



CYBER DEFENSE
MAGAZINE

eMAGAZINE

DECEMBER
2023

In This Edition

Bolstering IoT Cybersecurity Amid an Evolving Landscape: A CEO's Perspective

What's The Role of Gaslighting in The Cyber Security Context of Social Engineering?

Generative Ai: The Future of Cloud Security

...and much more...

MORE INSIDE!

CONTENTS

<i>Welcome to CDM's December 2023 Issue</i> -----	8
<i>Bolstering IoT Cybersecurity Amid an Evolving Landscape: A CEO's Perspective</i> -----	21
By Ron Konezny, President & CEO, Digi International	
<i>What's The Role of Gaslighting in The Cyber Security Context of Social Engineering?</i> -----	25
By Anna Drescher, Freelance Writer and Mental Health Specialist	
<i>Generative Ai: The Future of Cloud Security</i> -----	30
By John Riley III, Cyber Business Development, Alan B. Levan NSU Broward Center of Innovation	
<i>2024 Predictions: The Rise of AI Brings New Security Challenges</i> -----	36
By: Imperva Executives: Karl Triebes, Lebin Cheng, Peter Klimek, Lynn Marks, and Terry Ray	
<i>AI and the Next Wave of Robocalls: Protecting Carriers and Consumers from Sophisticated Voice Fraud</i> -----	41
By Tim Ward, Chief Strategy Officer, XConnect	
<i>Building a Secure Data-Protection Infrastructure to Protect against the MOVEit Hack</i> -----	44
By Carl Cadregari, Executive Vice President, FoxPointe Solutions	
<i>Do You Know Where Your Data Is? How Law Firms Can Protect Their Most Valuable Asset</i> -----	48
By John A. Smith, CSO, Conversant Group	
<i>Safeguarding the Code That Drives Modern Vehicles</i> -----	51
By Soujanya Ain is a Product Marketing Manager at GitGuardian	
<i>Phishing Campaign Exploits Open Redirection Vulnerability In 'Indeed.com'</i> -----	55
By Brett Raybould, EMEA Solutions Architect, Menlo Security	
<i>The Ethics And Privacy Concerns Of Employee Monitoring: Insights From Data Privacy Expert Ken Cox</i> -----	58
By Ken Cox, President of Hostirian	
<i>The Balancing Act for Mid-Market Firms: Navigating Digital Growth and Security Hurdles</i> -----	61
By Kevin Beasley, CIO, VAI	
<i>How Autonomous Vehicles are Revolutionizing the Last-Mile Logistics Industry</i> -----	64
By Anar Mammadov, CEO, Senpex Technologies	

<i>What You Need to Know to Embrace the Imminent Quantum Shift for Your Cryptography Future ---</i>	67
By Eddy Zervigon, CEO of Quantum Xchange	
<i>How Cloud Solutions Can Lead to Stronger, More Secure IT Operations -----</i>	70
By Mike Wiseman, Vice President, Public Sector, Pure Storage	
<i>Addressing Bias in Insider Risk Monitoring -----</i>	73
By Chris Denbigh-White, Chief Security Officer, Next	
<i>Industry Benchmark Report, Issued by The FAIR Institute, Unveils the Dollar Impact of Cyber Incidents -----</i>	76
By Luke Bader, Director, Membership and Programs, FAIR Institute	
<i>Beyond Resumes: Uncovering Hidden Talent at the New Jersey Judiciary-----</i>	79
By Darrin Straff, Senior Staffing Consultant, NinjaJobs	
<i>Deepfakes and AI's New Threat to Security-----</i>	82
By Luke Arrigoni, Founder, Loti	
<i>Unmasking the Vulnerabilities in Telecom Signaling: A Call for Enhanced Security -----</i>	85
By Rowland Corr, Vice President and Head of Government Relations, Enea	
<i>Introducing GitHub Insights, Latest Solution to Combat Growing Threat to APIs -----</i>	89
By Scott Gerlach, CSO - StackHawk	
<i>Prioritizing Action After the Threat Headlines -----</i>	92
By Douglas McKee, Executive Director, Threat Research, SonicWall	
<i>How to Identify and Respond to End-of-Life and Out-of-Service Operating Systems? -----</i>	98
By Chahak Mittal, GRC Manager, Universal Logistics	
<i>Classic Information Security Management Errors-----</i>	104
By Zsolt Baranya, Information Security Auditor, Black Cell Ltd.	
<i>Cybersecurity Threats in Global Satellite Internet-----</i>	107
By Gizem Yilmaz, Master Expert Data Analyst, Turkcell Technology	
<i>Does Zero Trust Improve Productivity?-----</i>	111
By Zac Amos, Features Editor, ReHack	

<i>Enhancing The Nation’s Cybersecurity Workforce</i> -----	115
By Randall Sandone, Executive Director, Critical Infrastructure Resilience Institute at The Grainger College of Engineering at the University of Illinois Urbana-Champaign	
<i>What are the Essential Skills for Cyber Security Professionals in 2024?</i> -----	120
By Sarah Gilchriest, Chief People Officer of Workforce Learning, the group encompassing QA, Circus Street and Cloud Academy	
<i>Attackers Keep Evolving: Lessons from Expel’s Q2 2023 Quarterly Threat Report</i> -----	123
By Aaron Walton, Threat Intel Analyst, Expel	
<i>Implementing ZTA: Benefits and Best Practices</i> -----	126
By Eric Sugar, President, ProServeIT	
<i>Institutionalizing Awareness to Stop Cyberattacks</i> -----	130
By Aimei Wei, Founder and CTO, Stellar Cyber	
<i>Key Differences in Securing OT & IT Environments</i> -----	133
By Joe O’Donnell, EVP of Corporate Development, Cyolo	
<i>Making Our Infrastructure Resilient: 5 Priorities for Security R&D</i> -----	137
By Saurabh Amin, Professor of Civil and Environmental Engineering PI, Laboratory for Information and Decision Systems Massachusetts Institute of Technology	
<i>Manufacturing on the Cyber Frontlines: Enhancing Cybersecurity on the Factory Floor</i> -----	141
By Berardino Baratta, CEO, MxD	
<i>Open AI Exec Warns AI is “Extremely Addictive,” Humanity Could Become “Enslaved”</i> -----	144
By Sai Mattapalli and Rohan Kalahasty, Co-Founders — Vytal.ai	
<i>Organizations Are Shifting Ransomware Defense Tactics, But Malware Is Still the Problem</i> -----	147
By Trevor Hilligoss, Senior Director of Security Research at SpyCloud	
<i>Passwords In the Air</i> -----	150
By Gautam Hazari, Chief Technology Officer, Sekura.id	
<i>Protecting Data in The Final Stretch of The Supply Chain</i> -----	153
By Dan O’Toole, Chairman & CEO, Arrive	

<i>QR Code Phishing Attacks: Threat Actors Are Now Shopping Online with You</i> -----	157
By Olesia Klevchuk, Director of Email Protection, Barracuda	
<i>Real Time Exposure Detection Is the Missing Element of Every Cybersecurity Strategy</i> -----	160
By Or Shoshani, CEO and Co-founder, Stream Security	
<i>Government Communications: The Threats</i> -----	163
By Nicole Allen, Marketing Manager at Salt Communications	
<i>SASE and Zero Trust: A Powerful Combination</i> -----	167
By Elena Thomas, Digital Marketing Manager, SafeAeon Inc.	
<i>Speaking Cyber-Truth: The CISO's Critical Role in Influencing Reluctant Leadership</i> -----	172
By Craig Burland, CISO, Inversion6	
<i>Strengthening Financial Services: Embracing the Digital Operational Resilience Act (DORA) for Cybersecurity Resilience</i> -----	175
By Boris Khazin, Head of Governance, Risk & Compliance at EPAM Systems, Inc.	
<i>The Case Study: The Exploitation of Mechatronics Systems</i> -----	178
By Milica D. Djekic	
<i>The Pitfalls of Periodic Penetration Testing & What to Do Instead</i> -----	183
By Erik Holmes, CEO, Cyber Guards	
<i>The Quantum Shift</i> -----	187
By Sercan Okur, VP of Technology, NextRay	
<i>The Role of Identity Data Management in Achieving CISA'S Strategic Goals</i> -----	190
By Wade Ellery, Field Chief Technology Officer at Radiant Logic	
<i>Three Key Threats Fueling the Future of Cyber Attacks</i> -----	194
By Rishi Baviskar, Global Head of Cyber Risk Consulting at Allianz Commercial	

@MILIEFSKY

From the

Publisher...



As we publish this final issue of Cyber Defense Magazine for 2023, we would like to extend our appreciation to all participants in our publishing and promotional activities. As always, we are dedicated to bringing our contributors and readers the most up-to-date and relevant actionable intelligence to conduct the most effective cyber security program for your own organization.

We would also like to remind our contributors and supporters that CyberDefenseCon 2024 has formally announced a call for speaker proposals to present to our Top Global CISO audience for this conference, taking place October 31 - November 1, 2024 in The Ritz-Carlton, Orlando, Florida, USA. Speakers should be willing to lead CISO roundtable sessions during the conference, as well as participate in CISO panel discussions, if so requested. [Click here](https://cyberdefenseconferences.com/) to fill out the call for speakers form. More information is available at <https://cyberdefenseconferences.com/>



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

We continue to strive to be the best and most reliable set of resources for the CISO community in discharging these responsibilities. With appreciation for 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>

Copyright © 2023, Cyber Defense Magazine, a division of
CYBER DEFENSE MEDIA GROUP

1717 Pennsylvania Avenue NW, Suite 1025

Washington, D.C. 20006 USA

EIN: 454-18-8465, DUNS# 078358935.

All rights reserved worldwide.

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 December 2023 Issue

From the Editor-in-Chief

We are pleased to publish this December issue of Cyber Defense Magazine, with a broad array of articles on the topics most relevant to CISOs and your colleagues.

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

Looking back over the 2023 offerings from Cyber Defense Magazine, including the topics and positions in our published articles, I am pleased to report that we continue to receive and publish new and important articles on the current challenges and responses in cybersecurity.

At the same time, I would like to remind readers that CDM is not a political forum, but a place to notify colleagues of important developments in the cybersecurity industry. Our readers are principally CISOs and their colleagues, so our focus is on our value to them in discharging their cybersecurity responsibilities, rather than pursuing any political agenda.

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™2024

San Francisco | MAY 06-09 | Moscone Center

**Stronger
Together**

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

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , 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 <https://www.rsaconference.com/>

#RSAC



FOLLOW US



THE SECRETS OF HARDENING ACTIVE DIRECTORY

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

GET YOUR FREE eBook

Get <https://cionsystems.com/>



CYBER
INITIATIVE **27**

< 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.

Meet the bot and
online fraud protection
**most hated by attackers,
and most loved by customers.**

Top Infosec Innovator
Award Winner



DATA  OME

datadome.co



NIGHTDRAGON



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

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

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

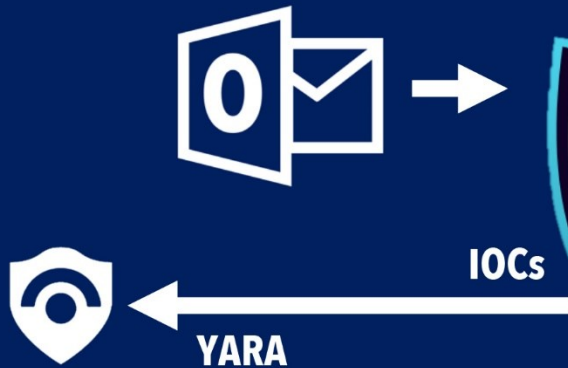
ACCELERATE

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

www.nightdragon.com

UNKNOWN CYBER

EMAIL O365



EMAIL O365 Integration:

Problem:

Generative AI like ChatGPT is exploding obfuscated and polymorphic malware variants, increasing alerts more than 100% over the first three quarters of 2023. SOCs and Threat Investigators are overwhelmed with alerts. Mean-time-to-detection (MTTD) of malware is over 200 days.

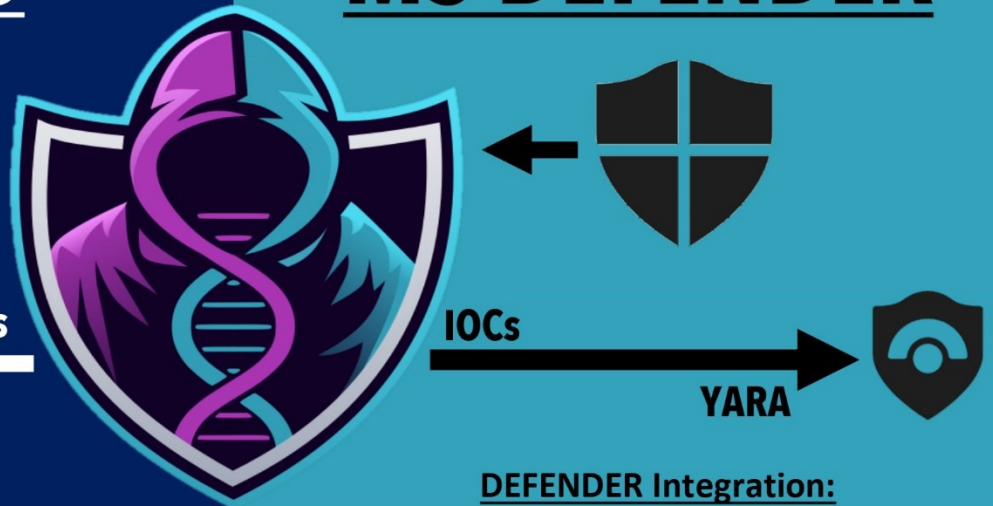
Solution:

UnknownCyber conducts deep code inspection in minutes to identify new malware based on code similarity. Using automated semantic analysis to investigate adds capability to identify, classify and resolve unknown malware and false positives that signature and behavior-based solutions cannot.

About our tech:

UnknownCyber is an In-Q-Tel Portfolio Company. Our technology originated in the DARPA Cyber Genome Project and has been enhanced through multiple innovations. Our capabilities have been independently validated by MIT's Lincoln Labs and a Fortune 500 SOC which demonstrated UnknownCyber's ability to detect new threats in minutes through our automated analysis of code.

MS DEFENDER



DEFENDER Integration:

Our UnknownCyber - Microsoft Defender integration enhances your other defenses' capabilities by automatically resolving and accelerating resolution of the alerts they create through our automated deep code inspection.

- ✓ Reduce Time, Expense, & MTTD
- ✓ Resolve Alerts
- ✓ Clear False Positives
- ✓ Enhance Defenses with IoCs
- ✓ Enhance Defenses with YARA
- ✓ Detect new unknown variants
- ✓ Detect AI obfuscated malware

Easy, Easy, Easy:

We know security teams are overwhelmed that's why UC focuses on Easy. In under 15 minutes an organization can be fully enabled. Want to test? Simply set up an email account to be scanned and in under 10 minutes start your free trial.

www.unknowncyber.com

info@unknowncyber.com

KEY BENEFITS

Save Time and Money
Turn days of work to minutes
automatically resolving alerts

Easy full deployment in
10 minutes

Find unknown malware
before the rest of the world

Automatically generate
bytecode based YARA for
Sentinel

Automatically find new IoCs for
Sentinel

Automatically resolve false
positives with tagged code index

Connect notes and intel from
previous investigations
connected through code

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

cyber  GRX

DRAGOS

 CONCEAL

 varmour

ALLEGISCYBER
CAPITAL

www.allegiscyber.com



DATATRIBE

CYBER STARTUP FOUNDRY

Forging dominant companies
from nation-state domain expertise

CAPITAL | RESOURCES | GUIDANCE | SUCCESS

HOME TO THE WORLD'S FASTEST GROWING
CYBERSECURITY AND DATA SCIENCE COMPANIES

quickcode

DRAGOS

EN|VEIL
ENCRYPTED VEIL

INERTIALSENSE

PREVAILION

the cyberwire

Ntrinsec
Data Security Automation

SIXMAP

STRIDER

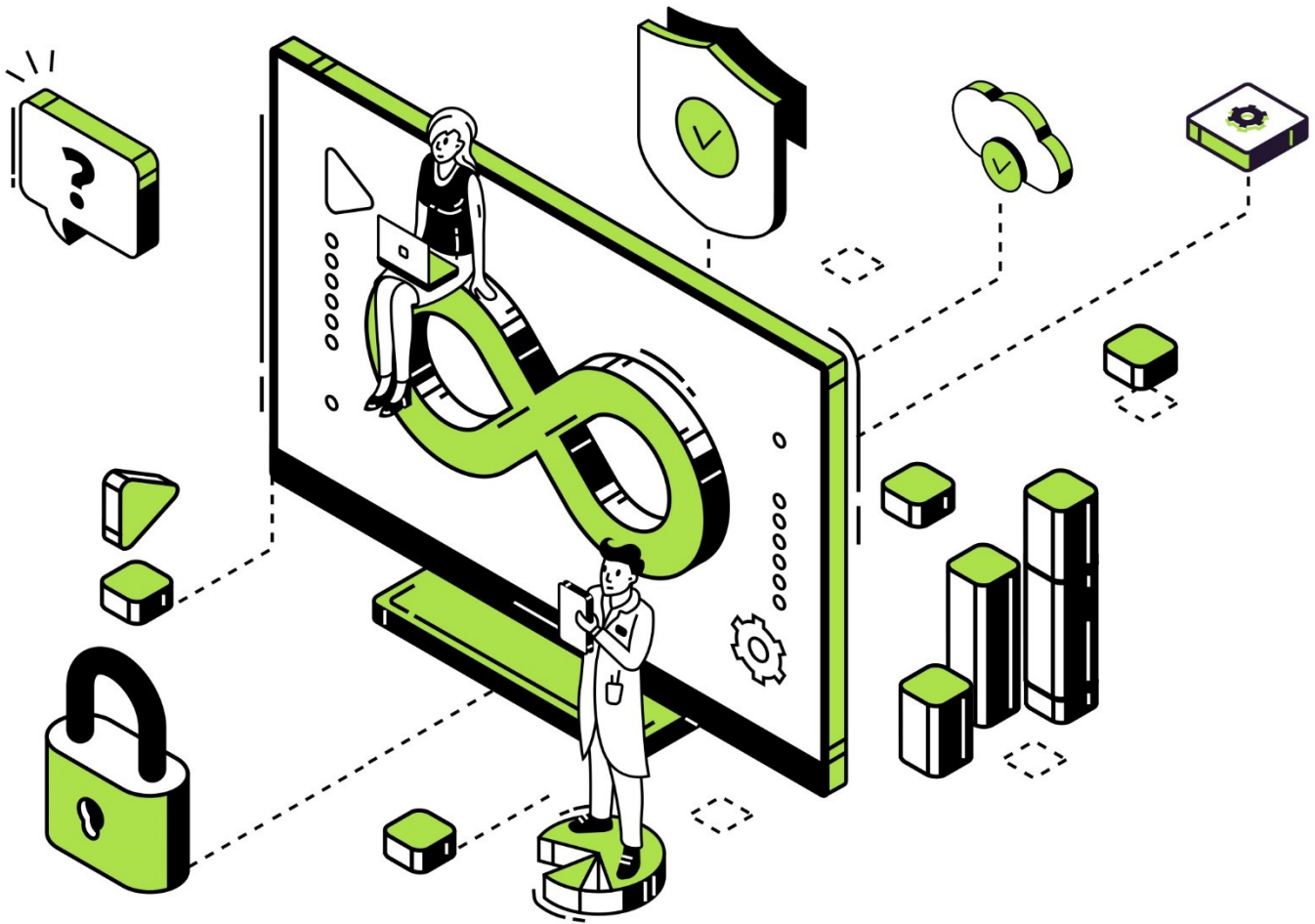
CONTRAFORCE

BLACKCLOAK™

SightGain

JOIN THE TRIBE

DATATRIBE.COM



LowOps. No Stops.

