html

About the Authors

Prathibha Muraleedhara, Cybersecurity Leader

Prathibha Muraleedhara is a Security Architecture Manager for a leading product manufacturing company. She holds a master's degree in Information System Security and 10+ years of professional experience in Security Architecture, Cloud Security, and Penetration Testing. She is a committee member of the Women in Security -Information Systems Security Association specialty group, ISACA SheLeadsTech Ambassador, and Cyber Wyoming member of the Board of Directors. She is a passionate researcher, and author, and enjoys educating people on security exploits and remediation.

Contact details: prathibha.muraleedhara@gmail.com, LinkedIn: https://www.linkedin.com/in/prathibha-muraleedhara-8a3976105/

Akhilesh Bhangepatil, Cybersecurity Leader

Akhilesh Bhangepatil is a highly accomplished cybersecurity professional with a Master of Science in Cybersecurity and a comprehensive set of cybersecurity certifications, including CISSP, CISA, GICSP, GCIP, and GRID. He has established himself as a recognized expert in the field of cybersecurity and a distinguished Cybersecurity Leader who specializes in Cyber-Physical Systems (CPS). Akhilesh is also renowned as a distinguished speaker in the realm of cybersecurity.

Contact details: bhangepatil.akhilesh@gmail.com, LinkedIn: https://www.linkedin.com/in/bakhilesh/


EVENTS

JOIN US ON **FEB 27, 2024**

www.theiecna.com

2ND EDITION
INFLUENCE EXCHANGE
CONFEX & AWARDS
IN SAUDI ARABIA

Connecting Marketeers, Influencers & Ideas

EVENT MEDIA PARTNERS

ORGANIZED BY





Join us *for for a one-of-a-kind event that will revolutionize the way influencers and marketers connect and collaborate. Following the success of* ***Influence Exchange Confex and Awards in Dubai****, we're thrilled to bring it to* ***Saudi on Feb 27****. With over 100 Marketeers and 100 Influencers, this unique platform promises exceptional networking, knowledge sharing, and business partnerships. Engage with industry leaders, benefit from keynote speeches, panel discussions, and workshops. Discover the future of influencer marketing and martech. Don't miss the opportunity. Visit our website www.theiecna.com for details.*

Be part of the future of influencer marketing!

UNLOCK OPPORTUNITIES AND INSIGHTS!

MOHAMED SUHEL: E: mohamed.suhel@7awi.com | M: +971 565873505 | F: +971 4 5665795

BAPCO

The Annual Event

RESERVE A FREE PASS

6-7 MARCH 2024

COVENTRY BUILDING SOCIETY ARENA

THE UK'S LEADING PUBLIC SAFETY EVENT

80+ public safety technology companies

Gain valuable insights from

world-class speakers

3 captivating theatres

NEW product launches

BAPCO-SHOW.CO.UK

@BAPCOEvent BAPCO Annual Event

DGI GEOSPATIAL INTELLIGENCE FOR DEFENCE AND SECURITY

20TH ANNIVERSARY

THE WORLD'S LEADING GEOSPATIAL INTELLIGENCE EVENT

USE CODE: CDM10 FOR 10% OFF

Focus Day. 11 March, 2024
Main Event. 12 - 13 March, 2024
The QEII Centre, London

800+ Geospatial Intelligence Professionals to Network With

100+ Geospatial Intelligence Experts Sharing Their Practical Insights

50+ Nations Represented from Around the World

15+ Hours of Invaluable Networking Time

3 DAYS of Insightful Content

HOSTED BY
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER
مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY
وزارة الداخلية
MINISTRY OF INTERIOR
شرطة دبي
DUBAI POLICE
TDRA
هيئة تنظيم الاتصالات والحكومة الرقمية
TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

ORGANISED BY
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

YOUR CONTRIBUTION TO THE TECHNICAL PROGRAMME

DUBAI
ITS World Congress
16 -20 September 2024
Mobility Driven by ITS

The submission portal stays open until 15 January 2024.

