CYBER DEFENSE MAGAZINE

eMAGAZINE

JUNE 2023

In This Edition

A Look into The Future: My Journey at the 2023 RSA Conference And The Exciting, Yet Troubling Path Of Cybersecurity Innovation

Why Inadequate Investment in Cybersecurity is a False Economy

The Power of AI In Today's Rapidly Evolving Financial Crime Landscape

...and much more...

MORE INSIDE!

CONTENTS

Welcome to CDM's June 2023 Issue ---------- *8*

A Look into The Future: My Journey at the 2023 RSA Conference And The Exciting, Yet Troubling Path Of Cybersecurity Innovation ---------- *33*

By Kylie M. Amison, Technical Reporter, Cyber Defense Magazine

Why Inadequate Investment in Cybersecurity is a False Economy ---------- *41*

By Luke Dash, CEO, ISMS.online

The Power of AI In Today's Rapidly Evolving Financial Crime Landscape ---------- *44*

By Pedro Barata, Chief Product Officer, Feedzai

7 Benefits of Implementing ZTNA ---------- *47*

By Howie Robleza, Freelance Writer, Avigilon

Biometric as a Service (BaaS) – An Opinion Piece ---------- *51*

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

Bad Hygiene: New Study Uncovers Common Security Failures of Cloud-First Organizations ---------- *55*

By Ruoting Sun, Vice President of Products, Secureframe

HEAT Attacks Vs Apts – What Is the Difference? ---------- *59*

By Mark Guntrip, Senior Director of Cybersecurity Strategy, Menlo Security

Why Cybersecurity Provision is Critical for Businesses, Large and Small ---------- *62*

By Astrid Gobardhan, Group Data Protection Officer at VFS Global, the world's largest outsourcing and technology services specialist

One Defense Against Data Breaches: Don't Have the Data to Begin With ---------- *65*

By Raj Ananthanpillai

Heard At RSAC 2023 - Protecting the Protectors ---------- *68*

By Chris Needs, VP of Product Management, Hyas Infosec

Changing the Status Quo of Cloud Security ---------- *71*

By Rodman Ramezanian, Global Cloud Threat Lead, Skyhigh Security

How the SEC's Proposed Security Rules Could Impact Businesses ---------- *74*

By Portia Cole, Emergent Threat Researcher, Avertium

Controlling Cybersecurity Risks ---------- *78*

By Hakan Kantas, Senior IT Director

What Will Cybersecurity Jobs Look Like in 2028? ---------- *84*

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

Don't Jump to Conclusions on Zero Trust Adoption ---------- *88*

By John Linford, Forum Director, The Open Group Security Forum and Open Trusted Technology Forum

Embedding Privacy-First Behaviors for Future Generations ---------- *91*

By Michael Levit, co-founder and CEO of Tempest

Ensuring Trust in Military Network Automation: Addressing Layer 8 Issues for Improved Operations and Security ---------- *94*

By Marc Packler, President, CISO Advisory, Silent Quadrant and Tony Thomas, President & Chairman, Tony Thomas & Associates LLC

Five Tips to Securing Your Organization Through Your People. ---------- *98*

By Dr. Inka Karppinen, CPsychol. Lead Behavioural Scientist, CybSafe

From Passwords to Passkeys – A Passing of the Torch ---------- *103*

By Tal Zamir, CTO of Perception Point

From Samsung to the Pentagon - Recent Stories Remind Us About the Importance of Sensitive Data Guardrails ---------- *106*

ByThomas Segura, Cyber Security Expert, GitGuardian

How We Grew Revenue by Strengthening Cybersecurity ---------- *111*

By David Weisong, CIO at Energy Solutions

Hybrid Mesh Firewall Management ---------- *114*

By Ulrica de Fort-Menares, VP of Product & Strategy, Indeni

Implement Machine Learning to Secure Your IoT Network ---------- *118*

By Zac Amos, Features Editor, ReHack

Measuring the Effectivity of Security with Data Analysis ---------- *122*

By Howie Robleza, Freelance Writer, Avigilon

Network Architecture Mapping Improves Security Posture and Saves Big Bucks ---------- *125*

By Matt Honea, Head of Security and Compliance, Forward Networks

OT Under Greater Scrutiny in Global Cybersecurity Regulatory Environment ---------- *129*

By Dr. Terence Liu, CEO, TXOne Networks

Out from the Shadows: SOC Teams Take Their Seat with the "Superheroes" ---------- *133*

By Karthik Kannan, Founder/CEO, Anvilogic

Penetration Testing- Shielding the Web Content Against Hacking ---------- *136*

By Aashi Mishra, Sr. Content Writer, Research Nester

Protecting Sensitive Information Within Translation ---------- *144*

By Ofer Tirosh, CEO of Tomedes

Our Risk Perception Is Broken How Do We Fix It? ---------- *148*

By Miguel Clarke, GRC and Cybersecurity Lead at Armor and former FBI Special Agent

SaaS Application Security: Why It Matters and How to Get It Right ---------- *151*

By Babar Khan Akhunzada, Founder, SecurityWall

A Cloud Security Conundrum: Protecting Your Company from Third-Party Software Supply Chain Gaps ---------- *154*

By Vrinda Khurjekar, Senior Director, AMER business, Searce

The Billion Dollar Problem: Securing Business Communication in the Financial Sector ---------- *158*

By Anurag Lal, President and CEO of NetSfere

The Industrial Control Systems and The Internet of Things ---------- *161*

By Milica D. Djekic

The Other Russian War – What Can We Do? ---------- *166*

By Jamie Eiseman, George Washington University

The Shodan as The Scariest Search Engine of Today ---------- *169*

By Milica D. Djekic

The Intersection of OT and IT: Why Unified Cybersecurity is More Important than Ever. ---------- *174*

By Craig Burland, CISO, Inversion6

Using Data Analysis to Identify Security Threats: An Overview ---------- *177*

By Howie Robleza, Freelance Writer, Avigilon

Why CISOs Should Prioritize Cloud Security and Access Management During Digital Transformation Initiatives ---------- *183*

By Ameya Khankar, Cybersecurity Consultant for Critical Infrastructure

Why Cybersecurity for Private Equity Is Urgent Now – And What Funds Can Do to Move the Needle. ---------- *188*

By John Hauser, EY Americas Transaction Support – Cyber Due-Diligence Leader, Ernst & Young LLP

Zero Trust Security: Pioneering Solutions on a 'Never Trust, Always Verify' Principle to Overcome Modern Cyberspace Security Challenges! ---------- *191*

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

@MILIEFSKY

From the

Publisher…

Dear Friends,

Between Cyber Defense Magazine and the wide array of services under Cyber Defense Media Group, we are experiencing the pervasiveness of cyber-related impacts on both modalities and professions. No longer limited to an arcane discipline for technical professionals, we now reach a broader set of contributors and readers.

Some of today's concerns are reflected in current initiatives in privacy and consumer protections, financial and identity fraud implications, and the challenges we face in the rapid expansion of artificial intelligence applications.

It is no surprise that we see a race between developers and regulators, private sector and government functions, and the hopes and fears of our society in understanding how these rapid developments will benefit or harm all of us.

As publisher, it's important to be mindful of the mission and contribution we have undertaken, to provide the most professional and up-to-date forum for keeping our readers informed of challenges and responses in today's cyber world. In so doing, we are pleased to count on articles that identify both threats and solutions, for the benefit of our industry and society.

With the support of our contributors and readers, we continue to pursue our role as the premier publication in cybersecurity.

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/

11 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 VENTURES WEBINARS

CYBERDEFENSECONFERENCES

Welcome to CDM's June 2023 Issue

From the Editor-in-Chief

As we near the halfway point of the calendar year, from the Editor's desk it appears that events continue to accelerate. With more developments occurring in less time, the challenges for cybersecurity continue to mount. Of course, we see this reflected in the focus of the articles we receive and publish.

It's no surprise that Artificial Intelligence (AI) has become an area of particular interest and concern. From worries about job replacement to privacy to weaponization and politicization of this rapidly-developing phenomenon, both our readers and contributors face daily challenges to relate to and digest the potential implications of AI.

Even so, the march of cyber threats and responses continues unabated in the world of cybersecurity professionals. While we must address the future of AI, there is no room for anyone to become complacent in assuring that all the everyday measures are completed to prevent cyber breaches.

Accordingly, we commend our readers to take the time to review this month's offerings of ways to address both old and new threats against your cyber systems, and to benefit from the expertise and experience of our authors.

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

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the 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™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

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

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

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

- See what the future holds in expert-led Track Sessions covering the hottest 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.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

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/

STOP BEING REACTIVE. START BEING PROACTIVE.

Get the Zero Trust endpoint security solution that offers a unified approach to protecting your business, users, networks, and devices against the exploitation of zero-day vulnerabilities.

Visit our website, or speak to a Cyber Hero to learn more about how the ThreatLocker® solution can help you better protect your business.

THREATLOCKER

threatlocker.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

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

2001 2023

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

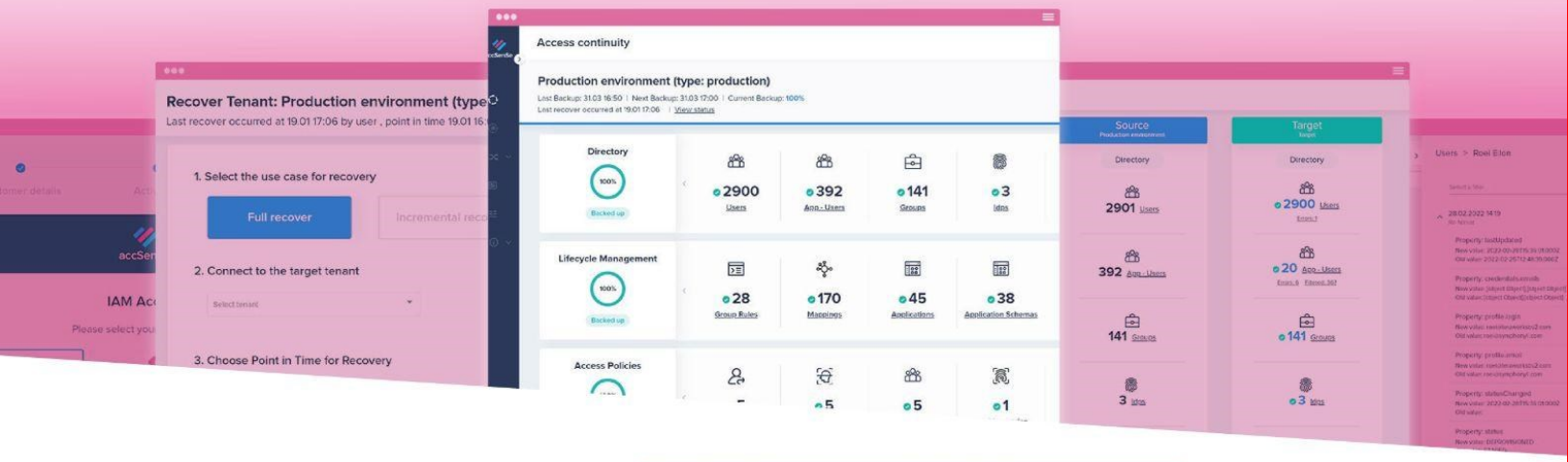
SkyHive | cyberGRX | DRAGOS | CONCEAL | varmour

ALLEGISCYBER CAPITAL

www.allegiscyber.com

accSenSe

A complete protection and recovery solution for your organization's most critical SaaS.
(Your IAM WF and CIAM)



The Road To Quick And Easy Recovery Starts With accSenSe and Okta

- Complete protection for your Okta tenant, which gives you full visibility to configuration and data history.
- The ability to recover means you can reduce RTO during a disaster, keeping your business running and financial loss to a minimum.
- Stay compliant with SOC2 & SOX. The audit capabilities mean you can easily control system changes.

With accSenSe you can rest secure knowing your Cloud Identity and Access Management system is fully protected and recoverable, no matter what tomorrow brings.

monday.com GLASSBOX bright data fiverr.

After running through endless Cloud Identity Access Management system implementation use-cases and disasters, the accSenSe team decided to solve the most significant problem of modern organizations relying on SaaS solutions.

We developed a platform to manage and protect cloud Identity and Access Management system to ensure business as usual isn't just a phrase.

START A 30-day TRIAL >>

https://accsense.io

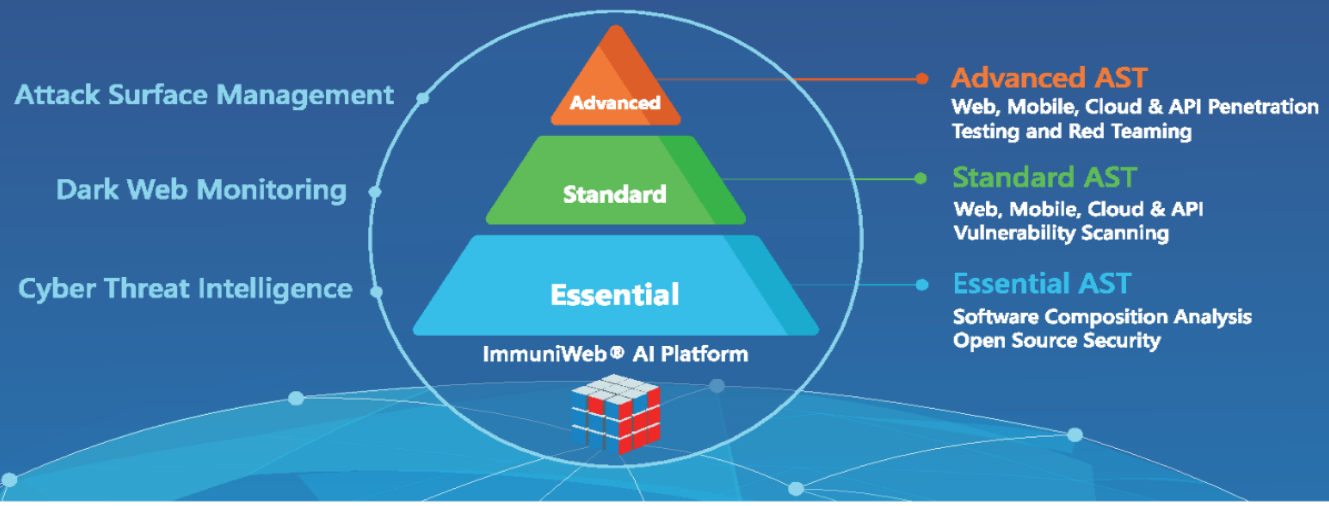

DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
quickcode
DRAGOS
ENVEIL
INERTIALSENSE
PREVAILION
the cyberwire
Ntrinsec
SIXMAP
STRIDER
CONTRAFORCE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

ImmuniWeb®

AI for Application Security

We Simplify, Accelerate, and Reduce Costs of Application Penetration Testing, Protection, and Compliance

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



ImmuniWeb® Discovery

ImmuniWeb® Discovery leverages OSINT and our award-winning AI technology to illuminate attack surface and Dark Web exposure of a company. The non-intrusive and production-safe discovery is a perfect fit both for continuous self-assessment and vendor risk scoring to prevent supply chain attacks.

ImmuniWeb® Neuron

ImmuniWeb® Neuron unleashes the power of Machine Learning and AI to take traditional web vulnerability scanning to the next level. While detecting more vulnerabilities compared to automated web scanners, every web vulnerability scan by Neuron is equipped with a contractual zero false positives SLA.

ImmuniWeb® On-Demand

ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology to accelerate and enhance web penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® MobileSuite

ImmuniWeb® MobileSuite leverages our award-winning Machine Learning technology to accelerate and enhance mobile penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® Continuous

ImmuniWeb® Continuous monitors your web applications and APIs for new code or modifications. Every change is rapidly tested, verified and dispatched to your team with a zero false positives SLA. Unlimited 24/7 access to our security analysts for customizable and threat-aware pentesting is included into every project.

One Platform. All Needs.
www.immuniweb.com

Email: sales@immuniweb.com
Phone:+41 22 560 6800

SCawards Europe Winner — Best Usage of Machine Learning and AI

AI FINTECH 100

Gartner peer insights
4.8 out of 5


HORNETSECURITY
ALL-INCLUSIVE
SECURITY
FOR MICROSOFT
365
SPAM FILTER & ADVANCED EMAIL SECURITY
SIGNATURE & DISCLAIMER
TOTAL PROTECTION
ENTERPRISE BACKUP
EMAIL ARCHIVING, ENCRYPTION & CONTINUITY
BACKUP & RECOVERY
FROM EMAIL SECURITY
TO BACKUP & RECOVERY
ALL IN ONE SOLUTION!
START YOUR FREE
30-DAY-TRIAL
WWW.HORNETSECURITY.COM

Gain control of your Attack Surface with a Cybersecurity Co-pilot

Headless

We embed directly to your platform, any SIEM, or ticketing Solution.

Agentless

Easy to onboard all known and unknown client assets.

Auto-Remediate

Triggers to protect unknown assets for management.

Get started with a demo at lucidum.io/request-demo

LUCIDUM
ATTACK SURFACE MANAGEMENT

CYBLE

Is Your Organization Protected Against External Threats?

GENERATE YOUR ORGANIZATION'S EXTERNAL THREAT PROFILE REPORT AND OBTAIN

01 Overview of vulnerabilities in your digital risk footprint

02 Risk assessment of your attack surface and threat landscape

03 Unique Risk Score as per your darkweb exposure

04 Critical information about your leaked data and security posture

SCAN ME

TO GET THE REPORT!

Phylum

The Software Supply Chain Security Company

Stop Software Supply Chain Risk at the Source

Automate software supply chain security to block new risks, prioritize existing issues and only use open-source code that you trust.

Protect the Organization

- Proactive OSS Risk Management
- Policy Standardization & Enforcement
- Improved Signal : Noise
- Modern Attack Prevention

Secure Innovation

- Developer-First Approach to Security
- Reduced Organizational Friction
- Accelerated Release Cycles
- Uninterrupted Developer Workflows

YOUR WEBSITE LOOKS GREAT!

BUT WHAT'S HAPPENING BEHIND THE SCENES?

reflectiz

Reflectiz maps all 1st, 3rd and 4th party risks, including compliance violations, web skimming attempts, and external domain threats.

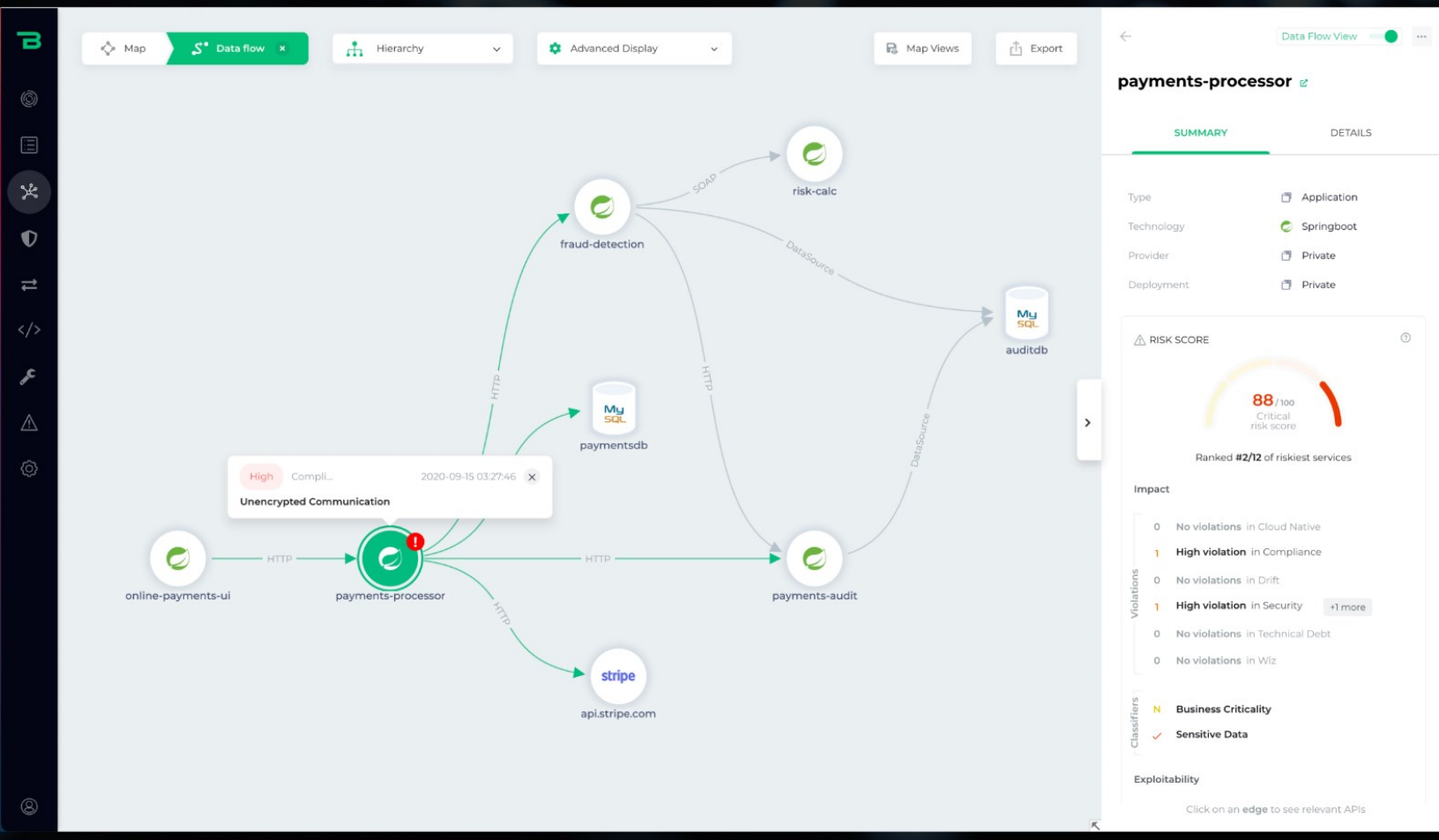
Get in touch for a quick PCI assessment.
www.reflectiz.com

BIONIC

ASPM

Application Security Posture Management

Make applications secure and resilient to significantly reduce business risk.



Start reducing business risk of apps today

www.bionic.ai

Phosphorus

Secure the Enterprise xIoT Attack Surface

FIND, FIX, and MONITOR every IoT, OT, and Network device.

See how Phosphorus can bring enterprise xIoT security to every cyber-physical Thing in your enterprise

xIoT Attack Surface Management + **xIoT Hardening & Remediation** + **xIoT Detection & Response**

Across all xIoT devices

- Enterprise IoT Devices
- Operational Technology Devices
- Smart Buildings & Cities
- Network & Cloud Connected Devices
- Industrial Internet of Things
- Internet of Healthcare Things
- Smart Ships
- Internet of Battlefield Things

Automated bot protection with 24/7 adult supervision.

From the **Top Infosec Innovator Award** winner.

TOP INFOSEC INNOVATOR
CYBER DEFENSE MAGAZINE
2022

DATADOME

datadome.co

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook

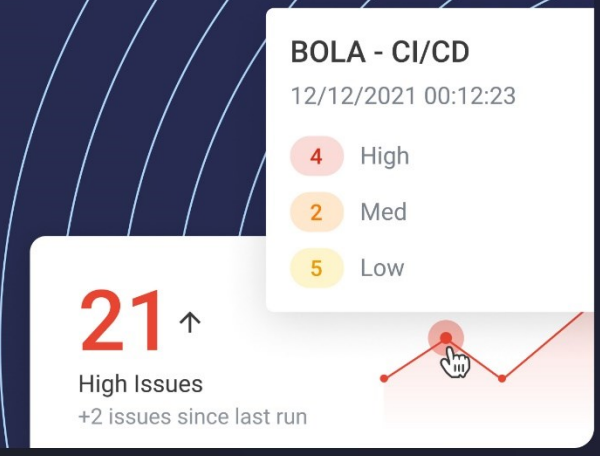
noname

The Complete, Proactive API Security Platform

nonamesecurity.com >

Shift Left with **API Security Testing**

Industry-leading posture managment, runtime security and API security testing




ARTICLES

A Look into The Future: My Journey at the 2023 RSA Conference and The Exciting, Yet Troubling Path of Cybersecurity Innovation

Exploring the Future of Cybersecurity at the 2023 RSA Conference

By Kylie M. Amison, Technical Reporter, Cyber Defense Magazine

As the recipient of Cyber Defense Magazine's 2023 Young Women in Cyber Award, I was granted the incredible opportunity to not only attend the 2023 RSA conference but was also able to interview dozens of C-level officers of both emerging and established tech companies. This allowed me the chance to witness firsthand the passion and innovation driving the industry forward. The innovating solutions covered were diverse, ranging from collective defense against undetected malware to the latest enterprise IoT security platform capable of remediating and repatriating any and all IoT devices.

In the following trip report, I will discuss five different companies and reflect on the details of the discussions had with each, adding some insightful key takeaways.

“The Future of AI in Cybersecurity” with Wib Security, Interview and Discussion featuring CTO Chuck Herrin

In light of the growing security threats in today’s landscape, companies’ focus on forward thinking solutions is particularly relevant and necessary. One of the most significant topics discussed throughout all of my conducted interviews and attended presentations was the future of AI in cybersecurity, with many industry experts expressing optimism about its potential to strengthen defense strategies. Although it was acknowledged that attackers currently hold the upper hand and are most definitely leveraging generative AI/ML to carry out swift and wide-ranging social engineering attacks, some CISOs voiced concerns that organizations may be adopting new technologies and approaches before fully understanding them, indicating a need for caution and thorough testing to ensure efficacy and avoid unintended consequences.

Chuck Herrin, the CTO at Wib Security, an API security company that serves as a one-stop-shop for all things API security, emphasized the importance of distinguishing between tasks that require human intervention and those that cannot be automated, reflecting the need for organizations to proceed with caution when utilizing AI in cybersecurity. “There’s a difference in my head between automating a repeatable process, and [executing] creative automation, and what we’re crossing the Rubicon now into creative automation, with most users not really understanding it, and the channel that we’re doing it is via APIs” [1].

AI is especially prevalent when discussing APIs—API traffic accounts for 91% of traffic in an organization, and most AI is delivered through these APIs [1]. Pair this with the fact that most defenders are only aware of about half of their APIs in use, and you’re left with an incomplete threat model. This obviously raises a huge challenge with actually understanding and assigning risk values to what’s happening across these interfaces and within the backend systems and data they expose. With deep expertise in the intricacies of API security, Wib Security has developed the Fusion Platform (see Figure 1) as a comprehensive solution for identifying, assessing, and mitigating API risks. Fusion platform employs advanced scanning techniques to thoroughly analyze API endpoints and detect vulnerabilities such as injection attacks, broken authentication, insecure data transmission and inadequate access controls.

As Chuck put it, most of cybersecurity is just doing the basics really well. Unfortunately, these basics have been and will be overlooked or neglected in favor of more advanced and flashy security measures. This proves to be concerning as its clear that we don’t yet fully understand the old attack surface, never mind the new one that will evolve at a rapid pace with the favoring adoption of AI. This seems to be a reoccurring theme, adoption before security. Unfortunately, it’s just what humans do.

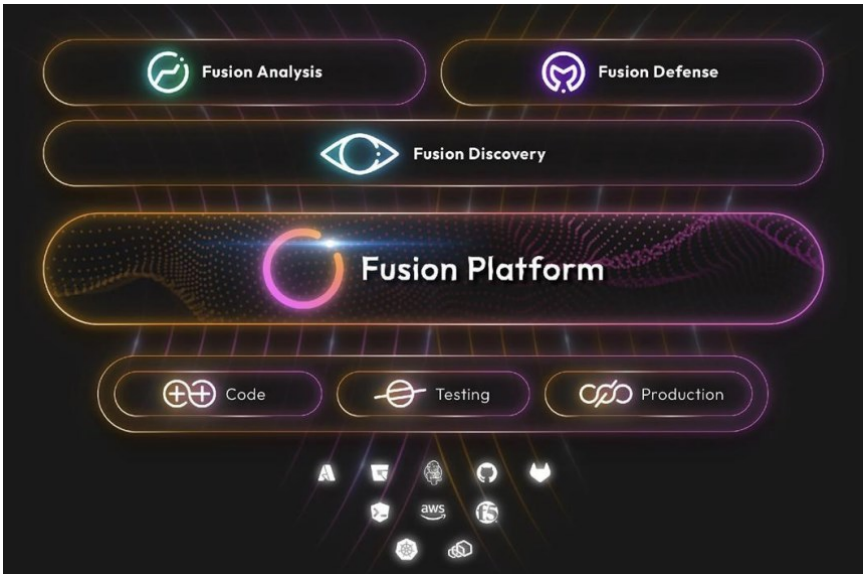


Figure 1: Wib Security's Fusion Platform

"Owning the Unknown" with Unknown Cyber, Interview and Discussion featuring CEO James Hess

Among the notable technologies I came across, an exciting one was with Unknown Cyber, a company that conducts automated deep static analysis of code and reverse engineering workflows to identify new viruses and malware that are often missed by antivirus and sandbox solutions, thereby achieving scale without compromising accuracy or time. The proprietary technology discussed is the result of over a decade of research funded by U.S. Department of Defense and independently evaluated by MIT. Cythereal MAGIC™, utilized by McAfee as part of their services, is a web-based platform that specializes in malware genomic correlation, which is a fascinating topic in and of itself.

Think of malware genomic correlation as an exploration into the genetic characteristics of malicious software, revealing hidden connections and patterns among different malware samples. Similar to how biological genomic analysis compares DNA sequences to identify relationships between organisms, malware genomic correlation compares the assembly instruction level code of malware samples to uncover similarities and potential relationships.

Unknown Cyber's proprietary Cythereal MAGIC™ leverages this paradigm, employing it to conduct semantic similarity analysis of programs. By focusing on the semantics of the program, rather than the structural or behavioral characteristics, MAGIC™ is able to provide quite insightful results. The system can identify similarities between submitted samples, detect variants of those samples from its database, and then generate YARA rules for searching other services such as VirusTotal [2]. Compared to its market competition, MAGIC offers improved effectiveness, particularly in identifying targeted attacks involving polymorphic variants.

The Unknown Cyber mission of "Owning the Unknown," resonates deeply with a prominent quote from former United States Secretary of Defense, Donald Rumsfeld, who said, "Reports that say that something

hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. [But] there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other countries, it is the latter category that tends to be the difficult ones" [3]. Unknown Cyber's mission of embracing the concept of unforeseen risks by identifying new viruses and malware exemplifies the commitment to innovation and pushing the boundaries of cybersecurity.

"Ransomware Resurgence: Emerging Trends, Threat Actors, and Cybersecurity Strategies" with Black Kite, Discussion and Research Report Synopsis featuring Head of Research Ferhat Dikbiyik

The rapid and innovative trajectory of cyber security technology is mirrored by the adversaries and their arsenal of tools, including the ever-evolving landscape of ransomware. Ransomware groups have emerged as formidable adversaries causing widespread financial and operational disruptions. After speaking with Ferhat Dikbiyik, Head of Research at Black Kite, and reading his research report on the 2023 Ransomware Threat Landscape, I was able to gain valuable insights into the latest trends in ransomware attacks. The report analyzes publicly named ransomware victims and identifies key trends and statistics, shedding light on the resurgence of ransomware attacks and the challenges faced by organizations globally.

The report finds that ransomware attacks have resurged in 2023 with the number of victims nearly doubling from last year. After an analyzation of 2,708 ransomware victims, the report found that the top targeted industries were manufacturing (19.5%), followed by professional, scientific and technical services (15.3%), and educational services (6.1%). Geographically, the United States was the top targeted country, accounting for 43% of victim organizations. The report also found that new ransomware gangs have emerged in 2023, including names like Royal, BianLian, and Play.

In addition, the report highlighted the rise of encryption-less ransomware, which emphasizes the importance of data protection, regulatory compliance, and business interruption risks posed by traditional encryption-based attacks. It also sheds light on the targeting of companies with annual revenues of approximately $50M to $60M, with third-party vendors often being exploited for client information extortion. The Ransomware Susceptibility Index™ (RSI™) introduced in the report, provides a measure of an organization's vulnerability to ransomware attacks. Over 70% of ransomware victims analyzed had an RSI™ value above the high-risk threshold, indicating their susceptibility. The identified common indicator among victims includes poor email configuration, recent credential leaks, public remote access ports, out-of-date systems, and IP addresses associated with botnet activity [4].

The dynamic and unpredictable nature of cyber threats, particularly ransomware attacks, poses a constant challenge for organizations worldwide. Ransomware groups have evolved into tech like entities, adopting strategies to maximize their illicit businesses. This poses a challenging and uneven playing field for cybersecurity professionals defending against ransomware attacks.

By understanding the complexities of the ransomware landscape in 2023, recognizing patterns, and acknowledging the challenges, organizations can make informed decisions about cybersecurity strategies and reduce their vulnerabilities. Both his research report and the discussion I had with Ferhat

provide valuable insight into the evolving ransomware landscape and is useful in equipping security professionals with the crucial data needed to combat these rapidly growing and resourceful adversaries.

I think it's important to remember that the evolution of technology is a double-edged sword. While it fuels innovation and unlocks new business prospects, it also amplifies the vulnerability of organizations. As the threat of ransomware continues to evolve, organizations must adapt their cyber security strategies, invest in the right defenses, and remain vigilant to mitigate the risks posed by these malicious attacks.

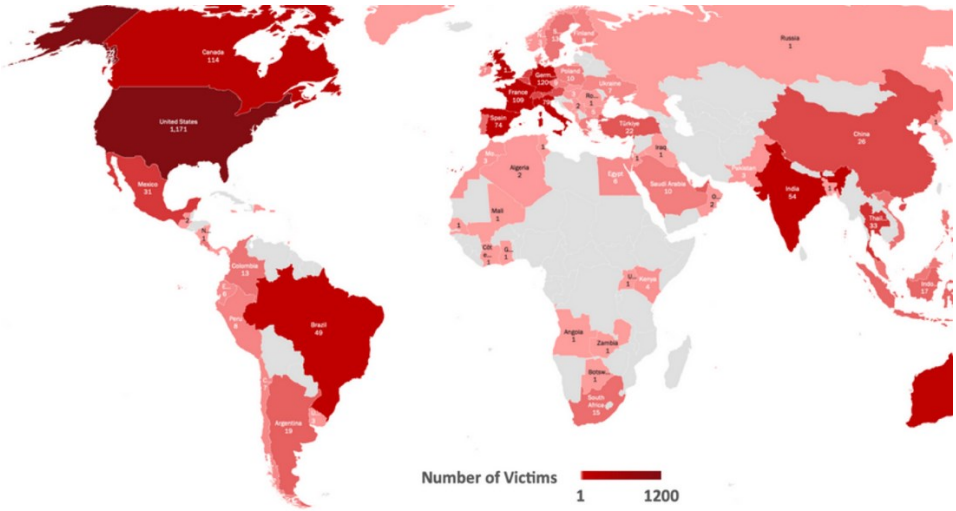


Figure 2: Ransomware Attacks Across the Globe

"Powering Proactive Security with Automated Verification and Monitoring to Keep Your IoT Devices Secure" with ViaKoo, Interview and Discussion featuring CEO Bud Broomhead

As just previously discussed above, cyber threats are evolving at an alarming rate. Organizations require cutting-edge solutions to stay ahead of their adversaries and safeguard their valuable assets. I had the opportunity to sit down with Bud Broomhead, CEO of ViaKoo, a leading cybersecurity company that has emerged as a trailblazer in this realm, offering innovative services that provide comprehensive protection against these emerging threats. The proliferation of IoT devices has revolutionized various sectors, offering enhanced efficiency and convenience. However, the widespread utilization of IoT devices has also, of course, introduced new cybersecurity challenges. ViaKoo has positioned itself as an innovator in addressing these challenges by offering services focused on IoT device remediation and repatriation.

The number of IoT devices deployed in our daily lives is staggering. In fact, during our interview, the ViaKoo team and I pointed out at least ten different IoT devices in the small hotel conference room we were in. From smart home devices and industrial sensors to thermostats and physical cameras, IoT devices have permeated various industries, streamlining operations and enhancing user experience.

However, the sheer volume and diversity of IoT devices present significant security risks as they become entry points for attackers. ViaKoo recognizes this inherent vulnerability and has developed pioneering solutions to remediate and repatriate IoT devices effectively. At the core of Viakoo's offerings is their

automated verification platform (Figure 3), Viakoo Action Platform™, a solution that defends IoT attack surfaces and ensures every enterprise IoT device is 100% visible, operational, and secure.

This technology actively monitors the health and functionality of IoT devices ensuring they operate as intended. Viakoo's platform incorporates proactive monitoring capabilities as it continuously collects real-time data on performance metrics and network connectivity. In addition to monitoring, they also offer issue detection and alert features for each respective IoT device in efforts to facilitate timely remediation actions.

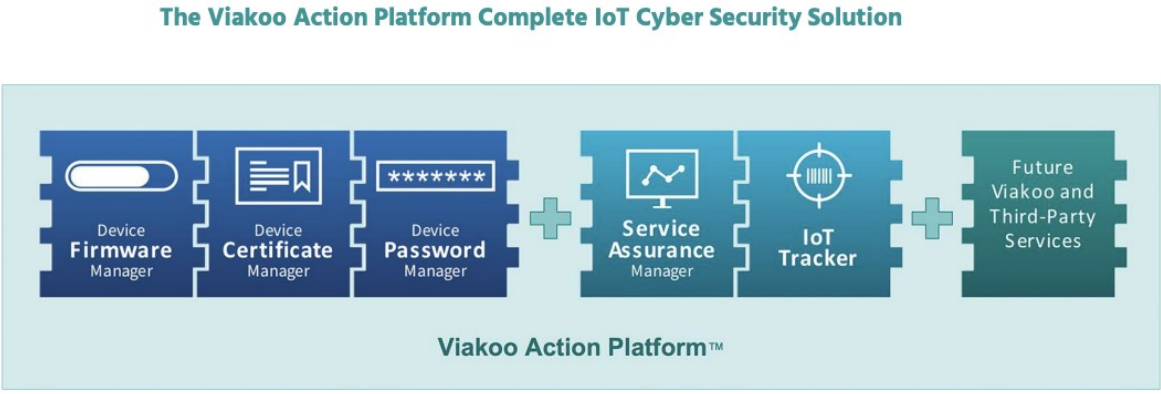


Figure 3: Viakoo Action Platform™

ViaKoo's innovative approach extends beyond remediation and repatriation, encompassing comprehensive IoT device management. They provide organizations with a centralized platform to monitor, control, and secure their IoT device ecosystems. Through the centralized management system, organizations gain enhanced visibility into their IoT infrastructure, allowing them to detect anomalies, apply security patches, and enforce access controls effectively. Securing IoT devices is paramount as they play an obvious role in critical operations across industries. In our ever increasingly interconnected world, where IoT devices are becoming pervasive, ensuring robust security measures is imperative in safeguarding assets and protecting privacy.