Pvot to the next generation of cyber security.

LowOps reduces dependencies on human intervention, and minimizes the risk of cyber attacks. It lowers the dependency on third-party security solutions, and instead makes the IT infrastructure strong from within.

Now, you can automate the development, deployment, management, security, and scaling of your business-critical software, easily, while reducing overall costs significantly.

Talk to a LowOps expert at Pvotal to know how your IT infrastructure can achieve a lot more, with a lot less.

pvotal.tech



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 Defense
& Response.**

It's what we do.

cyderes.com

A hand holding a pen over a notebook on a desk with a keyboard and a glowing blue network overlay.

ARTICLES



Bolstering IoT Cybersecurity Amid an Evolving Landscape: A CEO's Perspective

By Ron Konezny, President & CEO, Digi International

The most cybersecurity-savvy members of an organization are typically not the key decision makers. This disconnect may be one of the reasons that even while [cybersecurity budgets continue to increase](#), the [frequency and severity of cyberattacks and data breaches are not decreasing](#).

Yet many factors contribute to the complex cybersecurity landscape today, including the rapid adoption of connected IoT devices, the increasing sophistication of hackers, and evolving cybersecurity regulations. Consequently, it is time that cybersecurity initiatives switched from a bottom-up to a top-down and organization-wide approach. This article will discuss how leaders can implement a multi-layered strategy for IoT security to protect their organizations and customers.

The Importance of a Top-Down Approach to Cybersecurity Risk Management

In the traditional bottom-up approach to IoT cybersecurity, operational employees like security, systems and network techs typically report their findings and concerns to upper management. However, this

process can be slow and inefficient. A breach may occur before network security and cybersecurity engineers get the green light to implement critical initiatives. By instituting a top-down approach to cybersecurity, upper management underscores the importance of security policies and the necessity of securing connected devices and networks.

Top-down strategies also tend to be wider-reaching, as management teams recognize that the responsibility of protecting the organization does not rest on the shoulders of the IT department alone. Instead, everyone is equally responsible and accountable because every department, office and employee is susceptible to cyberattacks or unintentional data leaks due to non-secure processes or behaviors. When vulnerabilities lead to security and data breaches, they can have an enormous impact on a brand's reputation — not to mention the potential price tag in the millions of dollars to remediate these issues when they occur.

Today, organizations across every industry need to create a culture of safety where every individual receives training and understands their role in the broader enterprise's security posture. Underscoring this point, Opensource.com rightly points out that a [system is only as secure as the least safety-conscious team member](#).

The Four Levels of a Multi-Layered Security Strategy

There are many avenues by which bad actors can infiltrate a business network, including through unencrypted communication models, unsecured device ports, and connected technologies being deployed without have key security measures in place, like authentication. In addition to a top-down approach, businesses must incorporate a multi-layered strategy to establish company-wide protection against cyberattacks. Generally, a multi-layer approach has four levels: device, network, application, and cloud.

1. **Device-level security:** Consists of built-in security measures that protect the IoT device itself, such as encryption, secure boot, protected ports, and configuration monitoring. In particular, device-level security ensures that connected devices' firmware under corporate jurisdiction can get updated as new vulnerabilities arise.
2. **Network-level security:** Includes measures like firewalls, intrusion detection and prevention, as well as virtual private networks (VPNs) to safeguard the communication between devices on the broader network. In addition to being secure, a network must remain always-on, meaning that it is resilient and can continue to function amid challenges to normal operations and maintain service for customers and connected applications.
3. **Application-level security:** This layer entails those security measures that protect the applications and data running on IoT devices, like access control, data encryption and secure APIs.
4. **Cloud-level security:** The cloud is central to IoT, as companies cannot collect or analyze the data generated by their connected devices without uplink connectivity and a path to the cloud to store that data. This level of security includes measures like identity and access management,

data encryption and continuous monitoring, which protect the cloud infrastructure that supports IoT devices and business critical operations.

The Evolving Cybersecurity Landscape

For perspective on how persistent and sophisticated cybercriminals have become, consider that the [National Institute of Standards and Technology \(NIST\)](#) updates its [National Vulnerability Database \(NVD\)](#) hourly. Moreover, in 2022, [over 25,000](#) new common IT security vulnerabilities and exposures (CVEs) were discovered — the highest reported annual figure to date. In light of these ever-emerging threats, regulators constantly update existing standards or release new ones to protect IoT devices.

For example, in 2022, regulators amended the [FDA Act](#) to include requirements for connected medical devices. That same year, to address the increasing intersection of IoT devices and account-based payments, the Payment Card Industry Security Standards Council and the Consumer Technology Association [issued a joint bulletin](#) highlighting the importance of IoT security. Additionally, cybersecurity regulations have global implications for IoT technology, such as the [General Data Protection Regulation \(GDPR\)](#), the [EU Cybersecurity Act](#), and the [California Consumer Privacy Act \(CCPA\)](#). Failure to adhere to these standards can result in impact to the bottom line, including costly fines.

The shifting IoT security landscape can be daunting. However, a top-down approach to security allows upper management to more effectively direct the implementation of security practices and regulations throughout the organization, whether ensuring staff have the training to identify phishing and social engineering threats, mandating [FIPS 140-2 cryptographic encryption](#) or restricting physical access to the enterprise or specific assets. The good news is that the security industry has galvanized in recent years, and there are great resources today that enable organizational leaders and technical personnel to quickly grapple with the issues and put an actionable strategy in place.

Finding Help and Leading by Example

The ideal strategy for IoT security is a multi-layered, company-wide strategy — including procuring tested and proven devices with built-in security protocols, ensuring [the ability to continually update all connected devices](#) over their lifecycle, and mandating procedural and behavioral training for all staff members. While cultural and infrastructure change do not happen overnight, every business can implement a strong security posture and excellent security measures. When in doubt, brands should seek a total solution vendor that can help integrate IoT security best practices, including monitoring and management services to keep cyber defenses up to date. Ultimately, it is incumbent on an organization's leadership to take the initiative and promote company-wide adoption and cultural change.

About the Author

Ron Konezny is the President and CEO of Digi International. He joined Digi International December 2014, as President and Chief Executive Officer. Prior to joining the company he was Vice President, Global Transportation and Logistics division of Trimble Navigation Limited, a global provider of navigation and range-finding equipment and related solutions. He had served in that role since September 2013. Prior to this position, he served from August 2011 to September 2013 as the General Manager of this division and as the Chief Executive Officer of PeopleNet, Inc., after PeopleNet was acquired by Trimble in 2011. Ron was a founder of PeopleNet where he held a variety of executive positions since 1996, including Chief Technology Officer, Chief Financial Officer, Chief Operating Officer and, from September 2007 through PeopleNet's acquisition by Trimble, Chief Executive Officer. PeopleNet is a leading provider of telematics solutions for the transportation industry. Ron also presently serves on the board of directors of Atlas Financial Holdings (NASDAQ: AFH).



Ron has extensive experience in the wireless M2M industry working with solutions comprised of hardware and cloud-based applications. He brings extensive leadership experience in corporate strategy, manufacturing, operation, technology, finance and business development to the Board. Ron was the 2009 winner of the Ernst & Young Entrepreneur of the Year® award in the Technology category. Ron can be reached online at digi@globalresultspr.com and at our company website at <http://www.digi.com>.



What's The Role of Gaslighting in The Cyber Security Context of Social Engineering?

By Anna Drescher, Freelance Writer and Mental Health Specialist

A few years ago, I received an email from Apple stating that someone had made a purchase from my account. They urged me to update my details immediately as they were concerned it could be a security breach. Panicked, I clicked on the link and typed in all my personal and banking details. Not long after, my bank contacted me about an unusual transaction – someone had purchased a handbag worth £3000 using my account. I got my money back, but my reality had been stirred up and I felt violated, ashamed, and stupid.

What does this have to do with gaslighting? Let's explore.

Gaslighting is a term normally used in the context of relationships, but social engineering relies on some of the same psychological tricks. They are both forms of psychological manipulation and exploit human suggestibility, empathy, and vulnerability and involve the elements of reality distortion and power

imbalance. The outcomes for the victims are also similar: self-doubt, shame, and losing their grip on reality.

What is Gaslighting?

As 2022's most popular word, you've probably heard of gaslighting. The term originates from the 1938 play *Gas Light* (which was turned into a movie of the same name in 1944), in which a husband manipulates his wife into believing she is losing her mind.

One of his tactics was to make the lights in the house flicker by using the gas lights in the attic. Whenever she asked him "Why are the lights flickering?", he said (something along the lines of) "It's all in your head, darling. We should speak to the doctor about increasing your meds, you sound a bit cuckoo". As this goes on, she eventually starts to question her sanity. The play doesn't use the term gaslighting, but it demonstrates the type of manipulative behavior that now describes gaslighting.

While social engineering has elements of gaslighting, they're not entirely the same thing.

Gaslighting in the context of relationships happens repeatedly and over time, slowly dismantling the victim's sense of reality and self. Social engineering in cyber security is generally a one-off and doesn't usually involve the key element of attacking the victim's credibility ("you're so paranoid/ jealous/ crazy") that makes gaslighting so effective.

How Gaslighting Increases the Effectiveness of Cybercrime

Social engineering in the context of cyber security manipulates people into performing certain actions, like giving up access, credentials, bank details, or other sensitive information.

It's effective because attackers build rapport, distort reality, exploit the simulated power imbalance, and create a strong emotional reaction in their victims – some of the same tactics used in gaslighting.

Rapport Building

Gaslighting only works when there is some sort of relationship and trust. Likewise, scammers know that a person is more likely to engage with them if they've built rapport.

A scammer might call you on the phone, telling you "Someone has access to your bank accounts through PayPal, and they can take all your money. I'm calling to help you." They seem calm and professional and engage in a friendly chat with you and, believing they are calling to help, you let your guard down and do what they ask.

Doing this is not gaslighting, it's lying. But creating a false reality in which the attacker or scammer is a trustworthy person is similar to what a gaslighter would do when they're establishing a relationship and rapport with their victim – because it makes them easier to manipulate.

Reality Distortion

In relationship gaslighting, the perpetrator paints an alternate reality and tries to persuade their victim to buy into it. For example, a cheating husband tells his wife, "I never cheated on you, you're just paranoid!" even if she has evidence of his transgression. If he's convincing enough, she will question herself and her perception.

The attacker in cybercrime does something similar: they try to persuade their victim of the false reality that they are Apple, Amazon, the IRS, or similar. That means, the attacker distorts their victim's reality and instills doubt in their mind by claiming they are someone they are not.

Let's say you get a call from the IRS, and they tell you that if you don't pay a certain amount immediately, you will be fined or even arrested. You may know that you've paid all your taxes, but the call or email creates doubt in your mind like "Maybe I did forget".

By skillfully distorting reality, they make you doubt your perception and memory, thereby putting themselves in a position of power.

Power Imbalance and Vulnerability

Social engineering, gaslighting, and any other form of psychological manipulation work best when there is a perceived power imbalance.

Gaslighting is most effective in relationships where there is a power imbalance, such as between a health professional and their patient, or an abusive husband and his wife (or vice versa). Therefore, gaslighters tend to seek victims who are in some way vulnerable (e.g., a trauma survivor, someone with low self-esteem, or a patient) because the power dynamic is skewed.

In a similar vein, you're more likely to fall for a scam when you believe you are being contacted by an authority. Most of us have been raised to respect and obey authority, so when the "bank" calls saying your account will be closed unless you update your bank details immediately, you'll probably hand them over.

That's also why scammers often target vulnerable people, such as the elderly or recently bereaved. Likewise, those in a financially vulnerable position may be more willing to believe they will win a million dollars if they provide their bank details. Romance scammers tend to prey on the lonely, and scammers targeting banks or corporations often find the "weakest link" (e.g., a person who fears they'll lose their job if they don't act immediately).

Fear and Stress

When there is a power imbalance, it can cause fear and stress. Fear causes the critical thinking part of our brain to shut down and the fear center to take over. That means, when we're scared, we're not thinking rationally and are driven by the very powerful emotion of fear.

Gaslighting works best when your critical thinking capacity is switched off, like when you're scared of your abusive partner leaving or harming you.

Alone just dealing with an authority, like a government agency or bank, can make you feel anxious. But when it comes to the safety of your money, privacy, or relatives (e.g., the grandparent scam) that anxiety triples.

If someone contacts you saying you will go to prison if you don't pay immediately or claims to be your grandchild in dire need of help, you will experience fear and panic. Consequently, you can't think rationally and may do whatever you're told.

The Effects of Gaslighting and Being Scammed

Victims of cybercrime often think, "How could I have been so stupid" or "There must be something wrong with me". They feel violated, dehumanized, and lose trust in their perception and sense of reality, and the shame and guilt they experience often mean they don't tell anyone or seek help.

Gaslighting victims have a similar experience once the fog has been lifted. That's because relationship gaslighting is like a scam and has devastating consequences for the victim.

People and businesses have lost millions of dollars (if not more) to cybercrime, and most of the time, the criminals get away with it. So how do you protect yourself?

How to Protect Yourself from Gaslighting and Social Engineering

The best way to protect yourself from gaslighting is to know that it exists and how it works, and you must stand firm in what you know and believe. The same goes for protecting yourself from cybercrime and scammers.

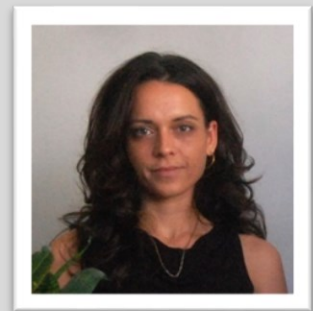
Chris Hednagy, an expert on social engineering and cyber security, gave several tips on how to protect yourself from scammers:

- Educate yourself on cybercrime and its tactics.
- If someone you don't know elicits a strong emotional response within you (like fear or a "gut feeling"), pause and ask yourself: am I being manipulated?
- Think critically: has this organization/ business/ agency ever contacted you to ask for personal information? (Most of them don't)

- Create a password with your relatives so when someone calls saying they're your relative in an emergency, make them give you the password first.
- If you did fall for it, don't let the shame and embarrassment stop you from seeking help. It can happen to anyone!

About the Author

Anna Drescher is a freelance writer and editor specializing in mental health and psychology. Her work includes collaborating with organizations and apps to advise on and create content related to psychology, mental health, meditation, and hypnosis. She is an author at Simply Psychology and has published articles with several mental health-related publications. For 10 years, Anna has worked in the mental health sector and supported people who struggle with their mental health. Her roles have included private practice, working in the UK's National Health Service, therapeutic work in in-patient and community care, in a prison service for men with personality disorder, and managing a co-production project at the UK's leading mental health charity. Anna has a bachelor's degree in Psychology and a master's degree in mental health/ psychotherapy, and is also a qualified solution-focused hypnotherapist and yoga teacher. Anna can be reached via LinkedIn (www.linkedin.com/in/freelancewriterannadrescher) or her website www.mentalhealth-writing.com.





Generative Ai: The Future of Cloud Security

By John Riley III, Cyber Business Development, Alan B. Levan | NSU Broward Center of Innovation

Generative AI: The Future of Cloud Security

As the digital landscape undergoes a relentless transformation, the dominance of cloud computing has become a cornerstone of our interconnected world. However, this rise to prominence brings with it a pressing concern - the security of cloud environments in the face of ever-evolving cyber threats. In the current climate, where the stakes are higher than ever, cloud security stands at a critical crossroads. With cyber-attacks growing in both frequency and sophistication, the need for innovative solutions has never been more apparent. In this dynamic landscape, Generative AI emerges as a beacon of promise, offering transformative capabilities that could redefine the very fabric of cloud security. Let's jump into why Generative AI is not just a choice but a necessity in the escalating arms race against cyber threats.

The Landscape of Cloud Security

The cloud environment, with its distributed resources and vast data storage, presents unique security challenges. Traditional security measures, while robust, often lag behind in terms of adaptability and real-time threat intelligence. As cyber-attacks become more sophisticated, the need for dynamic and proactive security solutions becomes increasingly evident.

Understanding Generative AI

Generative AI refers to a type of artificial intelligence that can generate new data or patterns based on the training it receives. Unlike conventional AI that interprets or classifies data, Generative AI can create, simulate, and predict, making it an invaluable tool in the realm of cybersecurity.

What is Generative AI?

Generative AI refers to a subset of artificial intelligence models that can generate novel data – be it text, images, sound, or other media – that is similar to but distinct from the data on which they were trained. Unlike traditional AI models that are designed for recognition or classification tasks, generative models are creators, synthesizing new content that can range from artistic works to realistic simulations.

How Does Generative AI Work?

Generative AI operates primarily through two key types of models: Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs).

Generative Adversarial Networks (GANs)

A GAN consists of two parts: a generator and a discriminator. The generator creates data, while the discriminator evaluates it. The generator continuously tries to produce data that is indistinguishable from real data, and the discriminator tries to differentiate between the real and generated data. This adversarial process enhances the quality of the generated results, making them increasingly realistic over time.

Variational Autoencoders (VAEs)

VAEs are another approach, where the model learns to compress data (encoding) and then reconstruct it (decoding) in a way that retains the core characteristics of the original data. This process enables the generation of new data points that are variations of the original dataset.

Why is Generative AI Beneficial?

In the realm of artificial intelligence, generative AI stands as a groundbreaking advancement, reshaping how machines learn, create, and interact with the world. This technology, transcending conventional boundaries, is not just about analyzing data but is capable of producing new content, offering a myriad of applications across various sectors. We will delve into the intricacies of generative AI, explaining its working principles and highlighting its numerous benefits.

Why Generative AI is Crucial for Cloud Security

Generative AI is becoming an indispensable tool in enhancing cloud security due to its advanced capabilities in threat detection, adaptability, and response. Unlike traditional security methods, Generative AI can predict and identify potential cyber threats proactively, creating a dynamic defense mechanism that evolves with emerging risks.

This technology also enables the development of adaptive security protocols and automated response systems, ensuring cloud environments are safeguarded against increasingly sophisticated cyber-attacks.

Additionally, Generative AI aids in maintaining data privacy and compliance by generating synthetic datasets for testing and improving security measures without exposing sensitive real data. By providing advanced risk assessment and realistic cyberattack simulations, it plays a crucial role in preparing for and mitigating potential threats in the cloud, making it a key factor in the future of cloud security.

Key Beneficial Areas of Generative AI Enhances Cloud Security:

Enhanced Threat Detection

Generative AI models, with their ability to learn and simulate patterns, can predict and identify potential cyber threats before they materialize. This proactive approach to threat detection is crucial in the cloud environment where data breaches can have far-reaching consequences.

Adaptive Security Protocols

The dynamic nature of Generative AI allows for the development of adaptive security protocols that evolve with the changing landscape of cyber threats. This adaptability ensures that cloud security measures remain effective against even the most novel attacks.