ITS World Congress | 16-20 September 2024 | Dubai World Trade Centre

The response to our call for contributions has been nothing short of inspiring. Thank you for your ongoing enthusiasm and dedication to making the Congress a resounding success.

More info: itscongress.com/technical-programme

ORGANISED BY ERTICO ITS EUROPE

CO-ORGANISED BY ITS AMERICA, ITS ASIA-PACIFIC

HOSTED BY RTA

SUPPORTED BY DUBAI, DXB, BestCities GLOBAL ALLIANCE

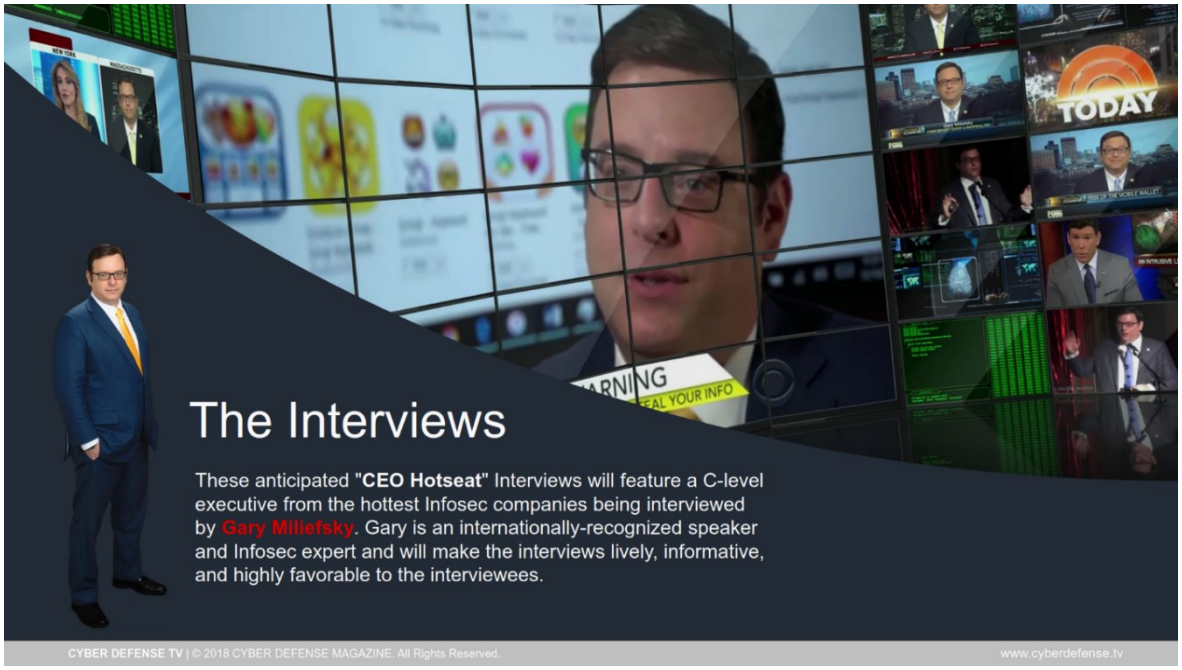
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