"Innovative Email Security Solutions" with Cofense, Interview and Discussion featuring VP CISO Tonia Dudley and Principal Threat Advisor Ronnie Tokazowski

In an era where email serves as a primary communication channel for organizations, and malicious phishing emails on the rise by 569% [6], the importance of diligently implemented email security measures cannot be overstated. I had the pleasure of sitting down with both Tonia Dudley, VP CISO at Cofense and her colleague, Principal Threat Advisor Ronnie Tokazowski as we discussed the capabilities of the services and products offered at Cofense, a leading provider of email security solutions.

As cybercriminals continue to exploit the vulnerabilities within email systems, Cofense has emerged as a formidable ally in the battle against phishing, malware, and other malicious threats. With email serving as a primary channel for communication and business operations, organizations face obvious substantial risks from targeted attacks that aim to exploit unsuspecting users. With advanced threat intelligence

capabilities, Cofense technology is able to identify and mitigate sophisticated email-based threats. By leveraging real time data, machine learning, and behavioral analysis, it proactively detects and neutralizes malicious emails, empowering organizations to stay one step ahead of cyber adversaries.

In addition, we discussed Cofense's state-of-the-art phishing simulation and awareness training platform. This interactive solution helps organizations educate employees about the latest phishing techniques, equipping them with the knowledge and skills to recognize and report suspicious emails. By fostering a culture of security fairness conferences training platform fortifies the human element of defense, creating a robust line of defense against email-based attacks.

My Perspective on RSA and the Cyber Defense Magazine

Out of the numerous things winning Cyber Defense Magazine's Young Women in Cyber Award has left me with, picking the minds of the innovative geniuses who lead our world in developing groundbreaking cybersecurity technology has given me a high that I will not come down from. It was such an inspirational experience and has gotten me so excited for my own future within the industry. What an exhilarating time it is for technology. However, we must be mindful of the unparalleled challenges we will face as we navigate the uncharted territories of innovation and its possibilities.

References

[1] C. Herin, "Wib Securiy - Real World Case Studies: How API attacks are evolving and how to protect your organization," San Francisco 2023 RSA, Apr. 26, 2023.

[2] P. S. Paranjape Sameer, "Did You Check Your Quarantine?!," *McAfee Blog*, Oct. 28, 2019. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/did-you-check-your-quarantine/ (accessed May 22, 2023).

[3] "Known and Unknown: Author's Note » About » The Rumsfeld Papers." https://papers.rumsfeld.com/about/page/authors-note (accessed May 22, 2023).

[4] "2023_Ransomware_Report_Black_Kite.pdf." Accessed: May 22, 2023. [Online]. Available: https://blackkite.com/wp-content/uploads/2023/04/2023_Ransomware_Report_Black_Kite.pdf

[5] "Viakoo-Action-Platform-Data-Sheet_v10.pdf." Accessed: May 22, 2023. [Online]. Available: https://www.viakoo.com/wp-content/uploads/2022/01/Viakoo-Action-Platform-Data-Sheet_v10.pdf

[6] "Phishing Protection Solutions | Cofense Email Security," Apr. 22, 2022. https://cofense.com/ (accessed May 22, 2023).

About the Author

Born and raised in Hamilton, New Jersey, I now reside in the DC metropolitan area after recently becoming a George Mason University alum. While at GMU, I obtained my Bachelor of Science degree in Cybersecurity Engineering with a minor in intelligence analysis. Along with writing technical pieces for CDM, I am working full time at a leading mobile security company, NowSecure, as an Application Security Analyst where I do all types of fun things like exploit vulnerable apps, secure mobile application development, and contribute to exciting projects and important initiatives that are consistently highlighted thought the security industry. In addition, I also work part time with startup company, Auspex Labs, as a Cybersecurity Software Developer, where I am the main developer on Diplomacy™, a geopolitical threat intelligence engine that combines a broad assortment of metrics and NLP sentiment analysis to calculate nuanced and real-time threat scores per nation state. Working at Auspex has been pivotal in my knowledge in creating secure software and has given me the opportunity to not only develop my first product, but to also start my own startup company, productizing the software and capabilities created in Diplomacy™. Which brings me to my final endeavor, I am presently co-founder and CTO of Xenophon Analytics, a company that grew from shared interests in international political affairs and my project of building the geopolitical risk engine. When I'm not researching or coding, you can find me watching anime, reading Sci Fi, painting, or playing with my dogs! My ultimate goal in life is to learn every single day, and I'm proud to be doing just that. I love to chat about all things tech and security, so feel free to shoot me a message anytime.

Kylie can be reached online at [1] or on LinkedIn https://www.linkedin.com/in/kylie-m-amison-8665a7194/

Why Inadequate Investment in Cybersecurity is a False Economy

By Luke Dash, CEO, ISMS.online

Already suffering the most cyberattacks than any other European country [RH1], the UK looks set to experience a proliferation of vulnerabilities as businesses struggle to manage costs prudently.

The country's cybersecurity agency has warned that the next five years will see an explosion of "hackers for hire" that will lead to more cyberattacks and an increasingly unpredictable threat landscape.

Already, the growth of cyber tools and services saw cyber-attacks reaching an all-time high in 2022 – exacerbated by increased hybrid working and geopolitical events such as the Ukrainian conflict. Adding to the threat is a broader range of off-the-shelf products that lowers the barrier to entry, with more state and non-state actors obtaining capabilities and intelligence not previously available to them.

Our latest State of Information Security report surveyed 500 information security (infosec) professionals in the UK and found that six in ten businesses faced at least one data breach fine in the past twelve months. Financial data was the most popular target.

Not just about the money

No organization is immune to cyber breaches, some of which can have dire consequences. Even a minor ransomware attack can do anything from halting production to collapsing a business.

The financial costs of cybercrimes continue to increase exponentially in the UK, with average fines soaring to almost a quarter of a million pounds over the past 12 months. But it's not just about the money. The reputational damage and loss of customer loyalty can be even more damaging in the long run.

Alongside this are expenses incurred by the targeted business to perform security repairs and damage control, which may even be a case of too little too late. Research from 2020 found that 59% of consumers would likely avoid doing business with an organization that had experienced a cyberattack in the past year.

Moreover, UK businesses are at the forefront of the country's cyber defences, obliging them to help defend against foreign threats. At the recent CyberUK conference in Belfast, newly appointed Deputy Prime Minster Oliver Dowden warned of credible incoming attacks by unpredictable actors targeting critical national infrastructure and supply chains.

The rise of this new cybersecurity threat is particularly worrying since these actors are more ideologically motivated than financially motivated. This tendency is a wake-up call for UK businesses to approach information security proactively.

Time to break down the barriers

Even though 90% of infosec leaders view information security as a top priority for leadership teams, only around two-thirds (64%) expect to increase their infosec budgets in the next 12 months. In our report, a significant cohort (39%) listed budget constraints as their top challenge.

But budget constraints shouldn't stand in the way of a business having solid cybersecurity measures in place. Companies need to understand that investing in infosec protects information assets, builds trust, wins business, and highlights efficiencies that make a noticeable difference to their bottom line.

The potential impact of breaches can be crippling for businesses. Yet, many companies are unaware of the severe damage fines could inflict on them, let alone the threat to reputation and customer loyalty. These costs are too hard to ignore, and companies must invest in strong information security practices to protect their assets and build trust with their customers.

Good information security practices are good for business as it reduces the risk of severe financial penalties. We must invest in them to protect our assets and build customer trust. In fact, investing in

information security before falling victim to a cyberattack places a company in a much stronger position and saves money in the long term.

Now's the time to prioritize information security, increase budgets, and invest in the tools and technologies to help us stay secure in the face of a growing threat landscape. So, when the time comes for companies to re-evaluate their budgets, don't be the one to skimp on cybersecurity.

[RH1]Source: https://techmonitor.ai/technology/cybersecurity/uk-cyberattack-europe-ibm

About the Author

Luke Dash is a dynamic, forward-thinking business leader passionate about technology and innovation. With over 15 years of experience leading successful sales, product and business development teams, Luke has built an impressive reputation as an expert in business strategy, operations, and commercial performance from start-ups to large enterprises.

Currently serving as the Chief Executive Officer at ISMS.online, a leading SaaS governance, risk and compliance solution, Luke has been instrumental in driving the company's growth and success and is passionate about the information security and data privacy compliance landscape.

Having seen first-hand that good infosec delivers business success, Luke is committed to ISMS.online's purpose to empower every organisation to achieve simple, sustainable security.

Luke regularly contributes to industry and broadsheet publications, including Computer Weekly, Business Insider, CSO Online and Tech Nation.

Luke can be reached at our company website isms.online.

The Power of AI In Today's Rapidly Evolving Financial Crime Landscape

By Pedro Barata, Chief Product Officer, Feedzai

Fraud has plagued the financial services sector for years. In today's rapidly evolving digital landscape, financial institutions are under increasing pressure to safeguard their customers from criminals - but the emergence and accessibility of new technology has both helped, and hindered, this mission.

Fraudsters are becoming more aggressive and innovative, utilising emerging technologies and adapting their strategies to target the weakest link in the financial chain - consumers themselves. Technology, such as generative AI has created a new set of challenges for banks and financial institutions, enabling fraudsters to steal or create new identities or fake existing ones, aimed at both fooling consumers and also financial institutions.

Our research shows that criminals are currently a few steps ahead of consumers when it comes to understanding and recognising AI. Despite over half (56%) of consumers having been a victim of a financial scam, many still lack the knowledge to detect and distinguish between the various types of financial crime. 52% of consumers are unfamiliar with deepfakes and 63% have never heard of ChatGPT - tools increasingly used by criminals to scam innocent people. This shows how crucial it is for banks to act fast to educate their customers first and foremost. The old adage rings true - prevention is always better than cure.

Leveraging AI technology

Ironically, AI is simultaneously the problem and the solution. With the recent significant jumps in AI, financial organisations can now leverage advanced machine learning models to detect and prevent fraudulent activities in real-time. By analysing large behavioural data sets, such as transaction trends, or what time or where customers typically access their online banking, AI can identify patterns of behaviour. This allows banks to build a better picture of their customers and flags when something is out of the ordinary.

The ability for AI to process huge amounts of data in milliseconds allows for banks to identify unusual or potentially fraudulent activity at speed and with increased accuracy. AI holds huge potential to keep customers safe whilst also solidifying customer loyalty - with recent research revealing over half (53%) of consumers feel safer knowing their bank uses AI to protect them.

Empowering banks to better detect fraud and financial crime is keeping institutions, and their customers, both safe and compliant. However, the need for accuracy when using AI is vital. False positives, a legitimate transaction that is flagged as suspicious, is one the biggest frustrations for customers and immediately can cut any customer loyalty. Research revealed that 46% of customers would consider leaving their bank if it stopped a legitimate transaction, even if the issue was resolved quickly.

Banks need to be careful not to block legitimate transactions, and implement effective safeguards to prevent false positives and avoid customer inconvenience. This highlights the critical need for banks to prioritise transparency, effective safeguards, and tailored communication strategies to ensure customer loyalty and satisfaction.

The regulatory hurdle

As we work together to detect the rising levels of fraud, regulators must ensure they work with banks, customers, and other stakeholders to reach a solution. However, some divergence in regulatory landscapes globally still remains.

In the UK, regulators have mandated banks reimburse customers for online APP fraud, creating a sense of security and trust. Meanwhile, no such regulation exists in the US, leaving customers more vulnerable to the financial repercussions as they are less inclined to report scams. This makes it much harder to

accurately measure the full extent of the problem and, more importantly, build defenses to better protect victims.

Despite varying regulation across the globe, maintaining customer trust and satisfaction is crucial across all jurisdictions. While it may not still be a regulatory obligation in some regions, it should always be seen as a competitive differentiator. Fostering long-term relationships and loyalty is vital in the competitive financial services landscape and how a bank tackles financial crime is an important factor for customers. AI can revolutionise the financial services landscape for the better and those that adopt AI, prioritise strong relationships with their customers, and deliver a seamless customer experience will excel.

About the Author

Pedro Barata is Chief Product Officer at Feedzai, where he leads product development and management to bring the most advanced financial crime-fighting technology to market. Prior to joining Feedzai, Pedro worked for Critical Software, where he helped design and develop systems for CMMi appraisals, globally supporting project management initiatives.

https://feedzai.com/

https://feedzai.com/leadership/pedro-barata/

7 Benefits of Implementing ZTNA

(Zero Trust Network Access)

By Howie Robleza, Freelance Writer, Avigilon

One of the most significant worries for business leaders in the current climate is the potential for an internal security breach - with the increased adoption of cloud-based technologies comes increased vulnerability.

Zero-trust network access protects you from internal and external security breaches. Without it, your data could be vulnerable. Are you considering implementing ZTNA but need to figure out how it benefits your business?

Here you will learn about the benefits of ZTNA, what it is, and how it can benefit your company by minimizing your risk and reducing your vulnerabilities.

What Is Zero-Trust Network Access?

Zero-trust is a cybersecurity policy that does not infer the trustworthiness of every user on the system simply because they can access it.

Zero-trust is needed to protect your business from the threat of an unauthorized user gaining access to all of your valuable data by simply gaining access to your network. Or, if an employee intends to steal data or cybercriminal breaches an employee's device or account, it prevents an internal cybersecurity breach.

Many businesses allow guests, visitors, and trainees to use their network without guaranteeing their trustworthiness. With zero trust network access, you can allow anyone to use your network by restricting their access.

Users are only granted permission to access the data necessary for daily operations and nothing further. This way, if an employee device or account is breached, you can ensure that only a limited amount of data is accessible.

To help you understand why ZTNA is so crucial to your business strategy, the rest of this post will discuss the key benefits of ZTNA to consider.

The Benefits of Zero-Trust Network Access

Here are the benefits you stand to gain by implementing ZTNA to protect your network and data.

It Enables Micro-Segmentation

When you only grant users permission to access the data necessary for daily operations, you create segments within your network. This means that should a cyberattacker infiltrate your network; they won't be able to move laterally and access more of your data. So, you decrease the attack surface and minimize your risk in the event of a security breach.

It Provides Protection Against Malware Codes

The division of your network minimizes the impact of a malware security breach, ensuring minimal damage. Additionally, by deploying ZTNA, you can implement regular health checks across connected applications, ensuring the health of your system at all times and fast-acting response to a breach.

Contains Breaches Caused By Rogue Employees

Many business owners like to believe that their employees are trustworthy. However, there is still the likelihood that your employee could poach information, client data, and other resources to leave your company, start their own company, or provide your competitor with an edge.

So, by implementing a zero-trust network access policy, you can ensure that any rogue employee won't be able to access all the critical and sensitive data hosted on your network. A zero-trust model will also mean that containers and microservices are connected and efficiently communicate.

Your Applications Will Be Undetectable

When you implement ZTNA, you establish a virtual darknet, making your apps unavailable to public internet users. This darknet can protect your business from potential ransomware and data leakage.

Supports A Hybrid Work Model

Hybrid work models require cloud-based technologies, meaning that you will store much of your valuable company data on the cloud and be more vulnerable to a cyber-attack. By implementing a zero-trust network access policy, you can ensure that implementing a hybrid work model is not at the cost of your cybersecurity health.

Additionally, since the pandemic, hybrid working has become an attractive feature to employees in the hiring process. By implementing ZTNA and opening your business up to hybrid work, you can increase your choices during the hiring process and make your roles more attractive to applicants.

Ensures GDPR Compliance

As a business, you must protect client and customer data. A security breach can lead to legal ramifications and extensive costs. Additionally, it can harm your reputation and put the trust of your stakeholders in the balance. Investing in a zero-trust network access policy can ensure GDPR compliance and reduce your risk of facing the consequences of a data breach.

Can Apply to Physical Security

Zero trust policies don't just apply to your network and cybersecurity health. You can take a zero-trust approach to your physical security, including a wireless door access control system. If an interviewee, visitor, or contractor enters your building, they shouldn't be able to access server rooms and areas housing sensitive assets or dangerous equipment.

Restricting these areas protects you from a data breach caused by a physical security breach. It reduces your liability if a visitor enters a room containing dangerous equipment and becomes injured.

Helps To Protect Cloud-Based Systems

If you're implementing cloud-based technologies to support hybrid or remote work, you need a system to enable secure access to company resources from anywhere. Cloudbric offers a Zero-Trust Based Access Control System that provides secure authentication processes, allowing you to access company resources without establishing a dedicated line or VPN. This access control helps you to provide strengthened security processes in a cloud-based system with easy set-up and simple authentication procedures.

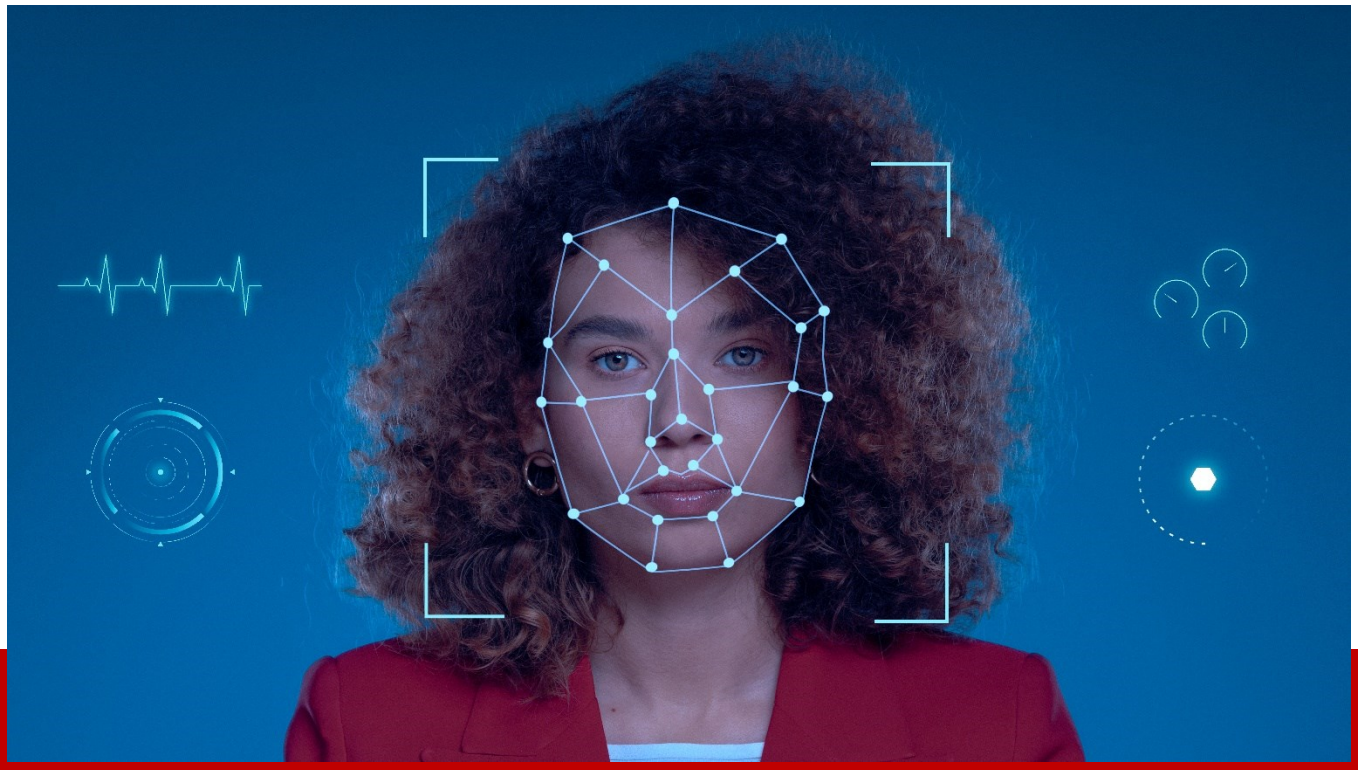
Summary

Zero-trust network access isn't just a priority; it's a necessity. If you're using cloud-based technologies or operating in a hybrid work model, you need to know that a security breach won't reveal all company data - only a limited amount.

About the Author

Howie Robleza, a freelance writer is interested in tech, legal, and property trends. When she's not writing, she works in commercial property management.

Howie can be reached at www.avigilon.com.



Biometric as a Service (BaaS) – An Opinion Piece

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

Biometric as a service (BaaS) works best as a striking alternative to other outmoded biometric software models. It becomes easy for organizations such as governments and telecommunication companies to use this technology in their everyday identity management operations. Companies hugely prefer using their technology as it allows employees to do fingerprint scanning and facial recognition easily by practicing. Consequently, getting rid of fraud becomes easy for organizations. Customers also use this technology as it streamlines customer service and takes less time to use. It is a less costly, and less time-consuming integration process. Biometric as a service market is growing because of the increasing demand for mobile biometrics.

Biometric as a Service (BaaS) – Provides Best Integration Services and Lessens the need for other Technical Resources to Integrate the Service

Biometric as a Service solution is accessible through the Internet and has all the functions, which allow for fingerprint scanning, facial recognition, and other biometric identification processes. Several biometrics-as-a-service providers provide integration services through which customers can easily

enhance their present systems by integrating biometric capabilities. With this technology, it is not necessary to look for any other technical resource to integrate the service.

The Benefits of Using BaaS – An Easy Identification System

One of the key advantages of using this system is it allows BaaS providers to manage biometric information easily. Organizations or customers do not need to manage the information. In the identification system, enrolling employees or business partners is easy. For the first time, it is required to take fingerprint scans through an internet browser on a computer connected to biometrics- capturing device. Another advantage of using this system is acquiring biometrics search and enrolling capabilities without building the systems.

With the use of a digital camera, capturing facial recognition records becomes easy. Once the employees are enrolled, their locations can confirm the identities of people through an Internet connection to cloud-based databases including biometrics information.

Why there is an increasing Demand for Biometric as a Service (BaaS) System?

If we observe, organizations prefer cloud-based services because of their advantages such as flexibility, agility, and low costs. Due to could deployment, organizations can easily employ biometric security capabilities without opting for any multifaceted setup. The cloud offers the benefit of hybrid cloud deployment that offers the advantage of public as well as private clouds. Consequently, organizations are employing cloud services to streamline the intricacies involved with traditional ones.

BaaS works as the best means to verify the identities of people without forming any other infrastructure. By integrating BaaS technology, organizations need to leave other worries like biometric recognition codes and databases. They will get all these things over an internet connection.

How Biometric as a Service (BaaS) Market Growing?

There is a growing demand for cost-effective solutions for accessing advanced biometric capability which in turn fueling the biometric as a Service (BaaS) Market. The healthcare industry provides several key opportunities in the BaaS market and is estimated to expand at a high growth rate during forthcoming years. It becomes easy for enterprises to combat fraud with the BaaS system.

How to Use BaaS and Its Use Spreading in Different Sectors

BaaS is an important asset for organizations, shops, banks, and different big organizations that handle terrorism. If we take an example, the Nigerian Communications Commission disabled nearly 10.7 million unregistered SIM cards for preventing terrorist and criminal activity. In Nigeria some parts, some criminals buy and resell SIM cards to those who want to make Internet banking frauds, kidnappings, and other

crimes using mobile technology. Biometric registration abolishes the anonymity involved with purchasing SIM cards. If somebody wants to purchase a SIM card, it is necessary to register a fingerprint with the telecom every time. Authorities will be able to know his or her identity easily when a SIM owner attempts to employ the related number for criminal activity, fraud, and robbery.

BaaS prevents from happening fraud, big crimes, and losses in many ways. Suppose a criminal attempts to open a bank account in the customer's present name. The onboarding system can easily identify him or her and tells the person is not who he claims to be by scanning the fingerprints of the criminal. Consequently, the customer service provider dismisses the transaction and makes it safe.

BaaS can help the banking industry and voting booths in many ways. For instance, BaaS may help authorities work in voting booths to avoid voter fraud. Authorities create virtual citizen IDs making use of facial images and fingerprints of people where voter fraud happens commonly. This system assures a similar person is not able to vote two times. It further abolishes the probability of somebody obligating ballot stuffing, since voting happens electronically.

Talking about the banking sector, this sector can use BaaS in many ways. If we take an example, suppose a customer has another bank account in another country and might ask to assure that only he or she can transfer money to foreign and domestic accounts. To fulfill this customer's requirement, a banking person needs to take a fingerprint scan for each transfer, whether the customer does it online or at a bank branch.

Factors that Increase the Adoption of Cloud-based Biometrics

Strict government rules for data security, increasing cyber-attacks, and demand for cost-effective biometrics are the factors increasing the adoption of cloud-based biometrics and consequently (BaaS) system as it is cloud-based biometric systems. Further, increasing BYOD adoption among enterprises and the rise in the IoT landscape also increase the adoption of these biometrics. The supply chain and sales channels of the electronic industry hugely affected biometric sales. Different technological advancements refer to the integration of biometric-as-a-service with laptops, tablets, smartphones, and other IoT devices. Such an aspect allows conducting of smooth business transactions through location-independent environments. These factors increase the demand for biometric-as-a-service systems.

BaaS system is in huge demand as their cost-effectiveness fascinates many enterprises toward the adoption of it. The industrial need for safe and rapid registration is also a crucial factor that contributes to fueling the demand for biometric-as-a-service systems. BaaS systems also allow for time recording, mobile access control, and web and workspace management.

BaaS has been crucially adopted in several industries and government offices due to its exciting features. Instant deployment, high reliability, and cost-efficiency are the features that this system comes with. BaaS has several benefits to provide such as it helps in identifying data duplication prevention, knowing employees, identifying patients, and knowing citizens. An increase in employee access monitoring and huge-scale funded programs increase the demand for BaaS systems.

About the Author

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

Mohit holds an MBA in Marketing and Finance. He is also a Graduate in Engineering in Electronics & Communication. He can be reached at https://www.linkedin.com/in/shrivastavamohit/.

You can visit our company website at https://www.futuremarketinsights.com/

Bad Hygiene: New Study Uncovers Common Security Failures of Cloud-First Organizations

By Ruoting Sun, Vice President of Products, Secureframe

The rapid rise of cloud-first organizations has revolutionized the way businesses operate. Yet with increased reliance on cloud services, information security is now business-critical. According to IBM's Cost of a Data Breach Report 2022, the average cost of a data breach in the US rose to over $9M. With an evolving threat landscape and increasingly sophisticated cyberattacks, organizations must go beyond baseline security measures to stay ahead of emerging risks and attack techniques.

Yet many organizations lack foundational security hygiene practices, leaving them vulnerable to costly security incidents. Our latest research reveals alarming statistics about the lack of best-practice security measures in cloud-first organizations.

1. Access key rotation for cloud service providers has the highest failure rate at 41%.

Access keys are an essential component of cloud security, granting users and applications access to various cloud resources. The high failure rate in access key rotation among cloud-first organizations poses a significant risk to information security.

Organizations must take proactive steps to maintain regular access key rotation. Implementing a key rotation policy and conducting regular audits of access key usage is essential. Security automation tools can also help manage key rotation and ensure consistency across the organization.

2. 40% of Identity and Access Management (IAM) accounts and 21% of root accounts do not have multi-factor authentication enabled for cloud service providers.

Despite well-documented benefits, many organizations do not have MFA enabled across their cloud environment, leaving them vulnerable to unauthorized access. In addition to mandating MFA for all IAM and root accounts, organizations should educate employees on the importance of MFA and security hygiene best practices.

3. 37% of organizations reuse passwords for cloud service provider logins.

The prevalence of password reuse makes it easier for attackers to gain unauthorized access to multiple accounts by exploiting a single set of credentials. There are several ways to address this problem, from implementing strong password policies to utilizing password managers to help employees securely store and manage unique passwords.

Strengthening Security Hygiene Through Automation

Failure rates for these common security configurations shed light on why account takeover is still one of the top threat vectors leveraged by bad actors. Top cloud platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform all provide capabilities around multi-factor authentication, access key rotation, and password reuse prevention natively within their platforms.

The critical question is: why are so many organizations failing to implement well-known best practices to secure their cloud environment? Too often it is because they are needlessly manual, time-consuming tasks that get neglected for other business priorities.

Forward-thinking organizations are embracing compliance automation tools as one solution to this pervasive problem. Automation allows companies to quickly and easily address routine security tasks and compliance requirements by continuously monitoring systems, collecting documentation for routine security audits, automating responses to security questionnaires, and streamlining annual employee security training. With routine security hygiene tasks automatically completed, IT security teams have more resources to contribute to complex business issues.

Automated security tools improve efficiency, streamlining time-consuming tasks and freeing up IT personnel to focus on critical security initiatives. They add consistency, helping maintain uniform security processes across the organization. And they enable scalability, accommodating expanding infrastructure as the organization grows.

There are several areas where automation can be effectively implemented to improve security hygiene:

- Vulnerability management: Automated vulnerability scanners can regularly assess an organization's infrastructure for potential weaknesses, ensuring timely identification and remediation of security risks.
- Patch management: Automated patch management tools can monitor and apply software updates and security patches, keeping systems up-to-date.
- Access management: Automating user access management can streamline the process of granting, modifying, and revoking access privileges, reducing the risk of unauthorized access.
- Incident response: Automated incident response tools can quickly detect and respond to potential security breaches, minimizing potential damage and ensuring a swift recovery.

While automation offers numerous benefits, it is essential to balance automation with human expertise.

Security teams must work closely with automated tools, leveraging their expertise to fine-tune and optimize these technologies. As the security landscape evolves, teams can adapt automated tools to new challenges and regularly assess performance, making adjustments to ensure automated tools continue to support the organization's security goals.

The Urgent Need for Good Security Hygiene

As cloud adoption continues to grow, it is crucial for organizations to prioritize proper security hygiene to ensure the ongoing protection of their valuable assets and data. By embracing automation, organizations can simplify and streamline routine security tasks, elevate their security hygiene, and demonstrate a strong security posture to customers, prospects, and partners.

Secureframe Trust empowers organizations to prove a strong security program and build customer trust using real-time data.

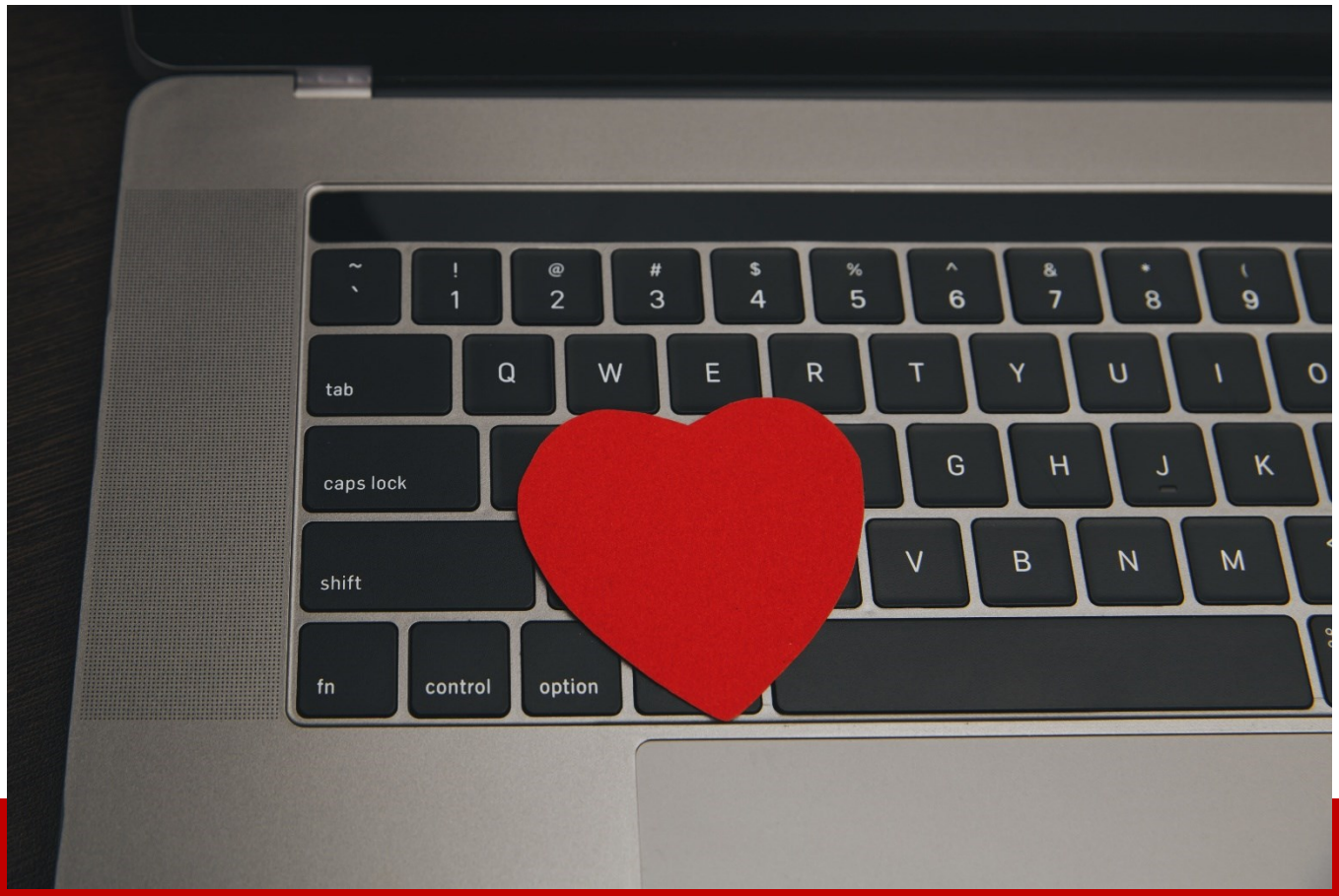
- A customizable Trust Center allows organizations to build a dedicated space to publicly demonstrate their security program with data continuously pulled from Secureframe.
- Questionnaire Automation streamlines the process of managing and completing security questionnaires using machine learning and AI, enabling organizations to quickly satisfy specific customer requirements.

- The Knowledge Base serves as an organization's privacy, security, and compliance system of record. In-house subject matter expert can edit details to ensure the Knowledge Base stays up-to-date, removing friction while allowing admins control over sensitive documentation.

Compliance automation offers cloud-first organizations a powerful way to maintain a robust security posture while proving their commitment to security and compliance to customers and prospects. As the cloud landscape continues to evolve, organizations that effectively leverage compliance automation will be better positioned to navigate emerging challenges and seize new opportunities for growth.

About the Author

Ruoting Sun is Vice President of Products at Secureframe, the leading all-in-one compliance automation platform. Build confidence with prospects and streamline security reviews with Secureframe Trust.



HEAT Attacks Vs Apts – What Is the Difference?

By Mark Guntrip, Senior Director of Cybersecurity Strategy, Menlo Security

A new breed of attacker has emerged, one that has learned to weaponize the web browser.

The Highly Evasive Adaptive Threats (HEAT) attacks they now use to compromise browsers, gain initial access to the endpoint and deploy threats like ransomware or malware, are notable for their ability to evade detection. This and their ability to get malicious payloads onto endpoints means that HEAT attacks can be confused with Advanced Persistent Threats or APTs. But there are some key differences between the two – and they operate in very different stages of the attack kill chain.

So, what are the differences between HEAT attacks and APTs?

What is HEAT?

When you look at HEAT attacks, there are many threats out there in terms of volume. The key thing for threat actors is to maximise their chances of success and it's a numbers game. The two key words, 'evasive' and 'adaptive', are most important for attackers because they want threats to be as evasive as possible to avoid detection.

That means they understand how to bypass a particular technology or security technique that typically is in place. Whether phishing detection on email or sandboxing, there is a reasonably well understood level of 'standard' technology in an organisation, and if they know they can evade this type of detection, they will have a much higher level of success.

With the 'adaptive' side of HEAT, this is how it changes over time in order to maintain that evasiveness. An example is evading URL reputation, where rather than moving fast to register a domain populated with content and malware and push it out, attackers adapt to how URL reputation systems find out whether a site is malicious or not and behave in a way they know will be classified as legitimate. Attackers register a domain for a certain amount of time before they use it, so it is not new. They then populate it with relevant content, so it's categorised in a certain way. Once they confirm the site is seen as good, they use it for an attack. If URL reputation solutions or engine change, they then change what they do before they use it for a HEAT attack.

Threats in general are going up, but HEAT attacks are also increasing. HEAT attacks can be used by Ransomware as a Service (RaaS) operators to gain initial access. Some attackers' entire business model is to gain initial access into as many networks as they can and then sell it onto someone who wants to deploy malware onto that network. They won't just sell it to one person, but to multiple people, with a single breach resulting in five, 10, 100 or more threat actors being able to put their malware on a network.

What are APTs?

APT is a class of threats designed to be undetectable. Once in the network, they stay there for as long as possible and do whatever it is that an attacker wants to do with it – whether looking around, stealing data or credentials, or deploying ransomware. They are often used by nation or state sponsored groups to go after high value targets, and more recently, by crimeware groups.

What's the difference between the two?

They are very much two sides of the same coin, or two parts of the same process. The main difference is that a HEAT attack gains initial access to a target network and an APT will do the damage once deployed inside. A HEAT attack itself is not going to do any damage but delivers the thing that does. But they shouldn't necessarily be thought of as distinct and separate because they can be put together and used in the same attack. The Nobelium attack, for example, used HTML smuggling, a HEAT characteristic, to deliver APTs to victims.

What should cybersecurity teams should know about HEAT attacks?

With hybrid and remote models and people working on any device connected to the corporate network, these all have to be treated like a single system. For example, if a user is on a Mac connected to their personal iCloud, anything coming through and attacking them can be relayed to a corporate device. The potential impact of this, especially when it comes to HEAT attacks, is huge. If somebody gets initial access to a personal device, it can then be used to access corporate resources. It's much the same as having initial access to a corporate owned device with all of those same rights.

Attackers are getting better at evading tools and systems that are already in place, but also at tricking users into clicking on a link or download a file to activate a threat. More education and awareness are needed about HEAT attacks, how they work and what they can do, as well as improved visibility around what a HEAT attack looks like. In the industry, we talk a lot about prevention, but we also need to have better levels of detection.

Finally, and most important though is having visibility into the browser. HEAT attacks exist in the browser, and endpoint security solutions do not necessarily have visibility into what is going on inside a browser. Not only is the browser a blind spot, but it is also the most targeted access point.

About the Author

Mark Guntrip is Senior Director of Cybersecurity Strategy at Menlo Security, responsible for articulating the future of threats to security leaders around the world. Prior to joining Menlo Security, Mark has been security strategist at Proofpoint, Symantec, Cisco, and several other leading cybersecurity providers.

Why Cybersecurity Provision is Critical for Businesses, Large and Small

By Astrid Gobardhan, Group Data Protection Officer at VFS Global, the world's largest outsourcing and technology services specialist

Against a backdrop of biting inflation and uncertainty across global markets, many organizations are now revising down their annual commitments towards internal work, such as IT, with some forecasters predicting as much as a 20 per-cent fall in spending across this area over the next year.