Automated Response Systems

Generative AI can automate the response to security incidents. By simulating various attack scenarios, these AI systems can generate immediate and effective response strategies, reducing the time and resources required for manual intervention.

Data Privacy and Compliance

In the cloud, where data privacy and compliance are paramount, Generative AI can be used to create realistic but synthetic data sets. This approach helps in testing and improving security measures without risking exposure of sensitive real data.

Advanced Risk Assessment

By analyzing patterns and predicting future trends, Generative AI can provide advanced risk assessment capabilities. This feature is crucial for cloud environments where risk landscapes change rapidly.

Training and Simulation

Generative AI can create realistic cyberattack simulations, providing invaluable training for security professionals. This hands-on experience is crucial for preparing them to handle actual threats in the cloud environment.

Challenges and Considerations

This year cybersecurity firm Barracuda Networks reported that in their Spear-Phishing trends report, 50% of companies were impacted by these attacks and will continue to grow even higher by the end of 2023.

Spear phishing is a sophisticated form of cyberattack where attackers target specific individuals or organizations with personalized, deceptive communications, often for malicious purposes like stealing sensitive information or distributing malware. Generative AI emerges as a potent defense against these attacks due to its advanced analytical capabilities.

It can detect subtle anomalies and patterns in emails and communications that may indicate a spear phishing attempt, often identifying risks that conventional security measures might miss. Generative AI's continuous learning ability allows it to adapt to evolving spear phishing tactics, ensuring up-to-date defense mechanisms. Additionally, it can simulate realistic spear phishing scenarios for training purposes, enhancing the ability of individuals and organizations to recognize and respond to such threats effectively. By automating threat detection and response strategies, Generative AI plays a crucial role in thwarting spear phishing attempts, bolstering cybersecurity defenses in a landscape where personalized and targeted cyber threats are increasingly prevalent.

Generative AI can be a powerful tool in combating spear-phishing attacks, which are highly targeted and sophisticated forms of phishing. Here's how it helps:

1. **Advanced Threat Detection:** Generative AI models can be trained to recognize the subtle indicators of spear phishing attempts, which often involve carefully crafted emails or messages that mimic legitimate communications. These models can analyze patterns and anomalies in communication styles, email headers, and content to identify potential threats that might be missed by traditional security measures.
2. **Automated Behavioral Analysis:** By learning the normal communication patterns within an organization, Generative AI can detect deviations that may indicate a spear phishing attempt. For example, unusual requests for sensitive information or transfers of funds, especially if they deviate from typical patterns, can be flagged for further investigation.
3. **Simulating Attacks for Training:** Generative AI can create realistic spear phishing simulations for training employees. By exposing staff to safe, simulated attacks, they can become more adept at recognizing and responding to real spear phishing attempts, thus reducing the risk of successful breaches.
4. **Response Strategies:** Upon detecting a potential spear phishing attempt, Generative AI can assist in formulating rapid response strategies, minimizing the time window in which the attack can be successful. This can include automated alerts to potentially affected parties and isolation of compromised accounts or systems.
5. **Continual Learning and Adaptation:** As spear phishing tactics evolve, Generative AI systems can continuously learn from new patterns and techniques, constantly updating their detection capabilities. This ongoing learning process is crucial in the arms race against cybercriminals who continually refine their strategies.
6. **Content Verification:** Generative AI can assist in verifying the authenticity of content within emails or messages. By analyzing linguistic patterns and cross-referencing information with known databases, it can ascertain the likelihood of a communication being part of a spear phishing attack.

While Generative AI offers immense potential, it also comes with challenges. There are concerns about the misuse of this technology, ethical considerations, and the need for robust governance frameworks to ensure responsible use.

Generative AI offers both opportunities and challenges in the realm of cybersecurity. While it can significantly enhance defense mechanisms and threat detection, it also opens the door to more sophisticated and hard-to-detect forms of cyberattacks. Balancing these aspects is crucial for leveraging the benefits of AI in cybersecurity while mitigating the risks.

1. **Enhanced Security Protocols:** Generative AI can be used to develop more advanced security protocols and systems. By learning from vast amounts of data on cyberattacks and security breaches, these models can predict and identify potential threats more efficiently than traditional methods.
2. **Automated Threat Detection:** AI models can continuously monitor networks for unusual activities, automatically detecting and responding to threats faster than human-operated systems. This capability is crucial for identifying and mitigating zero-day exploits, which are previously unknown vulnerabilities.
3. **Phishing and Social Engineering:** On the flip side, generative AI can be used to create more sophisticated phishing attacks. By generating realistic emails, messages, or even voice and video communications, attackers can trick individuals into divulging sensitive information or granting access to secure systems.
4. **Deepfakes and Misinformation:** The rise of deepfake technology, powered by generative AI, poses a new kind of cybersecurity threat. These convincingly fake videos and audio recordings can be used to spread misinformation, manipulate public opinion, or impersonate individuals for fraudulent purposes.
5. **Password Cracking and Cryptanalysis:** Advanced AI algorithms can be employed to crack passwords and encryption keys faster than traditional methods. This capability could potentially compromise even the most secure systems.
6. **Training and Awareness:** Generative AI can be used for training purposes, creating realistic cyberattack scenarios to better prepare cybersecurity professionals. It can also raise awareness about the potential threats and the sophistication of modern cyberattacks.
7. **Ethical and Legal Challenges:** The deployment of generative AI in cybersecurity raises ethical and legal concerns. There's a need for clear guidelines and regulations to prevent misuse of this technology, especially in areas like privacy, data protection, and the creation of misleading content.

Evolution of Cyber Threats: As generative AI continues to evolve, so will the nature of cyber threats. This creates a dynamic landscape where cybersecurity professionals must continuously adapt and update their strategies to stay ahead of potential attackers.

Generative AI stands at the forefront of a new era in cloud security. Its capabilities to predict, adapt, and respond to threats in real-time make it an indispensable tool in the arsenal against cyber-attacks. As cloud computing continues to evolve, integrating Generative AI into security strategies will not just be an

option but a necessity for ensuring the safety and integrity of cloud environments. The journey towards AI-enhanced cloud security is just beginning, and its full potential is yet to be unleashed.

About the Author

John Riley III, Cyber Business Development, Alan B. Levan | NSU Broward Center of Innovation

With a career spanning over two decades in the software application industry, John Riley III brings a wealth of experience to the table. His journey has been marked by a steadfast commitment to understanding and solving customers' challenges and a strong belief that collaboration with like-minded professionals is the key to success.

John's Specialties and Skills encompass a wide array of expertise, making him a versatile leader in various domains:

In the realm of technology adoption, he excels in End User Adoption, ensuring that technological innovations seamlessly integrate into user workflows. He navigates the intricate landscape of SaaS, guides organizations through the complex process of Digital Transformation, and harnesses the power of Digital Twins for enhanced insights.

John's career trajectory includes a significant tenure in the Oracle Applications space, with a focus on consulting services and education, assisting companies in software implementations, business process changes, and user adoption education.

Most recently, he held the position of VP of Business Development at Kilroy Blockchain and assumed the role of organizer for two Blockchain Meet-Up groups in West Palm Beach, FL. Presently, he is the Co-founder and CEO of C-N-C Blockchain Advisory.

Notably, John is a US Marine War Veteran, with a distinguished service record during Desert Shield/Desert Storm, underscoring his unwavering commitment to duty and leadership.

John can be reached online at

(jriley@nova.edu) and at our company website <https://www.levancentercyber.com/>





2024 Predictions: The Rise of AI Brings New Security Challenges

By: Imperva Executives: Karl Triebes, Lebin Cheng, Peter Klimek, Lynn Marks, and Terry Ray

The emergence of generative AI has put new resources in the hands of both attackers and defenders, and in 2024, Imperva believes the technology will have an even greater impact. Understanding how attackers are leveraging the technology will be critical for organizations seeking to keep themselves—and their data—protected.

In this piece, our experts and thought leaders will explore the ways in which organizations will evolve to address the emerging challenges associated with generative AI, API vulnerabilities, and the ever-changing security market.

Generative AI Disrupts the Cyber Threat Landscape

Karl Triebes, Imperva SVP and General Manager, Application Security, says it's easy to envision a future where 70% or even 80% of all web traffic comes from bots. He notes that one of the biggest factors driving that growth will be generative AI solutions, which operate by using automated web crawlers to scrape websites and collect information from across the internet.

As both businesses and individual users grow more comfortable using generative AI, there will be a significant spike in activity associated with those crawlers. Imperva Senior Product Manager Lynn Marks agrees, noting that data scraping is “becoming more of an issue for organizations” as their data is used to train the large learning models (LLMs) that inform generative AI tools.

Triebes points out that generative AI will make its presence felt in other areas, as well—including a shift toward AI-based coding in the future. Director of Technology within the Office of the CTO Peter Klimek agrees and says that “new and/or junior developers will benefit greatly” from AI-enabled development tools, increasing productivity and output by automating routine tasks. However, he acknowledges that those same tools will “help script kiddies graduate into skilled hackers capable of carrying out more complex exploits.” In the near term, Triebes believes generative AI will primarily be used to perpetrate fraud.

“It will be much easier for fraudsters to masquerade as somebody else—at least online,” explains Triebes. “AI will lead to a new breed of fraud and social engineering attacks. A fraudster could scrape the internet for information about you and then weaponize a voice recording of you. Through generative AI, they can create a pseudo version of you. If they package that effectively, they could contact your bank and request a password reset.”

Ron Bennatan, Imperva Fellow, Data Security agrees. He expects to see an increase in attacks as attackers leverage AI to fool their victims, noting, “because LLMs are so good at both understanding humans and creating text communications that really look like they were created by humans, attackers will be able to target and ‘hack’ individuals far better than before.”

Alan Ryan, AVP, UK & Ireland, notes that as attackers invest in AI, so too must defenders. Bad actors are investing heavily in AI in an attempt to gain an upper hand over defenders, which means organizations need to ensure they are investing in these solutions as well. Ryan says AI doesn’t necessarily “change the balance of ‘good vs. evil,’” but instead just represents the next evolution of the ongoing cat and mouse game between attackers and defenders.

API Security Will Take on Greater Prominence

As attackers target APIs with greater regularity, organizations will be forced to take a more proactive approach toward identifying, classifying, and protecting all API endpoints in production. This is particularly true for large organizations: enterprises with a revenue of at least \$100 billion USD are between [three and four times more likely](#) to experience API insecurity than small or midsize businesses.

Unfortunately, while API ecosystems are expanding rapidly, most organizations are still in the early stages of understanding how to effectively protect them. Although it’s common for today’s businesses to have between [50 and 500 APIs in production](#), many don’t know where they are deployed or what data they are accessing. That put the organization, and their valuable data, at extreme risk.

Peter Klimek says “most organizations are still in the early stages of understanding API security and don’t yet have a nuanced strategy for protecting their APIs”. Further, he believes organizations “haven’t implemented the right defenses or controls in place to manage identity and access management.”

Lebin Cheng, VP, API Security, Imperva, believes that will start to change this year. “In 2024, as pressure to mitigate API-related security incidents continues to grow, security leaders will look for, and invest in, solutions that integrate seamlessly into their existing Application Security technology stack,” says Cheng. “This approach will give organizations a more coordinated and unified view of automated threats that target APIs and critical applications—all of which connects to data stores where the businesses’ data is located.”

Alan Ryan predicts that relying on homegrown, in-house API and bot management will be a “risky strategy” as automated attacks become more sophisticated and adept at evading simple defenses. According to Ryan, global vendors have an opportunity to leverage the vast amount of data they collect from millions of endpoints around the world to provide customers with the actionable insights they need to effectively defend themselves against modern threats.

How Organizations Approach Data Security Will Change

In 2024, businesses won’t just continue to invest in the same old solutions—they will increasingly look to innovate in ways that help them stand out from their competitors. Many will invest in new analytics capabilities or leverage new or expanded cloud workloads—and they will assume the risk that comes along with them.

Dan Neault, SVP and GM of Data Security, believes organizations will need to explore new data security technologies that can “help them understand and manage their data risk and actually make their overall IT more secure.” Neault also points out that the rise of hybrid and multicloud environments makes it even more imperative for customers to have effective data security protection, insights, and risk mitigation across all of these systems.

There will also be a shift toward consolidation. Moshe Lipsker, SVP, Product Development, states that industry consolidation will lead to a rise in comprehensive solutions, creating end-to-end solutions that empower CISOs to “deliver a layered model of protection.”

Terry Ray, SVP, Data Security GTM and Field CTO, agrees, pointing out that “niche and single solution products and vendors find themselves increasingly in demand for acquisition and partnerships as consumers look to answer data security and regulatory requirements while minimizing necessary expertise, costs, and effort.” Ray expects consumers to see “rapid increases in enterprise data asset coverage, decreased skill requirements, and better collaboration between technologies that were traditionally segmented.” For most businesses, that’s good news—consolidation will allow them to streamline their security solutions and rely on fewer vendors.

Adapting for a Continued Change

The continued rise of generative AI and increased focus on API security will be trends to watch in 2024, as will the consolidation of the security market and shift in the way organizations approach data security. We look forward to having further discussions with our partners and customers to see what their biggest concerns and priorities are as we move into 2024.

About the Authors



Lebin Cheng is a technologist and serial entrepreneur with more than 20 years of experience in cybersecurity. Cheng cofounded Netskope and later cofounded CloudVector, acquired by Imperva. He was awarded 15 patents in areas such as network security, application infrastructure and API inspection. He holds an MBA degree from the Haas School of Business at the University of California Berkeley and a MS in Computer Science from Purdue University. Lebin can be reached online at [LinkedIn](#).



Karl Triebes is a technology leader that has helped some of the world's largest organizations conceive and build products, services, and businesses for networking, application software, storage, and cloud. As Senior Vice President and General Manager, Application Security, he oversees product roadmap and go-to-market strategy for the Imperva Application Security portfolio. Prior, he was Executive Vice President of Product Development and CTO at F5. Triebes has held senior leadership positions with Amazon Web Services, Foundry Networks, and Alcatel. Karl can be reached online at [LinkedIn](#).



Peter Klimek is a Director of Technology within the Office of the CTO at Imperva. Peter works closely with customers around the world, helping them protect their applications and data from complex and emerging security threats. Prior to Imperva, Klimek held roles at Kaspersky, TransUnion, and Zebra Technologies as a solutions architect, security analyst, and engineer. Peter holds a Bachelor of Science in Computer Engineering from the University of Illinois at Chicago. Peter can be reached online at [LinkedIn](#).



Lynn Marks is Senior Product Manager at [Imperva](#), overseeing the product and innovation roadmap for Imperva Advanced Bot Protection and Imperva Client-Side Protection. With more than 10 years of B2B security product experience, Marks helps customers protect their applications and websites from online fraud and other security threats. Prior to Imperva she was product manager at Model N and Distil Networks (acquired by Imperva). She holds a Bachelor's Degree in Economics from UC Santa Barbara. Lynn can be reached online at [LinkedIn](#).



Terry Ray is SVP Data Security GTM, Field CTO and Imperva Fellow at Imperva Inc. As a technology fellow, Terry supports all of Imperva's business functions with his years of industry experience and expertise. Previously he served as Chief Technology Officer where he was responsible for developing and articulating the company's technical vision and strategy, as well as, maintaining a deep knowledge of the Application and Data Security Solution and Threats Landscape. Terry can be reached online at [LinkedIn](#).



AI and the Next Wave of Robocalls: Protecting Carriers and Consumers from Sophisticated Voice Fraud

By Tim Ward, Chief Strategy Officer, XConnect

Robocalls are relentlessly targeting consumers and causing mistrust for the telecom industry as a whole. This is a problem that is accelerating as bad actors take advantage of generative Artificial intelligence (AI) to carry out more believable scams.

According to Juniper Research, fraudsters' ability to innovate robocalling methods will cause mobile users to lose \$70 billion globally by 2027. As it stands, these fraudulent and scam calls are already driving substantial financial losses for the entire telecoms value chain, from carriers to consumers. The rise of AI introduces new efficiency to fraudsters' scams, making it even more likely for them to successfully defraud their victims. This poses a massive problem for the voice industry and puts its reputation at risk as more consumers continue to ignore calls from unknown numbers.

Advancing robocalls is a challenge the voice industry must take a proactive stance on. On the 20th July 2023, the Federal Communications Commission (FCC) announced new rules to tackle robocallers and the rise of sophisticated scams, limiting the number of robocalls placed on landline numbers. These actions, however, have had an undesired effect, with some carriers fearing that they cannot adhere to these new rules and switching off termination into the US as a result. This removes risk but also reduces the footprint of where carriers can terminate traffic.

The FCC's latest regulations are a necessary step to mitigating robocalls in the US, and action must be taken on a global scale to truly address this rising risk. Deploying effective number information services is essential for not only meeting compliance with the FCC's latest rules but also keeping consumers safe from unwanted calls.

AI and New Robocalling Risks

Fraudsters are increasingly benefitting from AI to create convincing deep fake robocalls to impersonate business, banking and government executives, or even family members. Consumers are following the instructions of fraudsters and give in to financial demands.

On top of this, scammers are also leveraging AI to rapidly automate calls. This allows them to originate thousands of robocalls in minutes. They can analyse large amounts of data to understand calling patterns and effectively target their victims.

If this trend continues, organisations making genuine calls will witness their business impacted by lower answer rates, driven by consumer distrust of unrecognised calling line identifications (CLIs). This has the potential to cause permanent damage to the reputation of the voice and messaging industries and encourage voice users to migrate to other communications channels.

Restoring trust in CLIs is essential to securing the future of the voice industry and mitigating against fraud and spam calls. This requires reliable and up-to-date numbering data intelligence solutions to eliminate invalid numbers.

Cracking Down on Spam and Fraud

An increasing number of consumers and businesses continue to be majorly impacted by ongoing AI-powered robocalls. National voice infrastructure must implement basic security protocols to keep users protected.

To ensure that all carriers effectively address robocalls, they need to deploy simple and efficient methods to validate CLI and accurately block invalid traffic. They can leverage the following solutions to harden their stance against fraud in voice and protect consumers:

- Deploying a Dependable DNO List – A Do Not Originate (DNO) list protects users from fraudulent spam calls. The list identifies calls that originate from invalid, unallocated, and/or unused numbers, helping to prevent telecom fraud on known inbound-only and invalid numbers. Regulators across the world are increasingly deploying DNO lists for carriers and enterprises to check numbers against.
- Leveraging Trustworthy GNR Data – Carriers can also leverage Global Number Range (GNR) data to strengthen their defence against robocalls. Access to real-time GNR data provides organisations with the insight to block or accept traffic based on potentially fraudulent CPN/CLI modification. GNR data can cover thousands of operators across hundreds of destinations. Carriers benefit from visibility into the validity of numbers to identify which number ranges are unallocated, ensuring that their traffic is legitimate and has the potential to reach its intended recipient without being blocked.

Addressing Advanced Robocall Tactics

With generative AI causing a major rise in harmful robocalling, tackling this issue is a top priority. Deploying a comprehensive trusted DNO list and exhaustive GNR data arms carriers with the ability to detect invalid and fraudulent numbers, making it easier for them to protect their consumers and focus on building trust.

Taking proactive action against robocalling is essential to secure the future of the voice industry. GNR and DNO solutions are essential to support the termination of legitimate voice traffic while guaranteeing adherence to the latest robocalling rules.