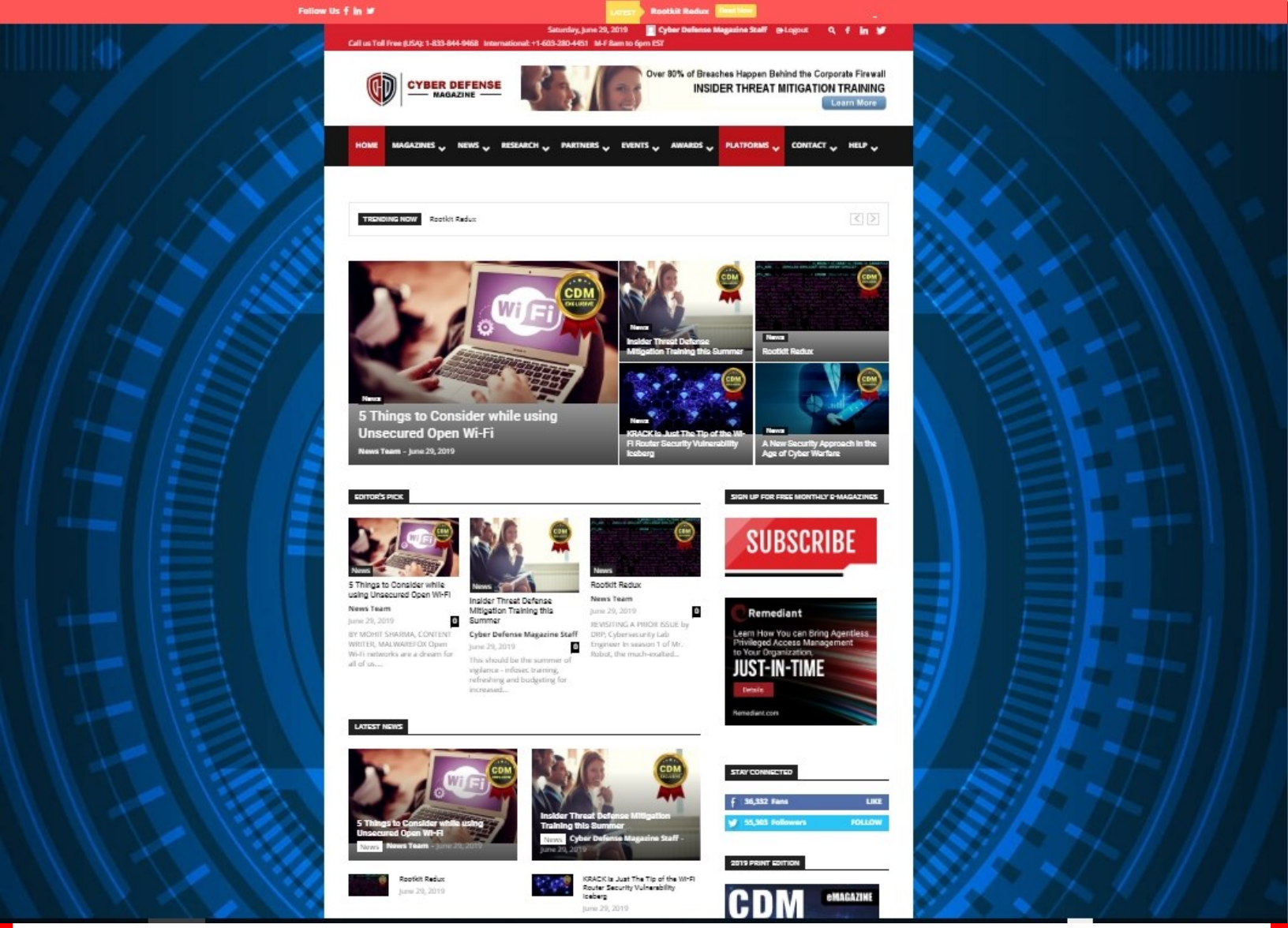
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 01/03/2024



Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

12 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 https://cyberdefenseconferences.com/ and our new platform https://cyberdefensewire.com/

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

LEARNING. NETWORKING. INNOVATION.

THE TRIPLE THREAT FOR CYBERSECURITY SUCCESS.

RSA Conference 2024 will bring the cybersecurity community together again in San Francisco for four industry-shaping days, and you can be a part of that important conversation.

From May 6 – 9, you'll be able to:

- See what the future holds with the hottest industry topics and emerging trends
- Expand your knowledge and be inspired by forward-thinking Keynotes
- Demo the latest products to find real-world solutions from over 600 companies
- Enhance your career through valuable networking opportunities

Let's redefine The Art of Possible by shaping solutions, tackling challenges, and encouraging the collective strength of coming together as a community.

Act now for the biggest discount!

Visit www.rsaconference.com/cyberdefense24 to learn more and register.

#RSAC

FOLLOW US

THE ART OF POSSIBLE

*** with help from writers and friends all over the Globe.**