Yet, interestingly and against the grain of anticipated budget cuts, a new survey, published by the Enterprise Strategy Group (ESG) suggests that almost two-thirds (65 per-cent) of senior leaders – including IT decision-makers – intend to increase their cybersecurity spend over the coming year, given the evolving threat and frequency of online attacks. In terms of a ballpark figure, the technological research firm, Gartner, anticipates spending on risk management and data security to touch a new high of $188billion (€174 billion) in 2023.

But what is driving this, and what can businesses do to improve their resilience when it comes to external attacks?

In the main, this spending shift towards risk management can be attributed to the effects of the COVID-19 pandemic and growing regulatory pressures. With the average cost of a data breach in the USA now standing at an eye-watering $9.44million, comparatively light spending on cybersecurity and education within a workforce can go a long way towards safeguarding critical infrastructure and an organization's future viability. There's also the reality that, today, businesses are processing more data than ever before, and increasingly storing this information between local and cloud-based servers. These tools, together with the roll-out of Zero Trust Network Access – which provide remote-workers with secure entry to an organization's applications, data, and services – mean that organizations are spreading their risks, and, in turn, having to commit more and more to this particular area, each year, from their IT spend.

In my role, as the Group Data Protection Officer at the world's largest outsourcing and technology services specialist, I know, first-hand, how important it is to establish and maintain security provisions around an organization. Cyber-security is an "always on" priority, given the risks involved, and it's crucial that business leaders see any investment as an insurance policy against an attack.

The challenges facing each business will vary, depending on their size and scope, but it is important to stress that no organization is immune to cyber threats. Here are several points that IT and business leader should consider, and potentially work into their risk strategies, over the coming year:

Educate employees about cybersecurity. Employees are the first line of defense against cyber-attacks. It, therefore, makes sense to have cybersecurity as a fixture of their work from day one. This should set out not only the risks entailed in their role but wider information and organizational processes, which they can turn to for guidance. By creating a climate where risk is analyzed, and openly discussed, organizations will be well-placed to prevent and respond to an attack.

Perform software updates and use complex passwords. Some of the most common ways attackers gain access to systems are by exploiting vulnerabilities in software and by gaining password credentials from brute force attacks and "third party" leaks. By ensuring that all system software is up to date, organizations can reduce the risk of local and external attacks. Passwords, used across organizations, should also be updated at regular intervals and comprise a mix of upper and lowercase letters, numbers, and symbols. There are password managers available, such as Dashlane or LastPass, which guard against hacking, and allow employees to generate individual, hard-to-crack, and storable passwords.

Use multi-factor authentication. Multi-factor authentication adds an extra layer of security to accounts and systems by requiring users to provide multiple forms of identification, such as a password and a code from a mobile device. This is a common practice now across many operations, and is an effective, and largely trouble-free, way for organizations to both reduce their risk, and, in the event of a breach, trace its origin.

Be aware of social engineering attacks. This work involves manipulating employees into breaking normal security procedures and best practices. Such attacks can sometimes be hard to spot, particularly

if they take the form of a line-manager or IT professional emailing to confirm login credentials or other organizational information. It is therefore important for employees, across an organization, to be aware of certain 'red flags', and to encourage them to be risk-averse in how they respond to these "out of the blue" demands. As a general rule, recipients should double-check with the sender, via a separate means of communication, such as text message or phone call, to check the veracity of a request.

Conduct "live fire" exercises. Even if an organization uses a third-party for its IT department, it is well worth performing periodic security tests, as part of a "live fire" simulation. Such exercises can provide a useful data bank on where an organization can improve, and also allow for refresher training, across identified weak points, with certain staff.

Perhaps the most fundamental point to consider, though, is that the digital landscape is constantly evolving. This means organizations will need to stay on top of, or at the very least introduce some barrier of protection against, emerging threats and quickly and effectively share new information with their teams to stave off an external attack.

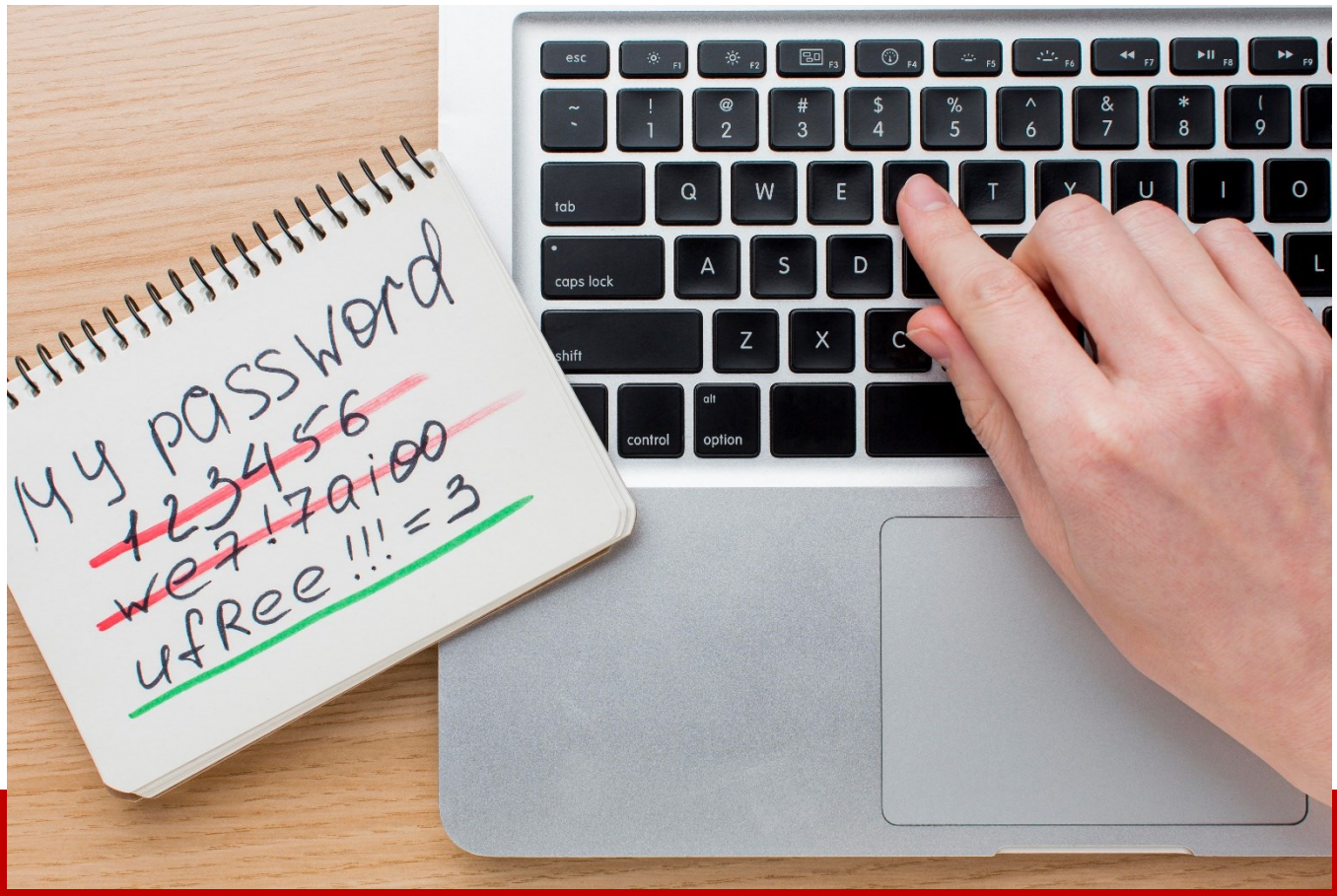
By introducing a number of the abovementioned suggestions to their operations, and adopting a prevention-first philosophy, organizations can take important and potentially critical steps towards reducing their exposure to risk.

About the Author

Astrid Gobardhan is the Group Data Protection Officer at VFS Global, the world's largest outsourcing and technology services specialist, serving 67 sovereign governments worldwide. VFS Global has processed over 251 million applications since its inception in 2001.

www.vfsglobal.com

https://ae.linkedin.com/in/astrid-gobardhan-94030221



One Defense Against Data Breaches: Don't Have the Data to Begin With

By Raj Ananthanpillai, Founder and CEO, Trua

When it comes to hackers stealing Social Security numbers and other personal identifiable information, even members of Congress aren't safe.

So why would we think any of the rest of us are?

After hackers accessed a healthcare marketplace for DC lawmakers and residents in March, investigators discovered Social Security numbers, birth dates, addresses, and phone numbers for lawmakers, their families, and their staffers on the dark web.

Hackers are brazen and relentless. Most businesses, no matter how conscientious, aren't equipped to serve as a fortress against cyber criminals who are eagerly and cleverly attacking them in search of PII.

And so often, that's exactly what they are after. A 2021 IBM report found that PII was included in 44% of all breaches that were studied in the report, making PII the most common type of records lost or stolen. Compare that to 28% of breaches when PII had been removed from customer data.

And the cybercriminals aren't slowing down. In fact, they were busy in the first quarter of 2023 when an estimated 89 million individuals in the U.S. were victims of data compromises, according to an analysis by the Identity Theft Resource Center.

Clearly, hackers view PII as valuable. That's why the less of that information is kept and stored by a business or government agency, the better. The question is: How do we put a stop to PII being spread around so widely, making an enticing target for those bad actors?

At least a couple of options should be considered.

The first is that businesses should give serious reflection to what information they really need from consumers, and whether they are collecting some of that data simply as a means to verify someone's identity.

For example, let's say you're the owner of a gym. Do you really need someone's Social Security number so they can complete the gym membership application? Or for health providers, do you need the SSN when patients have insurance?

Because once you're in possession of PII, you absolutely need to keep it as safe as possible. But as we see time and again in the news, keeping data safe from determined and clever cybercriminals is no easy task, and businesses put themselves at risk of liability when there's a breach.

Certainly, companies sometimes do have legitimate reasons for requesting PII. Employers, for example, need that information from employees for payroll purposes. Banks are required to obtain Social Security numbers when customers set up accounts.

But in many cases, the information just isn't needed.

I like to advise consumers to ask questions whenever a business wants their Social Security number or birthdate or any such information that those hackers crave. Why does the business need it? How will it be used?

Businesses should ask themselves similar questions. Aren't there better ways than gathering and storing this information that you just needed for identity verification, but now must protect?

A second way this problem can be solved is through more widespread adoption and use of verified digital identification. With verified digital identification, people won't need to provide their private personal information over and over. They will provide it once to have it verified when their digital ID is created. After that, when someone wants to verify who they are, they will present their ID rather than repeatedly sharing their sensitive information.

With this system, the individual's personal information is less likely to end up in the hands of cybercriminals, which also decreases the likelihood of people losing trust in the business. Businesses,

meanwhile, would know that the person's identity is verified, but they wouldn't have to take responsibility for storing and protecting the information.

As it stands now, though, the use of these digital IDs hasn't become prevalent. While many other things we deal with have gone digital, trust verification and assurance are still in the analog world.

That is certain to change, though. Consumers will insist on it as more and more data is compromised, and they learn there is an alternative to their information being stored in numerous places with questionable defenses.

Businesses should prepare for and embrace such a shift.

After all, this will give those determined hackers fewer reasons to target them.

About the Author

Raj Ananthanpillai is Founder and CEO of Trua, that provides privacy-preserving identity and risk-screening platforms that assure trust and safety in digital environments, sharing economy, employment and workforce screening.

Raj can be reached online at https://www.linkedin.com/in/raj-ananthanpillai-endera/, and at our company website http://www.truame.com/.

Heard At RSAC 2023 - Protecting the Protectors

Some Personal Risks to Individual Cybersecurity Practitioners Are Elevated Because Of The Work They Do. Is It Time for Workplace Cyber Protections to Follow Them Home?

By Chris Needs, VP of Product Management, HYAS Infosec Inc.

RSAC 2023 once again underscores the sheer number and variety of enterprise security technologies, as if every possible niche of cybersecurity has been addressed. But there's a growing sentiment that something is missing, something important.

Cybersecurity professionals epitomize RSA's Stronger Together conference theme of 2023 by simply doing what they always do. Perhaps it's working with law enforcement on a significant take-down. Perhaps you worked with your ISAC to remediate suspected APT activity, just as they were about to

achieve some actions on objectives. Oh, and that new social media post you just published on a cybersecurity topic? You're making us stronger together by sharing that information.

The problem with every one of these positive contributions is they increased likelihood that a cybersecurity professional will attract the ire of attackers, their network of friends, or their government. Meanwhile, they clock out (theoretically), go home, maybe has a family, and wants to go "shields down" for a while.

Attackers can act on grudges and start looking at you personally. Your home network, your personal devices, and even your family may all be viable attack vectors, whether to settle the score or to leap-frog back into your corporate network. In addition to commonplace adversary objectives - data exfil, malicious encryption, extortion, data destruction - there are other motivations. Bragging rights gained from compromising a security leader, the desire to understand what security researchers know about an adversary, and the satisfaction of poking a cybersecurity team or company in the eye are all motivations that may make your personal life part of the extended attack surface of your organization.

The fact is, our cybersecurity protectors are more highly targeted at the office and out of the office because of what they do at work, and we need to do more to protect our protectors. This is the product area that is weak. This is what is missing from the sea of vendors at RSAC and all of the (honestly) amazing technology that they bring to market.

Often the realm of "home" is for consumers and consumer products. We rely on our ISPs, email services, or social media companies to protect us like regular consumers. We have seen advancements in anti-phishing technology in our email. Our credit card companies offer dark/deep web services. And of course, that cybersecurity awareness training provided at work is transferable to home. I share the PowerPoint decks with my family, as well as the occasional story about successful friendly phishing against colleagues. But we in cybersecurity are more highly targeted and therefore have the need for additional protections. We also have the skills, knowledge, and interest to use more advanced tools at home.

We need to adapt the tools designed for protectors of the enterprise who go home and have a family to protect. Think about taking an enterprise-grade Protective DNS solution that actively blocks malicious domains, adapting it to the personal needs of an individual or family, and rolling it out to the practitioner at home. Your ISP may be offering some level of protection, but to what extent? There is an implicit trust that they've got your back, but you have no visibility on what they're doing for you.

Extra protections would be welcomed by most in our field. But it's not just about protection, it's about providing the tools that cyber pros can use to customize the solution to fit their concept of risk at home, just like what they would do at work. Give them the controls, the dashboards, and the alerting to protect effectively. Provide insight on web traffic, blocked domains, and threats just like they're used to at work but to leverage at home.

What new opportunities await both vendors and end users alike by reimagining enterprise security tools for the protectors at home? What additional security would be afforded the company that recognized its own security teams need more when they are away from the office? Companies adopting the concept of "duty of care" for its security practitioners may benefit from the acknowledgement that the enterprise has a duty to ensure it reduces risk that it creates for the employee.

Let's embrace the RSA theme of Stronger Together by strengthening defenses for the protector at home. We need free or low-cost versions of enterprise tools, and affordable delivery models for the individual that employers can purchase on behalf of their protectors. This is a potential triple-win: better protecting the enterprise by better protecting the employee with tools built by vendors that expand their own business.

Now that sounds like Stronger and Better Together.

About the Author

Chris Needs is VP of Product Management with HYAS, leaders in utilizing advanced adversary infrastructure intelligence, detection, and prevention to preemptively neutralize cyberattacks. He drives all aspects of the product management lifecycle including go-to-market strategy, prioritization and roadmaps, and Agile development methodologies. He has previously served as VP of Product Management and UX at Anomali, and as Director at NC4. He holds a PhD from UCLA, an MBA from the Boston University Technology Executives Program, and other professional certifications and degrees. Chris can be reached online at @HYASinc and https://www.hyas.com/.

Changing the Status Quo of Cloud Security

Skyhigh Security's The Data Dilemma report underscores major paradigm shifts in cloud adoption and risk.

By Rodman Ramezanian, Global Cloud Threat Lead, Skyhigh Security

Over the last few years, the ongoing cybersecurity transformations impacting organizations across the globe have shaken up the status quo of how data is managed and protected. Cloud adoption has risen astronomically, as seen in Skyhigh Security's *The Data Dilemma: Cloud Adoption and Risk Report*, with the use of public cloud services increasing 50% from 2019 to 2022. Driven by the pandemic and the adoption of work-from-home and hybrid models, there has become a crucial need for organizations to be able to access data from anywhere. Businesses can often accelerate their goals at a lower cost by relying on the cloud for data storage and access. However, this also means data is no longer on just endpoints – it's everywhere.

In the wake of this paradigm shift, it's become clear that traditional security measures are no longer enough to protect data. With cloud services replacing many applications formerly run on-premises, more organizations are storing sensitive data in the public cloud – 61% on average. This data, ranging from

personal staff information to intellectual property and network passwords, can easily damage a company's reputation and its ability to function if it lands in the wrong hands. As organizations continue to face a myriad of security issues during this transition to the cloud, threat actors wait in the shadows to capitalize on the growing data exposure.

Without visibility, data loss prevention is nearly impossible.

The complexities around securing data in the cloud highlight inconsistent security controls and a lack of visibility from organizations. In fact, over half of Software-as-a-Service (SaaS) products are commissioned without direct IT involvement – meaning a lack of expertise in business decision-makers may be putting organizations at risk. This is evidenced by 75% of organizations having experienced a cybersecurity breach, threat, and/or theft of data, emphasizing the criticality of modernizing and optimizing data management and security in the cloud.

Not only do organizations need to know where data is going in order to protect it, but they also must know in order to keep it from being stolen. It's essential that security teams have broad visibility and control over their entire cloud-native environment, but unfortunately 28% of organizations still report a lack of visibility into what data is stored in cloud applications. While Shadow IT, the use of IT systems without department oversight, has been around for some time, organizations are only now starting to see the negative impacts on data security. From 2019 to 2022, there was a 25% increase in organizations reporting that Shadow IT was impairing their ability to keep data secure – a massive shift indicating the ongoing demand for public cloud usage may be compromising existing data security systems.

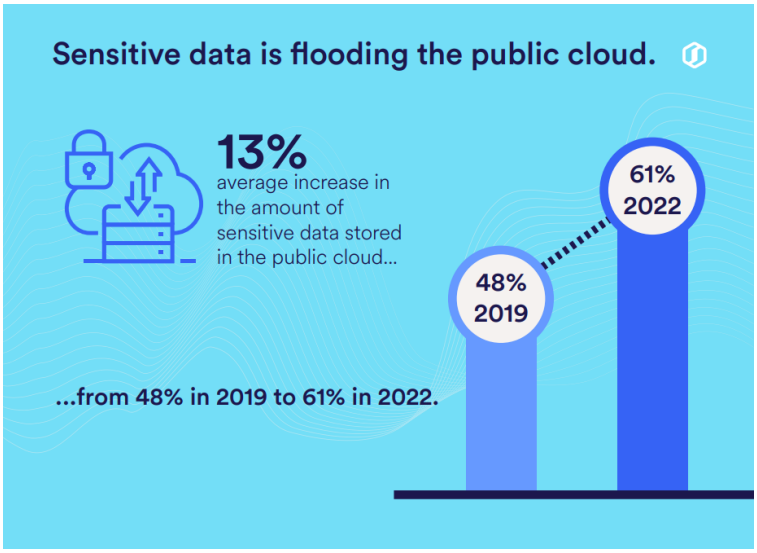
Combatting distrust and risk simultaneously

As the adoption of cloud services has grown, so has internal apprehension. In particular, 37% of organizations don't trust that the public cloud can keep their sensitive data secure. This could be explained by the never-ending onslaught of threat actors attempting to lay siege to critical data, or it could be that an increasing number of organizations allow employees to use personal devices to access data in the public cloud – six in ten, to be exact. This only compounds the risks associated with storing data in the cloud.

On the other hand, 93% of organizations say that their IT department controls what sensitive data is uploaded to the cloud from personal devices. This poses another question: do they have the correct controls in place, or are they naïve to the fact they have security gaps?

Evolving to meet the pace of cloud adoption.

Cloud security must grow at the same pace as adoption if organizations are to handle the complexities of controlling data flow. Most organizations' data protection practices have not kept up with the increased adoption, as demonstrated by the ongoing breaches making headlines every day. Even organizations that are not hybrid or 100% remote will more than likely find themselves storing and accessing data in cloud environments. The benefits are too great to ignore – scalability, capacity, accessibility, speed – but it also brings new challenges that warrant new solutions. Securing data is more challenging than ever before, but organizations across all industries must rise to the occasion.



Over half of organizations surveyed in The Data Dilemma report plan to invest more in cybersecurity. This gives us hope that more and more organizations will set their sights on preventing data loss and adopting security measures, such as Zero Trust principles, that can break what was once the status quo of cloud security.

About the Author

Rodman Ramezanian, Global Cloud Threat Lead at Skyhigh Security, has over 11 years of extensive cybersecurity experience. Rodman specializes in the areas of Adversarial Threat Intelligence, Cyber Crime, Data Protection, and Cloud Security. He is an Australian Signals Directorate (ASD)-endorsed IRAP Assessor – currently holding CISSP, CCSP, CISA, CDPSE, Microsoft Azure, and MITRE ATT&CK CTI certifications.

How the SEC's Proposed Security Rules Could Impact Businesses

By Portia Cole, Emergent Threat Researcher, Avertium

If the Security and Exchange Commission (SEC) has its way, it will soon do more than any other federal agency has done when it comes to putting cybersecurity disclosure requirements in place for public companies and covered entities and their boards of directors. The SEC proposed new regulations in March 2022 (the comment period was reopened a year later) and March 2023 that would, in part, require investors be informed "in a consistent, comparable, and decision-useful manner" about how cybersecurity risks are being managed.

The comment periods for both came to a close in May 2023. If adopted, new rules and requirements would be put in place regarding:

- The reporting of material cybersecurity incidents and updates about previously reported cybersecurity incidents.

- Reporting requirements regarding a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk.
- Management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.
- Annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise.

In the SEC's view, the purpose of the amendments is to keep investors better informed about an organization's risk management, strategy, and governance and ensure prompt notification in the event of significant cybersecurity incidents. The government also seeks to abandon its dated 2003 strategy, which established that federal regulation wouldn't be a main approach to securing cyber space—clearly, it has changed its mind. Let's dive into two notable regulations that deserve our attention.

Prompt Reporting

Our assumption is that the regulation regarding prompt disclosure of breaches is in response to organizations such as T-Mobile and BlackBerry. In 2021, both T-Mobile and BlackBerry faced public scrutiny after they failed to promptly inform customers and the public of server and software vulnerabilities that affected millions of people. T-Mobile's breach was significant because it exposed the data of more than 100 million customers—and troubling in terms of how investors learned of it. Vice.com broke news of the breach on August 15, 2021, but the company didn't confirm the breach until August 16, 2021—24 hours after the breach made headlines.

At the time, there were no existing federal regulations dictating the timeframe within which a company had to report a data breach. As a result, on September 1, 2021, Congress began examining a House of Representatives bill that included requirements around how quickly companies need to report attacks (between 24 or 72 hours), what kind of compromises need to be reported to CISA, and whether a fine should be implemented if there is non-compliance. Although Congress was unable to reach a consensus at that time, in March 2022 the Cyber Incident Reporting for Critical Infrastructure Act established two cyber incident reporting requirements for covered entities within 16 designated critical infrastructure sectors, and the SEC is now inching closer to finalizing similar disclosure rules that would benefit stakeholders, customers, and investors.

Among what the SEC wants: Similar to public companies, covered entities will have to disclose past and present cyber incidents to the SEC within 48 hours of discovery. Covered entities would be required to immediately notify the SEC in writing of a significant cybersecurity incident when they have reasonable grounds to believe that one has occurred or is occurring. In addition, companies must submit detailed information about the incident and their response to it using the proposed Form SCIR, which must be filed promptly and updated if new material information is discovered or upon resolution of the incident.

Board of Directors and Cybersecurity Risk

It's not enough for board members to simply be informed about a company's existing security measures. Boards should play a crucial role in supporting cybersecurity risk management, and the proposed SEC regulations will help force that along.

If the SEC has its way, public companies will be required to disclose if board members have cybersecurity expertise. The SEC will mandate that companies disclose how the board oversees cyber risks, as well as describe how management assesses and handles those risks. It gets even more detailed, requiring that companies disclose the ways in which the board is kept up to speed on cyber risks and how often the board discusses the topic. The regulation would require board members to increase their focus on cybersecurity and take responsibility for overseeing the organization's response and recovery plans in the event of a cyberattack.

Board members are going to have to get much more serious about cybersecurity. Gone are the days when it was enough just to get an update on what the CISO has been working on. As the *Harvard Business Review* puts it, “Board members must take the position that cyber-attacks are likely, and exercise their oversight role to ensure that executives and managers have made proper and appropriate preparations to respond and recover.”

Potential and Limitations of the Proposed Regulations

Should the new rules kick in, the only changes won’t be limited to the disclosures themselves. Companies may find they incur additional costs to comply with the new rules, including the costs of gathering and analyzing the required data. There is also the potential for increased reputational risks. With greater exposure, comes greater scrutiny. Companies that fail to adequately address their cybersecurity risks may face reputational damage and potential backlash from investors, customers, and other stakeholders.

The intent of these proposed rules is to protect the greater public by promoting transparency and holding companies accountable. But as with many regulations, there are limitations. There remains a degree of ambiguity around what covered entities are obligated to disclose and how they should disclose it. For example, different industries face different cyber risks and have unique risk profiles with different levels of confidentiality and security, making it difficult for stakeholders to compare the cybersecurity postures of different organizations across industries. Companies may also measure their risks differently, so for a stakeholder to know whether a particular company's risk measurement strategy is comprehensive or accurate can be difficult to determine.

But what the SEC is looking to do is to build upon or revise what is already in place, and organizations would do well to build upon what they’re already doing in order to be ready—and in a stronger cyber position whether or not the proposed changes formally become requirements. That includes educating your board about what may be coming and reviewing the written policies and procedures you have in place for your incident response program.

About the Author

Portia Cole, an Emergent Threat Researcher at Avertium, specializes in researching the latest cyber threats, threat actors, and vulnerabilities. As a member of the Capability Development team, she contributes valuable insights to the field of cybersecurity. Her work can be found on Avertium's website, and she can be reached through LinkedIn.

Controlling Cybersecurity Risks

Controlling Cyber Risks and Fraud by Risk Assessment

By Hakan Kantas, Senior IT Director

We are trying to protect all the Internet connected systems, users, network and other related structures with the renewed and evolving regulations, new applications, processes and services that come with new technologies, in parallel with the developing technology and innovations, and we call this as Cyber Security. The risks that come with so many interconnected structures need to be analyzed, and this is where the Cyber Security risk assessment comes to the forefront.

Digital Transformation, which is one of the most popular topics of the last period, attracts attention especially in societies that are open to innovation and like to adapt and use the latest technologies quickly. Institutions that want to adapt to new technologies and bring their customers into this area are quickly starting the digital transformation process. However, each new technology brings with it new and often unknown risks. Managing these sometimes unknown risks and preventing the loss of information, today's most valuable asset, is as popular as digital transformation and as important as cybersecurity.

These new technologies and applications are one of the reasons why cybersecurity has become so popular in recent years.

As the leader of the team that established and implemented the IT risk management methodology in my institution years ago, I would like to express that risk management is one of the fundamental building blocks of cybersecurity. At first glance, you may not see a direct relationship between these two concepts, or you may not understand why such a study is needed. However, you will understand how the methodology I will explain in the rest of this article will make a difference in terms of fraud prevention.

At this stage, it would be right to make a statement to those who ask, "Let's run cybersecurity directly, and what is the need for risk analysis." It is not generally known where the new technologies and applications introduced and implemented through digital transformation have gaps, problems and risks. Even if there is general awareness, existing risks may increase or shift during the process of implementation and adaptation from institution to institution. The only way to uncover these threats and vulnerabilities is to conduct a comprehensive risk assessment study. In this way, unknown potential vulnerabilities can be identified before an incident occurs and the necessary precautions can be taken.

Security and system vulnerabilities in new products and technologies can, to some extent, be uncovered by numerous cybersecurity tools. However, since these are new products, it takes time for existing security products to adapt and provide more serious controls. In the meantime, the greatest risk is in the process of adapting and adapting security products to new technologies. Cybersecurity risk assessment, which can prevent this, provide stronger measures, and is not very difficult to implement, can play a redeeming role here.

Cybersecurity risk assessment is a very critical aspect because this assessment makes it possible organizations to identify and prioritize determined critical risks. You will to create action plans to mitigate identified risks with this methodology. Without a risk assessment process in place, organizations may be vulnerable to data breaches, phishing and cyberattacks which can result in significant financial and reputational damages. A regular cybersecurity risk assessment is essential for any organization to be able to control potential vulnerabilities and comply with new regulations and laws. This routine study will not only reveal potential vulnerabilities and threats in the long run, but will also provide a more mature continuation of future evaluations as it will provide a basis for the next study.

We will begin our work by first discussing what the cybersecurity threats are. As mentioned above, the purpose here is not to list all the threats, but to convey the general working methodology with an example set. So we'll start the methodology by listing the most common threats overall.

1. Phishing
2. Ransomware
3. Malicious Software
4. Social Engineering
5. DOS/DDOS Attacks

Step-1 - Determine and Prioritize Assets and Value

Today, even the largest organizations do not have unlimited resources. Every work, project, product, in short, every process has a certain budget and resource. Based on this awareness, we need to set out by knowing that we have a limit for the risk study we will carry out.

Within the framework of the boundaries and limits we draw, we must first identify our most valuable assets. After creating the framework for this, you can start preparations by listing the assets in that area. In fact, having a catalog of all assets and categorizing them as very critical, critical, important, unimportant, etc. is the most critical work and the basic building block that needs to be addressed as the first step. Preparing a catalog of all assets as a first step is not an easy task. As we mentioned above, we should create an inventory with a defined scope, otherwise keeping the scope too broad may cause you to miss the target while trying to reach an endless inventory. Depending on the scope, in addition to the titles listed below, Cloud solutions such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) can also be included in this assessment.

1. Information security policies
2. Information Technology Architecture
3. End Users
4. Support Staff
5. Architectures that show information flow
6. Technical and physical checklists
7. Criticality information
8. Technical Data
9. Software
10. Hardware

After completing the extraction of assets according to the scope we have determined, we can determine the criticality of those assets by asking the sample questions below. Of course, you can elaborate these questions within the scope of the area you work in, how detailed the risk study is aimed to be, the scope and diversity of the asset list.

1. If I lose this information, will I experience a regulatory or legal event?
2. Will the loss of this data affect my institution financially?
3. Without this data, can the institution survive, can the work be done, can the operation be maintained?
4. How critical is this information to my competitors?
5. Which processes and structures are most vulnerable to data loss?

Step-2: Identifying vulnerabilities and cyber threats

One of the most critical points of risk analysis is to identify potential threats and vulnerabilities from the broadest perspective, without overlooking anything. Identifying the threats that can cause vulnerabilities and determining which vulnerabilities they are the source of will form the inventory we need to uncover in the second step. At this point, we immediately think of spoofing software and hackers. However, there are many threats that do not come to mind. For example, when you see natural disasters among the

items below, you may say "but this is not a cyber attack". What is meant here is whether the systems become vulnerable to a possible cyber attack after a natural disaster. It is important to look at the issue from this perspective.

Let us list a few of them:

1. Human Error: Has the staff in your organization been informed about cyber-attacks and their types?
2. System Failures: Are the systems that hold and process your most important data regularly checked and maintained, and are they actively monitored?
3. Natural disasters: How much can disasters such as earthquakes, storms, floods, fires affect the structures and systems that hold your critical data? It should be kept in mind that as a result of such a disaster, not only people but also the hardware and systems that hold this data may be affected.
4. Unauthorized Access: There may be unauthorized access to data due to the success of one of the cyber attacks on the organization.
5. Misuse of authorization: The risk that the users you authorize may use the data for different purposes or take it out of the organization for malicious purposes should not be forgotten.

Step-3: Risk Assessment

This is the point we have been trying to get to from the very beginning. In other words, this is the stage where cyber security risk analysis is done.

The risk assessment of the information and inventory we collected in the first two steps, that is, the likelihood and severity of the events mentioned, is evaluated at this stage.

Different organizations and methodologies make different levels of assessment here. While some standards assess at 3 levels such as low, medium and high, the general practice consists of 5 levels: very low, low, medium, high and very high. It would not be appropriate to use a statement that says, "Use this, this is correct". Because many factors such as the size of the organization, the area, the criticality of the data, awareness of cyber security, measures, human resources, etc. include criteria that will affect this decision.

Severity and Likelihood should be determined for each identified risk. As I mentioned above, the general practice is to evaluate both topics in 5 stages as you can see in the table below. For each risk, severity and likelihood values are determined individually and multiplied to obtain the risk rating.

Risk Rating = Severity X Likelihood

The risk ratings that emerge from this step can be named in different ways. Some may call these green, yellow and red areas Low, Medium and High, while others may call them Insignificant, Acceptable and Unacceptable.

While different organizations generally categorize the degree of risk in 3 categories, some consider risks with a very high severity and likelihood, i.e;

Likelihood 5 X Severity 5 = Risk Rating 25

They may categorize risks as NOT TOLERABLE in a completely separate way. This assessment may vary depending on the scope, method and methodology.

Step-4: Control Step

In this step, we determine the controls for our risks that we have uncovered in the 3 steps above and determined the degree of risk.

When we say control, we are talking about all kinds of actions that will ensure that the risk does not materialize. All kinds of measures to be taken to prevent potential risks from materializing, to prevent them, or to reduce the likelihood of the risk even if we cannot completely prevent it in any way, should be considered under this heading. One of the most critical steps of this work is to examine each risk individually and to produce controls by evaluating them by the relevant teams.

A few examples of controls can be given as follows:

- Data in the transfer or storage phase
- Installing and using special applications such as anti-malware, anti-phisting beyond anti-virus applications,
- Firewall regulations, rules, measures,
- Regular password change and secure password,

- And I think most important of all; Education, education, education...

Step-5: Monitoring, Evaluation and Reporting

These studies, which we have briefly mentioned above, require serious knowledge, labor, effort and analysis. We have done all this work and completed our Cyber Security Risk Assessment. So, what happens now?

First of all, a report should be prepared that includes details such as all identified risks, risk assessments, risk categories and controls taken/planned to be taken. The report should be forwarded to senior management and used as input for management decisions in areas such as budget, investment, policies and procedures.

With this study, you have also created a general operation and security map such as where your critical data is located, by whom it is used, what risks it carries, how and where it is processed. You can and should use this map both in projects or large-scale studies carried out within Information Technologies and in critical decisions to be taken by business units.

After running the process several times, maturity and awareness will increase even more, and after a while you will see that your cyber security risk analysis work has reached a much better and mature point. Of course, in this process, you should not ignore the improvement of your cyber security risk assessment process, if necessary, in line with the needs and technological developments.

I wish you good luck to creating safer and healthier working environment by applying the above method in your organization..

About the Author

Hakan Kantas is an IT Director. He started his professional career in 1993 in the IT department of Pamukbank, Turkey. He was the CIO of Vaillant Group in 2007-2008. He has been working for a private bank in Turkey since 2008. Currently, he's Senior Director of IT Continuity Management Department and he's responsible of following areas; Operational Resilience, Risk ve Cyber Security related to Resilience, IT Continuity Management, Disaster Recovery, Crisis Management, IT Capacity and Performance Management, Data Management and GDPR. He is an IEEE Senior Member, member of ISACA (Gold Member), member of Association for Computing Machinery (ACM), member of Information Technology Association, and member of Business Continuity Institute (BCI) and former board member of itSMF-Turkey Chapter.

Hakan can be reached at; hakkan@gmail.com, hakan.kantas@ieee.org, hakkan@hakankantas.com and https://hakankantas.mystrikingly.com/

What Will Cybersecurity Jobs Look Like in 2028?

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

What Will Cybersecurity Jobs Look Like in 2028?

Macroeconomic turmoil, the Great Resignation, and layoffs by all-star companies – the landscape appears bleak in the global tech jobs market, yet the demand for cybersecurity professionals remains impressively high in comparison. Why? Because bad times bring the bad guys out.

Market research company Sapio found that nearly 80% of CISOs believe the world is in a “perpetual state” of cyber warfare, which Forbes calls “digital civil disobedience.” While digital transformation and the adoption of new technologies mitigate many threats, these factors also create new and unforeseen challenges across every industry.

Although the cyber jobs market is in a good place, AI has the potential to both threaten and strengthen the sector and the people within it. Over the next five years, will we see a growth in cybersecurity jobs as businesses face up to future threats, and how will the ripple effect of AI make its mark? Let's find out.

Reviewing Future Risk Factors

Employers face an extreme reality: invest in cybersecurity or risk losing everything. The average cost of a data breach currently tops $4.35 million, and it's terrifying to imagine this figure in five years' time. Cyber insurance premiums have skyrocketed, and executives agree that a catastrophic cyber-attack is the most important scenario in their 2023 resilience plans. Deloitte's Technology Industry Outlook paints a similar picture, advising leaders to bolster their cybersecurity capabilities to keep up with evolving digital transformation efforts. With that in mind, it's impossible to review the future of the cybersecurity jobs market without considering the threat landscape that drives it forward.

The Metaverse: Into the Unknown

The metaverse has enjoyed lots of hype and little action so far. Although it is early days, metaverse cyber threats straddle the digital and physical worlds thanks to the use of software and hardware. As users further engage with the idea of an immersive digital identity, they will freely experiment with the blockchain, crypto payments, and NFTs. Unfortunately, hackers can follow every interaction made by a victim as each move is recorded on the blockchain, potentially contributing to phishing attacks and scams that could also have real-life implications. Promoting a zero-trust model, continuous authentication, and Multi Factor Authentication (MFA) will be essential to building a highly secure metaverse. But preparation will only take cybersecurity efforts so far – the metaverse era will be full of surprises.

Cloud Security: An Unrelenting Risk

According to PwC, 38% of business leaders expect more serious attacks via the cloud in the upcoming years. The migration journey is fraught with threats, as new and complex environments require culture changes (especially the development cycle and DevOps), different security tools, and also different perspectives. Remote working and the appetite for digital experiences will continue to add fuel to this fire. Employee leniency, extra devices, and increased outsourcing have created a perfect storm of risks that can't be controlled within physical parameters, and cloud security spending will rise almost 27% year-over-year to protect and defend infrastructure, data, and people. Robust cloud security will include policy-based IAM, a zero-trust approach (once again), encryption for data protection, and AI-based threat intelligence tools.

AI: Untapped Potential

As far as cybersecurity is concerned, AI is a blessing and a curse. Palo Alto's What's Next in Cyber report found that 39% of executives believe threat detection can be completely automated, helping enhance operational efficiency in light of the shortage of cyber talent. However, Europol continues to point out the power that deepfakes and generative AI have in launching a new realm of social engineering attacks, plus the ethics entanglement as businesses experiment with tech like ChatGPT for various use cases. As much as AI will continue to enhance velocity, productivity, and efficiency in the workplace, it will also be a major risk factor in the coming years. The question is: can the only defense against AI be itself?