About the Author

Tim Ward, Chief Strategy Officer, joined XConnect in November 2016 to lead the Number Information Services division, with responsibility for sales, marketing and product management, launching a range of innovative services for applications, messaging and interconnect providers that set new standards for access to network, service and user information.

Tim has over 30 years of experience in technical, sales and marketing roles across the telecoms industry.



He is passionate about establishing a level playing field across the industry, with a common set of standards to ensure the highest quality of service. He sees XConnect playing a pivotal role in this and, as such, works with key industry stakeholders and bodies such as MEF and GSMA to drive this agenda forward. Tim can be reached on LinkedIn and at our company website <https://www.xconnect.net>



Building a Secure Data-Protection Infrastructure to Protect against the MOVEit Hack

By Carl Cadregari, Executive Vice President, FoxPointe Solutions

Regardless of the industry in which they operate, organizations have likely witnessed the wave of destructive MOVEit breaches sweeping the globe during recent months. As a result, many organizations may be left wondering what they need to understand about the MOVEit hack and how they can guard against such attacks.

Understanding the MOVEit Hack

Before they can effectively fortify their organizations against the MOVEit hack, cybersecurity professionals must first understand the origins of these breaches. MOVEit, a managed file-transfer software product, is often used by healthcare, government, financial service, and educational organizations to encrypt and distribute large amounts of sensitive data. Following the discovery of a vulnerability within the software in May 2023, a wave of harmful cyberattacks and data breaches began. This vulnerability allows attackers to access MOVEit's database and steal files from systems through

SQL injection. According to the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), the MOVEit breaches are being conducted by Clop, a Russian-speaking cybercriminal group. As of August, more than 600 organizations worldwide have fallen victim to MOVEit breaches—affecting more than 40 million individuals.

Guarding against MOVEit Breaches

As organizations seek to protect themselves against the MOVEit hack, it is critical for them to understand that they will inevitably become the target of a data attack—it is truly just a matter of how and when. Attackers and attacks can stem from a variety of sources including external threat actors, such as Clop, internal disgruntled staff, or even within the supply chain. As a result, every organization should be focused on building a secure data-protection infrastructure. All known or suspected attack vectors, as well as the status of the controls required to reasonably protect the organization, need to be a part of every organization's risk-management consideration today.

Conducting a Risk Assessment

One of the best places to start is to have a thorough, accurate, and unbiased cyber-risk assessment performed, even if there is no law or regulation requiring the organization to complete one. Management cannot act or make cyber- and data-protection decisions effectively without reasonable information drawn from these types of documented assessments.

Before conducting a risk assessment, an organization must first identify its data sets and determine what requires protection. It's important to note that even if an organization doesn't have protected client data (health information, credit cards, SSN, etc.), it still likely possesses protected employee information (SSN, 401(k)/403(b), banking, etc.).

Next, organizations must assess which laws and standards apply to their data sets. Both client data and employee data require protection based on federal, state, and sometimes local cybersecurity and privacy laws. This will define what type of risk assessment needs to be performed.

For example, if an organization consists of 50 employees, all located within New York state, and it supplies a consumable to other businesses, it's likely that only the New York State SHIELD Act would apply to its electronic data. In addition, as it is a small business, a "smaller" risk assessment based on something like the Center for Internet Security (CIS) Top 20 would suffice.

Conversely, if an organization is large, such as a multiregional health system with several thousand employees, then its reasonable risk assessment would need to be much more robust. In that case, such an assessment would follow standards set by the National Institute of Standards and Technology (NIST) publications such as SP800-30r1 (Guide for Conducting Risk Assessments). That could be layered on top of standard control sets such as SP800-53r5 (Security and Privacy Controls for Information Systems

and Organizations) and SP800-171r2 (Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations).

Regardless of the organization and the specific risk assessment conducted, using the applicable experts is mandatory and appropriate scope is critical (people, processes, technology, administrative, third-party, etc.). All risk-assessment efforts must be documented and reasonable, actionable remediation expectations communicated to management for implementation. This risk assessment should be repeated on a regular cadence.

Vulnerability Testing

Another step that organizations can take to build a secure data-protection infrastructure and guard against the MOVEit hack is to conduct a technical vulnerability scan and website vulnerability test. These will show where cyber-hygiene may be needed. This vulnerability scanning and patching of internal assets should be conducted at least quarterly.

Security Training

Additionally, organizations should have a documented and effective security-awareness training program in place that all users attend upon hire and at least once annually thereafter.

Vendor Risk Management

Lastly, organizations should consider upgrading their vendor risk-management program by sending emails with direct questions to each vendor such as “Do you, or any of your third-parties, use MOVEit?” These should be sent out without delay.

An effective vendor risk-management program is needed as well, for any vendor who reasonably interacts with an organization’s data. Organizations should explore having at least annual internal and external penetration testing conducted to ensure that their protection programs are operating as expected.

It is clear from the rampant MOVEit breaches that a lack of controls and assured data protection, as well as misunderstood risk profiles, can allow weaknesses to creep into the overall data-protection infrastructure. These weaknesses are then exploited by those with nefarious intentions. Organizations must act now, understand their risks, and take the appropriate actions to protect their data.

About the Author

Carl is an executive vice president in the FoxPointe Solutions/Information Risk Management Division of The Bonadio Group. Carl has expertise in the areas of Data Privacy and Cybersecurity Controls; Physical, Administrative, and Technical Security; Enterprise Risk Management; Vendor Management; and Disaster Recovery Planning, having worked with companies across almost all vertical markets ranging in size from small businesses to multiregional and multinational organizations with thousands of employees. Carl can be reached online at ccadregari@foxpointesolutions.com and at our company website <https://www.foxpointesolutions.com/>.





Do You Know Where Your Data Is? How Law Firms Can Protect Their Most Valuable Asset

By John A. Smith, CSO, Conversant Group

If data is the new oil, this holds especially true for law firms as they are wholly dependent on the information they store and maintain regarding their clients. Further, law firms have a fiduciary responsibility to protect this sensitive information regarding cases and clients; and, their businesses are wholly dependent on trust and reputation, which can be easily broken in the event of data loss. Despite the significance the industry puts on proprietary data and information, it appears most law firms still aren't prioritizing how it is protected. A recent report issued by [Conversant Group](#) and the [International Legal Technology Association](#) (ILTA) titled "[Security at Issue: State of Cybersecurity in Law Firms](#)" found that only 11% of firms report data backups as a critical security control. In the event of a cyberattack like ransomware, [threat actors target backups](#) in roughly 94% of cases and are successful in compromising at least some data stores at least 68% of the time.

With ransomware attacks running rampant, law firms' IT and security teams must encourage and enhance backup protocols when it comes to protecting the organization's valuable data. Arguably, backups are the most important security control—when data is lost forever, many firms never recover. Thus, ensuring backups are redundant, immutable, recoverable, and have controls within and around them is essential for firms to protect themselves from catastrophic loss.

What is Immutability and How to Achieve it?

When it comes to data backups, being “immutable” means that data in storage is incapable of being changed, encrypted, or deleted. The only way it should be modifiable is by a two-key simultaneous lock turn (think of the dramatic nuclear bomb launch we may see in movies) and the expiration of a designated retention period, such as a timed lock on a safe.

Immutability for law firms is essential as they are frequently targeted by ransomware actors, and immutable backups are a requirement of many cyber insurance carriers. It is important to note that not all immutability is created equal; and redundancy and recoverability are essential components as well. Should a threat actor infiltrate a network and break controls around one data repository, it's critical that there be several others, all immutable and preferably of different types and differing manufacturers to hedge bets, to add additional layers of insurance against total loss.

How Secure Are Law Firm Backups?

Alarmingly, 38% of law firms confirmed their backup copies are either not immutable or they are unsure whether they are, and only 24% reported having multiple immutable copies of all data. As previously mentioned, not all immutability is created the same, and sometimes law firms are not correctly reporting whether their backups are immutable.

Storage snapshots emerge as the most common form of backup at nearly double most other backup methods. While this may not be the only method of backup for some firms, it is the most often used as it is most convenient; but it cannot be relied upon to be immutable. To my knowledge, only Pure snapshots offer immutability to the standards of cybersecurity professionals. Currently, only 9% of firms report using Pure snapshots for their shared storage, and all of those are likely not enabling immutable snapshots of all data. Since most firms use non-immutable local and remote storage, there are likely gaps surrounding immutability to truly safeguard organizations from targeted backup attacks.

Lastly, many firms have components of backup infrastructure as part of the Active Directory domain. This is another Achilles' Heel in firms' backup resilience strategy—no backup servers, proxies, or targets should be domain-joined, as any attacker that can penetrate the network can then access company data in storage.

How Should Firms Protect Backups?

We recommend organizations of all types, including law firms, employ the following approach:

- Always have five copies of its data:
 - One: The production data.
 - Two: All data backed up to physically redundant, immutable backup storage.
 - Three: All backups replicated to physically redundant, immutable offsite backup storage.
 - Four: All backups copied to digitally air-gapped, immutable storage.
 - Five: All volumes on all storage platforms (NAS, SAN, etc.) immutably snapped.

Through this method, firms can ensure redundancy, immutability, and recoverability—should a threat actor attack one data repository, other immutable copies exist on different technologies.

Putting Backups in the Forefront to Secure Business Operations

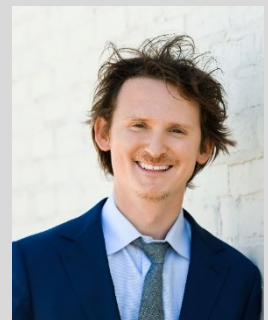
In the end, when your data is gone, so, too, is your business. Backups **MUST** be considered a first line of defense, and with this, law firms need to prioritize learning how to defend not only their front-line defenses, but also their resiliency in the event an attack occurs.

About the Author

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

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

John Anthony studied Computer Science at the University of Tennessee at Chattanooga and holds a degree in Organizational Management from Covenant College, Lookout Mountain, Georgia.





Safeguarding the Code That Drives Modern Vehicles

By Soujanya Ain is a Product Marketing Manager at GitGuardian

The automotive landscape has evolved dramatically, from mechanical marvels to sophisticated platforms on wheels driven by intricate computer systems. Surprisingly, these vehicles are governed by over 100 million lines of code, running across 50 to over 100 independent processors known as electronic control units (ECUs). To put this into perspective, the Ford F-150 Lightning, a marvel of modern engineering, operates on 150 million lines of code, surpassing even the Boeing 787 Dreamliner, which relies on a comparatively modest 6.5 million lines of code.

This intricate code is the lifeblood of modern cars, responsible for tasks ranging from lane-keeping assistance to seamlessly connecting with our mobile devices and playing our favorite tunes. It's often said that cars nowadays are essentially rolling computers. This sentiment is not without reason. Since 1996 for American vehicles and 2001 for European ones, standardized connectors (OBD/EOBD) have been mandated to interface with the local vehicle computer network (CAN bus).

Moreover, embedded LTE connectivity has been integrated into vehicles since 2014, allowing manufacturers to collect performance data and implement remote controls, such as lock/unlock and remote start functions.

However, this technological leap has its own set of challenges. With an extensive codebase, the risk of code leakage becomes a pressing concern. Unlike a software company, where an exposed AWS API key may result in unauthorized access to vital AWS resources, the stakes are much higher in the automotive world. Imagine [hurtling down the highway at 70 miles per hour and losing control of your vehicle remotely](#). This isn't just about data, it's about the lives of every individual in and around the vehicle. This underscores the reality that automobiles have evolved into valuable assets [susceptible to threats from both physical and remote adversaries](#).

The Era of the Software-Defined Vehicle (SDV)

The SDV market is projected to grow significantly, [from a \\$43 billion market size in 2023 to a potential \\$150 billion by 2030](#). Pioneered by Tesla, automotive companies are shifting towards becoming software-first entities. Ford's recent launches of electric vehicles, the F-150 Lightning and Mustang Mach-E SUV, underscore this transformation. However, it's imperative to recognize that code security practices must evolve in tandem as technology progresses.

Beyond flashy infotainment systems and seamless navigation experiences, the bedrock of any vehicle's security lies in its underlying security infrastructure. For instance, in-vehicle infotainment (IVI) systems, which operate on [embedded Linux](#), store sensitive information like personally identifying information (PII). These systems are often interconnected with vital subsystems, like the engine, brakes, and sensors, which create a broad attack surface in conjunction with the embedded LTE connection. This implies that if hackers target the infotainment system, they might gain access to sensitive information and potentially gain control over vital vehicle functions. Robust security measures here are non-negotiable.

The Grim Reality of Source Code and Secrets Leaks

One of the most critical concerns revolves around the leakage of hardcoded credentials. Unlike traditional attacks, where bad actors must identify and exploit vulnerabilities, hardcoded secrets can be exploited with minimal effort. This can lead to customer data breaches, intellectual property theft, company-wide systems manipulation, and even unauthorized access to mobile apps for controlling vehicles.

Manufacturers accumulate vast data lakes containing a wealth of information on consumer behavior. While this data is invaluable for refining products and enhancing user experiences, it poses a significant security risk. Any breach in these data lakes could have far-reaching consequences, affecting individual drivers and entire user bases.

The automotive industry faces the dual challenge of ensuring data privacy (GDPR and California Consumer Privacy Act (CCPA) compliance) and securing its assets against cyber threats. A breach here could result in customer identity theft, financial fraud, and hefty regulatory fines. The recent breaches involving major automakers are stark reminders of the urgent need for an improved secrets management posture. Daimler, [Nissan](#), [Toyota](#), and [others](#) faced incidents where sensitive customer data was inadvertently exposed due to misconfigurations and exposed secrets.

This should be no surprise, particularly for those acquainted with the alarming revelations from the [GitGuardian State of Secrets Sprawl report](#). The study unveiled a staggering 10 million secrets left exposed on public GitHub repositories in 2022 alone. It's a concern that casts a broad shadow, touching applications, the entire supply chain, and the backbone of critical infrastructure.

Elevated Risks of Neglecting Secrets Security

Approximately 85% of automotive software comprises open-source code and components sourced from upstream vendors. A breach in one component could impact multiple car models across different manufacturers. So, it's imperative to scrutinize every link in the automotive supply chain for potential secrets incidents. After all, hardcoded credentials in vehicles aren't limited to automakers alone; they extend throughout the supply chain. Each component, equipped with its software, may harbor embedded secrets, sometimes lacking robust security measures for safeguarding them.

Within this intricately connected ecosystem, the Telematics server is a pivotal gateway, receiving data from vehicles and executing remote commands. Unfortunately, they are often inadequately protected, leaving vehicles susceptible to unauthorized access. A breach in this system could have dire consequences – from locking owners out of their vehicles to initiating erratic and potentially dangerous behaviors. In extreme cases, attackers could even seize control of a vehicle's steering, imperiling lives on the road. This underscores the critical need for robust secrets security within Android and iOS applications, and the command and control (C&C) infrastructure.

There has been an ongoing "right to repair" debate in this broader industry landscape. A significant step forward has been taken, granting independent repair shops access to vital vehicle data. However, as this access expands, so does the concern for data security. Protecting important software-defined components becomes paramount, ensuring they don't inadvertently expose sensitive code and user information. In this regard, secrets detection emerges as a critical layer of defense, guaranteeing that even with expanded access, sensitive data remains secure.

As vehicles increasingly undergo updates via Over-The-Air (OTA) processes, it creates a potential entry point for attackers. Intercepting, dissecting, and manipulating these updates can unveil hidden features, functions, and sensitive information, including "hardcoded secrets," paving the way for [ransomware attacks](#). This highlights the critical importance of safeguarding sensitive code and user information. As the automotive industry hurtles into the digital age, one thing is abundantly clear: the safety and security of both vehicles and their passengers hinge on robust secrets protection.

Securing automotive software is a multifaceted challenge requiring collective effort from the entire supply chain. Integrating secrets security measures right from the start of the development process is paramount here.

The stakes are high, and the onus is on the industry to ensure that future vehicles dazzle with technology and are fortified with rock-solid code security measures. The road ahead is one of transformation and innovation; we must navigate it with vigilance and foresight.

About the Author

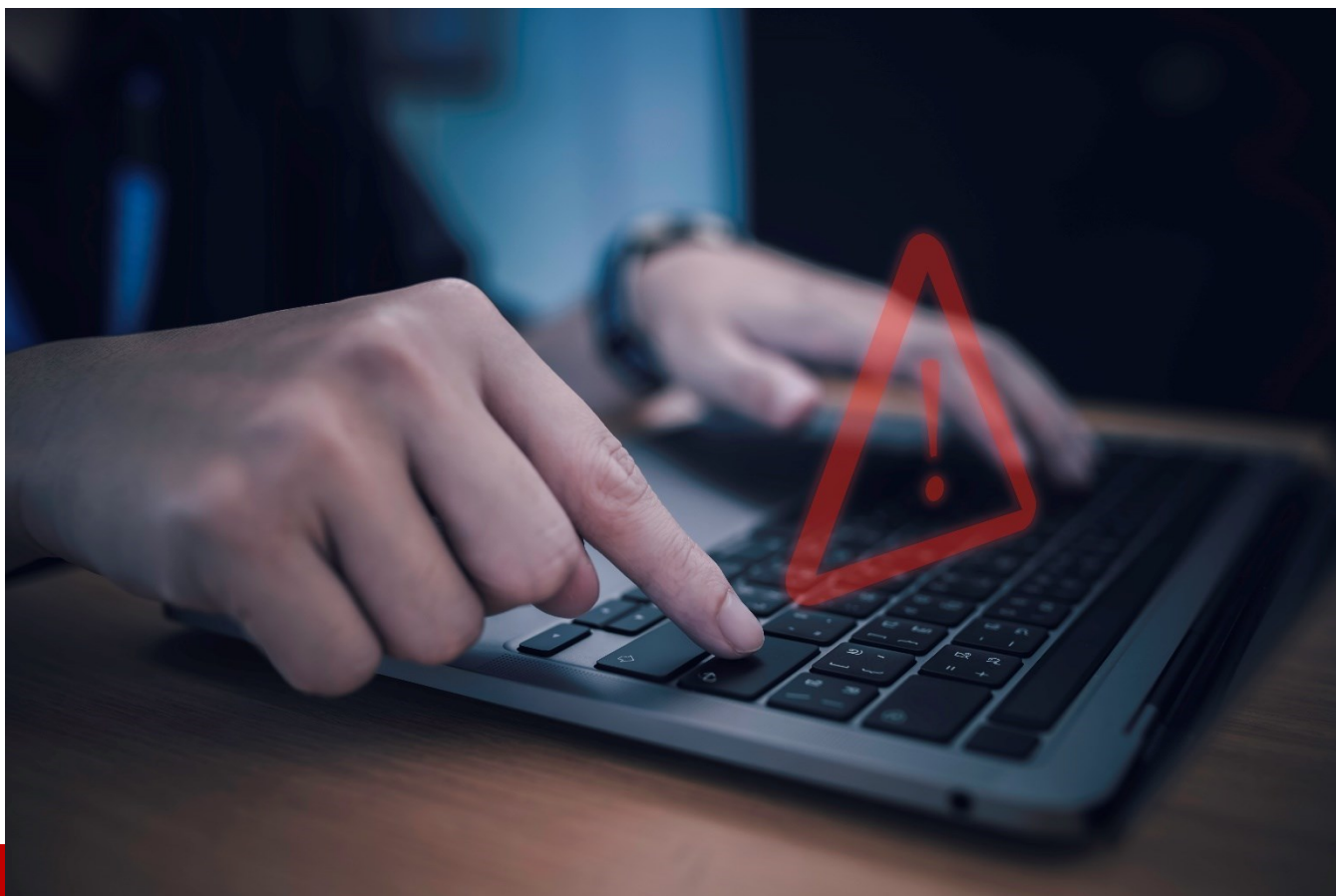


Soujanya Ain is a Product Marketing Manager at GitGuardian. She helps spread the story around application security and the AppSec challenges companies face today.

Website: <https://www.gitguardian.com/>

Twitter handle: <https://twitter.com/GitGuardian>

Linkedin: <https://www.linkedin.com/company/gitguardian>



Phishing Campaign Exploits Open Redirection Vulnerability In 'Indeed.com'

By Brett Raybould, EMEA Solutions Architect, Menlo Security

Phishing remains one of the most prevalent challenges facing organisations, with more than three billion malicious emails estimated to be sent around the world every day.

No-one is immune to the threat of phishing. From aeronautics firms, major banks, and pharmaceutical companies to household brands like Facebook, Google and Sony Pictures, enterprises of all shapes and sizes have fallen victim to the world's most common cyber threat in recent years. In fact, owing to the prevalence of the problem, [Verizon's 2023 Data Breach Investigations Report](#) estimates that more than a third (36%) of all data breaches involve phishing.

Of course, it's not just the sheer volume of attacks that is worrying. Concerns are more likely to focus on the heightening complexity of techniques that attackers are using. Phishing attacks are becoming alarmingly sophisticated.

From in-depth research of individuals and their interpersonal relations to the use of incredibly convincing spoofed social media profiles, threat actors are pulling out all the stops as they attempt to trick unsuspecting victims into clicking malicious links. We have heard recent accounts of cybercriminals dropping malicious links into zoom calls, while others are actively exploring the use of deepfake technologies, for example.

As a result, it is becoming harder and harder to discern attacks from genuine digital interactions, as has been demonstrated in another recent [phishing campaign](#) uncovered by the Menlo Labs team.

Analysing the Indeed.com attack chain

In July 2023, Menlo Security's HEAT Shield detected and blocked a novel phishing attack that attempted to redirect unsuspecting users of the popular job listing site 'Indeed.com' to a phishing page impersonating Microsoft.

The attack chain began with victims receiving a phishing email that was delivered via a link that had been deceptively crafted to make the victim believe it had come from Indeed.com. Victims would then click on a link which would redirect them to a fake Microsoft Online login page where they were asked to enter their credentials.

The tactic that this campaign tapped into is known as open redirection, where an application either intentionally or unintentionally redirects users to an untrusted external domain. In this sense, threat actors were exploiting the highly trusted nature of 'Indeed.com' while redirecting targeted victims to a phishing site.

Critically, the spoofed page was deployed using a sophisticated phishing kit known as EvilProxy that can fetch content dynamically, doing so from the legitimate login site. The phishing site then acts as a reverse proxy, proxying the request to the actual website and enabling the attacker to intercept the legitimate server's requests and responses.

With EvilProxy, the attacker is also able to steal session cookies, which can then be used to log in to the legitimate Microsoft Online site, impersonating the victims and bypassing non-phishing resistant multi-factor authentication (MFA) policies.

Combatting modern phishing threats

This attack chain is a prime example of an Adversary In The Middle (AiTM) phishing attack, harvesting session cookies to enable threat actors to bypass MFA protections.

In this instance, the Menlo Labs team saw that the threat actors largely focused on targeting executives in senior level roles across industries, such as banking and financial services, insurance providers, property management and real estate, and manufacturing. However, given that similar AiTM threats could

be used to attack any business, organisations of all kinds need to check they are comprehensively protected.

Of course, awareness and training are the first port of call when combating phishing attacks – something that many organisations already know about and implement. According to one study, [84%](#) of respondents conduct regular training to help staff understand phishing and reduce victimisation rates.

However, with threat actors becoming increasingly smart with their campaigns, it is important that firms go a step further, embracing a variety of policies, tools and technologies to develop multi-layered security strategies capable of bolstering defences against modern threats.

Here, we recommend technologies like HEAT Shield that can help protect users from credential harvesting and account compromise. Not only can it cut off the attack vector from the initial access stage, but also it can redefine the way in which security is implemented, enforcing a proactive approach to deal with such highly evasive threats.

In the case of the Indeed.com attack, the technology successfully detected the phishing site using AI-based detection models to analyse the rendered web page prior to any URL reputation service and other security vendor flagging the page as malicious. During this process, it also generates zero-hour phishing detection alerts, providing greater visibility and context of threats to security and SOC analysts.

The Indeed.com campaign is just one reminder among many of the importance of constantly evolving and enhancing security strategies to stay one step ahead of increasingly sophisticated threat techniques.

About the Author

Brett Raybould - EMEA Solutions Architect, Menlo Security. Brett is passionate about security and providing solutions to organisations looking to protect their most critical assets. Having worked for over 15 years for various tier 1 vendors who specialise in detection of inbound threats across web and email as well as data loss prevention, Brett joined Menlo Security in 2016 and discovered how isolation provides a new approach to solving the problems that detection-based systems continue to struggle with.





The Ethics And Privacy Concerns Of Employee Monitoring: Insights From Data Privacy Expert Ken Cox

By Ken Cox, President of Hostirian

Despite the technological advancements brought by automation and the enhanced capabilities of data analytics that have transformed decision-making processes, the digital age has proved to be a double-edged sword with an unsettling rise in employee monitoring technologies on the other end of its blade.

The digital eyes and ears watching our screens and tracking our movements have become a staple in workplaces worldwide. Whether we like it or not, employee surveillance is unlikely to go away.

As a vocal advocate of our fundamental right to privacy, I've felt this rise in surveillance might forever shut the door to personal privacy at work, giving center stage to unnecessary supervision.

But every human being has an inherent right to privacy—at the water cooler at work, and even in the common areas where we gather for a casual exchange of thoughts.

Over the years, as president of [Hostirian](#), I've strived to foster a work environment where employees can thrive. As a result, I've seen that people perform at their best when they don't feel constantly watched or judged.

That said - this approach is quite rare, with supervision having taken the reins. The new reality of being watched by employers has given way to critical questions about the ethics of monitoring and the impact it has on workers' behavior and morale.

To understand the complexities surrounding this issue, we must first inspect the legal framework. The 1986 Electronic Communications Privacy Act (ECPA) is the primary law that allows employers to monitor their workers' verbal and written communications - as long as they present a legitimate reason.

The problem here is that it was enacted during a time when digital tech was far different from what it is today, making its guidelines seem archaic.

To add another layer to the issue, there haven't been any comprehensive federal laws in the U.S. that regulate the extent of workplace supervision. This is shocking, considering the strides we've made in the digital space. This legislative vacuum has given employers broad discretion in implementing employee monitoring programs, sometimes without significant checks and balances.

This lack of surveillance regulation can leave workers feeling vulnerable and overexposed; this can transform into paranoia and mistrust - a far cry from the transparent and results-based environment many organizations claim to have.

Numerous studies support the fact that, though surveillance was intended to boost productivity and maintain integrity, it can produce the opposite effect - stifling creativity and hindering productivity.

An intriguing study from the [Harvard Business Review](#) has also found that excessive monitoring can spur an increase in rule-breaking behaviors among employees. It appears the constant pressure of being watched can push some individuals to act out as if rebelling against the intrusive supervision.

The psychological implications are the most concerning aspect of employee surveillance. Workers under constant surveillance have been reported to feel less accountable for their actions, leading to a potential rise in immoral behavior.

When people feel they're being controlled, they might exercise less self-control, which leads to a counterproductive cycle. Employers at this point might find themselves trying to control their employees, and the employees have a bigger pushback as a response to their employer's controlling behavior.

The ethical considerations surrounding electronic monitoring in the workplace cannot be overstated. Although illegal, employees have reported hidden cameras in restrooms, and employers now even track personal computer files, the extent of monitoring has reached alarming levels.

With the ability to oversee practically every movement at the office, often conducted without employee knowledge, employers wield an unacceptable deal of power over their employees' privacy.

The invasive nature of such surveillance is not just morally questionable, but it poses a huge threat to individual privacy rights - the very backbone of our democratic society.

The rise of remote work, facilitated by platforms like Upwork, has made supervision even more prevalent. While it's essential to ensure employers receive the work they've commissioned, the ways to achieve this must be reasonable.

One can't deny employers' legitimate interests in ensuring efficiency. The digital age has brought with it tools that can help businesses thrive, and it would be remiss not to use them. However, striking a balance between leveraging these technologies and respecting employees' privacy rights is paramount.

When done ethically and within reasonable boundaries, surveillance can be a powerful tool for businesses. Yet, the keyword here is 'ethical'. It should never be used as a means to control or intimidate - it should be a tool to improve performance, identify areas for improvement, and ensure the security of company data.

Additionally, workers should be explicitly made aware of when, how, and why they are being monitored. For instance, if a specific conversation is being recorded or if their desktop activities are under surveillance, it should be made abundantly clear.

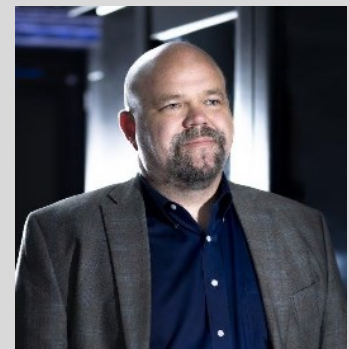
After all, without clear communication and mutual agreement, employers risk creating a workplace culture characterized by fear.

While workplace surveillance might be a necessary tool in specific contexts, it must be approached with caution and respect for individual rights. Transparency and consent are the only way forward. Without them, we risk creating a culture of fear and mistrust, which could have far-reaching implications for employee morale and, ultimately, business success.

Ultimately, the question isn't just about what employers can do with technology but what they should do.

About the Author

[Ken Cox](#), the President of Hostirian, a leading data privacy firm, is a passionate advocate for privacy rights, dedicated to fostering an ethical and nurturing work environment. From humble beginnings in Missouri, Ken Cox has conquered a life full of hardships and has come out on top. He's the President of Hostirian and a solutions-focused Senior Executive with over 20 years of solid success in the software, SaaS, telecom, and e-commerce industries. Ken Cox is an expert when it comes to helping companies with outsourced IT projects, IT infrastructure, compliance, marketing campaigns, sales strategy, or M&A activity. In his impressive career, Mr. Cox has held top leadership positions at Hostirian, Rivercity Internet Group, Mpower Communications, and Midwest Micro Systems. Ken can be reached on Instagram, [@clicksandbrickspodcast](#), and at the company website <https://hostirian.com/>





The Balancing Act for Mid-Market Firms: Navigating Digital Growth and Security Hurdles

By Kevin Beasley, CIO, VAI

Increased competition and new regulatory requirements are increasing the tempo of digital transformation among mid-market companies.

In fact, Deloitte's [2023 Mid-Market Technology Trend](#) report found that technology spending among this cohort is at its highest level since 2019.

However mid-market companies face cybersecurity challenges when it comes to their expanding digital footprints. It's hard to find the cybersecurity talent that businesses need to fend off ransomware attacks and manage software vulnerabilities. They are resource-constrained in other ways: with limited or non-existent recovery plans, and an absence of training for key employees.

"Cloud Enterprise Resource Planning (ERP) systems are a strong antidote to the cybersecurity maladies mid-market companies face. Here's why.

Ransomware and Evolving Threat Landscape

Ransomware attackers extorted at least \$449.1 million from organizations in the first half of 2023 alone, according to a [threat assessment from the Department of Homeland Security](#). While that number may be eye-popping on its own, what may be even more surprising to some is the complex economic environment that supports it.

Ransomware is big business. There are employees, managers, and executives in ransomware cartels. These criminal organizations conduct scams on their own, but they also license their service to other threat actors in exchange for a cut of the proceeds, a phenomenon known as “ransomware-as-a-service.” Threat volumes for all companies are extremely high, and the bad guys only have to win once, while security teams have to win every time.

And the effects of a ransomware attack can be disastrous.

The average business experiences a recovery period of 22 days before resuming operations following a ransomware attack, which frequently costs 50 times more than the ransom demand, DHS says.

Cloud ERP systems can offer a higher inherent degree of security due to their centralized updates and expert-managed security protocols. They eliminate the inconsistencies of individual end-point security measures by ensuring real-time, system-wide protection.

Cloud ERP systems serve as a lifeline in the high-stakes aftermath of a ransomware attack, by significantly reducing recovery time and costs. These systems offer robust data backups and redundancy measures, ensuring that businesses can restore operations quickly and efficiently without giving in to ransom demands.

They also perform the same function in the face of natural disasters and other business disruptions. By housing data in secure, remote servers managed by professionals with top-tier expertise in digital security, these systems mitigate the risk of local data breaches and physical server damage.

Simplifying the Talent Gap

There are, according to research, just [69 cybersecurity candidates for every 100 job openings](#) in the field. Large companies struggle to hire, and often pay large salaries for talent. Mid-market firms can be shut out.

Cloud ERP systems allow companies to draw on the expertise of the ERP maker, and they can further expedite the integration of new security protocols and software updates. Instead of allocating resources to find scarce cybersecurity experts, these companies can rely on the robust security measures that come inherently with cloud-based ERP systems.

These platforms are equipped with automatic updates and are backed by a team of security experts from the provider, ensuring that the system is always up to date with the latest security standards and protocols. This not only alleviates the pressure on mid-market firms to compete for cybersecurity talent but also mitigates the risks associated with human error and insufficient in-house expertise.

The Digital Footprint

Two trends dominate in the digital evolution of the mid-market. In food and pharmaceutical distribution, for example, there's a push for traceability across the entire supply chain, from raw materials to the consumer and from farm to table. Technologies like blockchain and IoT are helping to meet those requirements. Among distributors of non-perishable hardgoods, the need for superb customer service amid competition from bigger, resource-rich competitors are pushing mobile technologies into the mix to streamline ordering and logistics processes.

All these digital tools can be a target-rich threat environment.

Cloud ERP is a reliable and resilient component of many mid-market business architectures because they help to integrate this expanding digital footprint into a single, comprehensive system. This centralized approach not only counters the skills gap in cybersecurity expertise but also provides a proactive defense mechanism against the ever-evolving threat landscape.

About the Author

As CIO of VAI, Kevin Beasley oversees both the corporation's technology strategy in conjunction with product development and the internal information technology initiatives that support the goals of the company. He has decades of ERP, SCM, and WMS consulting experience and extensive experience in the IT space. For more on VAI, please visit vai.net.





How Autonomous Vehicles are Revolutionizing the Last-Mile Logistics Industry

Cybersecurity will be one of the key concerns as last-mile logistics companies look to enhance efficiency with autonomous vehicles.

By Anar Mammadov, CEO, Senpex Technologies

Travelers who hail a taxi in San Francisco may be surprised as they settle into the backseat to discover their vehicle lacks a driver. In August 2023, California regulators approved the operation of [autonomous taxi services](#) in that state, where Cruise and Waymo had already been providing driverless rides with some restrictions.

The growing acceptance of robotaxis is good news for delivery companies who see autonomous vehicles as a tool for reshaping last-mile logistics. It indicates that AI-driven delivery vehicles could soon be a common sight on roadways, harnessing the power of technology to make last-mile logistics more efficient and affordable.

The role of autonomous vehicles in last-mile logistics

Last-mile logistics focuses on the last leg of the delivery process, where products make it into the hands of consumers. The operational complexities involved combined with its labor-intensive nature make last-mile logistics the most expensive phase of the delivery process. By some estimates, it accounts for as much as [53 percent](#) of delivery costs.

As autonomous vehicles take over this phase of delivery, they empower a number of innovations that allow for greater efficiency. The primary cost savings result from removing the labor costs of human drivers. Wages and benefits represent a major component of last mile delivery costs.

Autonomous vehicles also do away with some of the limitations that exist with human drivers. Autonomous vehicles can operate 24/7 without the need for a break. The AI that powers navigation in autonomous vehicles does not get tired or distracted regardless of how long its shift lasts.

By doing away with the need for a human driver, autonomous delivery vehicles can also be smaller. In urban areas, [smaller delivery vehicles](#) lead to less congestion as well as enhanced ability to navigate more quickly in tighter spaces.

Improving delivery safety

Autonomous vehicles also have the potential to make last-mile delivery safer. They bring “superhuman” capabilities to navigation that make it easier to detect and avoid accidents.

AI-driven vehicles are capable of 360-degree monitoring with both cameras and sensors, making it virtually impossible for them to be surprised by situations that can lead to collisions. Their response times are also faster than human drivers, with some [studies](#) showing AI drivers responding three times faster than human counterparts.

Autonomous vehicles are also able to respond to changing conditions dynamically and objectively. Human subjectivity can impair decision-making when traffic or weather requires driving adjustments. Autonomous vehicles make changes based solely on conditions, adjusting speed, following distance, and other instrument settings as data dictates.

Addressing cybersecurity concerns

One of the downsides of autonomous vehicles is the heightened need for cybersecurity. Because autonomous vehicles are essentially computers on wheels, they are a target for hackers. Attacks that breach vehicle navigation systems could result in a number of issues.

The most dangerous result of a cyber attack would be erratic driving. Autonomous vehicles with compromised navigation systems could quickly become a life-threatening risk on the road. Bad actors could disable braking systems or shut down sensors that protect vehicles from collisions.

Attacks could also focus on the data autonomous vehicles collect. There is a growing debate on the [privacy implications](#) of autonomous vehicles. The data collected by vehicle navigation systems, especially if connected to specific companies or clients, could be considered sensitive.

By obtaining remote control of vehicles, hackers could stage Denial of Service attacks. These would not only keep autonomous vehicles from accomplishing their mission, but also potentially shut down the roadways on which they navigate. Ransomware attacks are another possibility that could leave vehicles stranded and vulnerable.

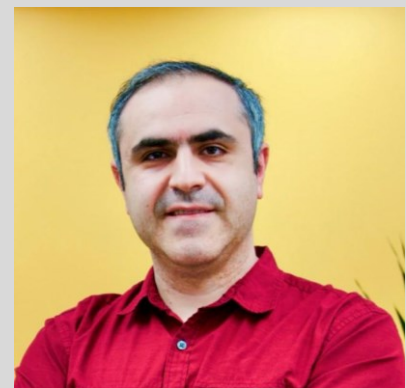
To address these concerns, autonomous vehicle developers are adding cybersecurity professionals to their teams. Waymo, for example, [reports](#) it “has developed a robust process to identify, prioritize, and mitigate cybersecurity threats in alignment with industry and government-defined security best practices.”