What Will Cybersecurity Jobs Look Like in Five Years?

An interview in Fortune magazine revealed that cybersecurity is "largely insulated from market downturns," but what will we see when we finally arrive in 2028?

Better Opportunities for Senior Leaders

By 2026, 70% of boards will include one member with cybersecurity expertise, and Gartner predicts that cyber leaders will be recognized further as business partners and influencers. The benefit of this is that the board will switch its focus from protection to resilience. New SEC regulations might require companies to disclose the cybersecurity expertise of their board members, which is interesting considering 59% of directors told PwC that their board is currently ineffective at understanding the causes and impacts of cyber risks on their organizations.

A More Diverse Pool of Thought

Microsoft Security is leading the charge in promoting diverse hiring practices thanks to its commitment to training 250,000 people in community colleges by 2025. There's no doubt that certification and academic prowess go a long way in the cyber sector. Still, requirements like these perpetuate the belief that cybersecurity is an exclusive club reserved for technical experts only. In reality, businesses that take the time to invest in women, minorities, and neurodiverse individuals will benefit from better problem-solving, collaboration, and knowledge sharing.

Employers Will Open Their Pockets

Fortinet found that 60% of firms struggle to recruit cybersecurity talent, and 52% find it hard to retain them. In response, they're putting their money where their mouth is. Demand for application and cloud security skills will grow by 164% and 115% in the next five years, respectively – and these skills carry salary premiums. The average cybersecurity salary in the US sits at a healthy $240k, and wage inflation plus a worker shortage should help boost this figure by an extra $10k or so.

Blended Roles and Responsibilities

Better cybersecurity is for the many, not the few. Developers will become more involved thanks to shift left principles, and organizations will continue to build a culture of awareness across all departments and job functions, led by CISOs. In light of the metaverse, there's also the thought that we may see cybersecurity professionals collaborating with ethics teams more so than previously. Organizations like NIST can develop standards and legislation, but these "good" principles must be embedded in the software and hardware from day one via development, DevOps, cyber teams, and more.

About the Author

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

Don’t Jump to Conclusions on Zero Trust Adoption

By John Linford, Forum Director, The Open Group Security Forum, and Open Trusted Technology Forum

The Open Group Security & Open Trusted Technology (OTTF)

Even in an industry known for rapid shifts and changing trends, the growth of Zero Trust in the cybersecurity zeitgeist over the last few years has been remarkable. It was until recently still just a germinating concept, and now it is on the roadmap of almost every security team in the world.

That is not an exaggeration. The fourth annual State of Zero Trust report from Okta, published last summer, found that 97% of survey respondents had “a defined Zero Trust initiative in place or planned to have one within the next few months”. That is a rise from just 16% in the first edition, and it is hard to think of another growth story quite like that.

So, should we just declare victory for Zero Trust now, safe in the knowledge that from here on out we are in the implementation phase, and that everyone will soon be benefitting from having replaced their old network edge model with continuous, granular authentication?

That might, unfortunately, be premature. One nice thing about Zero Trust is that, compared to some technological innovations, its fundamental principle is very simple to describe. The previous paragraph gave one way of phrasing it, and we could also accurately look at it in terms of shifting to data- and asset-centric security rather than network-centric approaches, or in terms of providing access only when required rather than denying access when necessary.

These overlapping definitions – and there are others in circulation – are fertile ground for hype. That means that, while 97% of Okta's respondents might have the term 'Zero Trust' in their plans and projects, there are real questions to ask about what a true Zero Trust Architecture (ZTA) should or will ultimately look like.

Although simply stated in theory, true implementation of Zero Trust can be more challenging. For businesses and users alike, security practices can be deeply embedded and difficult to change. Organizations have broad suites of security tools and processes which may need to be reworked, and just as importantly, users are highly familiar with traditional processes and will require determined effort and communication to adjust to this new culture.

The effort involved is worth it, though, because the changing nature of cyber threat is quickly outpacing the ability of the traditional security perimeter model to combat it. Malicious actors are becoming ever more skilled at moving laterally to points of value within networks once the perimeter is breached, and there is only so much that security teams can do to ameliorate that damage.

At the same time, the shape of that traditional perimeter is becoming still harder to define. Changing working patterns mean that there is growing pressure to enable personal devices to access internal networks, while digitalized relationships between businesses and clients increasingly require bridges between what would once have been strictly distinct systems.

All of that means that the boundaries between insiders and outsiders are blurring – to the extent that thinking of it as a boundary is becoming significantly less useful or realistic. Instead, we need an effective ZTA in which the user, asset, or data is the perimeter.

We need a shared understanding of what truly is (and, just as importantly, what is not) Zero Trust. Any organization pursuing Zero Trust should start from a position of relying on robust, open, tested, vendor-neutral definitions of the methodology in order to assure that the systems they roll out really will meet the demands of future security threats.

There are widely used definitions available including NIST® 800-207, and The Open Group has published a clear, readable guide entitled the Zero Trust Commandments which outlines what is non-negotiable for a successful Zero Trust strategy. We are also in the process of developing our own standard ZTA framework, which will help to create a shared understanding among businesses, vendors, government, and academia about how different elements of ZTA should interact in order to deliver effective security.

The fact that there has been a rapid, large-scale move towards Zero Trust is, to be clear, a highly encouraging development: the costs of digital security breaches reliably increase year-on-year, and the need for a new response is clear. To get ZTA right, we first need to properly define it.

About the Author

John Linford is the Forum Director of The Open Group Security Forum and Open Trusted Technology Forum. As staff at The Open Group, John supports the leaders and participants of the Open Trusted Technology Forum in utilizing the resources of The Open Group to facilitate collaboration and follow The Open Group Standards process to publish their deliverables. Prior to joining The Open Group in June 2019, John worked as a Lecturer for San Jose State University, teaching courses in Economics.

John is Open FAIR™ certified and was the lead author of the Open FAIR Risk Analysis Process Guide (G180), which offers best practices for performing an Open FAIR risk analysis with an intent to help risk analysts understand how to apply the Open FAIR risk analysis methodology.

Embedding Privacy-First Behaviors for Future Generations

By Michael Levit, Co-Founder and CEO of Tempest

As all of our lives have moved online, the collection and sharing of data by big tech and private companies has become the norm. This is a concern not only from a security point of view but also in that it reduces the freedoms of individual internet users. Data privacy and security are intertwined, and it is vital that technology is developed to make it easier for all users to adopt privacy-first behaviors.

Developing technology that allows people to understand how their data is being used and enabling them to take steps to protect their own data will take us forward into a better, safer world.

The state of play in search technology

Search engines have become a tool used by almost everyone on the planet. Google alone, it is estimated, processes 5.6 billion searches per day. The embedding of this practice into our daily online lives has also resulted in practices which put privacy and online safety at risk. Major search engines re-target users with search results and adverts based on highly personal information such as health concerns, relationships status, sexuality, and personal finances. This is a concern for users of the internet, with data

in 2022 from the research company Ipsos suggesting that 79% of internet users worry about their online privacy.

Search engines are now a core aspect of our online lives, but users are forced to make a data privacy trade off. The human need to access information now means that there are exabytes of personal data being shared by individuals every day and a mass collection of this personal data presents security risks. It is no secret that cybercriminals are becoming increasingly sophisticated and although search engines invest heavily in cybersecurity there are currently no perfect solutions. One way in which the industry can help to ensure the security of people's personal data is by educating users themselves on taking control of their own data and developing search technology that is privacy-first. Privacy-first solutions for privacy-conscious consumers is the future we need to build towards.

A private search revolution

It is a significant challenge to create a safer future where data collection is de-normalized and the risks it poses are reduced. Ultimately, it's about ensuring security by going right to source. Developing technology that does not collect PII (Personally Identifiable Information), is tracker-free and does not collect users' search history. This ensures that personal data isn't exposed to security risks. Innovation is vital and cybersecurity must sit at the heart the development of search and browser technology for the next generation.

However, succeeding in embedding data privacy into search depends on two things – experience and education. Internet users are not going to change engrained daily habits lightly, so developing privacy-first tools with a seamless user experience is vital. This includes everything from look and feel to providing privacy information (cookies, trackers etc.) in a way that is easy for people to interpret. In a new world of internet privacy, user experience and data security go hand in hand.

The second key part of the puzzle is educating users on how their data is being collected and the privacy and security issues this creates for them. We can invest in all the technological innovation in the world but without users who are empowered to use them, the problems will persist.

Data privacy and online security are often viewed as macro issues, but data is at it is very core, personal. By putting users back in control of their personal data, next generation internet companies can play a key role in a safer future.

About the Author

Michael Levit is the Co-Founder and CEO of Tempest. He leads on the strategic direction of the business across product, financial and operations. In 2017, he co-founded the company to embed private search into our everyday lives after observing a gap in the market for a mainstream private-focused search engine. Michael is an experienced and passionate entrepreneur – he is a co-founder of Spigot, one of the world's leading multi-platform application developers. Michael also held advisory and executive positions at prominent businesses in the tech sector, including Alibaba, Softonic, DeleteMe, Docker, Say Media and Revel Systems. He also has experience consulting the world's largest corporations during his time at Accenture from 1995 to 1999. Michael brings this wealth of experience to the Tempest team.

Michael holds a B.A. in Business Economics, a B.S. in Mechanical and Environmental Engineering and a Master of Business Economics from the University of California, Santa Barbara. When Michael isn't busy running Tempest, he enjoys spending time with his two wonderful children and chasing the wind with his kiteboard. Michael Levit can be reached online at https://www.linkedin.com/in/mlevit/ and at our company website www.tempest.com/.

Ensuring Trust in Military Network Automation: Addressing Layer 8 Issues for Improved Operations and Security

By Marc Packler, President, CISO Advisory, Silent Quadrant and Tony Thomas, President & Chairman, Tony Thomas & Associates LLC

Automation is becoming increasingly prevalent as technology continues to advance and companies see the value in automating more processes. The TEI study by Forrester found that organizations implementing automation technologies can benefit from both operational efficiency savings and infrastructure appliance savings. While automation has many benefits, it also raises trust issues, particularly in the military where trust is of the utmost importance for the security of sensitive information and the efficiency of operations. However, trust issues in the military don't necessarily involve lack of trust in automation technologies themselves. Rather, they are mostly the result of trust deficits within "layer 8," what Margaret Rouse of Techopedia defines as "a hypothetical layer used to analyze network problems and issues that are not covered by the traditional seven-layer OSI model." It generally refers to

the “user” layer of networks. In the military’s case, the lack of trust exhibited within layer 8 hinders automation and negatively impacts mission assurance.

Though the commercial sector is focused on profits and has different priorities from the Department of Defense (DoD), the military can nevertheless garner a multitude of mission assurance benefits from added network automation. Department of Defense Directive 3020.40, Mission Assurance (MA) (Change 1, September 11, 2018), defines mission assurance as “a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition.” Network automation is a critical tool toward achieving these ends in today’s fast-paced and mercurial cyber environment.

As defined by Merriam-Webster, automation is the automatic control of a system using mechanical or electronic devices to replace human labor. The trusted autopilot in a KC-135 during refueling operations showcases how trust in automation has gradually built over time and how important automation has become in certain processes throughout aviation. However, not all processes can be automated, and there are still instances where manual intervention is necessary, such as with the role of a boom operator in refueling. The integration of human behavior and technology is essential to achieving successful automation, a crucial component in achieving mission assurance and Joint All-Domain Command and Control (JADC2).

Such integration requires a multi-disciplinary approach involving experts from information technology, cybersecurity and operations, as well as effective leadership at all levels. JADC2 involves a networked military system that integrates and synchronizes operations across all domains of warfare across various platforms, such as sensors, weapons and communication systems. The integration of data from multiple platforms provides a comprehensive and accurate picture of the battlespace, enabling faster and more effective decision-making, while orchestration allows numerous programs to work together. However, achieving multi-platform capability is challenging, as JADC2 systems may use different communication protocols, data formats, and security measures.

Lack of trust among those in DoD’s layer 8 is a significant obstacle to achieving better integration of human behavior and technology in military networks. Mission assurance and JADC2 are negatively impacted by the lack of trust in each other's personnel, the policies implemented by different organizations, the different funding levels and avenues for each organization, and the validity of data generated by multiple organizations. Solving trust issues requires effective leadership at the lowest and highest levels. Trust between and among organization commanders should be the starting point, and individuals should follow orders to accomplish the mission, regardless of their personal trust issues.

To take full advantage of advanced data analytics and processing capabilities requires experts in information technology, cybersecurity and operations to work together to extract meaningful insights from the data that can inform decision-making. When different systems produce different findings, individuals tend not to trust the data, and traditional tools sometimes have difficulty verifying results. To ensure the accuracy and security of data used in automation, robust processes for monitoring and verifying data must be in place. Additionally, transparency and accountability in the automation process can provide clarity on how decisions are made and who is responsible for them. Orchestration, the key to automation, must be in place as well. Application program interfaces, or APIs, are examples of tools that allow different

programs to communicate with each other and enable automation of multiple processes simultaneously. The commercial sector is doing these things today, so it is not a technological issue for the DoD, but rather a lack of implementation at the layer 8 level.

Efforts to improve networks within the military cannot be achieved without sufficient funding. It is important that we recognize the value of networks as a crucial and primary tool for the DoD and allocate necessary resources accordingly. Trust is critical in this process as well. Organizations that work to retain funding they don't need or perhaps shouldn't even receive need to stop, but fear of losing financial resources is a reality. Some leaders equate reduced or reallocated funding with diminished power and authority, or they may not believe that the people who receive the reallocated resources will put them to best use. The overall military budget is certainly relevant to and impacts appropriate funding for networks and cybersecurity, but adequate funding also relies on trust among those in layer 8. To help build and maintain more trust, military decision makers should ask themselves the following question: "Am I doing what's best for my service, or am I only doing what's best (or perhaps easiest) for my organization?" If the answer and corresponding actions support the latter, then changes need to occur.

Without added funding and better allocation of needed resources, the military will likely continue to use unnecessarily manual processes that consume time and energy personnel can devote to other mission tasks. For example, personnel still manually patch network devices, a mundane and time-consuming task that can be automated. Additionally, automation should be applied across the board through process orchestration rather than being applied piecemeal to respective individual programs. Many commercial organizations have already adopted orchestration to seamlessly address IT service management tickets from start to finish without human intervention. For instance, if a router malfunctions, it would be beneficial to orchestrate the automatic loading of previously saved configuration files, which can quickly restore network service, without the need for human involvement. Automation and orchestration also reap manpower savings that can result in mission realignment, but the cyber community has not conducted a manpower study in 25 years, and many cyber organizations are already below required troop levels. If this is not rectified, then functionally appropriate and efficient manning is unlikely to occur, and this would do little to build the trust needed within layer 8.

Automation and orchestration technologies are essential in streamlining core business activities, managing systems, deploying applications, and achieving DevOps goals. Achieving better implementation is complex (though not unattainable) and requires many things of layer 8, such as process transparency and accountability, adequate funding, clear documentation and reporting, regular audits and assessments, ongoing education and awareness programs, a culture of continuous improvement, and a strong foundation of trust. Addressing layer 8 issues involves focusing on the human factor and the way people interact with technology, processes and policies. Such focus is necessary to garner the full benefits of automation and orchestration for mission assurance and JADC2 because the military cannot win future battles by running its networks and their security at the speed of Airmen; rather, it must run its networks and their security at the speed of automation.

About the Authors

Marc Packler, President of CISO Advisory at Silent Quadrant, is a seasoned cybersecurity expert with 25 years of U.S. Air Force experience. Specializing in digital security, transformation, risk management and strategic operations, Marc also serves as a Principal at Quadrant Four, implementing innovative technologies for the Department of Defense. Connect with him on the Silent Quadrant website, LinkedIn or email marc@silentquadrant.com.

Tony Thomas, President & Chairman, Tony Thomas & Associates LLC, has an over 34-year career in the U.S. Air Force as a cyber professional. Now, he leverages that diverse and vast innovative skillset to transform and impact digital governance, compliance, security and process improvement throughout all functional areas of industry and DoD. He can be reached on LinkedIn or email Tony.Thomas@TTandAssociates.com

Five Tips to Securing Your Organization Through Your People.

By Dr. Inka Karppinen, CPsychol. Lead Behavioural Scientist, CybSafe

While many commentators continue to tout technological solutions to various cyber security issues, with high-profile cyber-attacks and data breaches continuing to make headlines, it's evident the status quo isn't working. Aside from technology, the approach to cyber security in the coming year requires a more people-focused approach.

For too long, organizations have assumed that by explaining cyber risks, their employees would alter their behavior. Human behavior doesn't need to be a guess or an assumption, it can be measured and studied. As a result, people can be directed towards good behaviors, and their progress quantified. Organizations can use this knowledge to improve their cyber hygiene *while* promoting and spreading a positive and effective cyber security message.

Here are five steps businesses can consider making cyber security policies work *with* their workforce.

1 – Talk to people!

People are naturally predisposed to interact in communities and make sense of our environments. However, as technological advancements continue to evolve, we often turn towards technology alone as the cause and solution to cyber security problems. But employing a more “human-centric” approach to problem-solving adds alternative opportunities to organizational challenges.

Initiating conversations with people on the ground allows a better understanding of where the gaps are in their knowledge. For example, employees could be skipping through the security awareness training because it isn’t engaging, or because they are ‘fully protected by anti-virus software’.

The best way to get information is to bring the conversation to them, whether that be near the coffee machine, through a message on slack, or via a well-timed, well-worded survey. If someone is known to have developed a workaround to security processes or doesn’t take the right action when faced with a security decision, the likelihood that others are doing the same thing is greater.

Gaps in knowledge leave room for errors which might otherwise be avoidable. By engaging their people, security professionals will be better equipped to provide the information needed to fill the gaps and improve understanding.

2 – 24/7 is the new 9 to 5

The work environment has changed significantly in recent years. Previous insistence on a presence in the office meant that internal 9-5 cyber security measures were largely able to protect both individuals and tools in the workplace, especially within the physical spaces of office buildings.

With hybrid working becoming the new norm, 9-5 protection is no longer enough. Working from home has allowed for new and greater opportunities for cyber risk. Cybercriminals function 24/7, and with personal devices being used from home, or work devices being taken out of a comparatively safe workspace, it is important to make sure cyber security measures are effectively implemented around-the-clock to protect people and businesses from bad actors. In the first instance, that means providing people with the tools to effectively manage their cyber risk, no matter their working environment.

3 – Training and tools

Users should not be blamed for their errors if they have not been provided with the necessary training and, most importantly, appropriate tools to perform secure cyber practices or recognise threats. Worse still, is if a tool is not reliably performing and hinders the main job task, especially in environments that focus on productivity and outputs.

People don’t want to be a liability or feel vulnerable in their workplace; naturally, they want to be part of the solution. Therefore, the onus is on organizations to ensure employees are aware of what is expected of them, *and* that they have the tools to be successful.

CISOs don't need to be told the importance of proactivity in preventing cyber-attacks and breaches; it is about prioritizing organizational cyber hygiene and giving CISOs the resources to put people first.

4 – Positive messaging leads to positive responses

According to Tessian, a cloud email security platform, between March 2021 and March 2022, one in four employees who made cyber security mistakes lost their jobs. While every organization needs to make cyber security decisions that work for them, harsh penalties for honest mistakes will likely lead to fewer people reporting the errors they make to IT teams, even if their mistake compromises security. Driving these wedges between employees and executives' risks making cyber security increasingly challenging to manage.

Paradigmatically shifting the outlook towards viewing cyber security incidents as powerful learning opportunities is vital for encouraging employees to report errors. In fact, if errors are made, they can be positive learning experiences. Gaps in knowledge can be identified and rectified, and security can be improved, preventing similar future mistakes. A positive message also encourages people to learn more about cyber security and become champions for their colleagues around them. Transforming a blame culture into a collaborative, positive one can be a powerful way to improve transparency and address essential vulnerabilities.

5 – Layoffs and cyber hygiene

It's impossible to ignore that several high-profile mass layoffs punctuated the end of 2022 and the beginning of 2023. While no one wants to see such unfortunate events, we may see more in the coming months.

If the decision is made to let employees go, there's a risk that organizational cyber security may become compromised.

These risks come in two different forms, the first of which is the technology itself. Organizations should have a crisis management plan in place to ensure that the security of their tech infrastructure can be preserved. Whether it is to allow for effective patching or the avoidance of siloes, planning ahead is always important.

Second is how layoffs can impact an individual's psychology and behavior. Employees have access to a vast amount of organizational information, data and sensitive credentials, in addition to physical hardware belonging to their employer. In order to maximize protection, cyber security must be considered in the event people are let go. These processes must be in place before any announcements that may cause worry for one's livelihood are communicated.

Approaching redundancies through understanding and honest messaging encourages a much more positive, compliant response from understandably upset workers. Conversely, a more clinical or insensitive approach may provoke anger and discourage the same people from tying up cyber-security-

related loose ends. One need only look at the recent redundancies at Twitter to understand how confrontational messaging can lead to anger and non-compliance, not to mention bad PR!

Eliciting negative emotional responses can cause people to panic and act irrationally from a cyber security perspective. For example, individuals may start sending information to private emails, which might not be secure. Ultimately, an organization's employees are the first and last lines of defense for organizational security, meaning saying goodbye to several employees will inevitably leave weaknesses. So treating redundancies delicately, respectfully and offering support can be the first step in minimizing cyber hygiene issues in the future.

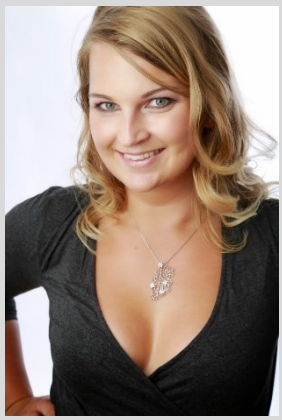
Making the change

As the frequency of cyber-attacks increases across all industries, CISOs have been thrust into the unfortunate position of trying to increase protection against a backdrop of reducing funds and resources. Solutions do not always have to come at a great organizational expense.

Encouraging open communication and identifying productivity-security touchpoints between employees and the C-suite can be fundamental in directing an organization's security culture in a positive direction.

Placing greater emphasis on the human aspect of cyber security can increase awareness and understanding surrounding cyber security best practices and protect organizations against damaging cyber-attacks. Keeping organizations safe is a complex problem. Keep these five tips in mind as you build iteratively towards a secure organization, from the bottom up.

About the Author



Dr Inka Karppinen is CybSafe's lead Behavioural Scientist, Cyberpsychologist and mixed methods Human-Computer Interaction (HCI) researcher.

Inka is interested in all aspects of helping people, which has led her on a unique path encompassing both industry and academia. She has a PhD and MRes in Security and Crime Science from the University College London (UCL) and MSc in Occupational Psychology from Birkbeck.

Her PhD was a multidisciplinary research investigation in a real-world organisational setting examining employee non-compliance with security procedures using human error/violation and behavioural economics frameworks. She specialised in various behaviour change models, training evaluation frameworks, persuasive technology and improving the organisation's security culture.

At CybSafe, Inka applies mixed methods research techniques to uncover people's cyber security attitudes and behaviours with an aim to design workable digital solutions. She loves narrowing the research gap between academia and practice creating a meaningful positive impact on people's cyber security behaviours. She is the lead researcher for CybSafe's yearly Oh Behave! Reports and lead researcher for the Home Office-funded project entitled: Cyber Security Quirks: Personalised Interventions for Human Cyber Resilience.

She is a Chartered Psychologist with the British Psychological Society (BPS), an Expert Fellow of the Security, Privacy, Identity, Trust Engagement NetworkPlus (Sprite+) and a Member of the Global Association of Applied Behavioural Scientists (GAABS). She is a strong advocate for bringing together people involved in research, practice and policy.

Dr Inka Karppinen can be reached on LinkedIn at Inka Karppinen, PhD CPsychol and at our company website https://www.cybsafe.com/.

From Passwords to Passkeys – A Passing of the Torch

The Promise and Limitations of 'Password-less' Authentication

By Tal Zamir, CTO of Perception Point

"Please enter your password."

For those without a password manager to keep track, that's a prompt that can be stressful, even panic inducing. But beyond the aggravation passwords often cause, the security that a password provides may no longer be worth the tradeoff. Circumventing a password, regardless of its supposed complexity, is often child's play for today's shrewd cyberthreat actors – and has been for quite some time.

In May, Google announced its decision to replace passwords with passkeys, the next phase of digital authentication that requires a fingerprint, a swipe pattern, PIN, or facial recognition to verify users' login credentials. With Apple and Microsoft gearing up for the same transition, password security will soon be, by and large, obsolete.

These security overhauls have taken precedence in response to surging credential theft, mostly via phishing attacks, which rose 50% worldwide in 2022 compared to 2021, largely due to the accessibility of hacking kits and new AI-enhanced phishing tools. By requiring a physical passkey, tech giants intend to make it far more difficult for attackers to gain unauthorized access to user accounts, even in the event that passwords and Multi-Factor Authentication (MFA) codes are compromised. This proactive approach aims to reinforce the security measures of tech giants and provide users with an added layer of protection against sophisticated cyber-attacks.

But passkeys are just one piece of the cybersecurity puzzle. While they're a promising next step, individuals and enterprises will still need to fortify their security posture even further if they hope to remain resilient against evolving threat landscapes.

A first step toward authentication security

Although not foolproof, 'password-less' authentication is a significant improvement over traditional password-based authentication. By using passkeys, users can set up a simple and easy-to-use system for logging into multiple accounts, without the need to remember complex passwords or decipher which password belongs to which account, offering a more convenient user experience. Moreover, passkeys eliminate the risks associated with weak passwords and password reuse, which are common unsafe practices. Shockingly, 85% of people use the same passwords across multiple sites, making them more vulnerable to hacking attacks. While password-less authentication does not guarantee absolute security, it goes a long way towards mitigating password-related risks.

The fact that physical passkeys are harder to steal or replicate than passwords or tokens has led the World Wide Web Consortium, FIDO Alliance, and Microsoft to promote passkeys as the future of user security.

As the transition from password-based authentication to passkey-based authentication gains momentum, it's crucial for users, employees, and security teams to bear in mind that the password-less approach isn't entirely immune to hackers. Despite the added security of physical passkeys, attackers can still find ways to exploit authentication vulnerabilities. Notably, there are numerous other threat vectors and hacking techniques that don't rely on passwords at all, so a passkey alone may not be sufficient to ward off determined attackers. Therefore, it's essential to remain vigilant and implement other security measures in tandem with passkey authentication.

For example, hackers leverage remote access trojans (RATs) to gain remote-control malware on infected devices in order to take over their apps and access data. Likewise, they can hijack sessions by stealing cookies stored on devices containing login tokens. Advanced social engineering attacks have also emerged as a significant threat. Threats like these, notably business email compromise (BEC), don't require credential theft, but are still just as concerning, given these attacks doubled in 2022 alone.

In some respects, cybersecurity with passkeys may leave users more vulnerable, considering that with passkeys, if a threat actor does gain access to a user's device, they can potentially access all the user's accounts and apps. This stands in contrast to passwords, where the attacker may only gain access to accounts with the same login credentials.

One change may not be enough.

Cyberattacks across the channels most used by businesses for communication and collaboration are growing increasingly sophisticated, with attackers using a range of tactics such as spear-phishing, domain spoofing, and AI-aided impersonation to convince their victims to take a specific action. And because these advanced attacks don't necessarily involve stealing passwords or user sessions, password-less authentication solutions, when made available, will ultimately be ineffective in preventing them.

Consequently, users and security teams must continue to adopt a multi-layer approach to effectively protect their companies. In addition to improving cybersecurity awareness training, organizations should strive to deploy modern security systems, such as advanced email security and web browser security, that identify and prevent the most advanced and evasive threats from ever reaching their users. Furthermore, the data from the security systems should be correlated to provide SOC and response teams the information necessary to rapidly analyze and remediate incidents,

Striving for a safer cyber-future

The migration towards password-less authentication will certainly be effective in mitigating security breaches. But it cannot be treated as a panacea. Rather, it will become another tool in the cybersecurity toolbelt – just one of many necessary security measures – albeit a crucial one.

Attackers will continue to look for and l exploit gaps even in password-less environments, and thus individuals and organizations alike must take a multi-layered approach if they wish to protect themselves against increasing cyber sophistication.

About the Author

Tal Zamir is the CTO of Perception Point, with a 20-year track record as a software industry leader solving business challenges by reimagining how technology works. He has pioneered multiple breakthrough cybersecurity and virtualization products and prior to joining Perception Point, Tal founded Hysolate, a next-gen web isolation platform operating at the endpoint level. Tal can be reached online at LinkedIn and at our company website.

From Samsung to the Pentagon - Recent Stories Remind Us About the Importance of Sensitive Data Guardrails

By Thomas Segura, Cyber Security Expert, GitGuardian

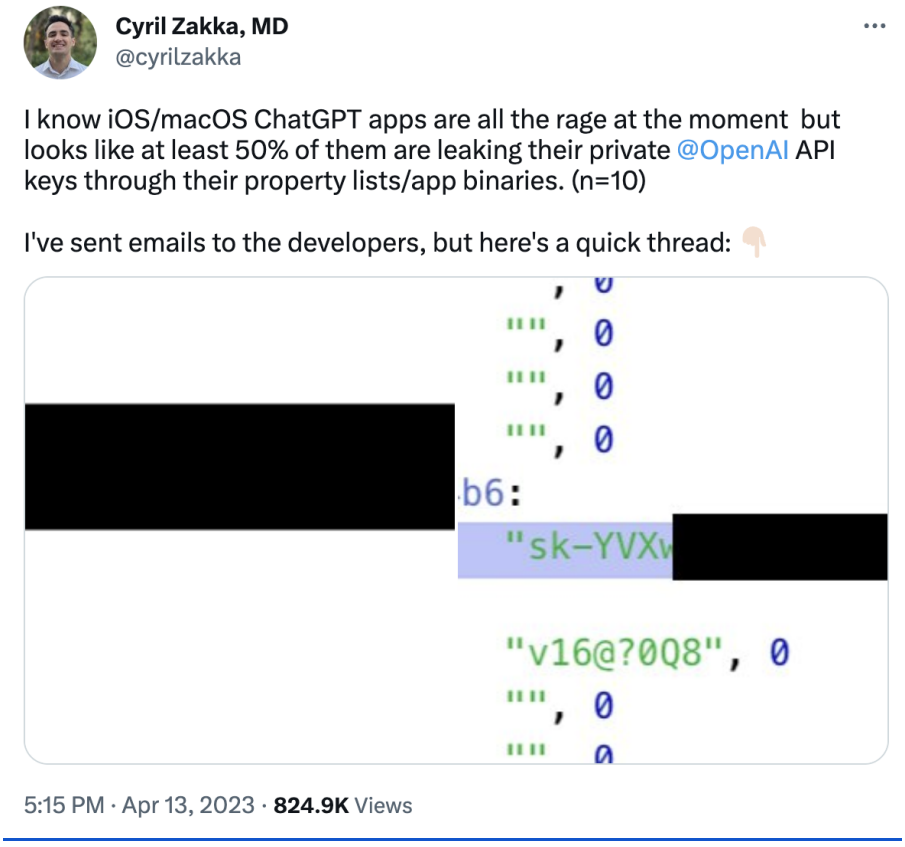
The last few weeks have been very challenging for data protection experts. In a very short period of time, several stories have dealt a blow to the efforts of businesses, consumers, and governments to protect sensitive data.

From a 21-year-old leaking classified military intelligence to Discord, to Samsung employees leaking corporate secrets to ChatGPT, to third-party developers rushing to develop OpenAI-based apps and leaking API keys in their code, all these stories have a lesson to remind us: the potential for sensitive data leaks is ever-present and necessitates fundamental protective measures within organizations.

Sensitive Data Exposure

One common thread among these stories is the human factor. In the case of Samsung, employees reportedly uploaded sensitive information to ChatGPT on three different occasions just three weeks after the South Korean electronics giant allowed employees access to the generative AI tool.

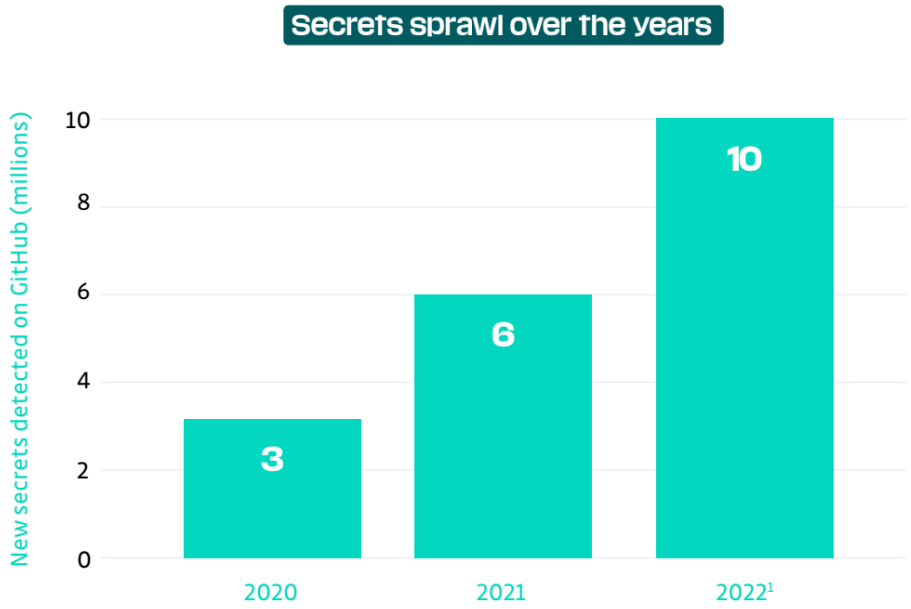
Similarly, third-party developers rushing to create OpenAI-based apps were storing API keys in plaintext, as revealed by Cyril Zakka on Twitter recently:



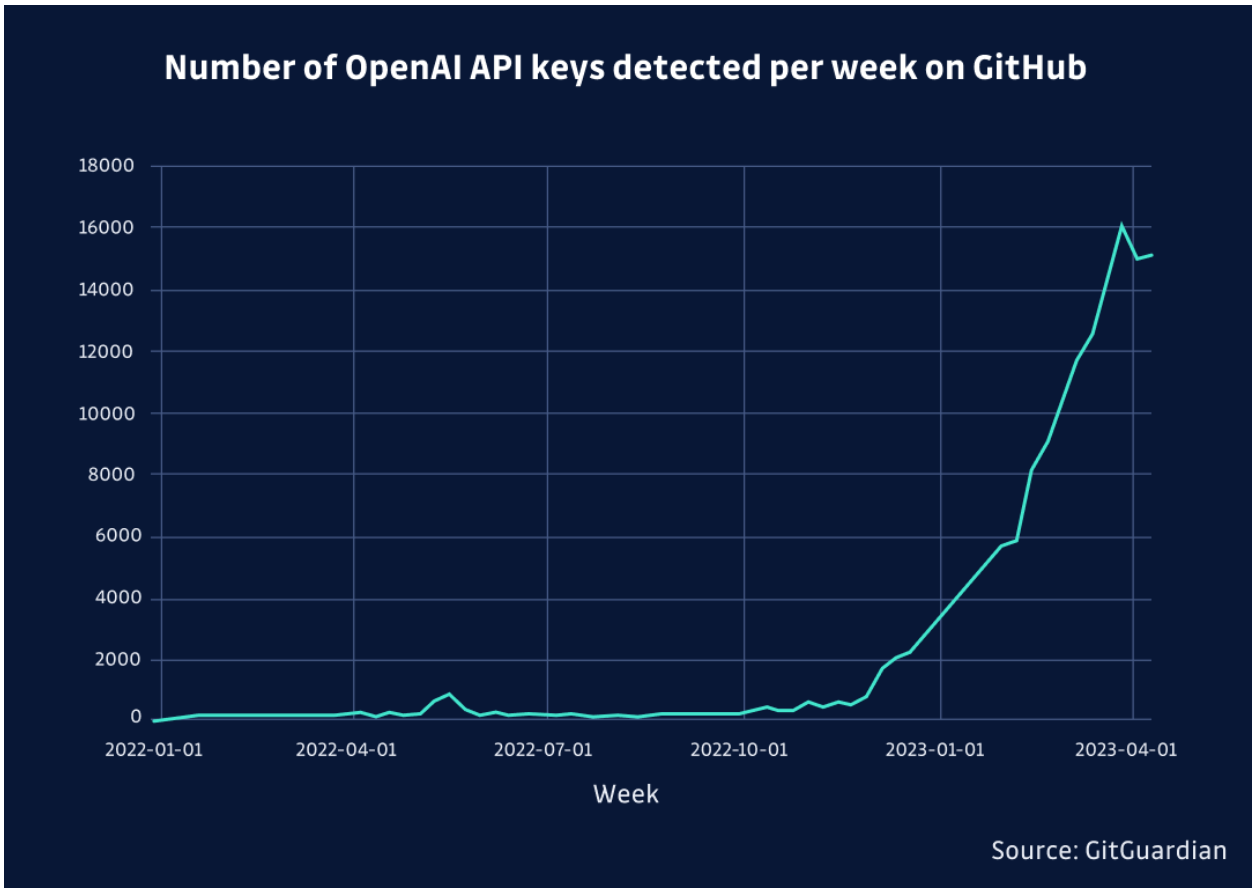
As highlighted in the thread, storing API keys within an application package "*makes it particularly easy to extract since they're made available in plain string without requiring any fancy tooling or much effort.*"

This is exactly what GitGuardian's State of Secrets Sprawl has been monitoring and reporting on for several years: the number of hard-coded credentials continues to expand at an accelerated rate. In fact, in its latest release, the report indicated an alarming growth of 67% year-over-year in the number of secrets found on public GitHub every year. GitGuardian detection engine scanned 1.027 billion new commits in 2022, finding 10 million secrets occurrences.

Secrets sprawl continues to expand worldwide.



If we zoom in to watch more specifically leaks of **OpenAI API keys** on GitHub, the results speak for themselves:



In short, when it comes to measuring the popularity of a red-hot new technology, such as OpenAI's GPT, one of the best metrics is measuring the number of related secrets leaked on public GitHub.

What is fueling this rocket? In the IT world, digital authentication credentials, such as the API keys we've been talking about, but also certificates and tokens, are the glue between applications, services, and infrastructures. These components are much more numerous today than they were a few years ago. Stacked together, they form the large majority of today's apps. For example, according to BetterCloud, the average number of software as a service (SaaS) applications used by organizations worldwide has increased 14-fold between 2015 and 2021.

Individuals working in the industry tend to casually insert sensitive information, such as secrets, directly into configuration files, scripts, source code, or even private messages by convenience. This practice of hard-coding secrets leads to a significant increase in what we call "secrets sprawl," where these sensitive pieces of information can spread across various code repositories as they are cloned or shared without proper protection.