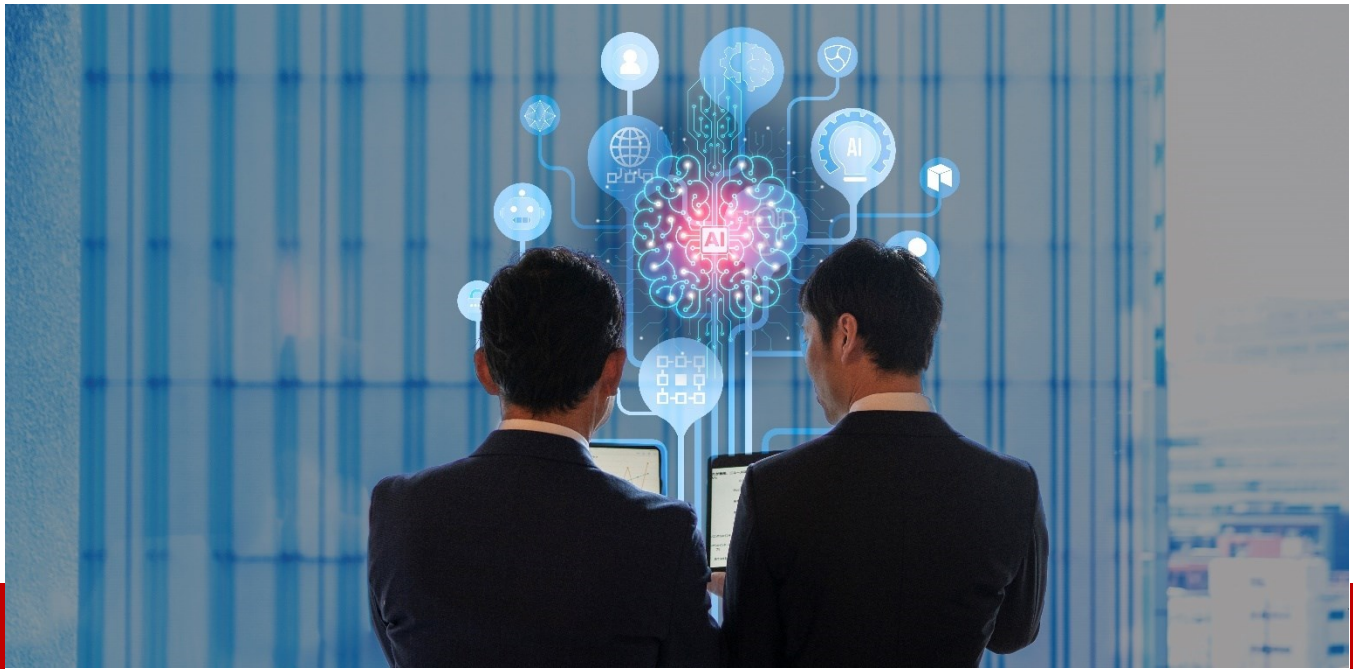
[Experts](#) say a critical step for cybersecurity is anticipating threats so systems can be built from the ground up to repel them. Encrypted communications, authentication protocols, and the isolation of critical systems should all be part of system architecture, rather than added later. Systems should also include defenses designed to detect attacks as they are occurring and trigger safety protocols.

Advances in technology have made autonomous vehicles a reality. The next step is expanding their use in ways that improve efficiency without compromising safety. In the last-mile logistics industry, autonomous vehicles promise to allow for faster deliveries at lower costs, resulting in better service to consumers and higher profits for businesses.

About the Author

Anar Mammadov is the CEO of Senpex Technology. He is a software development professional with more than 18 years of experience in enterprise solutions and mobile app development. He has applied his practical and results-oriented approach to business to create Senpex Technology, a personalized logistics and delivery service that utilizes groundbreaking artificial intelligence to optimize routes and to provide the fastest, most efficient, last-mile delivery resource for businesses. Senpex can be utilized 24/7, with no interruptions to your delivery needs. Anar can be reached online at anar@senpex.com and at his company's website, <https://web.senpex.com/>.





What You Need to Know to Embrace the Imminent Quantum Shift for Your Cryptography Future

By Eddy Zervigon, CEO of Quantum Xchange

Cryptography has long been essential in ensuring the protection of data and communication networks. However, even as we rely on it to safeguard sensitive information, vulnerabilities continue to give cause for concern. Remaining reliant on outdated cryptographic standards certainly adds to the dangers of compromise. Most legacy systems still cling to standards like MD5, SHA-1, TLS 1.1, and SSL 3.0 years after their prime.

The implications are significant. Networks are exposed to unnecessary risks with potential vulnerabilities that are ripe for exploitation by threat actors. As we usher in an era of cloud-scaling and quantum technologies, the stakes are raised even higher. With regulations such as CCPA, DORA, GDPR, HIPAA, PCI, SOX, and others in play, organizations face the need to evolve or risk breaches that could seriously compromise their operations.

The limits of PKE

For almost five decades, public key encryption (PKE) has been the standard-bearer for digital data protection. Its architecture, which relies on the exchange of public and private keys to encrypt and decrypt data, has been generally effective.

But inherent to this process of encryption is how it operates. The decryption key often travels alongside the data it's meant to protect. With quantum computers' potential to disrupt this system, our current data safety has become an illusion in a future where traditional computing will no longer be adequate, with many thinking of it in the same way we might have viewed mobile phones of the early 90s.

Think about it. Even if data is protected with PKE today, it can be copied and stored, waiting for the day when a more powerful computer is able to decrypt it. Adding impetus to the change is the fact that quantum computers have already demonstrated their ability to break PKE. A conventional computer would need 300 trillion years to break RSA encryption, which many see as the gold standard for PKE. A quantum computer can do it in 10 seconds.

The need for post-quantum cryptography

Fortunately, a shift is happening that has been dubbed one of the most extensive cryptographic transitions in the history of computing - moving from the well-established PKE to the emergent post-quantum cryptography (PQC). This represents a foundational change that will impact every facet of our increasingly digital lives.

The federal government is currently planning the upgrade of digital networks with post-quantum cryptographic standards as outlined in a May 2022 national security memorandum, anticipating the arrival of a fault-tolerant quantum computer. Last year, the National Institute for Standards and Technology (NIST) shortlisted quantum-safe encryption algorithms to preempt the quantum threat.

Of course, making the change will be massively disruptive, given the scale of the environment. PKE and its dependencies underpin the bulk of the public internet. In the US alone, it protects 4.5 billion internet users, powers 200 million websites, and secures \$3 trillion of retail e-commerce transactions annually. Now, expand that to the rest of the world, and the enormity of the challenge becomes clear.

Challenges of transition

Change, especially of this scale, is never straightforward. The NIST's 2021 report, 'Getting Ready for Post-Quantum Cryptography,' highlighted the complexities of adopting PQC. The reality is that even after the standardization process concludes, making a full transition could easily span up to 15 years. That's a long time to become fully secure in a quantum world.

Adopting a multi-faceted approach in this regard is vital. For instance, using PQC, QKD (Quantum Key Distribution), QRNG (Quantum Random Number Generator), or even different combinations will ensure organizations are no longer reliant on any single encryption method.

Taking the leap

Recent innovations like the Quantum Xchange CipherInsights tool can provide a strategic advantage. This solution monitors network activity, discovers cryptographic assets, and assesses risks to bring an additional layer of defense. Deployed as a virtual appliance, CipherInsights goes beyond traditional scanning of endpoints only. It analyzes traffic in real-time, pinpointing sanctioned and unsanctioned encryption. Within 90 minutes, it can evaluate whether networks are compliant with regulations, ensuring that businesses remain on the right side of the law.

Beyond this, organizations must continually undertake extensive risk assessments if they're to navigate the quantum future effectively. This involves segregating data based on protection urgency – classifying them as "severe," "soon," or "stable." A vital step here is to identify data guarded by quantum-susceptible solutions.

Here, we refer to solutions like symmetric algorithms with key sizes under 256 bits or traditional asymmetric cryptography. The strategy of choice merges the principles of diversification, akin to spreading risk across various investments in a financial portfolio, with crypto-agility. This approach involves the organization adopting crypto-agility, a flexible system that supports a variety of cryptographic methods, while simultaneously remaining vigilant to threats by utilizing multiple security techniques.

As the digital landscape evolves, organizations must be proactive. They must look at ways to future-proof their operations against the known and the unforeseen. Investing in quantum-safe solutions is a building block for the new world.

About the Author

Eddy Zervigon, CEO of [Quantum Xchange](#). Eddy Zervigon is a seasoned senior executive with extensive operational, restructuring, and turnaround experience. Throughout his career in investment banking and corporate advisory, Zervigon has amassed an impressive track-record working with management teams to craft, refine, and execute winning business plans; hire highly effective teams; and lead successful investment monetization via sale or IPO. As a Managing Director in the Principal Investments Group at Morgan Stanley from 1997-2012, Zervigon was responsible for technology, media and entertainment and energy investments throughout Latin America and the U.S. He has been a Special Advisor at Riverside Management Group, a boutique merchant bank, since 2012 and currently sits on the board of directors at Bloom Energy (NYSE: BE) and Maxar Technologies (NYSE: MAXR). Zervigon holds an MBA from the Amos Tuck School of Business at Dartmouth College, a master's in taxation from Florida International University as well as his undergraduate degree in accounting.



Eddy can be reached online at our company website [Quantum Xchange](#)



How Cloud Solutions Can Lead to Stronger, More Secure IT Operations

By Mike Wiseman, Vice President, Public Sector, Pure Storage

In fiscal year 2022, the federal government [spent](#) a total of \$12.3 billion on cloud goods and services – a 30 percent increase from a year before. Cloud services, which offer tools such as networks, servers, and data storage, can help federal agencies deliver better IT services while minimizing costs. But, without adequate security measures, these services can expose agencies to cyberattacks.

The Government Accountability Office recently released a [report](#) on how agencies can improve their cloud security practices – including replacing aging IT systems, consolidating varying platforms, and utilizing cloud to improve how they store and manage federal data.

By focusing on these areas for IT improvement, agencies can ensure more effective and efficient services for citizens and employees.

Replacing Aging IT Systems

Government agencies are under immense pressure to deliver on their missions regardless of today's increasingly challenging cyber environment. Agency IT systems are experiencing more strain than ever, and events such as changing federal regulations and the looming threat of a ransomware attack, often require new tools and data storage and management solutions to support and protect mission-critical functions.

To address the impact of aging legacy systems, agencies must focus on implementing the proper IT modernization systems and migrate to modern, interoperable IT infrastructures. As IT leaders make these shifts, they should seek technology solutions that best meet the needs of their agencies and stakeholders. With many different solutions on the market, those that offer agile and flexible consumption models are the most efficient and cost-effective as they allow agencies to scale up or down without massive disruptions.

Consolidating Operations

Agencies often operate with a lean staff and need solutions that maximize productivity without compromising cost and security. Federal IT leaders continue to look for the best ways to equip employees with the right tools and technologies, but staffing issues persist, further deterring the push toward modernization. Agencies should look to solutions that require less maintenance and can free up staff for other mission-driving activities, along with continuing education and professional development.

One of the important ways IT teams can be more efficient in developing and delivering applications in private and hybrid cloud environments is by consolidating a larger number of applications on fewer storage systems. The ability to do this type of application consolidation and unlock its many benefits means less management and maintenance with a faster return on investment.

By consolidating applications into a cloud-centric platform, agencies can reduce costs, lower risk, and support a more integrated and interoperable infrastructure.

Investing in Cloud Services

With the pace of digital transformation, governments must streamline and accelerate technologies to deploy integrated cloud, hybrid, and multicloud architectures and upgrade the legacy applications that they rely on.

As technologies continue to evolve, agencies must ensure that they implement the most advanced IT systems, including container-based applications, as they provide agencies with a complete data storage infrastructure solution capable of delivering premier citizen services. Container applications give IT development teams the tools to modernize their applications, as they can gain speed, agility, and scale, while offering easy backup and restore and enhanced disaster recovery. This protects the entire application, including data, application configuration, and container-based objects.

Government IT leaders aiming to modernize with Kubernetes, containers, and microservices must keep one point in mind: the storage equation has changed. Kubernetes platforms give government IT development teams the tools to modernize their applications, using containers and microservices to gain speed, agility, and scale.

Investing in right-sized efficient storage systems and applications, containers can help agencies elevate citizen service capabilities while addressing the critical areas of cyber protection, legacy modernization, and cloud services. A clear cloud strategy is essential to unlocking critical insights and advancing agency missions.

Secure, Collaborative Solutions

Agency missions never stop; they need secure, efficient, sustainable, and agile solutions that can keep pace. IT leaders should focus on executing a comprehensive strategy for implementing modern solutions that will continue to serve citizens' changing needs.

In addition, agency IT leaders can partner with private-sector corporations to modernize their IT infrastructures. Working collaboratively, the government can make strides in adopting modern practices. By creating an individualized path to modernization, agencies can better deliver services to citizens in more specialized ways and continue to grow in their service capabilities.

Agencies should not treat IT strategies as static plans. Instead, they must revisit their strategies on an ongoing basis as they move toward modernization. Modern and secure systems can lead to enhanced platforms and applications, which leads to more substantial business process improvement.

About the Author

Michael Wiseman is the Vice President, Public Sector at Pure Storage, bringing over 25 years of experience as a tech sales leader in government IT. He is responsible for developing a team to enable the transformation of how public sector customers protect, serve, and educate their constituents by leveraging technology to connect, innovate and lead. Mike can be reached mwiseman@purestorage.com and at our company website <https://www.purestorage.com>.





Addressing Bias in Insider Risk Monitoring

By Chris Denbigh-White, Chief Security Officer, Next

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

Defining Monitoring Bias

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

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

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

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

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

Legacy Approaches Don't Address Bias

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

Eliminate Bias and Improve Data Protection

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

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

About the Author

Chris Denbigh-White is Chief Security Officer of Next DLP (“Next”). He has over 14 years of experience in the cybersecurity space including in the office of the CISO at Deutsche Bank as well as cyber intelligence for the Metropolitan Police.

Chris can be reached online at <https://www.nextdlp.com>





Industry Benchmark Report, Issued by The FAIR Institute, Unveils the Dollar Impact of Cyber Incidents

The 2024 Cybersecurity Risk Report Provides CISOs Insights into the Likelihood and Financial Impact of Top Cyber Risks.

By Luke Bader, Director, Membership and Programs, FAIR Institute

The FAIR Institute, the leader in education for cyber risk quantification (CRQ) based on FAIR™ (Factor Analysis of Information Risk), has released its 2024 [Cybersecurity Risk Report](#). This document provides CISOs, CFOs and other business decision-makers the clearest visibility into the financial impact of cyber risks, based on quantitative analysis of actual cyber incidents through 2023.

This Report is sponsored by EY and Safe Security which provided research on cybersecurity program development and data-science support.

“The FAIR Institute 2024 Cybersecurity Risk Report leverages our most extensive data set ever and applies advanced techniques in quantitative analysis to reveal the underlying risk factors that organizations need to understand to mount their most cost-effective defenses against data breach and other loss events,” said Nick Sanna, President of the FAIR Institute.

“The insights within demonstrate the value of CRQ to empower organizations to manage their cyber loss exposure in the financial terms that boards and senior management understand. It’s especially timely considering the rules on disclosure of material cyber risk adopted by the Securities and Exchange Commission (SEC) in 2023, a powerful signal to public companies to improve their cyber risk reporting practices, and move to a data-driven, risk-based approach based on a transparent, defensible model such as FAIR,” adds Sanna.

Key Findings

The Report is augmented by material from the [EY 2023 Global Cybersecurity Leadership Insights Study](#), based on interviews with 500 C-suite and cybersecurity leaders, that reveals valuable insights into the traits of “Secure Creators” who successfully implement cybersecurity programs.

- The two top industries by average loss exposure are Public Administration and Healthcare, driven by a relatively high probability of loss event.
- Systems Intrusion and Insider Error are the top 2 risk themes for small businesses, while Basic Web Application Attacks and Social Engineering top the list for large enterprises.
- Bigness raises risk. A large organization - measured in revenue and employee count - has a higher likelihood and severity of cyber loss events compared to a mid-market firm. For example, a large healthcare company has a better than 50% chance of a serious insider-error event in a year versus 26% for a mid-size company in the same sector.
- Businesses could reduce loss exposure to data breaches by as much as 80% by basic improvements in security posture (such as patching or securing endpoints) and reduction of data retention.

In response to the new rules from the SEC on material cyber risk, the FAIR Institute Cybersecurity Risk Report also introduces the FAIR Materiality Assessment Model (FAIR-MAM™), the only standard taxonomy to comprehensively define what forms of losses contribute to the measure of materiality in financial terms.

For a complimentary copy of the Report, please click on [the link](#).

About the FAIR Institute

The FAIR Institute is a research-driven not-for-profit organization dedicated to advancing the discipline of cyber and operational risk management through education, standards, and collaboration. The driver

behind our mission is the breakthrough achieved by FAIR™, the risk taxonomy and quantification standard, key to effective risk management.

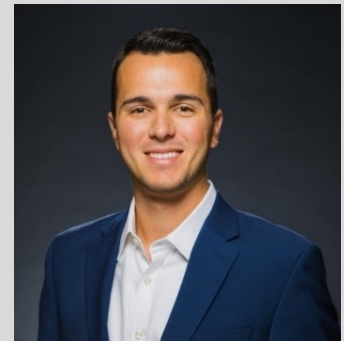
Its members - forward-thinking risk officers, cybersecurity leaders and business executives - now exceed 15,000 in over 100 countries, with representation of 50% of Fortune 1000. The FAIR Institute has been recognized by SC Media as one of the three most influential industry organizations of the last 30 years.

To learn more and get involved, visit www.fairinstitute.org.

About the Author

Luke Bader is the Director of Membership and Programs at the FAIR Institute. He has worked to grow and support an international membership of over 15,000 at the Institute. He focuses on the member experience including education, events, and networking opportunities.

Luke lives in Washington DC with his dog, Rip, and holds both a Master of Science in Business and a bachelor's degree from The Catholic University of America.



Luke can be reached online at lbader@fairinstitute.org. Twitter: @FAIRInstitute, LinkedIn: FAIR Institute: <https://www.linkedin.com/company/fair-institute>, LinkedIn: <https://www.linkedin.com/in/lukebader/>, and at our company website www.fairinstitute.org



Beyond Resumes: Uncovering Hidden Talent at the New Jersey Judiciary

Illuminating the individual beyond the black and white

By Darrin Straff, Senior Staffing Consultant, NinjaJobs

A Deeper Dive

In my recent articles, I've discussed the importance of looking beyond resumes during the hiring process. Today, I want to share a personal account involving the Information Security Unit (ISU) of the New Jersey Judiciary.

Earlier this year, searching for new opportunities led me to ISU. During an initial conversation with Sajed Naseem, CISO, my background in writing surfaced and he mentioned the need for a technical writer. Would I mind writing a short technical brief to show him what I was capable of? Sure! Nailing that led me to a consultancy role, culminating in the development of a 60-page training manual for their budding

cybersecurity analysts. The twist? My resume barely touched on my writing background, a testament to the power of genuine conversation.

Leadership that Dares to be Different

Given my work as a technical cybersecurity recruiter, I have noticed some distinct differences in the New Jersey Judiciary – Information Security Unit. The team is cohesive and varied, they come from backgrounds in engineering, finance, art, and various other majors. The environment is positive, collaborative, and serious when necessary. It is quite a unique environment.

From my observations, the staff include engineers as well as those who possess leadership skills. They speak their mind and are put in positions to grow in areas that would not be typical in most environments. One former intern, now a full-timer, is eyeing a lead cyber engineer role. ISU finds next level analysts and engineers from college level classroom debates. So, when talent doesn't always shout from a resume, I mean it.

ISU's internship program is pushing the envelope in cybersecurity training. In the past two years, ISU onboarded 24 interns. Each one secured a full-time role – some with cutting-edge cybersecurity companies and others within the very walls of the New Jersey Judiciary. This 100% placement rate showcases not just the program's quality but the deep connection ISU fosters with its interns.