Although these credentials leaks might not always represent an immediate threat, the growing number of secrets exposed on GitHub every year is a red flag highlighting the need for software-driven organizations to prioritize secure coding practices and keep sensitive information and secrets out of source code.

Increasingly Serious Consequences

Finally, as if we needed another reminder that sensitive data protection has real consequences, another recent event has shaken one of the most powerful institutions on the planet.

The "Pentagon leak," a case under investigation, refers to a massive leak of top-secret military intelligence on a private Discord server—a popular gaming chat platform— that spread through the web in early April. According to the press, the documents included some of the most sensitive information for the USA, such as Ukraine-Russia war prospects and thousands of intelligence reports. The incident is already having international repercussions, such as a heightened suspicion of eavesdropping from United States' allies.

Beyond questioning the advancement of technologies used to safeguard military secrets, the leaks are a bitter reminder that even the most robust security protocols can be compromised by human error or malintent.

Conclusion

The recent headlines about sensitive information leaks highlight the urgent need for organizations to prioritize protecting their sensitive data. From corporate trade secrets to classified government documents, no organization is immune to the risks of data leaks. The human factor is a common weak point in security protocols, making it crucial for organizations to prioritize employee training and secure coding practices.

In the field of software, programmatic credentials or secrets are one of the most sensitive data. As recent breaches have illustrated, their compromise can lead to a full takeover of an organization's IT systems.

GitGuardian, a cybersecurity company, specializes in identifying and preventing hard-coded secrets, providing organizations with the tools they need to keep their sensitive data safe. We believe that prevention is the best defense against data leaks. Using our platform, organizations can identify leaked secrets before they become a vulnerability, protecting their sensitive data and mitigating the risks of reputational damage, revenue loss, and legal liabilities.

Contact us today to learn more about how we can help protect your sensitive data and get a free complimentary audit of your secret leaks on public GitHub.

About the Author

Thomas Segura, Cyber Security Expert, GitGuardian. Thomas has worked as both an analyst and a software engineer consultant for various large French companies. His passion for tech and open-source led him to join GitGuardian as a technical content writer. He now focuses on clarifying the transformative changes that cybersecurity and software are undergoing.

Thomas can be reached online at our website: https://www.gitguardian.com/ or **Twitter**: https://twitter.com/GitGuardian and **LinkedIn**: https://www.linkedin.com/company/gitguardian.

How We Grew Revenue by Strengthening Cybersecurity

Make your security strategy good for business.

By David Weisong, CIO at Energy Solutions

Utility companies are, like just about all industries, increasingly concerned about cybersecurity—and for good reason. A malicious actor successfully infiltrating utility systems could potentially interrupt power delivery or critical processes, doing the kind of costly damage leaders in the industry have nightmares about. At the same time, utilities also face more mundane but no less threatening cybersecurity risks, including potential breaches of customers' sensitive personally identifiable information (PII) and location data.

Recent increases in the quantity and, even more dangerously, in the *quality* of maturing cyberattacks on utilities have leaders tightening security across their ecosystems. This includes requirements that external partners must prove security best practices via third-party validation. Utilities raise the bar on these requirements each year, and rightfully so: any shortcomings in the security regimens of the businesses they rely upon can ultimately leave their own systems and data exposed. Our consulting firm is one of those companies that work closely with utilities and often handles their sensitive data to implement market-facing energy efficiency and demand energy response programs. In the face of our

customers' ever-escalating requirements, we made the business decision to lean deeply into security, rather than merely keeping pace with necessary practices.

What we've found is that committing to modernized cybersecurity has unlocked a key competitive differentiator for our business, driven by our ability to demonstrate holistic protections, check every box on validation tests, and remove any doubt in the minds of utility leaders that we're the most secure partner they could choose.

You don't want to overspend on security (on duplicate technologies, for example), but the risks of not having a robust security strategy implemented are just too big to ignore. There's the financial cost of a data breach, and then there's often the bigger cost: long-term reputational damage. Those factors alone would have been enough to get the C-suite buy-in required for security modernization at our firm, but the other big variable was that a revamped cybersecurity stack would enable us to gain more clients. While that may not be true for every organization, it was a clear path for us and certainly made it an even more clear case that cybersecurity changes were going to be well worth the investment.

Here are three key steps we took on our road to implementing the cybersecurity practices that have driven business growth for our firm.

1) Start with an existing and proven cybersecurity framework.

Rather than reinventing the wheel when it comes to structuring a cybersecurity stack that achieves holistic protections, we found it far more effective to begin by using SOC 2 Type 2 certification as our framework. SOC 2 Type 2 certification is designed to require service organizations like us to properly secure access to clients' data and systems. It specifies security controls to assure that client data is secure, available, and private, while also carefully safeguarding processing integrity and user confidentiality. By enforcing SOC 2 Type 2 compliance as our own standard, we have an organized structure for methodically providing any security protections our utility customers could need.

2) Introduce encryption and access controls aligned with your framework.

In our case, our existing encryption and access control tooling and practices weren't up to modern standards—a fact that's true of most vendors in our industry and beyond. Pursuing SOC 2 Type 2 certification meant replacing implementations of our Microsoft BitLocker and Apple FileVault encryption key management tooling. While BitLocker and FileVault are capable of effectively securing data at rest, they have a relative lack of management options and require a high degree of manual effort to operate.

We launched a search for encryption and access control that could provide finer control and robust automation to make our security protections more proactive and effective. In our case, we landed on BeachheadSecure, which takes a zero-trust approach to delivering encryption and access control. We now prepare automated responses to myriad risk conditions that might arise, so that we have an action plan already in place. For example, any PC, Mac, phone, tablet or USB device that holds our customers' data will have access automatically removed if it leaves an approved geofenced location, or if a pre-set

number of failed logins occurs. Importantly, we also now have automated compliance reporting whenever our security practices are audited.

3) Secure endpoints with modern protections.

To defeat both file-based and fileless script attacks upon our clients' endpoints, we leveraged several Webroot security products including Webroot SecureAnywhere. To prevent inbound malware and other DNS-based attacks, we chose Webroot DNS protection to provide threat intelligence and filtering automation that block risky domain requests. Finally, Datto RMM equips us with efficient remote device monitoring and management across the cloud. Remote endpoint security capabilities now allow us to deliver more effective security management and support.

Better security can grow your business

With the right security strategy in place, we are able to meet—and, importantly, exceed—the security mandates that many of the utilities required of us. Utilities regularly update their cybersecurity requirements and questionnaires to account for the latest protocols and an ever-changing IT environment. We have little, if any, influence to modify any client requirements to be considered a vendor. You must either accept and meet the full scope of the heightened security standards, or seek business elsewhere. Our cybersecurity investments aligned us squarely with the former, and the ROI case for doing so has been stellar.

Out-securing the competition has given us a distinct advantage in securing new customers, and our path is one that others can follow. Do so, and customers will regard your business as a singular source for their complete technology and security requirements, and one worthy of a long-term partnership.

About the Author

David Weisong is the CIO at Energy Solutions, a clean energy solutions firm. Energy Solutions combats climate change through market-based, cost-effective energy, carbon, and water management solutions that make big impacts. For over 25 years, Energy Solutions has been pioneering end-to-end, market-driven solutions that deliver reliable, large-scale, and cost-effective energy savings and carbon reduction to our utility, government, and private sector clients across North America. David can be reached via LinkedIn (https://www.linkedin.com/in/davidweisong/) and at https://energy-solution.com/.

Hybrid Mesh Firewall Management

By Ulrica de Fort-Menares, VP of Product & Strategy, Indeni

What is Hybrid Mesh Firewall?

With the rise of hybrid workforces and cloud networks, there is growing demand to secure on-premise environments, multiple cloud environments and remote users with firewalls. As a result, vendors are introducing multiple firewall deployment types, including FWaaS and cloud firewalls. Hybrid mesh firewalls are platforms that help secure hybrid environments by extending modern network firewall controls to multiple enforcement points, including FWaaS and cloud firewalls, with centralized management via a single dashboard.

Hybrid mesh firewalls do not necessarily mean that you have to buy your firewalls from a single vendor. In fact, many enterprises continue to choose from best-of-breed vendors for specific use cases. For example, they may choose FortiGate for the remote sites because of the integrated SD-WAN and firewall functions. For the data center, enterprises have Palo Alto Networks NGFW and Check Point Secure Gateways. In enterprises' cloud environments, they have Check Point CloudGuard Network Security. For

remote users, they have Zscaler Private Access to protect user traffic from anywhere. In many cases, enterprises have a multi-vendor strategy in their environment to avoid vendor lock-ins. Incidentally, the latest Magic Quadrant for Network Firewalls indicated that enterprises are experiencing frequent increases in the prices of network firewalls causing dissatisfaction. This is another reason why many enterprises insist on a multi-vendor strategy. Besides, buying from the same vendor doesn't guarantee simplicity and centralized management.

Demystifying Unified Management

Unified management is the most critical capability of a hybrid mesh firewall. If you need multiple dashboards for your data center, remote site and cloud firewalls, you don't have a hybrid mesh firewall. Unified management can mean different things to different people. It is certainly an interesting topic for hybrid mesh firewall with its several deployment types. There are additional dimensions such as multiple administrative domains and more personae to consider. Let's explore the different deployment types to understand what unified management means:

#1 - Conventional On-Premises Firewalls

Unified management for on-premise firewalls is generally well understood. These firewalls are under your administrative domain. You should have a single dashboard to manage your data center and remote site firewalls.

#2 - Cloud Firewalls

For cloud-based firewalls, they can either be under your administrative domains or they may be managed by your providers. For the former, you should treat them like your on-premise firewalls and manage them from a single dashboard. For the latter, it is a firewall as a service (FWaaS) that you purchase from a third-party or cloud service provider like AWS. See the next section for requirements.

#3 - FWaaS

It may sound like a bit of an oxymoron, but unified management for FWaaS that is not managed by you warrants some clarification. In this case, although you don't manage the firewall, you want to ensure the provider's firewalls are working. You expect them to detect issues before they cause disruptions. You need to ensure the necessary components on your side that are connecting to the service are working to avoid finger pointing. The primary requirement is visibility to the FWaaS availability.

#4 - Securing Remote Users

This type of firewall secures user traffic on mobile devices or personal computers from anywhere. You deploy an agent on the device to ensure traffic is sent to the cloud-based firewall for inspection. These firewalls control which SaaS and on-premise applications are available to the users. Effectively, this is another form of FWaaS that is not managed by you. This solution is also known as Secure Access Service Edge (SASE).

This is where additional personae come into the picture. Firewalls are typically managed by the infrastructure team. This FWaaS is a remote access service running on Windows, Mac, iOS or Android. Traditionally, the infrastructure team does not cover support for endpoints. It typically falls into the lap of the endpoint team who are accustomed to dealing directly with end users. The interesting question is, what does unified management mean for this FWaaS deployment type that spans multiple teams and device types? From the infrastructure team perspective, they need to ensure the data center is connected to the cloud-based firewall service so that remote users can access on-premise applications. The infrastructure team is typically not responsible for SaaS applications, nor are they directly responsible for the end users.

Summary

Let's summarize unified management for hybrid mesh firewalls in a multi-vendor environment. Specifically, we are looking at it through the lens of the infrastructure team.

Firewall Deployment Type	Is it under your administrative domain?	Requirements (Infrastructure Team)
On-premise (data center & remote office)	Yes	A single dashboard to manage your firewalls
Cloud-based firewalls from network security vendors	Yes	A single dashboard to manage your on-premise and cloud-based firewalls
FWaaS - Cloud-based firewalls from Cloud Service Providers (e.g. AWS, Azure)	Partial (shared responsibility model)	Ensure your management platform integrates with these firewalls, at a minimum you want visibility to firewalls availability
FWaaS connecting your remote offices from network security vendors	No	Ensure components connecting your data center and the service are functioning (e.g. GRE tunnel, IPSeC tunnels, App Connector)

		Visibility to FWaaS availability
Remote Access for users	No	Ensure connection between your data enter and the firewall service is functioning Visibility to FWaaS availability

I hope this gives you some insight into what unified management means for hybrid mesh firewall deployments.

About the Author

Ulrica de Fort-Menares is the Vice President of Product and Strategy at Indeni with over 30 years' experience developing software in networking and security technologies. She loves explaining complex technology and building high-profile and high-performance teams.

Ulrica can be reached online at our company website http://www.indeni.com/.

Implement Machine Learning to Secure Your IoT Network

By Zac Amos, Features Editor, ReHack

Connected devices pose unique security risks and are prone to bot attacks, requiring a tool capable of quickly processing a large amount of information. A machine learning model can rapidly react to attacks, making it an ideal choice for protection. An organization can implement it to secure its IoT network through threat detection, recognition and response.

Vulnerabilities of an IoT Network

More organizations are incorporating IoT devices, and concerns over network security grow because that brings additional vulnerabilities. It expands their connectivity at the cost of creating new surface areas for attackers to target. Implementing a security model is complex because the devices often lack basic security features.

Cybercriminals can exploit the connectivity with distributed denial of service (DDoS) attacks by overwhelming them with excess requests. For example, a single DDoS attack from 2022 lasted only 30 seconds but created 17.2 million requests and came from over 20,000 bots. Integrating IoT devices for businesses can be beneficial, but they need enhanced security.

1. Threat Monitoring

Most machine learning algorithms make predictions without long-term reasoning or real-world interactions, so they're taught through the supervised learning of a data set. It can be fed information on previous cyberattacks or the current IoT network to establish how it informs its decisions. It can then identify patterns and make logical conclusions.

Many organizations use machine learning models to monitor and detect attacks because they can train on the huge amount of data IoT devices produce. They collect information in real time, so actions are well-informed and accurate. ML pays attention to anomalies and can send alerts if it finds a threat while monitoring.

2. Secure Data Collection

Previously, data leakage of sensitive consumer or user information was a growing concern with IoT and machine learning. However, that's no longer the case with federated learning. It is a machine learning technique where algorithms are trained to access IoT device data without exchanging information, meaning there isn't a central data set it uses to store any.

Federated learning allows machine learning to occur securely because the data is unidentifiable and doesn't need to be accessed directly. Its decentralized nature ensures its protection. In addition, its actions are more secure since the model is informed by safe data collection.

3. Incident Response

Machine learning can secure IoT networks through incident response. It sends alerts once an attack occurs and creates defensive patches without human input or intervention. Since it reacts in real time, it can respond to a threat much faster than a human would.

4. Threat Recognition

A machine learning algorithm analyzes data sets and identifies patterns to rapidly detect a cyberattack. Once it recognizes actions similar to the data, it classifies it as a threat. Since it can quickly identify potential cyberattacks, the response time for dealing with them will be much faster.

5. Patching and Updating

IoT devices are often unprotected, making it easy for attacks to access them. People don't tend to treat them as a security threat since they're regular machines, but they're more open to cyberattacks when not patched or updated properly. Machine learning can also ensure continuous security for an IoT network because it can address weaknesses as soon as it detects them.

A predictive model can use past data to determine the best solutions for each vulnerability without human input. Essentially, it mimics decision-making and fixes each one using its extensive knowledge. It can continue working in the background to repair security gaps before they're a known issue or leave the final decision up to the cybersecurity team.

6. Risk Assessment

A machine learning model offers insights into a network's security based on the data it collects. While it can use past information to inform its current decisions, it also can enhance traditional risk assessment by collecting real-time data from IoT devices.

Machine learning can be embedded at the edge of an IoT network to offer predictive and intelligent risk analysis for devices. It continuously assesses everything and can warn of concerning changes. The result is heightened security since it provides awareness about the current state of the IoT network.

7. Risk Prediction

Since machine learning is capable of rapid analysis, it can detect patterns and make inferences at speeds people cannot match. It's not constrained by human processing limits and doesn't require much time to think or analyze.

Cybersecurity threats constantly evolve, so accurate manual risk prediction would take too long. Around 99% of cyberattacks are created by making minor alterations to previous attacks to create something new that appears nonthreatening. Therefore, they're treated as harmless traffic through an IoT network. A machine learning model can combat this with risk prediction.

With continuous data collection, it can learn the preferences of attackers and align them with potential system vulnerabilities to find likely targets. It can then logically conclude when the next attack will occur. Ultimately, it can improve the resiliency of an IoT network against attacks.

Secure IoT Networks with Machine Learning

Connected devices are prone to bot attacks that quickly overwhelm them, so a rapid detection and response tool is necessary. Machine learning models can accurately predict threats, patch vulnerabilities automatically and respond to incidents without human intervention. They can secure IoT networks in multiple ways to enhance security.

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.

Measuring the Effectivity of Security with Data Analysis

By Howie Robleza, Freelance Writer, Avigilon

Effective security strategies are fundamental to the success of any business with both physical and cyber security of equal importance. Businesses, even with the most brilliant ideas or superlative products, will not succeed and survive if a secure working environment is not maintained and sensitive information and data are not protected. Profit, customer relations, and potential expansion can all be sabotaged by lax security.

The Need for Security Evaluation Tools

The digital revolution has undoubtedly facilitated industry and commercial entities in their operations, but it has also opened the door to a new generation of security challenges. Scams and viruses are constantly attacking business operations while hackers are developing new methods for penetrating security

processes making online security among the top priorities for companies. Security data analysis is one very effective tool for the evaluation and verification of the effectiveness of security protocols.

The inevitable integration of physical and cyber security strategies has brought a new series of control challenges. Integrated security methods can benefit significantly from data analysis evaluation from building security cameras to sensitive data storage. Many companies will hire data analysts to identify anomalies and vulnerabilities in security processes. They then implement security protocols to address these challenges, but with today's evolving technology, security processes must be measured for their continuing effectiveness. Companies need to ensure that security protocols function well.

How Are Security Controls Measured for Effectiveness Using Data Analysis?

There are several methods for evaluating if security systems work and if and how they can be improved.

Track Incidents, Response Times, and Results

The data analysis of incidents is one of the more important and efficacious tools when judging security protocols for their effectiveness. Incidents happen in many forms, from an employee not being able to access an email account to corruption observed on company devices. Incidents can supply important information such as how quickly the incident was reported, how quickly the problem was addressed and resolved, how the problem was resolved, and how often the problem or incident occurred. By analyzing risks and results more effective strategies can be developed for the future by identifying vulnerabilities and patterns.

Make Use of Security Audits Against Company Servers at Regular Intervals

Cybersecurity audits function as fake attacks on your company's business operations. They should be managed by security risk experts. These simulated cyberattacks are intended to identify weaknesses in software used and in servers. Often viruses or malware appear in the form of phishing, emails, and website links that infiltrate and access company data, corrupting it. Hackers may introduce ransomware to block data and extort money. Weaknesses and potential entry points must be eliminated.

Check Entitlements and Permissions

Many businesses concede access to various types of information through their websites to clients. They are also supplied to company employees and team members. Known as entitlements and permissions, these become potential security risks. If these permissions are violated, hackers can obtain access to company systems and data which can then be used for gain. All entitlements and permissions need to be verified and evaluated to protect them from hacking.

Assess Employee Risks and Conduct Regular Training

The weakest link in any organization is the employee pool. Often hackers will prey on employees to access a company's business servers. With proper training, employees can offer an important line of defense and contribute to increasing company security. Employees should be educated on all security matters and protocols pertinent to their work.

Risk assessments of employees are an important factor in ensuring security. When monitoring employees through data analysis regarding incidents, some employees may be identified as experiencing more frequent incidents. This should be analyzed in relation to their workflow. These employees may need better training on security risks and protocols to protect the company. High-risk employee behavior needs to be identified and mitigated. Guidelines for security protocols should be provided to team members with instructions on how to handle emails from unknown sources as well as links to unknown websites. This will aid in limiting the risks that hackers will be able to access your company's sensitive data.

Security Effectiveness Is Vital to Business Success

Company success and expansion are just as dependent on security and safety measures as on the quality of the services and products it provides. Measuring the effectiveness of security protocols will aid management in identifying vulnerabilities and anomalies in security risk management and correcting them. This will increase customer satisfaction as clients prefer to work with companies that have high levels of security to protect sensitive data.

Security procedures need to be constantly overseen, re-evaluated, and updated as a proactive method for maintaining company safety. This is especially important for small businesses that are often targeted because they invest less in IT security. All businesses, from small family ventures to large corporations must invest in cybersecurity and then constantly check its effectiveness to guarantee survival as much as success.

About the Author

Howie Robleza, a freelance writer is interested in tech, legal, and property trends. When she's not writing, she works in commercial property management.

Howie can be reached at www.avigilon.com.

Network Architecture Mapping Improves Security Posture and Saves Big Bucks

By Matt Honea, Head of Security and Compliance, Forward Networks

The challenge to adequately secure a large complex enterprise network, including the infrastructure and critical data assets, continues to plague CISOs. The cost, the breadth, the shortage of skilled security professionals, fast-evolving tech stacks and integrations, cloud migration are all headwind examples. For some CISOs, especially those in industries with high degrees of risk such as financial services and healthcare, conversations begin with the technology. For others, it's the security budget. Enterprises are struggling to figure out exactly how big their network is, where their assets are, and how much security an arbitrary amount of data is going to cost to protect. It's an overwhelming undertaking.

Visibility and Scalability

For effective security tool planning, the CISO needs visibility and monitoring capabilities across cloud, hybrid, and on-premises environments to understand the scope of the infrastructure and

data. An accurate network architecture map serves as a blueprint and provides visibility to identify assets, risks, and redundancies.

For example, a network architecture map can detect how many devices are connected to the network and areas of the network or data that may be at risk. It can also reveal firewall redundancies, which when eliminated reduce operational costs. This level of granular network visibility empowers enterprises to scale their architecture with more precise insight across any and all environments, maximizing efficiencies and reducing costs.

Developing a map or digital twin of a network is also much less expensive than buying multiple solutions piecewise. Both security and network teams can track devices as the number of systems increase or decrease, enabling organizations to know what they need to secure and, therefore, pay for what they use versus buying unnecessary, expensive servers. This dramatically reduces migration costs and outages. Minimizing downtime maximizes revenue for most organizations.

Cloud Security and Asset Management

A network architecture map will also improve cloud security and asset management. For example, when an organization has an accurate and up-to-date inventory of devices and how they are connected to the network, rogue devices are detected faster. Incident response becomes easier as the enterprise gains a full account of its processes and technologies and can more easily detect and pinpoint issues.

This becomes more complex in a multi-cloud environment. Imagine an enterprise with AWS, Azure, and GCP environments. Without a network architecture map, the organization must go into each cloud map and overlay them with the architecture. This is 3x the work versus having one map that can represent all cloud, hybrid, and on-premises environments, globally.

Inventory management fails to account for a high number of devices with stripped down operating systems. An architecture diagram may reflect servers but doesn't account for firewalls, routers, and switches. Knowing this, attackers go after these devices because they're generally unpatched, they're easier to exploit, and teams aren't looking at them.

In fact, Cisco recently released information that its devices were being targeted by Russian-backed hackers and urged customers to start patching them. Nation-state-backed activities are often mimicked by other hackers, which compounds such risks. Having a complete inventory of assets dramatically improves an organization's ability to identify and remediate threats, especially across a global, multi-cloud environment.

Compliance and Visualization

Industry-specific and geographically driven legislation is also adding to the complexity and cost of securing enterprise networks. In addition to HIPAA, PCI DSS, SOX, and the like, Europe, North America, and Asia have issued or soon will issue local privacy acts and compliance regulations. The California Consumer Privacy Act (CCPA) now has an affirmative obligation to have reasonable

security, which includes, among other things, patch management, adequate logging and timely notifications of incidents.

Most security budgets today don't account for new legislative requirements. And new legislation doesn't account for the actual economic cost of moving and retaining data and duplicating infrastructure to meet compliance requirements. This exponential data growth means organizations now have an estimated 3x surface area to monitor and secure.

Eventually, organizations will be required to prove to regulators that they have control of their data. A network architecture map or digital twin can efficiently convey what systems are in place, how access is controlled, and what measures are protecting the attack surface on a global scale. A network map provides a detailed visualization region by region of what is connected and what technologies and processes are in place to secure critical assets. This level of visibility is crucial to managing, maintaining, and protecting an evolving and highly complex network.

How to Frame the Security Budget for Cloud

As organizations begin to grasp the technology and financial impact of new legislation, they will likely need to revisit their security budget. This is a good time to hit the reset button. The security budget for the cloud should be proportional to overall cloud spending.

Unfortunately, it's more common to find security budgets that are proportional to, say, engineering costs or that are historically earmarked to account for around 5% of the total IT budget. This was fine back in the day. But today cloud costs can be tens of millions of dollars per month because systems are completely hosted in IaaS.

Enterprises need to take some time to evaluate their security posture next to their business risk. Two common areas that come up are related to Cloud Security Posture Management (CSPM) and Identity and Access Management (IAM). Both focus on patching systems and maintaining proper access to systems. Attackers love rooting around for these types of vulnerabilities, hence why they are a major cause of breaches.

Map the Journey to a More Secure, Cost-Effective Network

Most wouldn't attempt to drive across the U.S. without some sort of mapping system. Why? Because wrong turns mean delays and additional costs. Developing a secure enterprise network architecture also requires a map to navigate existing resources, find assets, identify redundancies and risks, and determine what security layers make sense to protect the network and meet compliance regulations.

Every CISO is wrestling with data security, attack surface management, inventory management, and authoritative data. An accurate network map gives security professionals the visibility they need to implement processes and technologies that best protect the network on-premises and in the cloud and prove compliance. With this direction, enterprises will dramatically improve their security posture and save big bucks.

About the Author

Matt Honea is Head of Security and Compliance for Forward Networks where he is responsible for leading the organization's security practice and is focused on helping customers achieve accurate visibility of the entire network across on-prem, hybrid, and the cloud.

Matt has decades of experience as a security professional and leader. Most recently, he served as Head of Security for SmartNews. He also spent time at Guidewire Software as Senior Director of Cybersecurity, the U.S. Department of State, Foreign Service, as Chief of Technical Analysis and Special Operations, and as Security Engineering Officer, and Ziguana as Co-Founder, Developer, and Designer. In 2019 he was named to Silicon Valley Business Journal's "40 under 40" list.

OT Under Greater Scrutiny in Global Cybersecurity Regulatory Environment

By Dr. Terence Liu, CEO, TXOne Networks

Highly publicized cyberattacks have focused governments globally on re-examining and bolstering their cybersecurity regulations and policies, and it's not just information technology (IT) under heightened scrutiny. The Colonial Pipeline ransomware attack in the United States, disruption of regional petroleum trading via attacks on refineries in Belgium and the Netherlands and Russia's cyberattack on the U.S. satellite company Viasat in the early stages of the invasion of Ukraine are among the events to have galvanized regulators' attention on operational technology (OT).

Indeed, evidence of the intensified government regulatory focus on OT cybersecurity is found in markets worldwide, as agencies seek to thwart hackers in their targeting of urban power, water supply, corporate and personal data security and other critical resources.

United States

In the United States, for example, President Biden in 2021 signed both Executive Order 14028 "Improving National Cybersecurity," which for the first time emphasized that protection and security must encompass both IT and OT, and the National Security Memorandum, which established a voluntary initiative to foster collaboration among the federal government and the critical infrastructure community in adopting minimum cybersecurity standards of industrial control systems (ICS) and OT.

The following year, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act, providing legal protections and guidance (e.g., cyber incidents must be reported within 72 hours; ransom payments, within 24 hours). Also in 2022, the U.S. Transportation Security Administration introduced performance-based directives to boost cybersecurity in the aviation, pipeline and rail sectors, as well as performance goals to illuminate the value of investing in cybersecurity.

The U.S. government, furthermore, passed bipartisan law to encourage cybersecurity investment in the modernization of infrastructure, such as providing for stronger network protection in expansion of the nation's stations for electric-vehicle charging. The same legislation introduced the first cybersecurity grant program for state, local and territorial governments to invest in digital security as high-speed Internet is rolled out to underserved areas of the nation.

European Union

A landmark moment in regulation of EU cybersecurity management came in 2016: announcement and implementation of the Security of Network and Information Systems (or, "NIS Directive"). In response to increasingly serious cyber threats, the European Commission (EC) proposed NIS 2 Directive, an amendment to address the new and future threat landscape and to align with the post-COVID-19 and 5G eras.

Critical infrastructure such as energy systems, medical networks and transportation services get the majority of attention in the proposed upgrade. The scope of regulated objects in NIS 2 Directive is expanded to include additional management agencies, such as district heating and cooling facilities, hydrogen energy-related agencies and government administrative departments. It also establishes a response center, "EU-CyCLONe," to aid EU countries in their monitoring and responding to cyberattacks.

Furthermore, in 2022, the EC proposed the Cyber Resilience Act (CRA) to boost cybersecurity of digital products and streamline the EU regulatory framework. Applying to all digital products directly or indirectly connected to another device or network (and stipulating potential penalties of up to €15,000,000 or 2.5% of a manufacturer's global annual revenue), CRA could turn out to be one of the most significant EU cybersecurity laws.

Japan

Evolution of Japan's National Security Strategy is in keeping with the rest of the world in its increasing emphasis on securing critical infrastructure and ICS. The version released in 2022 stresses the

importance of boosting Japan's response capabilities—to the vanguard of national competencies globally—in terms of safe and stable use of national cyberspace and especially key infrastructure.

The measures specifically outlined in the latest version of Japan's National Security Strategy include:

- Creating a means to continuously assess the security of and manage vulnerabilities in government agency information systems
- Improving responses based on lessons learned from the most recent cyber threats
- Introducing "active cyber defense" to avert serious potential cyberattacks
- Enhancing cybersecurity information collection and analysis
- Establishing a network for public and private information sharing, detecting attacks and initiating countermeasures
- Reorganizing the National Cybersecurity Incident Preparedness and Strategy Center (NISC) to coordinate cybersecurity policy
- Aligning with other countries to strengthen information collection and analysis, attribution and publication and to develop international frameworks and rules

To the last point, Japan's Ministry of Economy, Trade and Industry (METI) has struck agreements with the Ministry of Industry of the Republic of Indonesia, the Ministry of Industry of Thailand and the U.S. Department of Homeland Security to cooperate in areas such as ICS security.

Smart industrial safety is one of Japan's primary areas of focus. The Industrial Cybersecurity Research Group was launched in 2017 to identify cybersecurity challenges faced by Japanese industry and to promote relevant policy responses. Furthermore, METI has established working groups and published guidelines for the cybersecurity and physical security of the country's buildings and plant systems.

Conclusion

With varied threat research data confirming that OT-focused cyberattacks are growing more prevalent globally, OT cybersecurity awareness and adoption also are climbing. Regulations and standards are bringing consistency to both cybersecurity execution and quality across critical infrastructure and strategic, nation-sponsored industries.

The success of this effort also will depend on a respect for the unique complexities of the OT world and developing a specialized approach, as opposed to merely adapting IT solutions for the operational environment. Proactive defense strategies such as supply-chain security, asset inspection, endpoint detection and threat intelligence, network segmentation, vulnerability management, patching and continuous monitoring undergirded with OT zero-trust solutions will be necessary for organizations everywhere to better avert or respond to OT cyberattacks and achieve the higher degree of cybersecurity that their national governments seek.

About the Author

Dr. Terence Liu is the chief executive officer of TXOne Networks, the leader of industrial cybersecurity. He started his career at Broadweb, where, as CEO, Terence defined and created the company's Deep Packet Inspection products and business, winning numerous leading networking and security vendors as customers. Then, following its acquisition of Broadweb in 2013, Terence served as Trend Micro's vice president. He led the company's Network Threat Defense Technology Group, expanding the company's footprint into the telecommunications network and extending protection for IoT devices and services from on-premises to the edge and the core. Since 2019, Terence has led TXOne Networks, which offers cybersecurity solutions that ensure the reliability and safety of ICS and OT environments through the OT zero trust methodology. TXOne Networks works together with both leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense. Terence can be reached at https://www.linkedin.com/in/rongtai/ and https://www.txone.com/?utm_source=CyberDef.

Out from the Shadows: SOC Teams Take Their Seat with the "Superheroes"

By Karthik Kannan, Founder and CEO, Anvilogic

Watch any superhero movie and it follows the same playbook: the story revolves around the superhero, at the midpoint of the movie there is a fight scene where the superhero fights the villain and saves the day. There is widespread destruction. The superhero "saves the day" and then heads home. They had one mission: to stop the villain.

What next?

The movie ends, but we don't think about the real work that begins next: figuring out where to start and re-building the city and building the process to bring the people back to the city. It takes a lot more effort, and a lot more than one "hero" to rebuild the city. We celebrate the superhero with the "S" on their capes. The S should stand for "security", the unsung heroes working through the year to prevent the attacks or rebuilding the city to make it stronger than before after a battle.

The folks that come out to rebuild and the ones that assess how the villain got in, in the first place. They are the people that work behind the scenes every day of the year to prevent attacks from occurring on a regular basis. They may not wear a cape; they may not make it into the "movie" and they often don't even have a seat at the table with the other superheroes. Sometimes, they are even thought of as a "cleanup crew." Truth is, without the team members working in the SOC (Security Operations Center), no one would know how the villain got in and how to prevent it from happening again, the villain could have overtaken the city, and the city may not have been able to be rebuilt.

Today, we celebrate these unsung heroes, shine a light on what they are doing from the trenches and what they need from their teams (the ones who are in the spotlight) to be successful.

Why are These Heroes in the Shadows?

Not all villains take out cities in the same way. It is the SOC teams who understand who the different villains are, what they do, how villains influence other villains and may use exploits from other hacker groups. It is not always obvious where the entry points are and the vulnerabilities could be. Sometimes people just doing their jobs unknowingly create entry points, like through a phishing attack. It is the SOC teams who set up parameters without which the cities could have seen a lot more

destruction and impacts on the most critical infrastructure. It is the SOC teams that makes the best out of a bad case scenario. Cool new security tools come out all the time. And even if a superhero has a full toolbelt of tools, there still needs to be training and understanding of how or what to use. It's the SOC teams that work to help delineate what tools are needed and when to use them.

In this story it's the superhero that should be the one preventing more security breaches to make sure villains don't get in, and in the rare event that they do, studying how they got in and their attack patterns to ensure that the city can be rebuilt faster and more fortified against future threats. So, why are these heroes the "unsung heroes"? How did they get into the trenches? They have two problems:

● They do everything from the "task-based" work, to transforming security architecture to staying up on the latest threats while also pivoting based on different business priorities to help keep organizations stay safe from attacks. Since security teams work around the clock and have to spend most of their time on low-level tasks that should be automated, their burnout leads to high- churn that leads to loss of knowledge transfer and only perpetuates this cycle.

● The second problem is a lack of understanding of what they do by the C-suite and line of business executives. They often (60% of the time according to a recent survey of decision makers responsible for threat detection) don't recognize, or underestimate, the role of SOCs in mitigating business risk and helping drive business success.

If SOC teams are empowered with ways to do their jobs more easily, they wouldn't be stuck on cleanup. Teams that can leverage automation to help with the detection lifecycle they wouldn't be able to keep up with trending threats and reduce the time it takes to detect and threat. While hackers are working 9-5 to gain access to an organization's infrastructure and gather information to exploit, SOC teams are only

able to focus a third of their attention on attack mitigation. This means that they are sometimes going to lose the battle to attack groups.

There's an idea of security being a bottleneck (like when they email you to change your password), but it doesn't have to be this way. Security can join forces with all the superheroes to do an even better job protecting the city (your company). How do we ensure that the "unsung hero" is able to win more battles against the attack groups, and come out of the trenches to be seen as a strategic partner to the C-Suite?

The Dollars are in the Detections - Helping the Unsung Heroes Soar

The right detections can make the unsung hero soar. There are currently trade offs in SOCs being made between getting things out faster and good detections. And, according to the threat detection decision makers survey noted before, more than three quarters (77%) desire new ways to engineer detection rules. The right detection engineering platform can be a lifeline in the trenches and simultaneously the rope that pulls security teams out of the periphery and into the forefront where the C-suite can recognize their contributions and achievements.

Detection engineering is the facet of security operations that the C-Suite cares most about. With the right platform in place and using AI in concert with security professionals, security teams can do their jobs faster, do their jobs better and let the platform handle the cleanup.

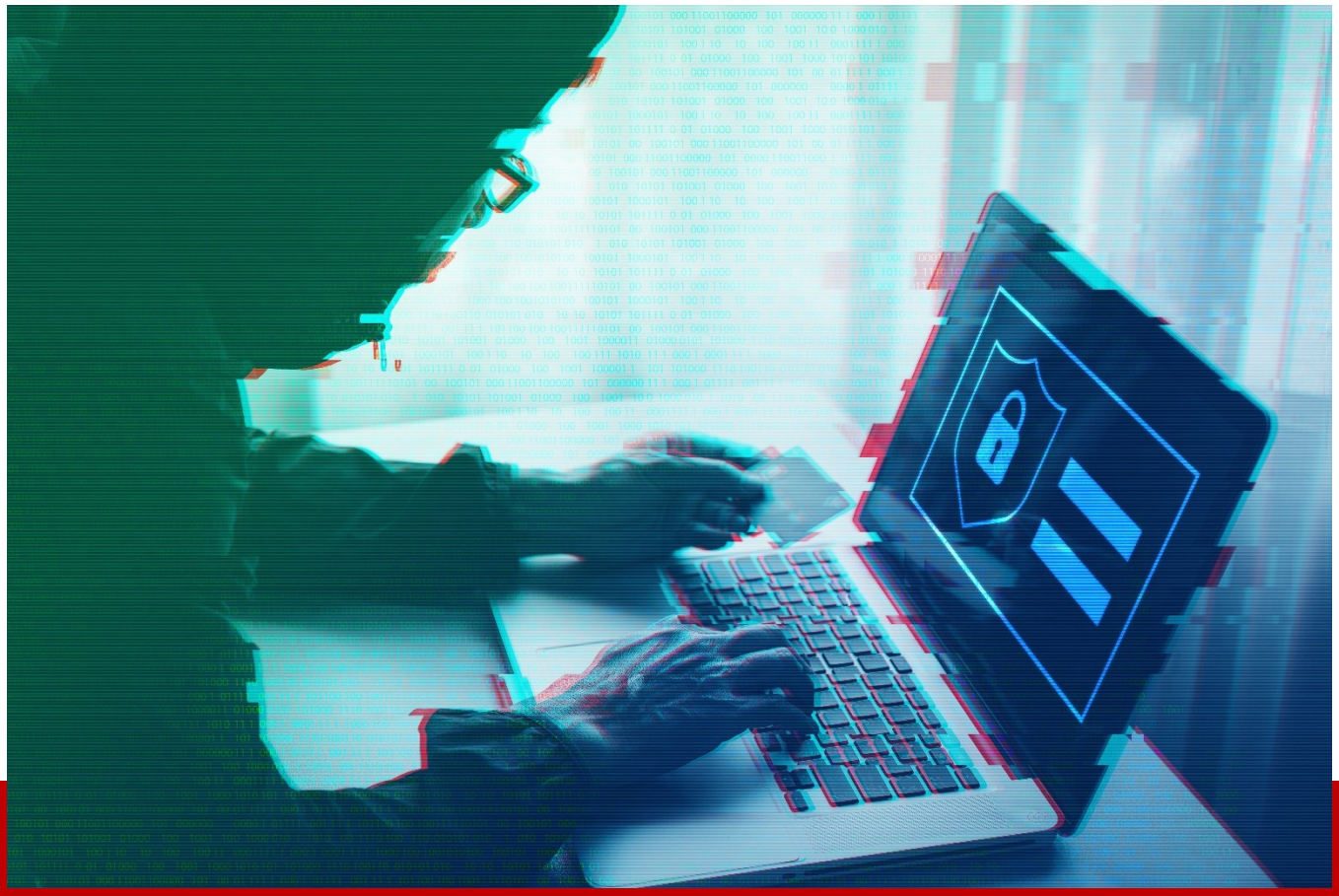
Security teams can not only focus more of their time on strategic thinking and chasing the real

threats before they destroy a city and less on task-based work that can be automated, but can become a part of strategic C-suite discussions so that they are best supported to continue fighting off the villains.

Having the right strategies and technology in your toolkit can be the difference for your team. Let's let the unsung heroes use their powers to the fullest extent, and what they were meant for. Let's make sure the right hero is being recognized.

About the Author

Karthik Kannan is the Founder and CEO of Anvilogic, a venture-backed cybersecurity startup based in Palo Alto. He previously led Security Analytics at Splunk following the acquisition of his previous company, Caspida. Before co-founding Caspida, Karthik was a founding executive member of other successful startups ultimately acquired by large public corporations. He's also worked at NetApp and Goldman Sachs. Karthik has three decades of experience across cybersecurity, analytics, and big data specializing in general management, product development,strategic planning, marketing, and advisory. He's an active volunteer in programs benefiting the local community in the Bay Area and his native India. Karthik can be reached at karthik@anvilogic.com and at our company website: https://www.anvilogic.com.



Penetration Testing- Shielding the Web Content Against Hacking

Penetration Testing Market size worth over $5.5 Bn by 2031

By Aashi Mishra, Sr. Content Writer, Research Nester

In January 2023, a news surfaced the internet that 235 million twitter accounts were leaked in a massive breach. Later, the social media platform hit by a drop of approximately 40% drop in the revenue. This case is alarming and re-establishing the importance of shielding the businesses from the hacking through measures such as penetration testing.

This twitter attack is just the tip of the iceberg and it is estimated that 2023 will witness around 33 billion account breaches. Owing to exponential rise in the hacking cases, there has been escalating number of the bug hunters, penetration tester, and security engineers. Technologies such as penetration testing are extensively used by businesses to save the IT infrastructure. In this blog, we will understand the meaning, types, benefits and various other aspects of the penetration testing.

What is Pen Testing and Why is it Important to Perform?

The process of penetration testing, also called ethical hacking, refers to the imperative security process of assessing applications for susceptibility and vulnerabilities. With the help of penetration testing, a person can eschew the vulnerabilities of bugs or the design flaws.

These pentests are also called white hat attacks as there are benign attempts to break into the system. Nowadays, approximately 77% of the companies use penetration testing as a security testing method to evaluate the security measures.

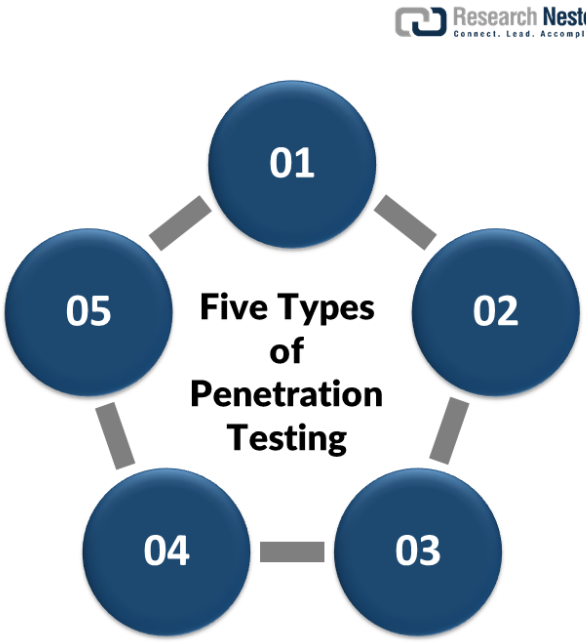
Furthermore, the average cost of data breach has escalated 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022. Hence, the penetration test prepares the organization for an attack or malicious entity. In fact, the penetration testing services that are offered by several penetration testing companies, render solutions which are known to help organizations to not only detect attackers but also debar such intruder. These pen tests render insights into the applications which are at extreme risk. Let us now understand the types and approaches of the physical penetration testing.

Types of Penetration Testing

Five Types of Penetration Testing

S. No.	Types
01	Network Penetration Testing
02	Web Application Penetration Testing
03	Client Side Penetration Testing
04	Wireless Network Penetration Testing
05	Social Engineering Penetration Testing

Source: Research Nester Analysis



1- Network Penetration Testing

The certified pen tester inspects the network environment and undergoes security testing for the detection of any security vulnerabilities. This process can be further sub divided into 2 main categories:

- External tests: This involves testing of the public IP address
- Internal tests: This gives the tester network access to imitate the hacker

Furthermore, the network testers examine areas such as firewall bypass testing, intrusion prevention system deception, DNS level attacks, etc.

2- Web Application Penetration Testing

This web application test helps in recognizing the real-world attacks which could get success at accessing the systems. Also, website penetration testing identifies loopholes in the infrastructure before an attacker could harm it. Web application penetration testing focuses on websites, browsers, and web application.

3- Client-Side Penetration Testing

This kind of testing is also called internal testing in which the certified penetration tester exploits the probable vulnerabilities in email clients, macromedia flash and other client-side application. Furthermore, on the client side, cyber security testing is performed to identify cyber-attacks including-

- Clickjacking attacks
- Cross site scripting attacks
- HTML Hijacking
- Open redirection

4- Wireless Network Penetration Testing

The wireless network penetration test helps in identifying weaknesses in the wireless infrastructure which involves the following parameters-

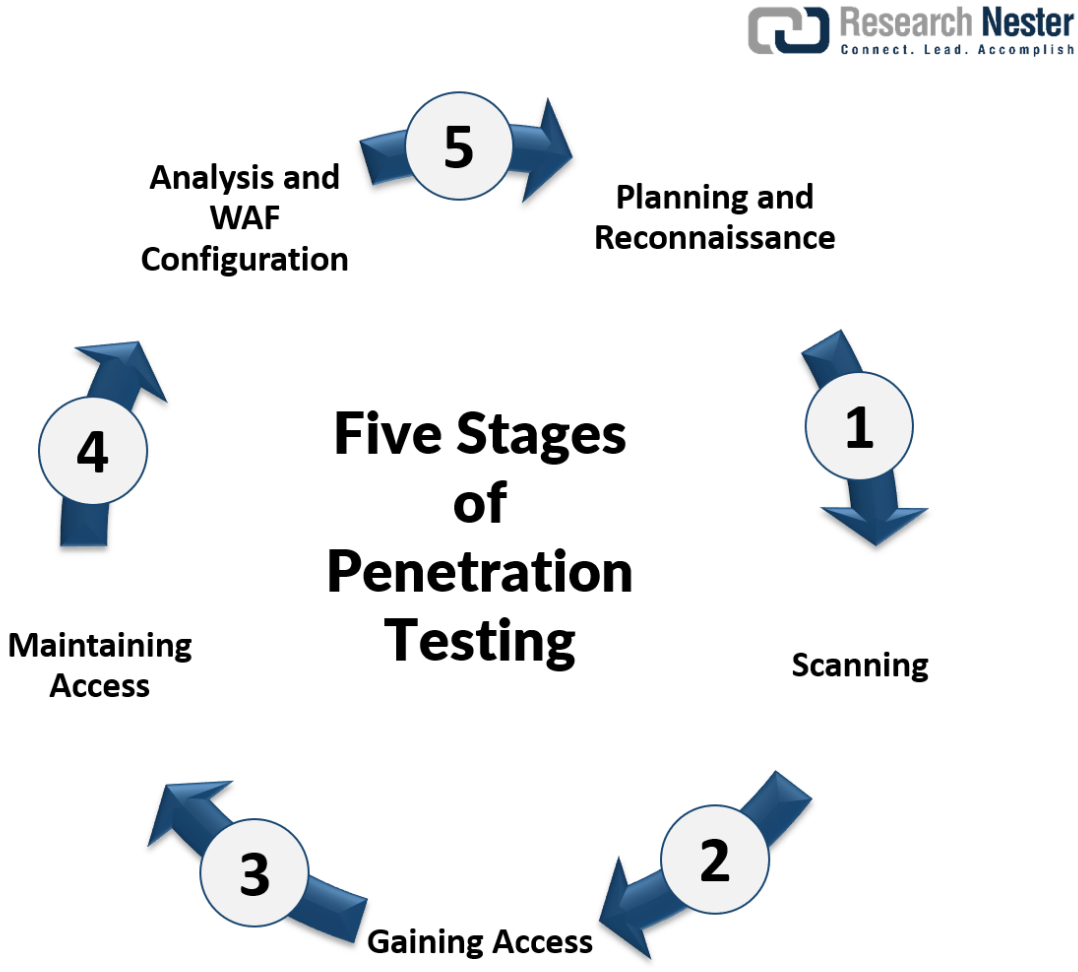
- Recognizing vulnerabilities in the wireless infrastructure
- Safely using the identified vulnerabilities
- Fabricating the report which incorporates a list of various issues, risk and remedies.

5- Social Engineering Penetration Testing

Social engineering attacks like phishing, vishing, smishing, impersonation, dumpster diving, USB drops, tailgating, etc. are threat to internet connectivity. It consists of the ethical hackers who conducts myriad of social engineering attacks. The goal of these tests is to recognize the threat and render proper remediation.

These kinds of tests are adequate for making the application system robust and shielded from attacks. The tests are executed in the following stages-

1. *Planning & reconnaissance*
   In this stage, test goals are defined and intelligence is gathered.
2. *Scanning*
   The scanning tools are utilized to understand how the target reverts to intrusions
3. *Gaining access*
   Web applications attacks are staged to reveal a target's vulnerabilities
4. *Maintaining access*
   APTs are emulated to witness if a vulnerability can be utilized to maintain access
5. *Analysis & WAF configuration*
   The obtained results are utilized to configure WAF settings before testing runs again



Source: Research Nester Analysis

It might sound absurd to hire a hacker to exploit your IT infrastructure but to protect the IT infrastructure penetration testing has now become an imperative tool.

Advantages of Penetration Testing

The process of physical penetration testing poses numerous advantages which are mentioned below-

1- Getting a New Insight into Security System

The pen testing method renders unseen insights into the IT infrastructure by exploiting the hidden flaws and loopholes. Also, it is crucial for fabricating accurate report analysis and efficiently revamp the system. The pen testing allows an in-depth analysis of the IT infrastructure.

2- Reveal the Hackers' Methods

The primary goal implementing the pen testing is to imitate real attacks on the systems. After analyzing vulnerabilities, hackers exploit the applications to identify the parts which needs improvement.

3- Protection from Financial Damage

A single breach of the security in any company lead to millions of dollars of loss. Penetration testing is extremely crucial for business as it render an efficient approach to combat cyber security issues. There is also reputational risk attached with the data breach.

A recent report published by Forbes found that 46% organization suffered massive reputational damage as the consequence of the data breach. This reputational damage also causes economical damage to the organization. A proper penetration testing leads to strengthening of customer loyalty and trust in the business.

4- Compliance With Regulation and Security Certification

The IT departments address the auditing and compliance procedures such as HIPAA, PCI DSS, SARBANES, GLBA. The overall records of the pen tests can help in eluding the penalties for the non-compliance. The pen tests also allow the user to demonstrate current due diligence by sustaining the required security controls.

5- Provides a Cyber Chain Map

The penetration test imitates the real hack where the user is able to see the direction a hacker might go through the system. This movement is usually known as the lateral movement. If the tester is conducting penetration test, he or she will be able to map full route through the security of system.

The procedure also gives a full map of how various connections are made amongst the layers in the system itself.

Also, sometimes penetration testing is confused for the same kind of service. Let us dive a little deeper into the difference between vulnerability scan and penetration scan.

Penetration Testing vs Vulnerability Assessment

- *Penetration Testing* - The penetration testing copies the actions of an internal or external cyber-attack which are intended to break the information security. It utilizes the advanced tools and techniques by making an effort to control critical systems.
- *Vulnerability Assessment* - It is the technique to discover and measure security vulnerability in the given environment. It identifies the probable weaknesses and provides impeccable mitigation measures.

Penetration Testing vs Vulnerability Assessment

Research Nester
Connect. Lead. Accomplish

Vulnerability Assessments	Penetration Testing
Makes a directory of resources and assets in a given system	It examines the scope of an attack
Tracks down the probable threats	Data collection of the sensitive scenarios
Allocates quantifiable value	Accumulates the targeted information
It attempts to eradicate the probable vulnerabilities	Cleans up the whole system and gives the final report
Perfect for lab environment	Perfect for network architecture and physical environments
It is meant for non-critical systems	Meant for real time systems
Non-intrusive documentation	Comprehensive analysis

Source: Research Nester Analysis

Both vulnerability assessments and penetration testing have different approach and functionality. Researchers suggest that both the techniques should be extensively used as security management systems and should be performed on regular basis.

What is Penetration Testing Quizlet?

The penetration testing quizlet will be giving ideas about the terminologies involved in the technologies such as passive reconnaissance, active reconnaissance, box testing, black box testing, gray box testing, etc.

Although, online penetration testing can be done by an expert pen tester in an efficient way to secure the IT infrastructure.

Why is it Important to Continuously Conduct Penetration Testing for a Strong Security System?

In order to shield the IT infrastructure, penetration testing has become the need of hour. According to Research Nester analysis, when pentest were performed for the repeat clients, the data came out to be like this-

- *29.1% of the targets had at least 1 critical vulnerability*
- *43.9% had 1 or more important vulnerability*
- *62.1% had medium, critical or important vulnerability*
- *47% had 1 or more medium vulnerability*

The data occupied of the pen testing is the testimony that there is a requirement of frequent testing to secure IT infrastructure.

Penetration testing should be performed at least once a year to ensure a robust IT and network security management. Although, the test frequency hugely depends in how alluring the business is for the hackers. Owing to the threats posed by malicious players there is a need to perform regular pen testing.

How can Businesses be Benefitted from Penetration Testing?

We have already read that data breach and malicious attacks can hamper the company in economic terms also. A prominent pen testing company, Tenendo claims that it has capability of reducing high vulnerability exposure by up to 97%. Let us see through a case study where Tenendo has resolved the challenge.

- *What was the challenge which company was facing?*

The Tenendo team was given task to execute an external black box engagement of a banking institution. The task was to perform without any restriction on the access. The test was conducted when there was no prior information was given. The only information given was rules of engagement and customer name.

- *What was the solution to it?*

The whole procedure had various constraints, but the team was able to intrude into personal information, achieve persistent internal access, and fabricate internal attack scenarios.

The second case handled by the Tenendo specialists was payment processing API penetration testing.

- *What was the challenge which company was facing?*

The team was given a task using external penetration test. The process was to done on an undisclosed payment processing company.

- *What was the solution to it?*

Tenendo specialists were able to discover an unattended staging environment. The team achieved complete compromise of the of the transaction processing API.

The case studies show that physical penetration testing can avoid attacks and probable threat to the company. Let us now see, how the penetration testing holds major importance in the future.

Future Scope of Penetration Testing

The pentesting amalgamated with the artificial intelligence is able to make impactful results in the future. Also, certified pen testers will be in demand for their knowledge and experience to decide the best course of action to perform assessment.

According to Research Nester analysis, in the future, the global penetration testing market is anticipated to grow with a CAGR of 14.9% from 2022 to 2031, and it is expected that its market size would increase from USD 1395.6 Million in 2021 to USD 5537.0 Million in 2031.

In a nutshell

From the above discussion, we can conclude that penetration testing has already become an imperative part of businesses. In future, as the threat of cyber-attack on businesses is rising, the need for testing is also becoming crucial. Almost, 2 in 3 businesses have online presence which equates to around 24 million online shops all across the world. The types of crimes that businesses could fall victim to are exponentially rising and penetration testing is no less than a silver bullet to shield the business.

About the Author

Aashi Mishra **-** Sr. Content Writer**.** An experienced research writer, strategist, and marketer with a demonstrated history of research in a myriad of industries. I love to distill complex industrial terminologies of market space into simpler terms. https://www.researchnester.com/.

Protecting Sensitive Information Within Translation

Strategies for Preventing Data Breaches in the Translation Industry

By Ofer Tirosh, CEO of Tomedes

When it comes to translation, it's not unusual to come across sensitive information such as financial reports, legal documents, and medical records. It doesn't need to be explained that such important details must be kept confidential and secure, as the resulting data breach can be disastrous to both the translation company and its clients.

This comes with its own set of hardships. Thus, safeguards must be in place in order to ensure the privacy, integrity, and security of both service provider and customer. Sharing information during business transactions is a show of trust, and failing to do their part can have terrible long-term repercussions, a loss of credibility, financial and clientele loss, and a damaged reputation for the translation company among them.

For clients, the consequences of a data breach can be even more severe. Exposed sensitive information can lead to identity theft, financial and reputation loss, and damage to personal and career life. Clients may also be subject to legal action if they cannot protect the private information of their customers. Therefore, it is critical for translation companies to take measures to prevent data breaches and protect the sensitive data they handle.

The Risks of Data Breaches in Translation

No matter how secure a translation company thinks it is, it is still vulnerable to cyberattacks and data theft. Hackers and other cybercriminals may attempt to gain access to confidential information by exploiting vulnerabilities in the company's systems. This can come in the form of malware, spyware, and other malicious software on the company's systems. These attacks can result in the theft of sensitive information, such as financial information or personal data, which can be used for identity theft, fraud, and other criminal activities.

Insider threats from employees and contractors are another major risk for translation companies. Employees and contractors with access to sensitive information may deliberately or accidentally leak confidential data. Employees who are disgruntled or have been terminated and contractors who may not be properly vetted can easily be bought or convinced to reveal what they know. Insiders can also fall prey to phishing attacks and other social engineering tactics used to gain access to sensitive information.

Additionally, one of the main challenges translation companies also face is the sheer volume of data that translation companies have to process. This can lead to errors and oversights, which can put sensitive information at risk. Another potential issue is the diversity of the information that is being handled, as confidential knowledge can be delivered in a range of different formats, including audio recordings, video files, and written documents.

On a brighter note, there are some defenses already in place. Some countries and organizations have already put privacy and data regulations that all companies, including those in the translation industry, should comply with. This includes the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) among others. This bolsters companies to implement data protection measures that are appropriate for the types of data they handle, including policies and procedures for data collection, storage, and sharing. It also pushes businesses to secure systems and processes for handling this data, including encryption, secure storage, and access controls. Failure to comply with these regulations can result in significant fines and reputational damage.

Strategies for Preventing Data Breaches in Translation

However, even with these safety nets in place, securing confidential data should start at the company ground level. There are already a few general steps that a company can do to begin the process, but for translation companies, these strategies should be more stringent. They can range from putting strong security protocols and procedures in place, training employees on best practices for secure information management, ensuring secure data storage and transmission, and conducting regular security audits and assessments.

For security protocols and procedures, use secure encryption methods to protect sensitive data, ensure that all software and hardware is up-to-date and regularly patched for security vulnerabilities, and put into practice access controls to restrict who has access to sensitive information. Other security protocols may include multi-factor authentication, firewalls, and intrusion detection systems.

However, using machines may not be enough. Employees also play a critical role in preventing data breaches. It is essential that translation companies train employees on best practices for secure information management, including how to identify and report potential security threats, how to handle sensitive information, and how to protect data during transmission. Employees should also be trained on how to avoid phishing scams and other social engineering tactics used by cybercriminals to gain access to sensitive information.

Once human and machine are trained and prepared for any breach possibilities, companies must then ensure that the data is stored and transmitted securely. This can be done through secure cloud-based platforms for data storage and transmission, implementing secure file transfer protocols, and using encryption to protect data during transmission. The information should also be backed up regularly and stored in secure locations to prevent loss in the event of a security breach. These procedures can also be automated to reduce human error.

Finally, to keep security effective in the long term, conduct regular security audits and assessments to check and discover potential vulnerabilities in their systems and processes. Do regular penetration testing to identify potential security weaknesses, and perform regular audits of their security protocols and procedures to ensure consistent compliance with data protection regulations. These assessments should be conducted by qualified professionals and include a comprehensive review of all security controls and procedures. Any identified vulnerabilities should be addressed promptly to minimize the risk of data breaches.

Best Practices for Secure Information Management in Translation

In the translation industry, secure information management has become essential. This is conducted through a combination of sensitive data encryption, access controls, authentications, data backup and recovery, and monitoring and logging access to confidential data.

First and foremost, sensitive data, such as personal information, financial records, and confidential business information, should be encrypted during storage and transmission. For instance, translation company Tomedes has its certified translation orders go through a Secure Sockets Layer ("SSL") protocol to ensure that data cannot be accessed by unauthorized users, even if it is intercepted or stolen. Other industry-standard encryption methods, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS), can also be used to encrypt sensitive data.

Another method of preventing unauthorized access to sensitive information is access controls and authentication measures that open or restrict the types of data employees receive based on user roles and responsibilities. Common examples include biometric or two-factor authentication for programs, which can also enhance security by requiring users to provide additional forms of identification before accessing sensitive information.

Translation companies should additionally provide secure methods for regular data backup and recovery to prevent data loss in the event of a security breach. All backups should be stored in secure locations to prevent unauthorized access, and disaster recovery plans put in place to ensure that potentially lost data can be restored quickly in the event of a security breach or any other disaster.

Steps can be followed to maintain security even during company operations. Monitoring and logging access to sensitive information can be a dealbreaker for detecting and responding to security incidents. Implement systems that track and log access to sensitive information, including who accessed the information, when it was accessed, and what actions were taken. These logs should be reviewed regularly to identify potential security threats, and to ensure compliance with data protection regulations.

Conclusion

No matter how secure a translation company may be, the threat of data breaches and compromises will always be around the corner for as long as there is the knowledge of private, sensitive information being traded back and forth between clients and service providers. Privacy and data protection regulations are an attempt to keep on top of the danger, but there is only so much that can be done if companies themselves do not put their best foot forward and prevent, if not minimize, the risks that are already present and waiting for an opportunity to strike.

The translation industry is constantly evolving, and companies must adapt their security strategies to keep up with emerging threats and new technologies as best they can. By implementing best practices for secure information management, translation companies can minimize the risk of data breaches and protect sensitive data from cyber threats and other security risks, keeping clients safe, happy, and secure in their translator choice.

About the Author

Ofer Tirosh is the CEO of Tomedes, a translation company that offers language-based solutions to businesses and Fortune 500 companies worldwide. With over 15 years of experience in the language industry, Ofer has developed strategies to protect his company from data breaches, making Tomedes' certified translation a trusted partner to businesses worldwide seeking to protect their sensitive information during the translation process.

Our Risk Perception Is Broken How Do We Fix It?

By Miguel Clarke, GRC and Cybersecurity Lead at Armor and former FBI Special Agent

I was first introduced to the concept of cyber security in 2000. Back then, the Dallas FBI Field Office had fewer than 25 email addresses, which were for the exclusive purview of the Cyber Squad, known at the time as a "National Information Protection Center" or NIPC Squad. To outsiders we were just a bunch of geeks playing with computers.

In reality, we were 12 FBI Special Agents trapped in a desperate tussle to stay ahead of a newly emerging threat, not yet publicly acknowledged. Behind the scenes the United States Intelligence Community was alarmed, coming to terms with the fact that our nation's enemies were already using networks to make their spies and spying campaigns ever more effective.

In those distant days, the security function was just a collateral duty for information technology teams, who were charged with making sure the technology was available and functioning properly. The modern-day breach had not been widely deployed. 'Attacks' took the form of defaced web pages and Denial of Service Attacks. But that was OK, because as soon as the bad guys got ahead, the good guys came back with a solution and saved the day.

The problem is that today's perception of risk is rooted in that history, a reliance that the good guys, armed with their 'silver bullet' technology, will overcome. It gives the modern-day network defender some comfort that reasonable preparations will provide adequate protections. But the issue now is that technology is ubiquitous. We use it for everything, from communication and entertainment, to banking. This reliance on technology has made us more vulnerable to cyber security risks. The attacker now has two vulnerabilities to exploit, the people and the technology. And even the technology designed to protect them from the risk.

But everyone reading this knows the size of the problem. Cybercrime is a six trillion-dollar industry and cyber security is a 200 billion dollar industry. But no matter how much we spend, we are not getting any safer. This has become a problem we can no longer outrun. And, as a business, you cannot spend your way to safety. This is an asymmetrical war.

As an FBI Special Agent, 'mindset' was a crucial part of both my training and the way I approached investigations. As humans, our brains are more complex and magnificent than any computer, but I worry that when it comes to risk and cyber security, our reliance on the technological 'fix' is stopping us from using them. Bruce Schneier, a public interest technologist, said: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology", and I could not agree more. Somewhere along the line we have forgotten the importance of the human factor, both as a vulnerability and as a solution.

Let's first examine the human factor as a vulnerability. Most organizations extend high levels of trust and access to their employees and this immediately exposes them to both malicious actions and non-malicious mistakes made by employees. Unfortunately, whilst it has delivered many benefits, our increased connectedness through multiple devices, apps and programs has delivered two things: a greater number of outlets for leaking information and a higher number of people with greater access to critical information.

The human factor is undoubtedly the weakest link in the security of any IT infrastructure. Threats such as Ransomware and Business Email Compromise rely on an exploitation of the human mindset, so ignoring people related risk comes at your peril. Also remember that behind the threat is another human being, capable of manipulative and nuanced behavior, so whilst policies and technology can impede malicious actions, risks cannot be eliminated, because people are inherently unpredictable.

Acknowledging the risk of the human factor means remembering that every technology user in your business must be considered. Risk and cyber security are not the sole domain of your IT department and keeping IT governance and risk management siloed is counterproductive, as hackers are not likely to target the cyber security savvy.

How then, can we turn the human factor to our advantage? We need to make a mindset shift away from threats and vulnerabilities. A risk-based mindset enables a much more useful conversation. It starts with better questions, such as:

- What is the worst that I expect to happen?
- Which assets are the most critical to the business? What are the conditions which would result in a "business-ending" outcome?
- How much can we devote to preventing that outcome?
- What contingencies do we need to have in place to survive that event?
- What resources will we need?
- What does recovery look like and how long will it take?
- How do we capture the lessons we learned so that we can be better prepared for future events?

This is just a sample of the questions resilient organizations will use to start more meaningful conversations. Next in line is developing a focus on building the skills needed to observe, understand, and remediate significant events across the board. Really? Yes. Keeping risk conversations behind closed doors helps nobody. Instead, consider forming a multi-disciplinary team, including IT, HR and comms to discuss potential risks and to communicate and educate the wider business.

We should establish a culture of cyber security and risk awareness within every organization. This culture should prioritize cyber security as a key business priority and encourage employees to report security incidents or potential threats. It should also promote a sense of ownership and accountability among employees for the security of the organization's data and assets.

The right mindset combined with the commitment to building relevant skills with sophisticated tools is the path to resilience. Resilience is the antidote to the growing cybercrime economy. When fully matured, there will be no more "victims" of cybercrime. There will only be combatants.

About the Author

Miguel Clarke is the GRC and Cyber Security lead for Armor Cybersecurity. He spent nearly 24 years as a Special Agent with the FBI, where he was a founding member of the National Cyber Investigative Joint Task Force and the Defense Collaborative Information Sharing Environment. He was awarded a NIMUC (National Intelligence Meritorious Unit Citation) for contributions to the United States Intelligence Community

Miguel can be reached online at Miguel.Clarke@armor.com and at our company website www.armor.com.

SaaS Application Security: Why It Matters and How to Get It Right

Protecting Emerging Startups from Advanced Cyber Threats with Proactive Security Measures

By Babar Khan Akhunzada, Founder, SecurityWall

Startups are known for their agility, speed, and innovation. They often disrupt entire industries with their unique solutions and ideas. However, they are also vulnerable to cyber-attacks and data breaches that can harm their business and reputation. During the disruption they catch eyes of hackers as startups are low on resources initially and hackers take benefit of it to attack and hit low hanging fruits and create backdoors or proceed with data theft which leads to financial bankruptcy and impact reputation negatively.

SaaS (Software as a Service) applications have become an essential part of startup industry as majority of emerging startups operate via apps over web and mobile. Web and mobile app platforms allow startups to provide a seamless user experience. This leads to increased engagement and better user retention.

Even if we look into top startups almost 90% are virtually act as SaaS ranging from ride hailing, food, ecommerce, health, and financing.

It is interesting to note the contrast between the significant amount of investment pouring into startups this week and the staggering estimated cost of cybercrime to the world by 2025.

According to recent startups funding reports, this week alone $15.7 billion was invested into startups, highlighting the strong interest and support for emerging businesses. However, Cybercrime report estimates that cybercrime will cost the world $6 trillion annually by 2025, up from $3 trillion in 2015. This highlights the importance for startups to invest in cybersecurity measures to protect their businesses from potential attacks and financial losses and as application matters considering:

- Customer Trust: Customers trust startups with their personal and financial information. A data breach can result in a loss of customer trust, which can be difficult to regain.
- Compliance: Startups must comply with various data protection regulations such as GDPR, CCPA, and SOC 2, ISO 27001, HIPAA. A data breach can result in non-compliance penalties and legal action.
- Business Continuity: A data breach can result in loss of critical business data and disrupt business operations, affecting revenue and customer satisfaction.

Startups must learn from past security incidents and take proactive measures to prevent security breaches.

1. 2015 Ashley Madison Breach: In July 2015, the personal information of 32 million Ashley Madison users was exposed. The breach was caused by a vulnerability in the company's web application.
2. 2017 Equifax Breach: In September 2017, Equifax announced that a data breach had exposed the personal information of over 143 million customers. The breach was caused by a vulnerability in the company's web application.
3. 2018 Careem: In 2018 Careem was breached but earlier reported to be rescued but due to low engagement reasons startup got an attack over application layer and users data was at risk later learned that Careem faced a data breach of their 14 million users.

These incidents highlight the need for startups to take security seriously and ensure that their SaaS application is well secured in 360-degree manner which range from application, cloud and API's security especially.

Ensuring SaaS Application Security, Startups should look into penetration testing, audit and industrial compliance (HIPAA, SOC2, OWASP etc) for their web and mobile application to make sure their infrastructure security and users security at same time. This can enhance the trust and usability of app without hesitation and provide comfort within the startup and community but not limited to:

- Conduct Regular Security Audits: Regular security audits help identify vulnerabilities and security gaps in your SaaS application. It enables you to take proactive measures to fix them

before they are exploited. Audit should not be automated scanning audits as hackers are much more advance and go logically.

- Use Multi-Factor Authentication: Multi-factor authentication adds an extra layer of security by requiring users to provide two or more pieces of evidence to log in. It ensures that only authorized users have access to your application.
- Encrypt Sensitive Data: Encryption converts sensitive data into a format that is unreadable without a decryption key. It ensures that even if data is stolen, it cannot be read or used.
- Regularly Patching: Regularly patching ensures that any known vulnerabilities are addressed and patched, reducing the risk of a security breach.
- Train Employees on Security Best Practices: Employees are often the weakest link in the security chain. Training employees on security best practices ensures that they are aware of the importance of security and how to protect customer data.

SaaS application security is critical for startups. It not only protects customer data but also ensures compliance with data protection regulations and maintains business continuity. Startups must prioritize security

About the Author

Babar Khan Akhunzada is a cyber wizard and entrepreneur, the Founder of SecurityWall, a cyber security firm focused on Hybrid Auditing approach serving startups and enterprises for Penetration Testing, Audit, Compliance (SOC2, IBM AS400). Babar is acknowledged by tech giants within Silicon Valley for security contributions. The author is a well-known speaker who gives his thoughts and analyses on Application Security, Cyber Warfare, OSINT, Cyber Policy, Forensics, and Red Teaming.

For more information, the author can be reached online at email, twitter or website.

A Cloud Security Conundrum: Protecting Your Company from Third-Party Software Supply Chain Gaps

By Vrinda Khurjekar, Senior Director, AMER business, Searce

The sky is the limit for cloud migration as Gartner predicts that worldwide end-user spending on public cloud services is forecast to grow upwards of 25% in 2023, led by software-as-a-service (SaaS) as the largest public cloud services market segment, forecasted to reach $176 billion in end-user spending in 2022. The average number of SaaS applications used by organizations worldwide jumped from 16 in 2017 to 110 in 2021. In the last half-decade of rapid mass cloud adoption, tech businesses enjoyed a newfound sense of cybersecurity in dispensing with on-premises perimeters. However, in 2022, 45% of data breaches occurred in cloud services. With enterprises increasingly turning to public cloud, multi-cloud and hybrid cloud environments, securing third-party SaaS platforms will need to come of age swiftly to keep pace with increasingly sophisticated cyber criminals.

Software supply chain challenges in cloud environments

CISOs and other security leaders are already prioritizing securing their data and ensuring compliance in their cloud software supply chain. Thirty-eight per cent of business, technology, and security executives expect more serious attacks via the cloud in 2023. With so many third-party solutions in use, companies are most challenged by their lack of visibility into user data and activities and managing application configurations with consistency. Employing 10, 20, or 100 cloud solutions with virtual machines and various storage containers means a much wider attack surface to defend, numerous identity and admin privileges to manage, and greater potential for misconfigurations and unpatched 3rd party servers. The 2021 Volkswagen Group data breach exposing sensitive financial data involving 3.3 million customers was caused by one of its vendors, who left a storage service unprotected for almost two years.

Criminals attack the cloud from all directions

Many enterprises are still migrating to cloud services and must get up to speed on the inherent vulnerabilities present in cloud environments, primarily misconfiguration, insufficient identity access management security, insecure APIs and interfaces, and inadequate change controls. Ransomware, once a minimal threat in cloud environments, is growing rapidly in line with increasing cloud adoption. Distributed Denial-of-Service (DDoS) attacks are rising in which criminals attempt to block the company from conducting business and then extract relevant information. Meanwhile, martech and adtech companies provide numerous cloud tools to every big brand imaginable for digital advertising and marketing, which are proving to be the highest dataset and broadest spectrum of consumers that makes them fruitful targets for criminals. Financial services, education, manufacturing, and healthcare are sectors bearing the most losses at the hands of bad actors.

There's money in hacking healthcare

Most experts name the financial and healthcare industries as the most vulnerable to data breaches. Attackers are swarming to healthcare organizations to harvest personally identifiable identification (PII) data and to financial institutions to capture valuable financial data. For the 12th year in a row, healthcare had the highest average data breach cost of any industry, at $10.10M in 2022. Hospitals now in the midst of digital transformation are a prime target for cyber villains. Some hospital administrators store all their X-rays in one location and often use two third-party vendors to send X-ray data in a digital format. Plus, they call upon external machine learning vendors to help make advances like predicting cancer five years earlier than we can today, which is great. However, if they haven't vetted the receiving entities' security posture, how they host their applications and how they run their models, hospitals are exposing their patients and themselves to highly sensitive risks.

Third-party vendor's responsibility or my responsibility?

When a tech company adds another cloud vendor to its software supply chain, its buyer may assume the liability rests with the SaaS provider to make sure their environments are properly controlled. Although tech companies and cloud providers are engaged in a shared responsibility model (customer's

responsibility + service provider's responsibility), it is sensible for security leaders to adopt a more authoritative mindset, since ultimately it is their sole responsibility to safeguard a company's data and identities, devices and applications. And the reputational and financial damage will fall squarely on the company instead of its vendors.

Scrutinize cybersecurity when shopping for third-party vendors

The fact is that, while they should, all enterprises fail to run cybersecurity risk assessments on each and every SaaS they onboard. Given the setups and the nature of the accesses that are inherently granted to third-party vendors, there is a lot less clarity on where security gaps can be for an organization. It can be especially tempting for a startup or early-stage cloud native company to focus on acquiring customers, building a cost-effective tech stack, and raising the next round of funding first, and then think about how to secure the organization's data assets later. For small and medium sized businesses, a data breach and the subsequent business interruption can be potentially catastrophic. Rigorous vetting standards should be normalized for every enterprise that is onboarding a third-party vendor. They should scrutinize a third-party vendor's security posture as much as they scrutinize the cost and the quality of the offerings.

Avoid a set-it-and-forget-it vendor security approach

In addition to the intensive vetting of third-party cloud solutions' cybersecurity posture during the purchasing process and risk assessments during the onboarding process, CISOs should also endeavor to avoid a set-it-and-forget-it approach. Lot of enterprises have recently started thinking more about software supply chain security vigilance, but they're not yet performing it actively. They implement no alerting or monitoring tools until some incident has already happened. They should identify and track all third-party cloud software, conduct periodic reviews of the third-party resources to remove unnecessary products, and revoke access or permissions as needed. Since cloud technology is advancing at a furious pace, quarterly security reviews, just like quarterly business reviews, should become the norm in the c-suite. Even after purchase, SaaS vendors are going to keep adding new modules and new offerings, which may require new security standards to stay current with the technology. Finally, as the Cloud Security Alliance recommends, CISOs should do regular penetration-testing of applications, use secure coding practices, and use static and dynamic application security testing solutions.

Governance of the entire vendor journey

About 94% of enterprises now use cloud services for virtually all business functions, from human resources and customer relations to supply chain management. CISOs should build different governance models for each stage of the vendor journey, from the buying stage to onboarding and implementation, and then on an ongoing basis. Company leaders can take a great first step in securing cloud software supply chains by ensuring their own security posture meets the modern standard, because cybersecurity frameworks from 2005 or 2010 will not protect against today's threats nor will they meet regulatory standards, no matter how robust a vendor's posture. Many forward thinking CISOs and CTOs are enforcing their third-party vendor security standards by building in, for example, three-month benchmarks

into the contracts, no matter how essential a particular software might be for their go-to-market plans. In some cases, we've observed that these third-party providers aren't refusing to fortify their security posture. Many times, they either don't know the best route or they've just not yet been compelled or even asked to follow through.

About the Author

Vrinda Khurjekar – Sr. Director – AMER Business – Searce. A genuine problem solver at heart, a compassionate listener and a trusted client partner, Vrinda Khurjekar is the Sr. Director – AMER business at Searce leading the AMER region. A techie turned business leader, Vrinda is passionate about driving technology-led transformation and helping businesses futurify by leveraging the latest technologies. Vrinda has been in various roles over the last 14 years at Searce, is a Happier Culture ambassador at Searce and a core member of the Searce global exec team. Vrinda has personally participated in leading many large clients through their digital transformation journeys. Vrinda believes in the power of customer empathy, listening to clients & partners & being a trusted partner to anyone she works with.