Innovative Edge

ISU is not just safeguarding data; they're pushing the envelope with tech like AI and Big Data Analytics. While I can't reveal all their strategies, let's just say their data game goes way beyond basic firewalls and antivirus software. They're not just playing defense; they're redefining the whole game. They are adding quality and value to the New Jersey Judiciary's mission.

The Takeaway

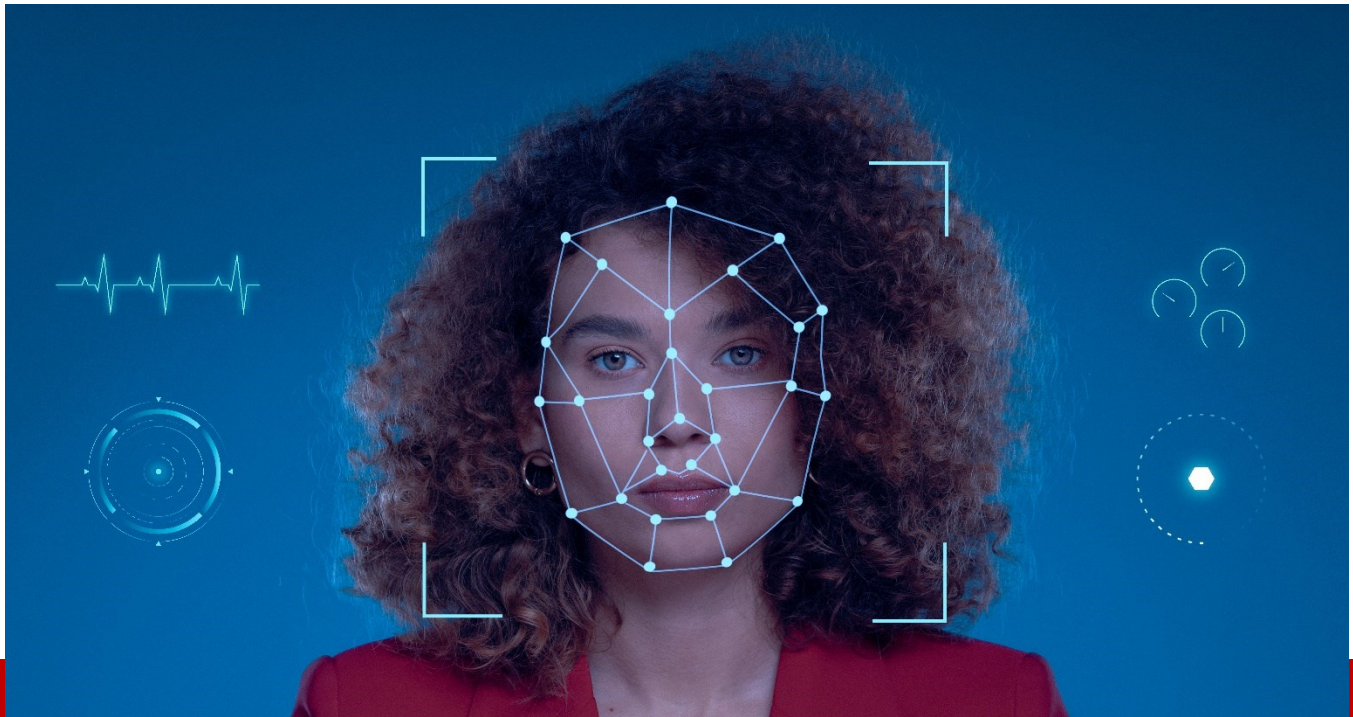
My experience with ISU perfectly encapsulates what I've been advocating in my articles – the need to look beyond resumes and recognize the whole person. ISU is a real-world testimony to the power of holistic recruiting in cybersecurity. It's not just about filling roles; it's about envisioning and shaping the future of cybersecurity.

About the Author

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

Darrin Straff can be reached online at (<https://www.linkedin.com/in/darrinstraft/>) and at our company website <https://ninjajobs.org>





Deepfakes and AI's New Threat to Security

The high cost of free open-source generative software.

By Luke Arrigoni, Founder, Loti

The rise of deepfake technology poses significant risks to celebrities, high-net-worth individuals, and the general public, with its ability to manipulate reality, infringe on privacy, and facilitate crimes ranging from fraud to character assassination. This article delves into recent events highlighting these dangers, emphasizing the need for vigilance and protective measures.

In an age where technology is advancing at an unprecedented pace, the emergence of deepfake technology, such as stable diffusion software, poses a profound and unsettling threat. This software, once the domain of specialized experts, has now become alarmingly accessible to the general public, raising serious concerns about privacy, security, and the integrity of digital content.

The disconcerting ease with which stable diffusion software can be downloaded and operated has opened a Pandora's box of potential misuse. With just a few clicks, an individual with minimal technical skills can access these tools, capable of generating hyper-realistic deepfakes. This software, leveraging sophisticated artificial intelligence algorithms, can manipulate images and videos to an extent that the fabricated content appears strikingly real, blurring the lines between truth and deception.

This ease of access dramatically lowers the barrier to entry for creating deepfakes, democratizing a technology that was once restricted to those with substantial computational resources and technical expertise. Now, anyone with a basic computer and internet access can harness the power of stable diffusion software. This shift has profound implications for personal privacy and security. It raises alarming questions about the potential for misuse, particularly against public figures, celebrities, and high-net-worth individuals who are often the targets of such malicious activities.

The growing availability of this technology has been met with widespread concern from cybersecurity experts, legal professionals, and ethicists. They warn of a future where the authenticity of digital content can no longer be taken for granted, a world where seeing is no longer believing. The potential for harm is vast – from damaging the reputations of individuals through fabricated scandalous content to influencing public opinion through false representations of political figures.

As these tools become more user-friendly and accessible, the challenges in combating deepfake content grow exponentially. Traditional methods of verification are becoming less effective against the advancing capabilities of deepfake technology. This creates a pressing need for new solutions to detect and combat these digital deceptions.

Recent Incidents Involving Celebrities

1. **Rashmika Mandanna Incident:** A deepfake video that appeared to show Indian actress Rashmika Mandanna in an elevator, which was later revealed to be a fabrication using the body of British-Indian influencer Zara Patel, caused widespread concern. This incident underscored the ease with which AI can manipulate images and the severe impact it can have on the victims, leading to distress and damage to reputation
2. **Katrina Kaif Deepfake:** Another troubling case involved Bollywood actress Katrina Kaif. An original scene from her movie "Tiger 3" was morphed to present her inappropriately, causing public outrage. This example not only illustrates the ease of creating convincing deepfakes but also their potential to harm the dignity and public image of individuals

Impact on High Net Worth Individuals and Businesses

1. **Rapid Increase in Deepfakes:** The number of deepfake videos online has surged at an alarming annual rate of 900%, according to the World Economic Forum. This increase has led to a rise in cases involving harassment, revenge, crypto scams, and more, signaling a growing threat that can affect anyone, particularly those in the public eye or with substantial assets
2. **Elon Musk Impersonation:** In a notable example, scammers used a deepfake video of Elon Musk to promote a fraudulent cryptocurrency scheme, resulting in significant financial losses for those duped by the scam. This incident highlights the potential for deepfakes to be used in sophisticated financial frauds targeting unsuspecting investors

3. **Violation of Privacy:** The use of deepfakes in violating individual privacy is a significant concern. For instance, deepfake videos have been created showing celebrities' faces superimposed onto pornographic content, causing considerable distress and reputational damage
4. **Targeting Businesses:** Deepfakes pose a serious threat to businesses as well, with instances of extortion, blackmail, and industrial espionage. A notable case involved cybercriminals deceiving a bank manager in the UAE using a voice deepfake, leading to a \$35 million theft. In another instance, scammers attempted to fool Binance, a large cryptocurrency platform, using a deepfake in an online meeting

The Financial Sector's Struggle

The financial sector, including banks and FinTech companies, is increasingly targeted by deepfake scams. These scams exploit vulnerabilities in digital systems and the trust of individuals, leading to significant financial losses and a loss of consumer confidence. Banks are now investing in defensive technology and educating consumers about these risks

Conclusion: The Need for Protective Measures

The incidents mentioned above underscore the urgent need for protective measures against deepfake technology. This is where services like Loti come into play, offering tools to detect and combat unauthorized use of a person's image or voice. For celebrities, high-net-worth individuals, and businesses, employing such protective measures is not just about safeguarding their privacy and reputation but also about defending against potential financial and emotional harm.

In conclusion, while deepfake technology continues to evolve and pose new challenges, proactive steps and awareness can help mitigate its risks. Companies like Loti offer a valuable resource in this ongoing battle, helping to ensure that personal and professional integrity remains intact in the digital age.

About the Author

Luke Arrigoni is an expert in artificial intelligence with a rich history of collaboration with leading U.S. companies like UPS, J&J, Getty, AT&T, Goldman Sachs, CAA, and Sephora. He's built robust machine learning and data science programs. His visionary work predates the formal recognition of such technologies in the industry. Luke's entrepreneurial journey includes successfully building and selling an econometrics business, showcasing his acumen in creating and scaling innovative tech ventures. Currently, as the Co-Founder of Loti (<https://goloti.com>), Arrigoni leads in digital identity protection, leveraging advanced AI to monitor and control personal image and video dissemination online, including takedowns of unauthorized content and deep fakes.





Unmasking the Vulnerabilities in Telecom Signaling: A Call for Enhanced Security

Mobilizing Collective Action for Telecom Signaling Security

By Rowland Corr, Vice President and Head of Government Relations, Enea

Telecommunications, particularly mobile networks, have become the backbone of our modern, interconnected society. They facilitate seamless communication and real-time information sharing, and underpin numerous vital services that touch every aspect of our daily lives. As these networks have proliferated, their complexities have grown, making them both a marvel of modern engineering and a potential point of vulnerability.

While the telecom industry has made strides in fortifying the security of these networks, there remains an often-underestimated weak link: mobile signaling security. This crucial component, responsible for tasks such as call routing, message delivery, and data transfers, has become a prime target for threat actors. Exploits in this domain can lead to a myriad of issues, from personal data breaches to disruptions that can impact national security. As we delve deeper into the world of telecom signaling vulnerabilities, it's imperative to understand the risks at hand and the measures needed to mitigate them.

Understanding mobile signaling

Mobile signaling can be aptly described as the "traffic controller" of telecommunications networks. It's the underlying mechanism that manages and directs the flow of data, ensuring that calls, messages, and other forms of communication reach their intended destinations. Signaling protocols are responsible for the entire lifecycle of these communication sessions, from their initiation and the transfer of data to their eventual termination. This intricate system not only facilitates communication within a single network but also interconnects telecom infrastructures of countries globally, sometimes referred to as the interconnect environment.

One of the most pivotal protocols in mobile signaling is Signaling System 7 (SS7). For decades, SS7 has been the cornerstone of global communication, enabling functionalities like call setups, SMS routing, mobile roaming, and number portability. Designed in the 1970s, SS7 was conceived as a closed network, built on mutual trust among all its participants. This design, which once was its strength, has been exposed as inherently vulnerable as cyber threats have evolved. Yet, the adoption of adequate measures to protect signaling interfaces has been slow to materialize, due on the one hand to a lack of capability to detect such threats on the part of mobile operators, and on the other to a prevailing focus on IT-based security threats. This has led cyber policymakers and practitioners to overlook mobile signaling. As we progress into an era of exponentially heightened digital connectivity, understanding signaling vulnerabilities and their implications, and the role of signaling security as a pillar of cyber resilience, becomes ever more critical.

The neglect of mobile signaling security

As the digital threat landscape has evolved, the focus of cybersecurity has predominantly shifted toward IT security, often sidelining the unique challenges posed by mobile signaling. This trend was notably highlighted by entities like the European Union Agency for Cybersecurity (ENISA), which emphasized the disparity in definitions and understandings of "cyberspace" across industries. Such disparities have inadvertently led to a concentration on internet-borne threats, leaving mobile signaling, with its distinct technicalities and vulnerabilities, in the shadows.

This oversight is further exacerbated by the specialized nature of signaling, which requires its own sets of expertise, tools, and systems. Historically, signaling experts have been more engrossed in managing network operations and troubleshooting performance issues rather than proactive threat hunting. This has resulted in a significant gap in many operators' Security Operations Centers (SOCs) and national cybersecurity frameworks, creating a blind spot that threat actors can readily exploit.

The inadequacy of too basic 'baseline' security measures

The vulnerabilities inherent in mobile signaling came to the forefront of industry attention in 2014 when the security of SS7 was publicly questioned, both due to geopolitical events and research revelations. These investigations showcased how the protocol could be manipulated by threat actors to track user

locations, intercept calls, and read text messages. While SS7's widespread use in global telecommunication infrastructure raised concern, today there is a pressing need for more than basic 'baseline' security measures. The fact that even Diameter, the more secure successor to SS7 used in 4G and 5G networks, has shown substantial susceptibility to exploitation by attackers, creates a growing imperative not only for multi-protocol signaling protection but for continuously optimized security measures in the face of determined and sophisticated threat actors.

Operator blind spots and the need for better regulation

Not only are basic baseline security measures no longer enough, but there is now an urgent need for evolved incident reporting requirements to incentivize and prompt action by operators. Current regulatory frameworks often lack the scope and efficacy to capture the societal impacts of signaling-related incidents and threats. This is because in any single instance, signaling threat events are often comparatively low in volume and non-disruptive in nature, and yet when executed by state-level threat actors can be sufficient to jeopardize national security. Moreover, the resultant data breaches can also add up over time to a very high volume of impacted users yet without any single event meeting the typical reporting threshold for incident notification by operators. This gap in national frameworks can allow extended attack campaigns to go undetected, simply not being 'on the radar' of operators, regulators, or national cyber agencies. Accordingly, regulatory frameworks must be updated and informed by a suitably evolved approach to defining significant impacts and security incidents. This may serve as the catalyst for fit-for-purpose telecom security and comprehensive cyber resilience.

Where operators find themselves ill-equipped to detect and counteract threats involving mobile signaling the deficiency isn't merely a result of inadequate protection but also stems from a systemic lack of awareness and prioritization in the industry as a whole. While compliance is essential, it's equally crucial for operators to possess the capability to identify and respond to threats proactively. This has the added potential to facilitate threat information sharing among the telecoms security community, which has been called for for many years, but which has progressed very little. Since the first line of defense is threat visibility, regulators and government more broadly have a crucial role to play in enabling operators to address the security blind spot presented by signaling, by ensuring that control plane threats to data confidentiality and integrity, as well as availability, are made visible. With the right support for capability development where needed, countries can close this critical gap and fortify the cyber resilience of their mobile telecom networks.

What's next?

The vulnerabilities in telecom signaling are not just technical challenges; a broader call to action throughout the entire telecommunications ecosystem must be heeded. As digital threats grow in sophistication, the need for a strategically aligned, mission-oriented response becomes paramount. The future of telecom security hinges on transcending traditional boundaries and fostering collaboration among operators, regulators, and the greater cybersecurity stakeholder community. By embracing a

collective approach, we can anticipate emerging threats, share insights, and drive innovative solutions. The question isn't whether we can secure our networks, but whether we can come together with the urgency and unity of purpose this mission demands. The time for siloed approaches has passed; the era of collective resilience through collaborative action is upon us.

About the Author

Rowland Corr is the Vice President and Head of Government Relations of Enea. He helps cybersecurity agencies, regulators, and other government stakeholders evolve and execute their national cybersecurity strategies. Prior to joining Enea, Rowland served in Ireland's Department of Defence in interdepartmental advisory and international engagement roles on security matters such as cybersurveillance, non-proliferation, and hybrid threats. Rowland can be reached online at our company website <https://www.enea.com/> and <https://www.enea.com/insights/eneas-experts-meet-rowland-corr/>





Introducing GitHub Insights, Latest Solution to Combat Growing Threat to APIs

By Scott Gerlach, CSO - StackHawk

The accelerated demand for software applications and application programming interfaces (APIs) across industries has caused organizations' attack surfaces to become larger than ever before. Most modern organizations continue to struggle with sustaining adequate visibility over their key software components. It's no secret that the constant influx of new APIs, combined with the responsibility of maintaining security coverage for existing ones, is straining AppSec teams and leaving APIs susceptible to potential risks. In fact, a recent [Salt Security study](#) found that 4,845 attackers targeted APIs in December 2022 alone, resulting in a 400% increase compared to earlier in the same year, and 94% of respondents had experienced some security issue with their production APIs. These alarming numbers are likely because a mere 12% of respondents deploy 'advanced API security strategies' and 30% admitted that they lack an API security strategy of any level. To address these common and emerging pain points in the industry Stackhawk, an API security testing company, recently introduced GitHub Insights to offer developers and security teams modernized API security with enhanced visibility and full control of an organization's attack surface.

GitHub Insights - Here's How it Works

GitHub Insights is StackHawk's latest feature that offers security teams continuous discovery and visibility into their organization's threat landscape, allowing them to identify gaps in coverage, align security testing with the rapid pace of software development, and work more closely with the engineers writing the code. By seamlessly integrating with GitHub repositories, this new feature eliminates blind spots and fosters efficient collaboration between security and engineering teams. Instead of manually tracking and testing hundreds or thousands of APIs, GitHub Insights provides software developers with visibility into their API threats from every possible angle, allowing companies to be hyper-aware of vulnerabilities and bugs before they disrupt business operation and product development timelines, a critical asset with teams launching and retiring APIs and software applications daily. With GitHub Insights, users will be able to efficiently coordinate security testing and new software development, identify gaps and blind spots in API coverage, allow security teams to work more effectively and collaboratively with software engineers, and maximize productivity by coordinating security testing in the early stages of software development.

How GitHub Insights Addresses API Security Pain Points

Since it's nearly impossible for organizations to protect themselves from threats they can't see, StackHawk's GitHub Insights provides heightened visibility so that teams can coordinate the implementation of effective security measures when new APIs are added or old ones are retired, and allow teams to observe if any current security measures need to be altered. This visibility gives teams the upper hand in catching deficiencies – a game changer in today's world with the rapid development of new API routes.

Here's how StackHawk's GitHub Insights addresses these common pain points:

- **Code-based API discovery:** Traditional discovery tools have to rely on web traffic to identify API routes; however, with StackHawk's GitHub Insights, organizations can discover APIs at the source code level. This feature enables teams to assess their complete API catalog prior to production release.
- **Continuous visibility:** Stackhawk's GitHub Insights examines the API layer, links its discoveries to the source code, and offers thorough insights regarding the ongoing development, contributors, and testing frequency. This helps ensure that security measures keep pace with fast software development, granting organizations complete visibility into their attack surfaces and API security posture.
- **Bridging the gap between developers and security experts:** Stackhawk's GitHub Insights fosters collaboration between security and developer teams by establishing connections between testable APIs and their associated codebases and teams. As a result, security teams can quickly identify and assign accountability for resolving issues as they occur and identifying suitable collaborators for testing new APIs.

Looking Ahead with GitHub Insights?

The recent rise in API adoption has expanded organizations' attack surfaces, creating holes and blind spots in software development processes and leaving businesses vulnerable to API-focused attacks. Ineffective collaboration around API development, testing and maintenance has put organizations at risk, as many struggle to keep pace with proper security testing to match their rapidly increasing APIs, resulting in the potential for data breaches and malicious access to sensitive information. StackHawk's launch of GitHub Insights not only helps proactively safeguard against API-related threats and vulnerabilities by giving organizations a holistic view into their entire attack surface but also creates a stronger dynamic within developer and security teams for a more cohesive and effective API security strategy.