Vrinda can be reached at: https://www.searce.com/.

The Billion Dollar Problem: Securing Business Communication in the Financial Sector

By Anurag Lal, President and CEO of NetSfere

Securing business communication in the financial services industry is now more than ever a bottom-line issue. That's because unsecure business communication creates massive business risk for the highly regulated financial sector. Mounting fines for compliance violations, hefty costs associated with data breaches and significant reputational damage are just some of the costly consequences that result when financial institutions don't lock down business communication.

Digital transformation, bring your own device (BYOD) practices and hybrid and remote working are expanding the cyberattack surface, introducing compliance and data security risks in enterprises across sectors. The use of consumer-grade messaging apps like WhatsApp along with widely used collaboration platforms such as Slack and Microsoft Teams are intensifying these risks.

Recent regulatory actions against banks for the misuse of messaging apps serve as a cautionary tale that highlights the importance of securing business communication with enterprise-grade mobile messaging and collaboration platforms.

Last year, the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) fined major Wall Street banks and brokerages a collective $1.8 billion dollars for the misuse of messaging apps. This enforcement action reflects increasing concern among regulators over the use of unsanctioned communication apps.

Financial institutions are also grappling with growing data security risks associated with messaging apps and collaboration tools. As repositories of lucrative personal data such as account data, credit card information and social security numbers, banks are prime targets for cyber criminals.

According to the latest EY and Institute of International Finance (IIF) bank risk management survey, cybersecurity is at the top of the list of near-term risks for banks around the world. The survey revealed that 72% of chief risk officers (CROs) identified cybersecurity risk as their top concern over the next 12 months.

CROs have good reason to be concerned as cyberattacks continue to grow in sophistication and frequency. A recent report by Contrast Security found that 60% of financial institutions have been victimized by destructive cyberattacks. Cyberattacks that result in data breaches are costly for financial institutions, reaching an average cost of $5.97 million in 2022 up from $5.72 million in 2021.

As the use of consumer-grade messaging apps and unsecure collaboration tools continues to compromise compliance and data security, mobile messaging and collaboration solutions designed to lock down business communication become vital to protecting the bottom line.

To ensure compliance and data security, financial institutions should look for mobile messaging solutions that provide:

Security by design and default

Financial institutions need mobile messaging and collaboration tools that are built from the ground up with enterprise-grade security and don't require any configuration to activate that security. Always-on end-to-end encryption (E2EE) encrypts messages and data at rest and in transit across all devices and channels. E2EE provides iron clad protection, safeguarding sensitive information and privacy and locking down data to help financial institutions meet compliance requirements, and ensure proper data governance.

IT control

To achieve information security, regulatory compliance and bottom-line business improvement, banks should adopt mobile messaging technology equipped with a slate of administrative controls for managing users, monitoring activity and enforcing corporate policies. Mobile messaging platforms with robust

administrative, technical and physical data security features make it easy for financial institutions to meet compliance requirements such as Sarbanes-Oxley, Dodd-Frank, FINRA and future-proof business communication to meet evolving global data privacy requirements.

Compliance guaranteed

Non-compliant mobile messaging and collaboration tools can elevate risk for banks. As compliance laws continue to evolve, financial institutions should adopt mobile messaging technology with built-in technical safeguards and security that guarantee compliance. To ensure compliance, financial institutions should also look for a collaboration solution provider that never collects or shares data.

Ease of use

Right-fit mobile messaging and collaboration platforms for financial institutions are designed to be easy to use without compromising compliance and data security. Providing employees with easy-to-use all-in-one platforms that allow them to securely communicate and collaborate across preferred channels - text, video and voice – will help eliminate the use of risky consumer-grade communication apps and unsecure collaboration tools.

Business communication is now a bottom-line issue for financial institutions. As non-compliance fines continue to increase and the cost of data breaches continue to rise, financial institutions today simply can't afford compliance and data security risks. It's a billion-dollar problem that can be mitigated by adopting secure by design and secure by default mobile messaging and collaboration technology.

About the Author

Anurag Lal is the President and CEO of NetSfere. With more than 25 years of experience in technology, cybersecurity, ransomware, broadband and mobile security services, Anurag leads a team of talented innovators who are creating secure and trusted enterprise-grade workplace communication technology to equip the enterprise with world-class secure communication solutions. Lal is an expert on global cybersecurity innovations, policies, and risks.

Previously Lal was appointed by the Obama administration to serve as Director of the U.S. National Broadband Task Force. His resume includes time at Meru, iPass, British Telecom and Sprint in leadership positions. Lal has received various industry accolades including recognition by the Wireless Broadband Industry Alliance in the U.K. Lal holds a B.A. in Economics from Delhi University and is based in Washington, D.C.

The Industrial Control Systems and The Internet of Things

By Milica D. Djekic

The industrial control systems (ICS) are usually the part of critical infrastructure to every country or nation. These systems have passed through information era and today – the majority of them has the access to the web or uses some of the internet techniques to communicate within each other. Here, how we would come to the Internet of Things (IoT) concept amongst the ICS. The role of the internet signal within ICS is clear! It serves to transmit the messages through the ICS network and make the asset's devices talk with each other. Through this chapter, we would want to discuss how the IoT deals with the ICS and also provide a better insight into some of the security's concerns of these systems.

What are the ICS?

The systems being applied in an industry could include industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and so on. All these

systems would strongly get correlated with the control engineering theory and use the minimum of human effort to operate on. The main characteristics of ICS are their stability and controllability. In other word, the industry systems would deal with the plant and its controller. This synergy of plant and its controller would make a control system which main role would be to obtain operations automatically.

Basically, stability and controllability are the attributes of a plant, while controllers rather deal with their control algorithms. The design of control systems is not that easy thing and usually requires lots of research and development in order to produce something that would work as required. The fact is that industrial systems could get controlled on a plant or remotely depending on the industry's asset needs. As it's known, the plants usually could be electric motors, turbines, some mechatronics objects or even boilers and heat exchangers depending which sort of process should be controlled. On the other hand, controllers are closely correlated with the computing units and can cover industrial PCs, programmable logic controllers (PLCs) or any other variations of industrial smart enforcers.

The figure on our right demonstrates how the control office within some power plant appears and why this sort of infrastructure demands highly skillful operators to manage those industry's processes. Indeed, any type of dealing with the ICS needs a great skill and even employees who maintain the plant directly need to know how to deal with – let's say water waste systems, power plants, nuclear reactors or another sort of a control system. So commonly, the ICS cannot work independently and many of them would need some sort of communication protocols to do information sharing or simple talking between their sub-stations. For such a purpose, modern industrial systems would use the internet signal and so often – get managed remotely. In other words, it's clear how industrial systems could get correlated with the IoT.

The link between the ICS and IoT

As we would mention before, the ICS are strongly linked with the IoT for a reason that many industrial assets would get the web connections. As we know, the entire human kind got vitally dependable on new technologies, so the similar case is with the industrial infrastructure. It's clear that if you talk about the factory being controlled to produce something – you need the internet connection at least to send an e-mail. Next, the purpose of the entire factory would not be to make an e-correspondence with the outer world, but rather force its production lines to work and produce their final products. Finally, that sort of process cannot get imagined without good communication protocols that would usually use the web signal to talk to the rest of the system.

So, the question here would be if the ICS already live in the IoT age. The answer to this question is partially YES! Why partially? The main reason to that

would be that the curve of a progress is not equally distributed within all parts of the world. The areas using smart technology including sensors, actuators, measuring devices and diverse sorts of cyber signals would definitely live the IoT age, while the rest of the globe would try to reach such a level of development. Finally, industrial control systems dealing with the new technologies are the privilege to some countries, but also the big threat to their security. The reason to that is those systems could potentially get hacked from the outside if not managed to follow the best practice.

The security's challenges of ICS

As we would suggest above – the main security's challenges of ICS could be addressed to their communication as well as safety procedures that should get followed during the working process. Everyone would agree that the best practice is something that should get applied within the industry's infrastructure. Many research publications would indicate how the networks within the industrial asset should get configured and why it's important to appropriately set up your both – hardware and software firewall – as well as deal with the strong authentication.

The big concern here would also be the existing IoT search engines that would offer so convenient access to IoT devices including the ICS computers. In addition, that could get critical for a reason of so many terrorist and organized crime groups that could take advantage over those technological advancements and so easily try to exploit the weaknesses of such an industrial system. Finally, we would suggest that those tools could get used to discover some industrial asset and consequently organize the hacker's attack to that. This would not be such a big concern if those systems are not the part of the nation's critical infrastructure making many people being dependable on them. In other words, the best practice should offer us some suggestions how those systems could get invisible to those tools and one of the most helpful advices would be to close your inbound ports. We intend to talk about these strategies further through this research material.

The concluding remarks

It's obvious that cyber technologies are getting the part of both – our private and business lives, so it's significant to understand that the ICS are also the segment of that tendency. It's crucially important to get some sort of awareness about the significance of these systems to the entire nation. Their role is undoubtedly critical to all of us, so we should put a lot of effort to protect something being so strategically important to everyone. At the end, many researchers would suggest that following the best practice could put our risk at the lower level, so it's not that bad idea to take into consideration some of these indications.

References:

[1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.

[2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine

[3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine

[4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine

[5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine

[6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine

[7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine

[8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine

[9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine

[10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal

[11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine

[12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine

[13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine

[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

[15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine

[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

About The Author

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

The Other Russian War – What Can We Do?

Russian hacking efforts have highlighted weaknesses in U.S. cybersecurity infrastructure.

By Jamie Eiseman, George Washington University

Russia is invading Ukraine, and Russian hackers are attacking the United States. In October, a Russia-affiliated hacker group known as Killnet launched an attack that took down several U.S. airport websites. The group also sounded a rallying cry to anti-U.S. hackers, and leaked lists of vulnerable American websites. Combatting Russian hacking must become a priority for U.S. national security.

Russian entities have conducted a consistent stream of large and small scale attacks in recent years. They have endangered sensitive information of millions of Americans and cost companies' massive amounts of money. Their attacks include the 2015 Office of Personnel Management hack, the 2016 election breaches, and the 2020 SolarWinds compromise. Americans are in danger. U.S. infrastructure is in danger. Our data and money are in danger.

The U.S. needs to focus on better information-sharing and coordination between the public and private sector to improve detection and response capabilities. The nation needs to focus on growth of the cybersecurity workforce. Finally, the U.S. needs to focus on implementing existing cybersecurity legislation, including offering federal incentives and providing oversight to ensure proper execution throughout the private sector.

Better information-sharing and coordination will result from following necessary protocols to protect national security interests. One key step would be convening the Cyber Safety Review Board, as described in Executive Order 14028. It would evaluate cybersecurity incidents at all levels and make recommendations for improvements, such as better encryption methods or multi-factor authentication processes. This multiagency effort for information-sharing and collaboration needs to take place quickly in order to prevent further Russian infiltrations.

The administration needs to grow the cybersecurity workforce. It must promote a uniform training standard that enables mobility of cybersecurity professionals. It should also support a robust system for rewarding talent. These steps, sustained over time, will attract highly specialized and experienced private sector professionals to employ their skills for the government's benefit.

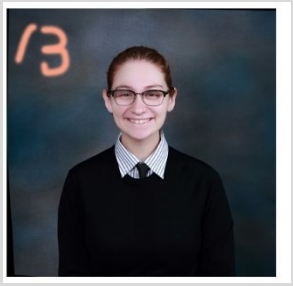
Greater oversight and collaboration with private entities would also close several gaps in the current federal cyber infrastructure. The government needs to incentivize the implementation of the National Initiative for Cybersecurity Education (NICE) framework to train both new and current employees. This Initiative would allow for the creation of uniform employment standards and training procedures for cybersecurity professionals across all sectors, and subsequently increase mobility between public and private roles. The training should be conducted at the federal level and offer certification of some form that is recognized and respected by both private and public sector employers. These incentives should also extend to providing adequate reports of identified incidents and vulnerabilities with recommendations for improvement.

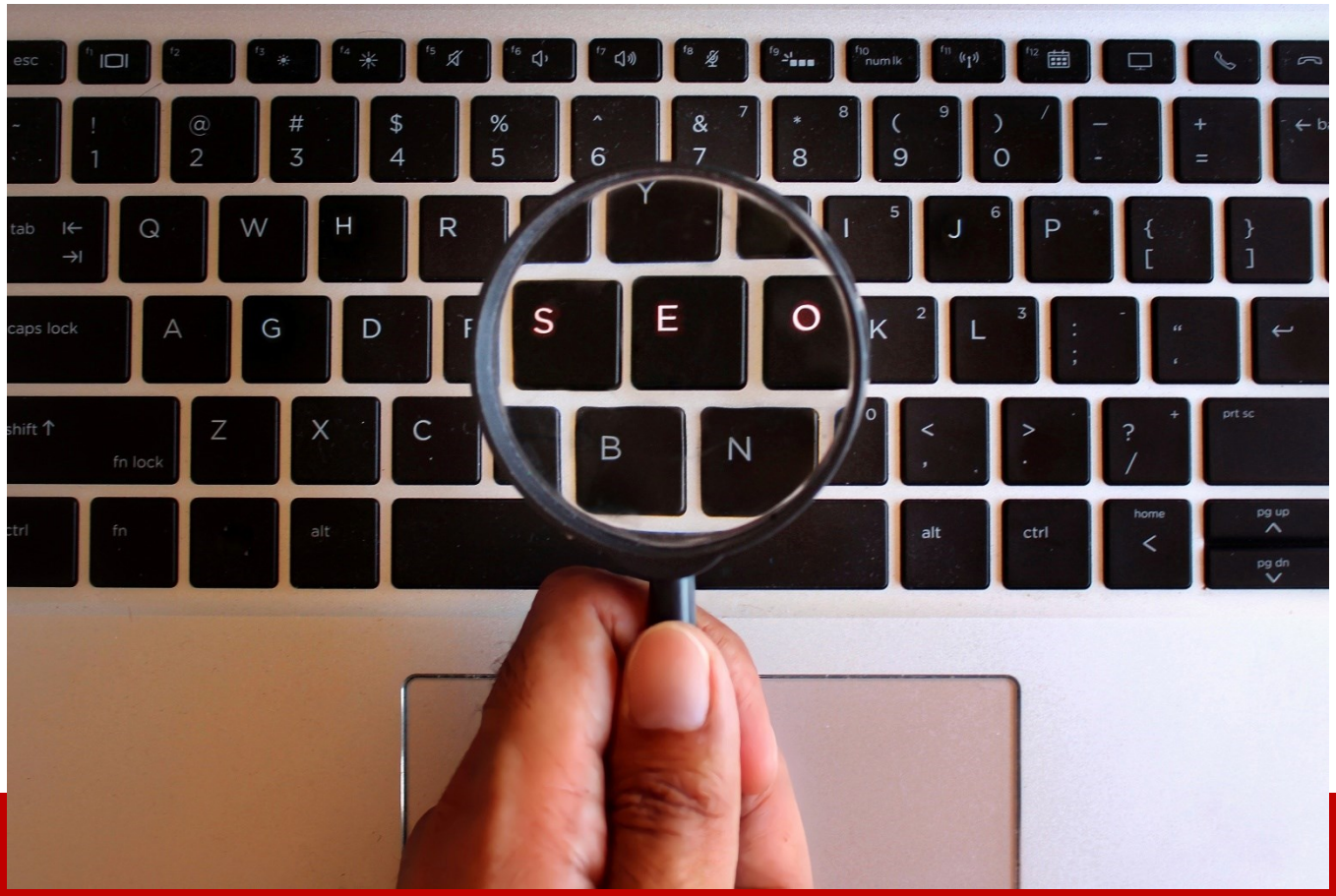
Critics worry about the security risks of increasing private sector involvement. This concern is not new and the government has already developed several services such as the Enhanced Cybersecurity Services (ECS) and Automated Indicator Sharing programs to address it. These programs serve to prevent malevolent actors from accessing information shared with private entities and inform the relevant authorities of malicious action attempts. In essence, the priority for the intelligence community is improving cybersecurity infrastructure. That means combatting the risks of including the private sector in the process.

The best way for the United States to respond to Russia's cyber-attacks is through greater collaboration between the private and public sectors. Bringing them together will reinvigorate U.S cybersecurity infrastructure and defenses. Better information-sharing and coordination between the public and private sector will improve detection and response capabilities. This united effort will save money, defend our values, and keep the American people safe.

About the Author

Jamie Eiseman is a Security Policy Studies graduate student at the George Washington University. She completed her undergraduate degree at the University of South Florida in Political Science and International Studies in 2019. Jamie can be reached online at j.eiseman97@gmail.com.





The Shodan as The Scariest Search Engine of Today

By Milica D. Djekic

According to many media's releases – the Shodan is characterized as the scariest searching tool of this modern time. The fact is such a search engine could provide us an access to private, business and critical assets and for such a reason – it can be considered as so frightening due to its capability to – once in hands of malicious actors – threaten our safety and security. The purpose of this chapter would be to discuss all aspects being covered with this emerging technology as well as analyze its security's capacities being offered to its expert's community.

The role of this search engine

The Shodan is a quite convenient tool for searching the Internet of Things (IoT). Some sources would describe it as so scary, but we would agree with that in case – it gets in hands of the bad guys. This

searching tool would offer an opportunity to obtain feedback information from many devices being connected to the web. At Shodan's homepage – you would notice that there is a searching bar which would allow you to enter some keywords being the criteria for your crawling. Also, you would notice that there would get provided some accesses to the next page which would deal with the web cameras, refrigerators, industrial control systems and much more. The Shodan's homepage is illustrated in a Figure 1 as follows. This homepage could offer you a good insight into how this system appears and works as well as remove some misunderstandings about its scariness.

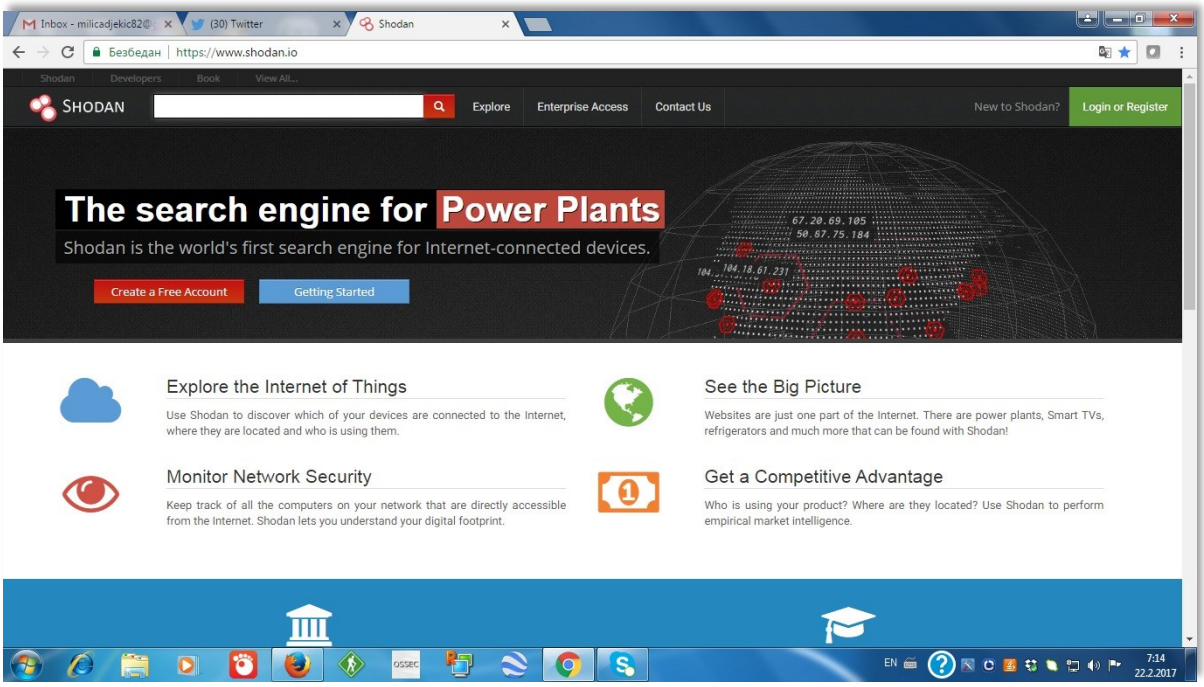


Figure 1. The Shodan's homepage

As it's presented through the previous Figure – the Shodan would appear as a quite typical search engine giving you a chance to make a search relying on many different parameters. For instance, you can explore the IoT, monitor network's security, see the big picture or get a competitive advantage. In addition, this tool would seek from you to create your own account doing some sort of a registration. The reason for so is that would make you leave some information about yourself and support the case if anything gets wrong. We are fully aware of that such a search engine could get exploited by the hacker's community that could work for organized crime groups or even terrorist organizations. The point is that these guys could try to do something, but they would get caught shortly. The next page within a Shodan's environment is given in Figure 2 as follows. That illustration would offer us an option to make a closer look at all the possibilities of such a tool.

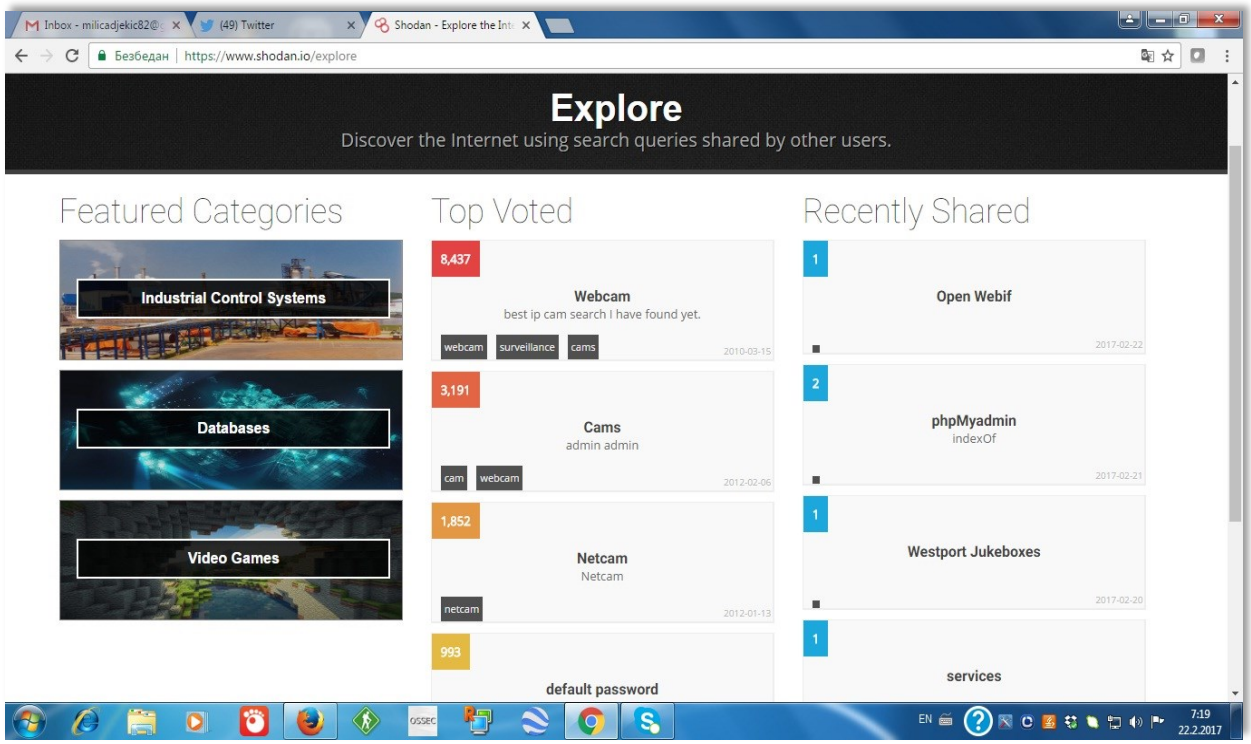


Figure 2. The typical Shodan's webpage

The illustration being offered in a Figure 2 would show us how it functions if we try to explore this searching tool. As illustrated – there would be many opportunities such as industrial control systems, databases, video games, web cameras, services, default passwords and so on. We would strongly encourage the expert's community or even an average user to try to play with these options and through such a research – attempt to discover all the potentials of this amazing tool. We are also aware of all the disadvantages that may occur if this service is used inappropriately and illegally. Finally, as already suggested through this learning material – the Shodan could get found at the following web domain – www.shodan.io – so we would recommend to everyone to try to track even their own devices being connected to the web and somehow discover how they could get protected from the malicious operations.

Would the Shodan be good or bad?

There would be many discussions trying to conclude if the Shodan is good or bad. As we would indicate – that depends on people using it. It's quite clear that people dealing with their private, business or strategically important infrastructure could use this tool to improve their security's capacities. So, if it's applied by good people – the Shodan would be good. On the other hand – if in the hands of bad guys –

this tool would get bad. As we would already say – this search engine could support us in resolving the case, but we are quite skeptical about its capacities in terms of preventing the crime even happens.

So, the only reason that could leave the bad guys far away from this service is that they would so commonly get aware of the consequences in case they try anything. Maybe some terrorist organizations would not think like so. They would seek an opportunity to obtain their task even such an operation would lead them into a certain death. Those folks are usually fanatics and we would strongly appeal to the international defense and intelligence to have this in mind any single time they deal with the Shodan and those cases of extremism.

Our recommendation would be that a technology should progress faster in order to alarm the Shodan's owners about any attempt of logging in from any concerning part of the world. As it's known, the terrorists could come from the westerns countries as well which would make this task being much complicated and leave this question remaining open as one of the challenges to the future.

The Shodan and expert's community

The Shodan would so commonly be correlated with the expert's community that would use it for its researches trying to find some vulnerability within the IoT functioning as well as some ways of improving its security's capabilities. Even the Shodan's creators would agree that their primary intent was to make something being so suitable to researchers who got interested to explore all the frontiers of an IoT technology. So, we would suggest to anyone dealing with this search engine to try to find the weaknesses of his own IT system as well as follow the best practice in order to leverage its computing abilities.

The concluding talk

As it's given through this chapter – we would begin this effort with the attributes such as the scariest searching tool of today and finish our talk with the quite peaceful conclusion saying that the Shodan is not that bad at all. So, what is the truth? The fact is this tool would obtain the tasks depending who would use it for which purposes. If it's in the hands of good people – it would be good. On the other hand, it would become our nightmare. In conclusion, we would highly recommend to all researchers, scientists and engineers to work hard on the next generation Shodan that would offer us much safer web environment.

References:

[1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.

[2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine

[3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine

[4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine

[5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine

[6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine

[7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine

[8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine

[9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine

[10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal

[11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine

[12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine

[13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine

[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

[15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine

[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

About The Author

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

The Intersection of OT and IT: Why Unified Cybersecurity is More Important than Ever.

By Craig Burland, CISO, Inversion6

Computer-controlled devices are all around us. From delivery robots to smart buildings to shipping and transportation, computer-controlled devices that affect the physical – not digital – domain are embedded in our daily lives. This Operational Technology (OT) connects and automates the factory floor, manages cutting-edge buildings, navigates ships across oceans, and will soon outnumber human drivers on our streets and highways.

OT also offers tremendous opportunities to mine data about systems that can directly translate into profits. Unfortunately, these computer-controlled devices carry steamer-trunks full of technical debt, raising a host of cybersecurity concerns that threaten to negate the upside and potentially create enterprise-wide disasters. The collision of the Information Technology and Operational Technology worlds has arrived.

OT security debuted on the world stage in 2010 when the, now infamous, Stuxnet virus infected the Programmable Logic Controllers (PLCs) managing the centrifuges of an Iranian nuclear weapons facility, causing an operational incident that derailed Iran's weapons program. The worm unintentionally spreads far beyond its intended target and infected thousands of other devices worldwide, bringing attention to the threat imposed by OT. More recently, Russia included attacks on unsecure UPS devices as part of its war on Ukraine, returning the spotlight to the flaws in OT security.

Four interconnected issues make securing OT a serious and challenging cybersecurity problem:

- Uptime is king
- Productivity is queen
- OT was built for the manufacturing lifecycle
- Cybersecurity was not part of the design process

OT solutions are designed for environments where uptime was the main requirement. Machines going down means that products are not being built, directly impacting customers and revenue. The need for multiple 9s of availability crowds out requirements like patching or dynamic protections. Manufacturers often employ extreme measures to avoid operational outages, going as far as stockpiling and cloning obsolete equipment like Windows XP PCs to avoid accommodating dynamic elements in the environment. This is why the Wall Street equivalent of "Cash is King" on the manufacturing floor is "Uptime is King."

Productivity, for the operators and engineers, falls a close second to uptime for similar reasons. More efficient workers produce more products for the same labor cost, generating more profit. Friction like entering a username and password is viewed as lost time. Increasingly, standardized automation systems are supported by engineers and designers that don't have physical access to the devices, but remote in to pull data or optimize machine parameters. For the organization, this maximizes efficiency. For cybersecurity, this maximizes the attack surface.

Devices in the manufacturing world are built to last decades and often cost millions of dollars. Maintenance on the factory floor means periodically shutting machines down to calibrate sensors, change the oil, tighten bolts or refurbish parts. It does not mean applying monthly security patches to the HMI or PLC. This is not an inconsequential miss. The lifecycle of these devices can be 15 to 20 years, not the 3 to 5 years of an IT asset which puts a considerable burden on the cyber and IT organizations.

The last challenge -- the absence of cybersecurity requirements in the design process -- is more than the simple derivative of technology designed to maximize uptime, productivity and long lifecycles. It underscores a lack of awareness or understanding of the threat. Unlike phishing or malware incidents, OT compromises rarely make headlines. They fall into an unaddressed quadrant of a standard heatmap – highly unlikely, but potentially catastrophic – typically leaving them as an unaddressed item on the priority list.

But despite these hurdles, organizations have options to reduce risk. These options must be employed smartly, recognizing that some control is better than none and understanding that too much friction will backfire. They must also be employed specifically, acknowledging that OT is not IT. Forcing strong credentials and Mult Factor Authentication (MFA) onto the machine operator won't work. Your preferred Endpoint Detection and Response (EDR) won't run on a PLC built with a custom version of Windows7. That standard GPO locking forcing a session timeout will disable a domain-connected Human Machine Interface (HMI).

The single most important control to employ is segmentation. To borrow a tagline from Las Vegas tourism, "What happens in OT, stays in OT." Establishing a boundary between the IT and OT environments is essential to gaining visibility, identifying risk and exerting a measure of control. In many respects, this mimics the barrier between a private network and the Internet. It's unthinkable for an organization to have unmanaged access to the Wild West of the Internet given its ungoverned nature

and unknown threats. Considering the hygiene of a typical OT environment, it should be equally unthinkable to allow unfettered access between IT and OT.

With a capable boundary in place, deploying other core elements of cyber defense becomes possible. In the world of cyber, Visibility (not Cash) is King. You can't defend what you can't see. Capturing traffic moving into and out of the OT segment can reveal surprising risks, but also opens the door to controlling those risks. Lots of SMB traffic moving into the OT segment? Find out why. Find out who. 3rd parties remoting into the OT segment. Find out who. Find out why. Devices beaconing out to known C2 sites? Well… just stop those. Then capitalize on the incident to build a comprehensive strategy to defend OT that runs the gamut from awareness to asset management, from procurement to active prevention, from cyber requirements to remediation.

Protecting OT is complex and unique because of its primary drivers – uptime, productivity and extended lifecycles – but not impossible. The principles cyber defenders use to protect information technology can be applied to operational technology; the tools used can be successfully adapted. While the worlds of IT and OT are coming together, a well-planned cyber response can help merge these worlds instead of causing a crash.

About the Author

Craig Burland is CISO of Inversion6. Craig brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. He is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Global Security, and Oracle Web Center. Craig can be

reached online at LinkedIn and at our company website http://www.inversion6.com.

Using Data Analysis to Identify Security Threats: An Overview

By Howie Robleza, Freelance Writer, Avigilon

Security is an important component for the development of any business. However, hackers are becoming more sophisticated and frequently developing new means of gaining access to company data. According to research published in recent years, hackers have gained access to more than 5.2 million records of personal data, posing a significant threat to the development of modern businesses by placing identifiable customer data at a heightened risk of attack.

Developing a way to reliably identify security threats is a major milestone that many businesses are yet to achieve. Though as the modern world is so reliant on usable data, companies that understand how to properly secure sensitive information stand a better chance of elevating their security standards to ultimately improve project developments and ensure business success.

The application of data analytics used to identify security threats is a broad field that involves different components designed to improve upon security standards, spanning from physical security technology such as keyless access systems, to cybersecurity analytics tools. This article discusses modern applications of data analysis used to identify and nullify security threats.

What is Security Threat Analysis?

Security threat analysis is a cybersecurity strategy dedicated to evaluating the security protocols present within a specific organization. This process involves several different methodologies and procedures designed to identify active threats to company data, and is intended to locate any vulnerabilities in data storage systems as well as collect information regarding potential attacks.

For instance, if a company is using cloud-based badge systems to reduce expenses related to on-site server maintenance, security threat analysts will be tasked with ensuring the security of all files stored within the system and creating protocols designed to prevent data breaches.

When security agencies use data to study the structure of any given organization, they'll often quickly detect a number of exposed security exploits that must be addressed. Engaging in this process helps teams to gain a clearer understanding of how sophisticated threats may pose a risk to company and customer data, as well as highlight possible solutions to combat issues.

The application of data analysis in security departments aids in the collection of usable data, which in turn helps teams to make vital decisions when safeguarding employees and customers alike. This holistic approach to business security has a successful track record of preventing security breaches and creating safer environments that can contribute to business success.

During a typical threat analysis process, several different types of security threats will be analyzed by security personnel, including:

Intentional Threats

Intentional threats are a primary concern for most companies due to the impact they can have on business development. These types of threats are typically conducted by malicious entities looking to gain access to valuable company data. Hackers will look to locate and access sensitive files like financial information or customer records that can be used for criminal means.

Internal Threats

Most companies design strategies to safeguard themselves from internal threats by siloing data systems to prevent large scale breaches. However, many business owners fail to understand that bad actors within security departments can have a huge negative impact on the efficacy of segregated systems, as

it only takes one team member deciding to act in a malicious way to expose essential networks to comprehensive data breaches and company-wide security threats.

Accidental Threats

Human error is a major component that puts many companies at high risk of attack, in fact, Verizon's 2022 Data Breach Investigations Report found that 82% of recorded breaches come as a direct result of employee mistakes.

During threat analysis processes, companies should make efforts to highlight systems likely to be at risk from human error, for example, multiple siloed data storage systems that share the same password. If hackers are to identify this weakness, large-scale breaches could occur.

Benefits of Data Analysis in Identifying Security Threats

As business technology continues to become more advanced, security risks are also increasing day by day. In order to appropriately defend essential systems from evolving cyber threats, security and IT teams must ensure that they're one step ahead of sophisticated cybercriminals.

The best way to overcome hacking activities is to gain a detailed understanding of how modern threats work and the main systems or technologies that these attacks are targeting. Below are some of the benefits of using data analysis to identify security threats within a business setting.

Reducing the Attack Surface

When a company enforces a strong threat analysis strategy, the available attack surface for hackers to target will be automatically reduced, effectively limiting the number of cyber attacks security teams will be required to face. By locating vulnerable systems using data-informed research, teams can ensure that security resources are being utilized as efficiently as possible.

Updating Risk Profiles

Analyzing threats regularly and identifying key areas of concern will make it easier for teams to create updated risk profiles that help security departments to improve incident responses. This allows businesses to elevate their security posture by developing a safe environment that supports wider business growth. In addition, an updated risk profile can be used to aid business leaders in conducting data-informed security audits within a secure business environment.

Collected data is used continuously to improve the security posture of any given business and can help teams make informed decisions with regards to incident responses, helping staff to monitor the progress of security systems and identify any extra measures that could be taken.

Continued Updates to Threat Modeling

A great way to foster a safer business environment is to create updated security models that will guide teams when making security decisions. Threat models are designed to give staff a clear picture of the current security state and determine some of the changes that can be made to create a safer environment. Note that threat models are constantly changing, meaning they will need to be updated frequently. For every new technology that's integrated into existing security systems there comes new threat models that will need to be appropriately addressed.

How to Conduct Threat Analysis

Using data-informed tools to conduct threat analysis is a detailed process that can take different forms. How the threat analysis process develops will depend on your security requirements and the goals you wish to achieve. Below are some of the steps required to perform threat analysis.

- **Define the Scope of the Threat Analysis**

If you want to conduct a successful threat assessment, you'll need to start by defining the scope of the entire process. This approach will help you to put in place a reliable foundation and will aid in the execution of an effective process. Teams must define all the major aspects that need to be covered throughout the threat analysis by conducting a pre-planning procedure that should present a clear roadmap of how to ultimately execute the task.

- **Establish the Processes and Procedures Required**

After building the scope and defining the goals you intend to achieve, you'll need to determine what needs to be covered during the analysis. Since the scope gives you a clear roadmap, the process and procedures chosen should work to generate your desired output. Choosing which systems to cover should present a clear way to perform any resulting threat analysis process.

- **Create a Clear Rating System for the Threats**

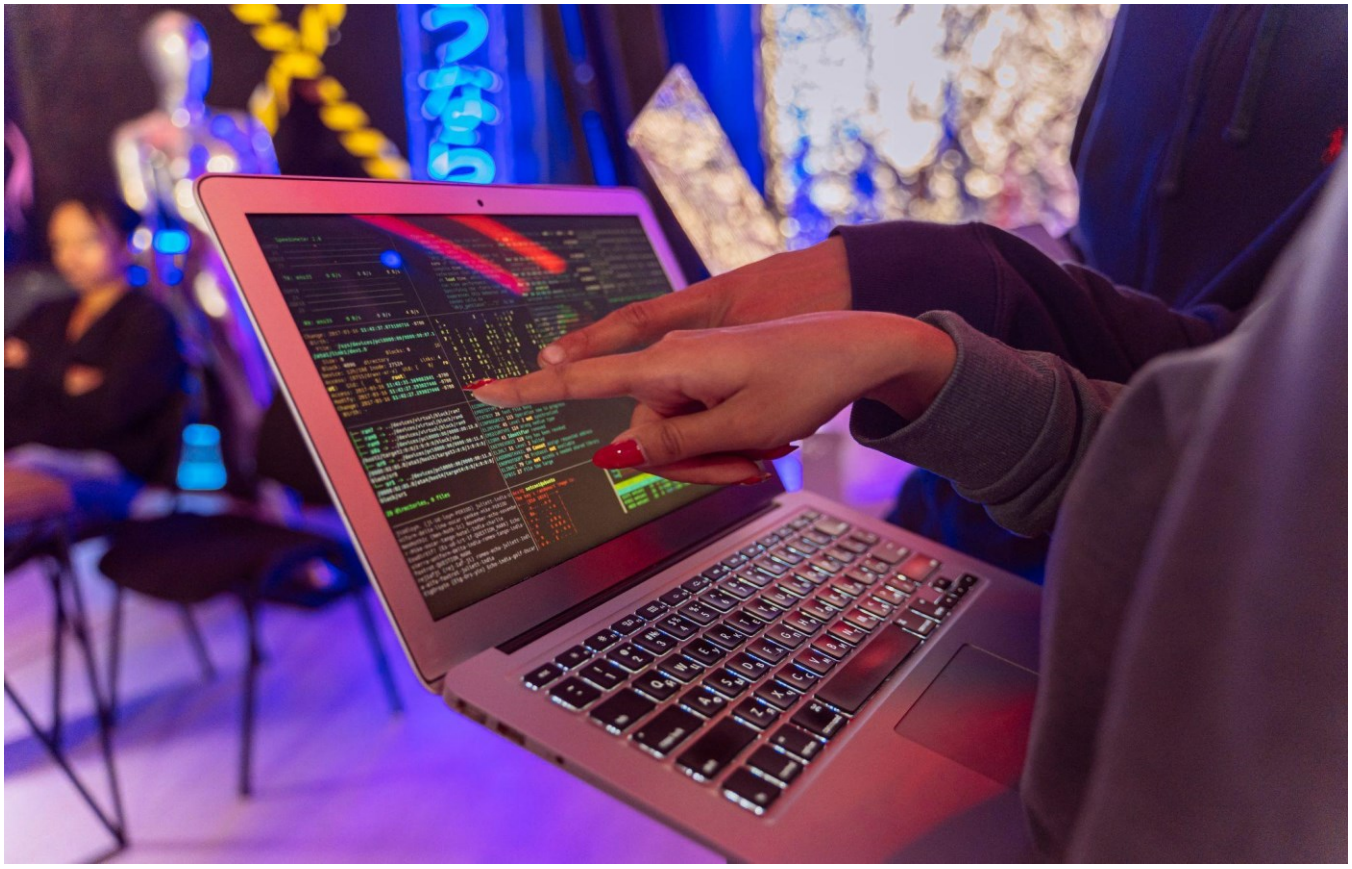
Creating a rating system will help you to define the severity of any potential security threats. This system should determine the risks and vulnerabilities that may impact critical stakeholders within the business as well as aid in the formation of a reliable post threat analysis report.

- **Conduct the Threat Analysis**

Once all other activities are complete and all procedures are in place, you can now conduct a threat analysis. At this point, companies need to maximize the capabilities of the security teams to gain crucial information from their systems, you may also choose to invite a third party to help in conducting threat analysis and offer impartial advice and opinions regarding the final process.

Security posture is essential to modern companies and must be considered by all stakeholders. Hackers are constantly working to identify new methods to break firewalls and access business data. Finding reliable ways to identify security threats is a vital process that companies must put in place to aid in the detection of unusual activities that can impact integrated security systems.

Data visualization and analysis helps security teams to detect unusual activities in their data, ultimately preventing unauthorized access to important business systems. This technique of converting general data sets into easily understood visuals like anomaly charts, comparison charts, and Sankey diagrams makes it easier for security agencies to translate information and implement required security measures. Data analysis is also a significant innovation that plays a crucial role in creating data reports designed to improve incident responses to future threats.



About the Author

Howie Robleza, a freelance writer is interested in tech, legal, and property trends. When she's not writing, she works in commercial property management.

Howie can be reached at www.avigilon.com.

Why CISOs Should Prioritize Cloud Security and Access Management During Digital Transformation Initiatives

By Ameya Khankar, Cybersecurity Consultant for Critical Infrastructure

Companies undergoing digital transformation have decided to take the plunge into modernizing their core product offerings. It can be an arduous process, but it gives organizations the unique ability to reimagine their business. They can implement modern digital best practices and set themselves up for continued success.

Part of that transformation process involves improving security. Companies undergoing digital transformation in 2023 likely aren't secured for modern security threats, especially not in the cloud, and have the opportunity to improve those controls.

CISOs should prioritize improvement in cloud security controls and access management in the cloud environment. Lax cloud security and access management controls have verifiable consequences as highlighted by high profile data exfiltration events that have hit Fortune 500 organizations in the past few years.

In this article we'll outline how digital transformation efforts prime security focused organizations for effecting change and why they should drive those changes.

Digital Transformation Efforts Prime Organizations for Continued Success

Digital transformation efforts are typically more than just lift-and-shift propositions, even if positioned as such. They frequently involve evaluating the business model and restructuring application architecture and refining elements of the code base to optimize them for cloud scalability and resilience. Doing so saves on unanticipated costs.

It's an opportunity for CISOs to reevaluate security posture and improve on security controls. Cloud services often include robust security safeguards and infrastructure that need to be configured and managed appropriately for sustainable security environments. These cloud security measures are critical.

Placing assets in the cloud ostensibly opens new and broader potential for access if environments aren't configured and secured appropriately. Erecting impediments to compromising sensitive data is important.

CISOs also need to ensure that the business continuity benefits of cloud hosting are realized. One of the main benefits of migrating assets to the cloud is the ability to failover to hot storage backups, scale those resources, and also have access to frequent cold storage backups. Failing to configure a cloud environment to utilize this functionality and its benefits may mean a missed opportunity with potential downsides.

Cloud environments also offer enhanced capacity for event logging and compliance monitoring. Major cloud services offer both and integrate well into numerous security monitoring and alerting infrastructure stacks. They also offer on-the-fly modification to compliance settings to ensure that sensitive and even highly regulated data is secured as needed. These compliance settings also streamline organizational audits by exposing relevant information to internal teams for monitoring.

Where CISOs can improve asset security and save resource investment, the result will be a foregone conclusion to improve security.

Significance of Cloud Security and Access Management

Cloud services are an essential aspect of digital transformation initiatives. Those services allow organizations to improve agile product delivery, resilience, scalability, and cost efficiencies. Cloud environments are complex and dynamic, making it challenging to secure them against cyber threats.

Cloud security refers to the set of practices and technologies designed to protect cloud-based data, applications, and infrastructure. The risks associated with cloud security include data breaches, misconfigurations, and insider threats which can lead to unauthorized access and misappropriation of information.

Access management is a crucial subset of cloud security concerned with ensuring that only authorized personnel can access the cloud-based resources, data, and applications they're authorized to access. Access management involves the processes and technologies that manage user identities, permissions, and authentication and authorization to control access to cloud resources.

Identity and access management (IAM) solutions are a critical component of access management in cloud environments. IAM solutions provide centralized management of user identities, authentication, and authorization policies. They help standardize and enforce a canonical basis for access controls whether that is role-based, attribute-based, or relationship-based.

Multi-factor authentication (MFA) is another critical component of access management that can help mitigate the risks associated with weak passwords and unauthorized access. It's become a de facto standard for mitigating authentication risks by requiring the use of an additional access token that should be unique to the end-user.

In some cases, on premises or collocated technology implementations can accommodate these technologies without a great deal of change. In other cases, they cannot. CISOs need to evaluate the security capacity of software technology to be migrated and modified in the context of their new environment. If those security measures aren't feasible in the cloud or would be overwhelmingly difficult to implement, CISOs need to emphasize the criticality of focusing on the safeguards.

Why CISOs Need to Prioritize Cloud Security and Access Control

Many organizations don't prioritize improved security measures. They also don't focus on modifying access control schema. There are many perceived reasons why security ends up on the digital transformation back-burner.

First, cloud security is novel. Organizations with heavy on premises or collocated infrastructure aren't experts in the new cloud security technologies available to them. Where organizations have to make an investment in training on revised architecture and application design to reduce costs, they may think that they don't have to do the same with security. Bafflingly, they may make the decision that old security practices are ok when nothing else is old about the technology stack.

The impact is tangible: security practices that are outdated or ill-suited for a cloud environment can result in the compromise of that environment. This is an educational and political hurdle and one CISOs need to overcome by enlightening their technology peers about the pitfalls of poor cloud security posture. Additionally, that education needs to highlight the architectural complexity of "fixing" security after the fact.

Second, cloud security can become a cost function. Many organizations stop their evaluation without realizing that additional cost is minimized and the return on investment maximized when cloud security is implemented during migration stages. Conversely, that cost is maximized and return on investment minimized when security is implemented as an afterthought to the cloud migration effort. As highlighted above, cloud security may require re-architecture of the underlying migrated assets. Failing to address that during the migration will result in increased and duplicative costs.

Some organizations may decide the additional cost isn't worthwhile. That's a penny-wise, pound-foolish approach in the extreme. Failing to implement those cloud security practices leaves the environment open to attack which can result in extreme costs to remediate an attack and support client efforts to do the same. Cyber-attacks are a matter of when and not if, so it's a foregone conclusion that a cyber-attack will happen. Preparing a solid defense pays dividends down the road in mitigating the blast radius of the attack.

Third, the best time to train a security team is during implementation of new resources. Training a security team after resource implementation, like a large-scale migration project, leaves the security team in the dark for how to best protect the environment and support infrastructure. That training failure ensures that industry standard security practices can't be implemented and therefore the environment won't be reasonably safeguarded. That's critical, say, in a post-breach event class action suit where plaintiff's counsel will want to understand whether or not those reasonable safeguards were in place.

Including security training credits or courses prior to a migration effort should be top of mind for CISOs. It's unlikely a migration would be undertaken without some kind of training and cloud security infrastructure training needs to be included in that. Including security training at the outset also helps lock in predictable pricing for that.

CISOs need to rally and focus organizational leadership around the need for robust security and access controls at the outset of a digital transformation project. Those considerations should be developed and implemented in parallel with other transformation initiatives. Once the digital transformation project is complete, it may make accommodating adequate cloud security a difficult objective.

If adequate cloud security isn't in place at the outset of a digital transformation project, it places those corporate assets at substantial risk. Organizational leadership needs to understand that the risks in a generally public cloud environment are more significant than the risks for on premises or collocated infrastructure and assets with easily definable ingress and egress points. Improper security and access configuration can proliferate access points and expose mission critical operations or information for compromise.

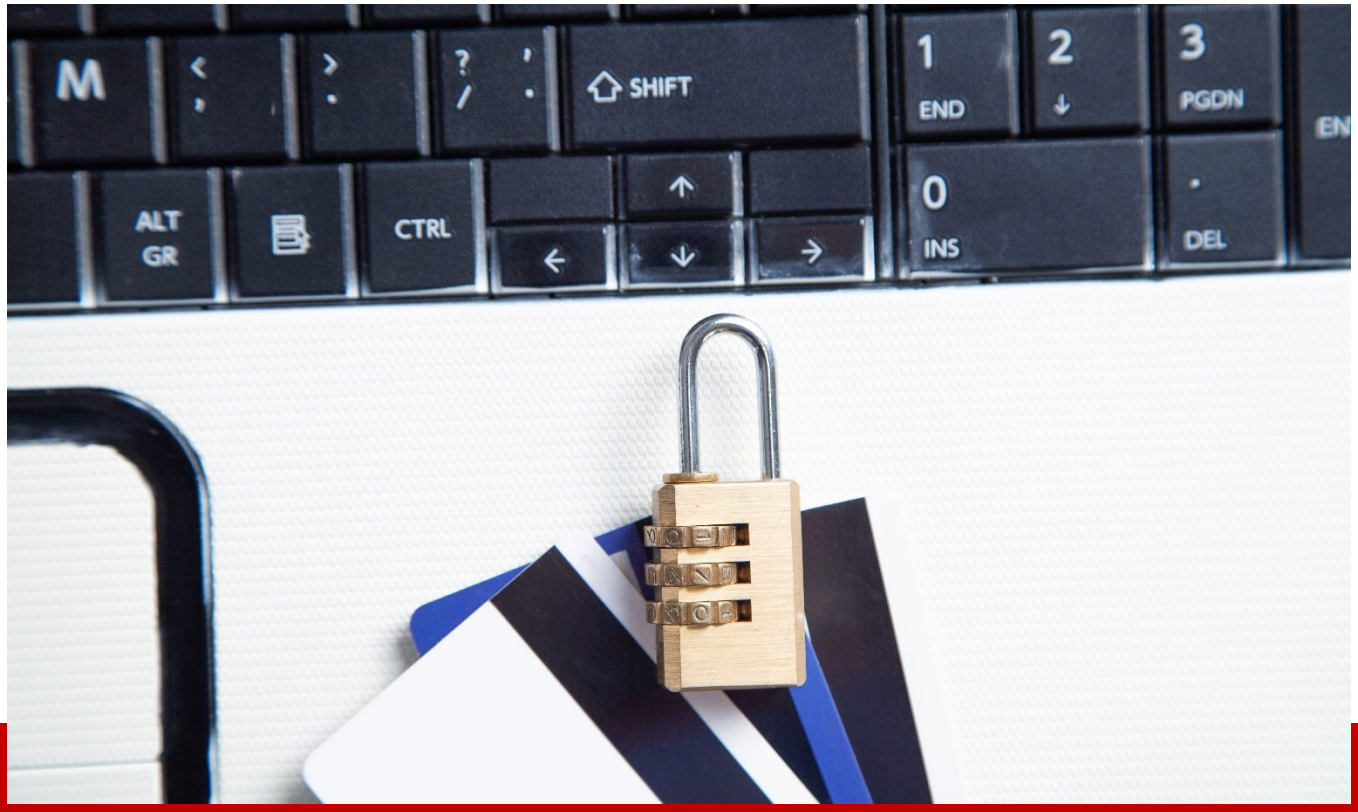
Conclusion

CISOs need to make a robust case for improved and modified security and access control considerations at the outset of a digital transformation project. Security and access in the cloud environment is qualitatively different than in an on-premises or collocated environment. The risks are also more substantial in a cloud environment, which is designed to facilitate broad client access.

Digital transformation projects are the perfect time to implement improved security measures. Other aspects of on premises or collocated assets will be modified to account for the new realities of cloud hosting. There's no reason security and access controls shouldn't be included in those efforts. CISOs need to advocate for those changes and ensure that they're implemented. Those changes can make or break digital transformation initiatives.

About the Author

Ameya Khankar is a global expert in the areas of business technology and cybersecurity access management. His deep expertise in the area of technology risk, cloud access management, enterprise transformations, and digital governance has helped numerous global enterprises strengthen their cybersecurity posture and improve their risk management practices. Ameya has advised several F500 organizations in the past with defining their business transformation and enterprise security strategies. He has been awarded the prestigious Indian Achiever's Award for Cybersecurity which is recognized by the Government of India and the Cybersecurity Excellence Award which is recognized by the National Institute of Standards and Technology (NIST) part of the U.S. Department of Commerce.



Why Cybersecurity for Private Equity Is Urgent Now – And What Funds Can Do to Move the Needle.

Private equity fund-level technology leaders can play an impactful role in protecting their portfolio companies from cyber-attacks, from due diligence through exit

By John Hauser, EY Americas Transaction Support – Cyber Due-Diligence Leader, Ernst & Young LLP

Private equity funds are struggling with a recent wave of cyber attacks affecting their portfolio companies. The FBI, private equity leaders and EY-Parthenon teams steeped in cybersecurity consulting are seeing a measured increase in cyber activity targeting PE transactions and portfolio companies, where victims are perceived to be easier targets with deep pockets to pay extortionate ransomware demands.

In addition, there is increasing legal and regulatory pressure on all varieties of portfolio companies. This pressure increases risk that an incident will have a domino effect on a company's reputation and add to its list of post-incident damage control and recovery efforts. For example, both the European Union and the United States have passed legislation which requires companies in critical infrastructure to timely

report incidents to the government. The Securities and Exchange Commission recently passed new rules which put pressure on senior management and boards to be engaged and disclose the efforts they are taking to reduce cyber risk. Recent litigation in the US has put companies on notice that they must incorporate cybersecurity into their diligence process to ward off claims of negligence in the event of a later breach.

A single significant incident can be so disruptive that it throws off a fund's investment plans and timetable for the company to exit the portfolio. Yet unlike corporate parents, funds are not equipped with their own cyber teams that can provide direct protection to portfolio companies. Some funds also worry that getting too involved in the portfolio company's cybersecurity could increase risk to the fund itself.

Still, funds can play a significant and impactful role in protecting their portfolio companies, even short of taking over portfolio companies' cyber programs. PE fund-level technology leaders can build a more comprehensive cybersecurity strategy throughout the portfolio company ownership lifecycle, from due diligence and acquisition through exit.

Here are some of the ways that funds can be helpful:

Stay focused on portfolio company cybersecurity throughout the ownership lifecycle

- Funds that use cyber due diligence as an early indicator of potential problems can protect themselves from claims of negligence and will gain an advantage over funds that don't.
- Funds can continue to emphasize cybersecurity during portfolio company onboarding, when cyber outcomes should be included as part of the strategic plan settled upon by senior leadership.
- A program during the value creation period that tracks deficiencies in portfolio company cybersecurity and escalates the response will help all parties stay ahead of risk instead of waiting for an incident to be the first indicator of trouble.
- A view of what cybersecurity success looks like prior to exit readiness will leave funds and portfolio companies in a much better position to preserve value and not make cyber a significant concern for a future buyer.

Leverage purchasing power to drive efficiencies

Without replacing portfolio company procurement, funds can establish "preferred partner" programs, with reputable security vendors driving vendors to reduce prices and allowing portfolio companies to enjoy discounted services. Funds can also vet security vendors to confirm that portfolio companies are using industry-leading providers. Meanwhile, vendors receive the benefit of being a trusted name in the portfolio and a streamlined channel to market.

Collect data on portfolio company cybersecurity programs in order to realize synergies

Recognizing its unique position of having an overview of all portfolio companies lets the fund drive extra cybersecurity value. For example, funds which can identify common pain points among different portfolio companies can bring in expertise to help reduce risk at scale.

Play a valuable role in enabling effective leadership.

Funds typically have one representative on the portfolio company board. That board member can drive greater accountability and focus on cybersecurity. In addition, funds can often influence the high-level leadership at the portfolio company so that the right talent is driving results. This oversight allows the fund to play its traditional role of high-level governance, while also making it clear that better cyber outcomes are expected.

The need to improve cybersecurity goes beyond the potential financial and reputational risks of a successful attack. Portfolio companies with lax cybersecurity also run the risk of being left out of competition for government contracts and private sector business.

The strategies above, however, can represent a groundbreaking shift for private equity's ability to mitigate the risk of a growing threat.

About the Author

John Hauser is the EY Americas Transaction Support – Cyber Due-Diligence Leader. John's career comprises nearly 20 years of public service and private sector experience. At EY US, he heads innovative, market-leading cyber due-diligence practices, which help clients navigate the heightened technology and legal cyber risks posed by transactions.

Prior to joining EY US, John worked as a Special Agent with the FBI and as an Assistant United States Attorney. He has extensive experience investigating and prosecuting complex, high-profile cases, including international cybercrime rings and nation-state hackers who stole trade secrets from US corporations.

John can be reached online on at ey.com.

The views expressed are those of the author and do not necessarily represent the views of Ernst & Young LLP or any other member firm of the global EY organization.

Zero Trust Security: Pioneering Solutions on a 'Never Trust, Always Verify' Principle to Overcome Modern Cyberspace Security Challenges!

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

Zero trust security is a method of cybersecurity that undertakes that no user or device can be reliable, whether outside or inside the corporate network. Unlike traditional security models that rely on perimeter-based approaches, zero-trust security eliminates the notion of trust to protect data, applications, and networks.

Zero trust security is intended to protect assets and information by providing fine-grained access control, unremitting monitoring, and risk-based verification. This means that all requests to access network resources are validated regardless of whether they come from untrusted or trusted devices or users.

The zero-trust security model is growing in popularity because remote work and the rise of cloud-based applications are creating new security challenges for businesses. This security model trusts no one and nothing. It provides optimal security against ransomware and cybersecurity threats.

The main principles of zero trust security infrastructure include continuous monitoring and validation, least privilege, multi-factor authentication, etc. Zero trust security solutions help to reduce an organization's attack surface.

Zero Trust Security: Protecting Business in a Perimeter-less World

The proliferation of endpoints and increased adoption of cloud technologies has augmented the need to implement a zero-trust security outline. Modern businesses thrive on network technologies and computerized systems that are vulnerable to attack to unofficial access.

Remote work guidelines due to the pandemic have further increased the need for a secure architectural framework. These are used to enforce multi-factor verification for access to sensitive data. This in turn is putting the zero-trust security market into the limelight.

Accordingly, the growing need to protect complex networks facilitates network management transparency and combats external & internal threats of unauthorized access will drive demand for security solutions, including zero trust security.

As per Future Market Insights (FMI), a leading market research firm, the worldwide zero trust security market size reached around US$ 25.4 billion in 2021. Over the next ten years (2023 to 2032), global zero trust security solutions demand is likely to surge at 15.1% CAGR. By 2032, the total market value is expected to reach US$ 118.7 billion.

Ratings of reported attacks and interruptions suggest that record disclosure rates and data breaches have increased over the years. Attacks like the WannaCry ransomware are complex and destructive, allowing unauthorized access and occasioning loss of data and revenue.

As cyberattacks and their associated consequences change, the vulnerability assessment industry is investing more in new technologies. These include analytics and artificial intelligence (AI).

The zero trust security market is set to witness a positive growth trajectory. This indicates that end-users are ready to counter vulnerability attacks and increasing investment in security strategy initiatives.

Zero Trust Security and SaaS Model: Adapting to the New Normal

Companies are outsourcing security services due to a lack of in-house trained workers. Security services for applying a zero trust security model enable professionals to deliver protection as a Security as a Service (SaaS) model without the need for additional staff or hardware.

Organizations struggle to keep their networks secure due to rapidly developing wide area network (WAN) environments and the rising difficulty of enterprise systems. The need for a more deliberate attempt to protect corporate networks and provide layered security is encouraging the adoption of zero-trust security solutions.

The pandemic has made organizations realize the position of a zero-trust environment to protect critical data.

The IT security landscape has changed dramatically as employees work remotely and use vulnerable network infrastructures. This makes it difficult for organizations to uphold a network perimeter-centric sight of security, letting tech-savvy hackers target indiscreet systems with phishing attacks.

Cloud Security: Ensuring the Safety of Data in the Cloud

The increasing acceptance of cloud technologies in the enterprise has increased the need for zero-trust security solutions. As enterprise IT infrastructures become more resilient and complex, the peril of internal security breaches through unauthorized access and external cyberattacks increases year by year.

Connected devices with AI and IoT capabilities are constantly collecting data and storing it in the cloud, making them vulnerable to hackers.

As such, security vendors have begun highlighting the adoption of a zero-trust model for a robust and holistically protected IT environment. Several vendors are also directing on scaling endpoint safety for digital revenue models.

From Office to Anywhere: The Benefits of BYOD for Remote Work

Bring Your Own Device (BYOD) trends are surging across all establishments. Benefits such as reduced costs in procuring terminal infrastructure and increased worker productivity from being able to work on familiar devices are pouring the spread of such perceptions.

The significance of the BYOD concept gained momentum during the pandemic as companies adopted a remote working model.

The increasing superiority of cyber threats and their negative influence on organizational operations are forcing multiple policymakers, governments, and institutions to implement and develop regulations. This in turn is creating lucrative opportunities for zero trust security solutions providers.

The Power of Data: Leveraging IoT for Business Insights

As the Internet of Things (IoT) spreads across the enterprise and more IoT applications collect customer data from multiple touchpoints, the peril of data theft or unauthorized access to data surges.

Privacy regulations and laws are significant to prevent such efforts. Such regulations force companies to comply with appropriate security regulations and develop zero-trust policies, thus driving the growth of the market.

Cyber threat agents or actors are constantly looking for different ways to infiltrate or gain access to IT networks, and vulnerabilities can be easily identified. Additionally, knowing your credentials can also help attackers break into cloud-hosted solutions and data.

Such challenges are expected to expand the scope of zero-trust security models and create high demand for advanced zero-trust security solutions.

The Bottom Line

Zero Trust security is an advanced approach to cybersecurity that provides fine-grained access control, and risk-based authentication. By assuming no trusted users or devices, this approach aids in protecting an organization's critical assets and data from evolving threats, such as those from remote work and cloud-based applications.

Zero Trust security symbolizes a fundamental change in how organizations approach cybersecurity.

Zero trust security has several benefits, including the condensed risk of data breaches, increased discernibility and control, etc., which are creating huge opportunities for the market. As organizations increasingly embrace remote work and cloud-based submissions, zero trust security is flattering a key component of their complete cybersecurity strategy.

To increase their revenues and expand their customer base, leading zero-trust security companies are launching new solutions. For instance, in June 2022 BlackBerry Limited introduced a new zero-trust network access solution with CylanceGATEWAY.

About the Author

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

About Future Market Insights (FMI)

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


EVENTS

6th Global Edition of
CYSEC GLOBAL SERIES

ORGANIZED BY
MAK

CYSEC SAUDI AND AWARDS

Building Saudi Arabia's Cyber Resilience for Critical Infrastructure Protection

INVITATION ONLY EVENT

- 150+ IT & OT Security Leaders and Government Authorities
- Two days of 1:1 Networking
- 30+ Speakers & Thought Leaders
- Keynotes, Panel Discussions & Case Study Presentations
- Cyber-Tech Exhibition & Demos
- CYSEC Awards & Recognition

SCAN ME
FOR MORE DETAILS

13 - 14 June 2023

Sheraton Dammam Hotel, KSA

SUPPORTING PARTNER

HEADLINE SPONSOR

HUAWEI

PLATINUM SPONSORS

kaspersky | CyberKnight | NETWITNESS | solarwinds | COLORTOKENS

GOLD SPONSORS

CIPHER | الحماية المرنة RESILIENCE | OIVAN

SILVER SPONSORS

Honeywell | LogRhythm | WALLIX | Barracuda | BULWARK | mimecast

BRONZE SPONSORS

ManageEngine | novigo

DEFENSE STRATEGIES INSTITUTE PRESENTS:
THE 3RD ANNUAL

CRITICAL INFRASTRUCTURE SECURITY SUMMIT

PROTECTING US INFRASTRUCTURE THROUGH ADVANCED CYBER CAPABILITIES

JULY 26-27, 2023

MARY M. GATES LEARNING CENTER

ALEXANDRIA, VA

INFRASTRUCTURE.DSIGROUP.ORG

JOIN THE CONVERSATION AND REGISTER TODAY

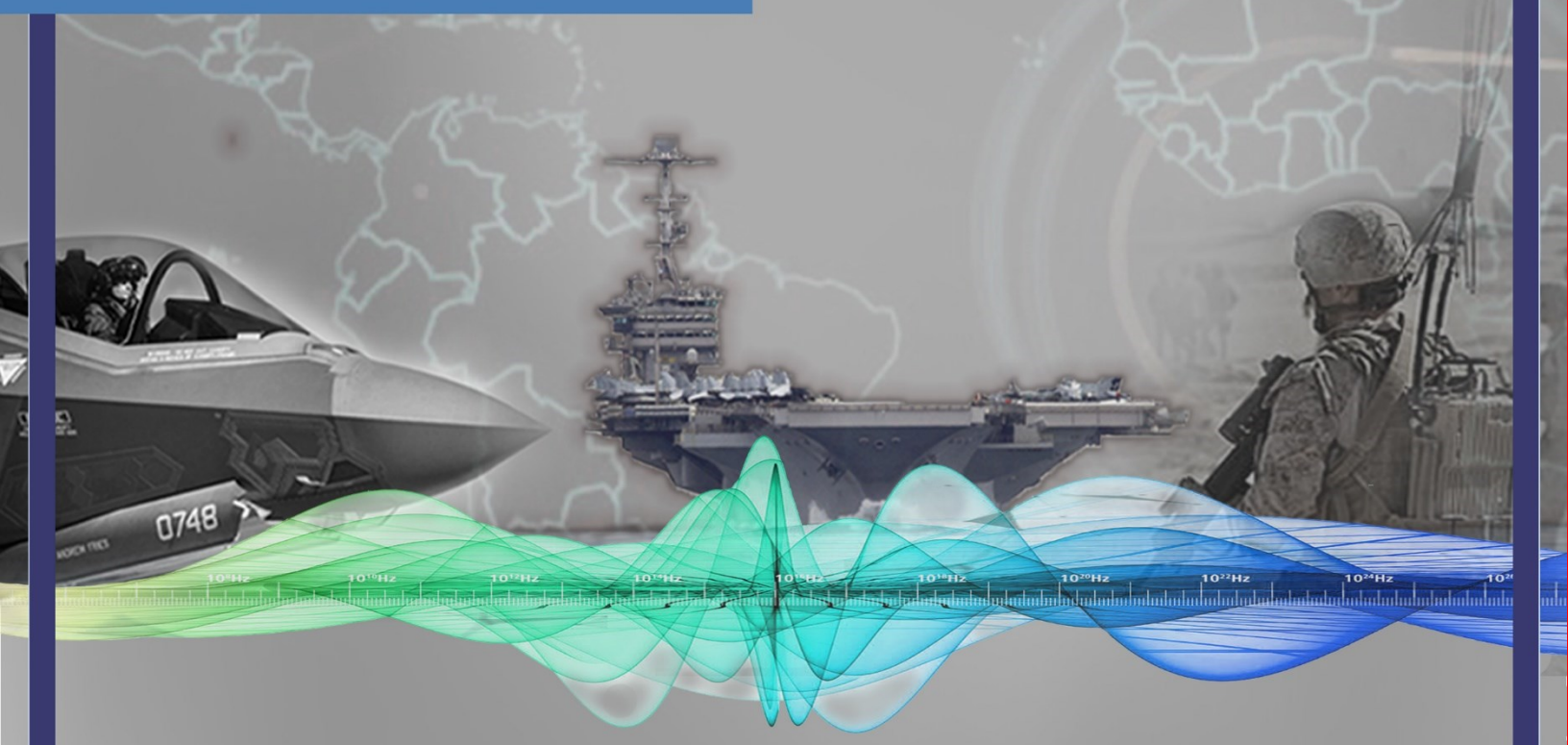
ACTIVE MILITARY AND GOVERNMENT EMPLOYEES ATTEND FREE

5TH INFORMATION WARFARE SYMPOSIUM

MILITARY/GOVT ATTEND FREE

NATIONAL HARBOR, MD

JULY 26-27, 2023



INFORMATIONWARFARE.DSIGROUP.ORG

Organized and Conceptualized by

3rd Edition

CONNECTED AFRICA

Africa's premier Telecom Event

"Transforming to Telco's of the Future"

July 25, 2023

Johannesburg, South Africa

For More Details

CYBER DSA 2023

15 - 17 AUG 2023 | KUALA LUMPUR CONVENTION CENTRE

ADVANCING DIGITALISATION & SECURITY THROUGH COLLABORATION

Have You Registered?

Get ready to connect with the top players in the **cybersecurity industry** at **CyberDSA 2023**

Scan the QR:
Register for **FREE Visitor Pass** to Exhibition.

Scan the QR:
Ticket for attending **All Access Conference** is now **ON SALE**

Forum & Tracks Schedule:
https://bit.ly/ForumTracks

www.cyberdsa.com | CyberDSA

SUPPORTED BY:
MINISTRY OF COMMUNICATIONS AND DIGITAL | MALAYSIAN ARMED FORCES | ROYAL MALAYSIA POLICE

STRATEGIC PARTNERS:
DEFENCE CYBER AND ELECTROMAGNETIC DIVISION (MAF) | CyberSecurity MALAYSIA

HELD IN CONJUCTION:
SIBER SIAGA 2023 | MALAYSIA CYBER SECURITY AWARDS | WBF WORLD BLOCKTECH FORUM

ENDORSED BY:
MATRADE

ORGANISER:
AEROSEA EXHIBITIONS SDN BHD (1357130-A)

TECHEX
EUROPE

Co-Located Events:

CYBER SECURITY & CLOUD EXPO
EUROPE

IOT TECH EXPO
EUROPE

BLOCKCHAIN EXPO
EUROPE

AI & BIG DATA EXPO
EUROPE

EDGE COMPUTING EXPO
EUROPE

DIGITAL TRANSFORMATION WEEK

Contact:
> www.**techexevent**.com
> enquiries@techexevent.com

CYBER SECURITY & CLOUD EXPO

EUROPE

26-27 September 2023, RAI, Amsterdam

The Cyber Security & Cloud Expo will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

6 Co-Located Events

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6,000+ Attendees

76% of attendees are **Director Level & above**

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com

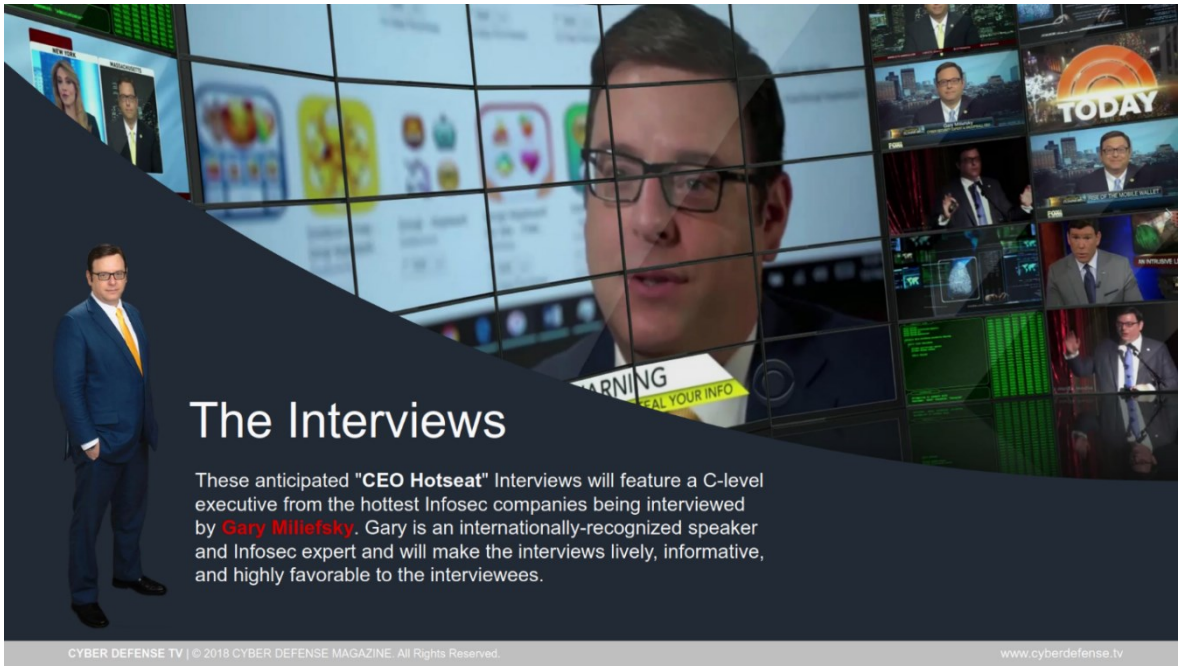
CYBER DEFENSE TV

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.

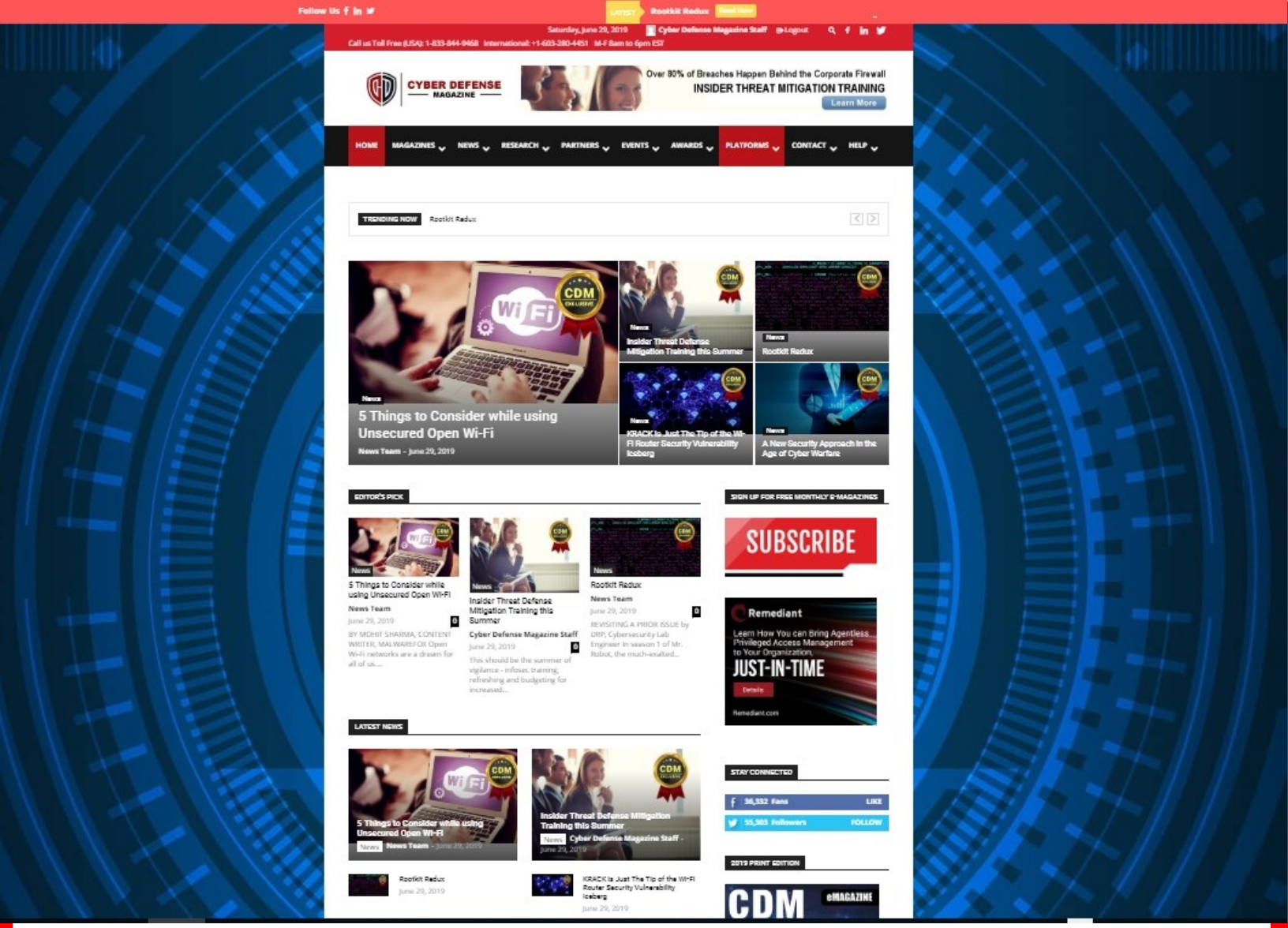
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 06/01/2023



Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

11 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched https://cyberdefenseconferences.com/and have another amazing platform coming soon.

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

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

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

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

- See what the future holds in expert-led Track Sessions covering the hottest 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.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

*** with help from writers and friends all over the Globe.**