About the Author

Scott Gerlach is the CSO at StackHawk. Scott has more than 20 years of experience in information security. Scott is a passionate Security Officer with expertise in identifying security gaps and working with companies to develop safe and effective policies and procedures to mitigate those risks. His expertise spans developing, implementing, and managing IT security strategy and policy, risk management, intrusion detection, vulnerability assessment, network security design, application security and incident response. Prior to founding StackHawk, he was CSO at Twilio. He also spent nearly a decade in security at GoDaddy. To learn more about StackHawk please visit: www.stackhawk.com





Prioritizing Action After the Threat Headlines

By Douglas McKee, Executive Director, Threat Research, SonicWall

As Ferris Bueller once said, “Life moves pretty fast.” Most people, especially cybersecurity professionals, know the feeling. Minutes - sometimes seconds - matter in dealing with cybersecurity incidents. But how do you slow down time? What makes it so difficult to stay current or to prioritize what is on today’s agenda for a security operations center? It’s all in the *minor details*.

Parents can often recognize this instinctively. If your son or daughter wakes up one morning and you ask them, “How did you get home last night?” And they respond with, “I hitched a ride with a complete stranger,” a protective parent may gasp with surprise and concern. However, if the response has more details such as, “I took an Uber at 3 a.m. from my friend’s house, because I wanted to get home safely,” the same protective parent could react differently and prioritize the conversation accordingly.

On October 3, Daniel Stenberg [Posted](#) on X about a new “High” vulnerability in the curl ecosystem that would be publicly disclosed on October 11. Due to the popularity of both curl and Daniel’s social media influence, the cybersecurity world exploded with anticipation of a highly impactful and severe security issue; however, the post provided very few details about the actual issue.

The Windup

Daniel's initial post on X sparked many questions, some of which people were not afraid to ask on X.

The screenshot displays a series of tweets on X. The first tweet is from **Mathematica Ken** (@MathematicaKen) asking if a CVE impacts the MS compiled version. It has 1 reply, 5 retweets, 5 likes, and 13.9K views. A reply from **daniel:// stenberg://** (@bagder) states, "I rather not reveal any further details until October 11." with 1 reply, 3 retweets, 43 likes, and 16.1K views. The second tweet is from **Dan Lorenc** (@lorenc_dan) asking "Only HIGH? I didn't know the NVD still went that low!" with 1 reply, 1 retweet, 23 likes, and 11.1K views. A reply from **daniel:// stenberg://** (@bagder) says, "This is *our* score though. NVD is likely to go full meltdown on it..." with 3 retweets, 58 likes, and 10.8K views. The third tweet is from **Alexander** (@alexfoo) asking "Same score as the theoretical ddos?" with 1 reply, 1 retweet, 1 like, and 15.1K views. A reply from **daniel:// stenberg://** (@bagder) responds, "pretty much, yes. But this time actually the worst security problem found in curl in a long time." with 2 replies, 19 retweets, 72 likes, and 102.5K views.

Phrases such as “likely to go full meltdown” and “worst security problem found in curl in a long time” coupled with resistance to provide any additional detail, sent media outlets and security experts writing articles about how this vulnerability would be the next big security concern for the computing world. It’s also important to note the context around the term “High” in regard to the [National Vulnerability Database](#) (NVD). From a standard scoring perspective, a “High” vulnerability has a CVSS score of 7.0-8.9.

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

This is important since there is a precedent that “meltdown” level vulnerabilities are typically 9.0 or above, hence the “Critical” rating. This means there is a potential conflict in the *minor details*, but in our culture, often the mismatch will be ignored for a more severe outcome.



daniel:// stenberg://
@bagder



T minus 47 hours to the pending curl release

2:20 AM · Oct 9, 2023 · 22.1K Views

The Details

On October 11 as promised, the details of the vulnerability were made public, and the world was set on fire, but in a different manner than one may have expected.



daniel:// stenberg:// @bagder · Oct 11
curl 8.4.0 is here.



[daniel.haxx.se/blog/2023/10/11/...](https://daniel.haxx.se/blog/2023/10/11/)



13

366

959

133.7K

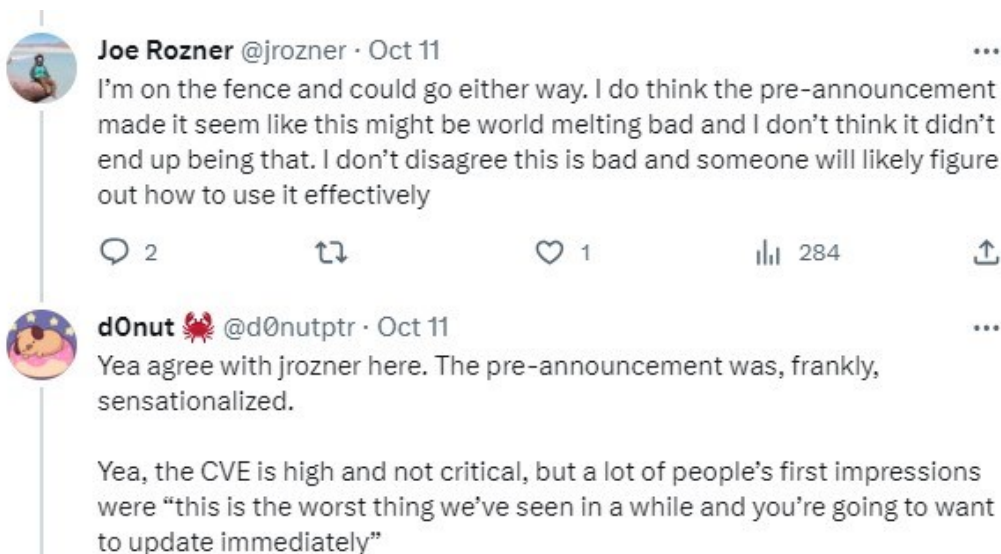


It's important to take a moment to acknowledge the main lesson learned from the release is the absolute professionalism and care [Daniel Stenberg](#) took in addressing this issue. If every vendor and open-source project followed his example, we would have a more secure computer world without question. A vulnerability was discovered and reported by a security researcher on a highly impactful platform, and it was patched in a timely manner with full transparency on the issues and how it was addressed, before, to the best of the community's knowledge, any active exploitation had occurred. More simply put – the process worked flawlessly.

What did the release say?

In nutshell, the published details revealed a memory corruption vulnerability in a large number of installed versions of both curl and libcurl. That exploitation required a special set of conditions to be true. Instead of the main conversation being about the technical details of the vulnerability, a conversation about the hype which surrounded the vulnerability took center stage. Why? While it was clearly stated in the initial messaging the issue was a “High” severity bug, the extreme language provided a false sense of a critical issue.

Officially, at the time of writing NVD hasn't published a CVSS score indicating an official “High” vs. “Critical” rating. Some researchers have taken the details and predicted a score which has varied from a 7.5 to an 8.8 rating, both of which are high ratings. Therefore, the details surrounding the exploitation requirement of the vulnerability indeed confirmed a “High” level vulnerability and not a critical vulnerability, however these details were originally left to the imagination of the reader.



joernchen @joernchen

Your thoughts on the curl vuln?

	85.1%
	11.3%
Other, comment below	3.5%

141 votes · Final results

3:15 AM · Oct 11, 2023 · 1,886 Views

2 replies · 1 retweet · 1 heart · 1 bookmark · Share

Post your reply Reply

アルミ @schrotthausen · Oct 11

I kinda had hoped for more [redacted] we can't patch this as fast as it needs patching" 😞(ツ)_/

The Impact of Change

If the vulnerability is patched and the disclosure information is accurate, does it matter? The problem with overhype is it often causes a reaction or change in prioritization. Cybersecurity is already overwhelmed with events and starving for resources to address them. This dictates that prioritization of actions is the most important task for any organization. What risks are the highest risk right now and how do I address them? While sometimes the cost of change is minimal, at other times it's a cost that can't be afforded.



Justin Elze ✓
@HackingLZ



The primary reason I'm salty about Curl is all the conversations and hype around it. Companies already have a hard time prioritizing patches and determining exposure for various vulnerabilities. Fire drills like this eat up cycles when they could be focusing on things like KEV(cisa.gov/known-exploite...), their shiny new cloud, or AD.

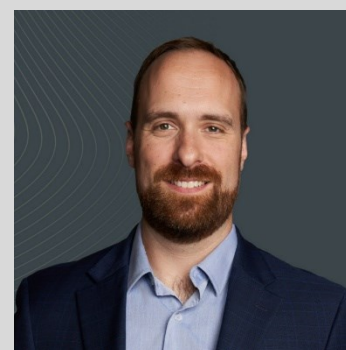
7:40 AM · Oct 11, 2023 · 41.9K Views

It is imperative that security researchers continue to responsibly disclose vulnerabilities to closed and open-source projects. Transparency of these vulnerabilities along with patches (as well done by the curl project) is the only way for defenders to have the necessary information required to defend our ever growing technology stack. It is also our responsibility to keep a factual, data driven, non-emotional response to these events, focus on the details and work together to responsibly use the resources we have at our disposal.

So, the next time “life comes at you pretty fast,” it pays dividends to “stop and look around once in a while.” It helps in making sure your team focuses your resources and efforts on the most critical and urgent issues that pose the greatest threat to your organization by paying attention to the minor details.

About the Author

Douglas McKee is the Executive Director of Threat Research at SonicWall where he and his team focus on identifying, analyzing, and mitigating critical vulnerabilities through daily product content. He is also the lead author and instructor for SANS SEC568: Combating Supply Chain Attacks with Product Security Testing. Doug is a regular speaker at industry conferences such as DEF CON, Blackhat, Hardware.IO and RSA, and in his career has provided software exploitation training to many audiences, including law enforcement. His research is regularly featured in publications with broad readership including Politico, Bleeping Computer, Security Boulevard, Venture Beat, CSO, Politico Morning eHealth, Tech Republic, and Axios. Douglas can be reached at dmckee@sonicwall.com





How to Identify and Respond to End-of-Life and Out-of-Service Operating Systems?

By Chahak Mittal, GRC Manager, Universal Logistics

In the ever-changing world of technology, managing end-of-life (EOL) and out-of-service (OOS) operating systems has become a critical concern for organizations of all sizes. These outdated systems pose a significant security risk and can hinder operational efficiency.

What are EOL and OOS operating systems?

An EOL operating system is one that is no longer supported or maintained by the vendor. This means that the vendor will no longer release security patches or updates for the system, leaving it vulnerable to known and emerging threats.

An OOS operating system is one that is still supported by the vendor but is no longer used by the organization. This can happen for several reasons, such as a merger or acquisition, or a change in business requirements.

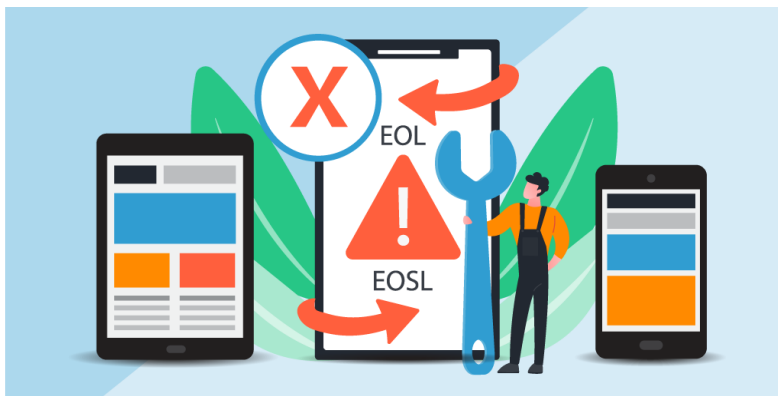
Why are EOL and OOS operating systems so dangerous?

EOL and OOS operating systems are dangerous because they are vulnerable to cyberattacks. Hackers know that these systems are no longer supported and are often able to exploit known vulnerabilities to gain access to networks and systems.

In addition to security risks, EOL and OOS operating systems can also impact operational efficiency. They may not be compatible with newer software and hardware, and they can be slow and unresponsive.

How much EOL and OOS systems are pervasive?

According to [Kaspersky](#) research, nearly 41% of consumers still use unsupported or approaching end of support desktop operating systems (OS) like Windows XP or Windows 7. Similarly, 40% of very small businesses (VSBs) and 48% of small, medium-sized businesses (SMBs) and enterprises still rely on these systems for their security needs. Another 2021 report by Kaspersky [revealed](#), more than 73 percent of healthcare providers use medical equipment that runs on a legacy OS. This paints a concerning picture of the ubiquity of these systems, with many organizations unknowingly operating on outdated platforms. These systems often lack vital security patches and updates, making them prime targets for cyberattacks.



How do you to Identify EOL and OOS operating systems?

There are several steps that organizations can take to manage EOL and OOS operating systems, including:

Harnessing the Power of Vulnerability Scanners

Vulnerability scanners have proven to be effective weapons in the arsenal against EOL and OOS operating systems. Some popular vulnerability scanners include Tenable Nessus and OpenVAS. These scanners operate by scanning networks for EOL and OOS operating systems and cross-referencing detected software versions with a database of known vulnerabilities. If a vulnerability is found, the scanner generates a detailed report that can be used to remediate the vulnerability.

Vulnerability scanners can be used to identify EOL and OOS operating systems on both on-premises and cloud-based networks. They can also be used to scan for EOL and OOS operating systems on mobile devices.

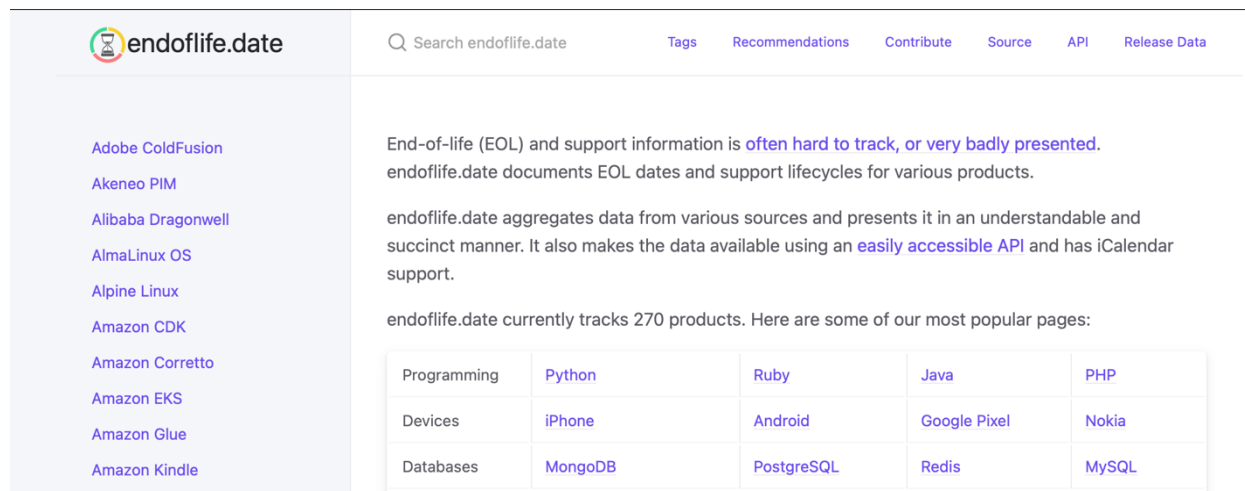
Endpoint Management Tools for Centralized Control

Endpoint management tools are essential allies in the fight against EOL and OOS operating systems. These tools provide organizations with a centralized view of all devices within their ecosystem, including their operating systems and software versions. This information can be used to identify, assess, and remediate EOL and OOS systems, thus preventing security vulnerabilities.

Some popular endpoint management tools include Microsoft Endpoint Manager and VMware Workspace ONE.

The Power of Public Databases

Public databases, such as the well-regarded End of Life Date (EoLD) [database](#), provide readily available resources to identify EOL and OOS operating systems. The EoLD database offers an extensive list of operating systems, complete with their respective end-of-support dates. For organizations seeking a straightforward method to track EOL systems, this database has proven to be an asset.



The screenshot shows the endoflife.date website. The header includes the logo, a search bar, and navigation links for Tags, Recommendations, Contribute, Source, API, and Release Data. The sidebar lists various products like Adobe ColdFusion, Akeneo PIM, Alibaba Dragonwell, AlmaLinux OS, Alpine Linux, Amazon CDK, Amazon Corretto, Amazon EKS, Amazon Glue, and Amazon Kindle. The main content area explains that EoL and support information is often hard to track, and the database documents EOL dates and support lifecycles for various products. It also mentions that the database aggregates data from various sources and provides an easily accessible API. A table lists some of the most popular pages tracked by the database.

Programming	Python	Ruby	Java	PHP
Devices	iPhone	Android	Google Pixel	Nokia
Databases	MongoDB	PostgreSQL	Redis	MySQL

How do you craft the right approach?

The best way to identify EOL and OOS systems depends on your organization's unique needs and resources. If you already have vulnerability scanners or endpoint management tools in place, repurposing them is the most efficient approach. If you do not have access to these tools, using a public database like EoLD is a viable option.

No matter which approaches you choose, it is important to identify and remediate EOL and OOS systems as soon as possible. These systems pose a significant security risk to your organization.

How to remediate?

Once you have identified EOL and OOS systems in your environment, it is important to take prompt action to remediate them. This can be done in several ways, including:

Upgrading the operating system.

This is the most effective way to remediate EOL and OOS systems, as it will provide your organization with the latest security patches and updates. Of course, upgrading your operating system can be a complex and time-consuming process. It is important to carefully plan and test your upgrade before deploying it to production systems.



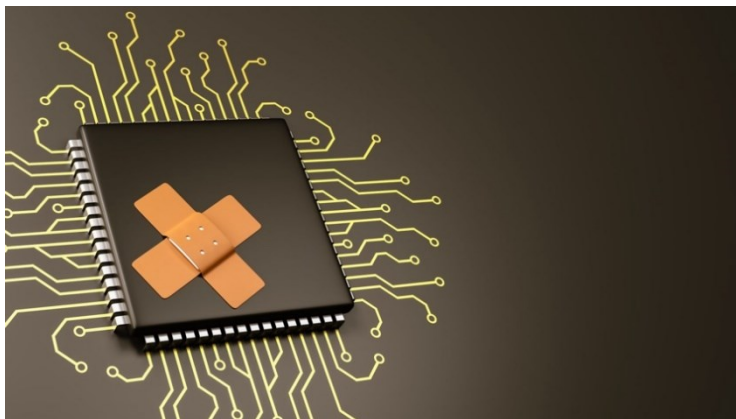
Applying patches.

If upgrading the operating system is not possible, you can try to apply patches to the EOL or OOS system. However, it is important to note that patches may not be available for all EOL and OOS systems.

Applying patches is a process of installing updates to software to fix known vulnerabilities. Patches are typically released by software vendors and can be downloaded and installed manually or automatically. To apply a patch to an EOL or OOS system, you will need to first identify the patches that are available for the system. You can usually find this information on the software vendor's website. Once you have identified the available patches, you will need to download and install them on the system. It is important to follow the instructions carefully when installing patches. Installing patches incorrectly can cause problems with the system or even make it unusable.

Migrating to a supported platform.

If upgrading the operating system or applying patches is not possible, you may need to migrate the EOL or OOS system to a supported platform. This can be a complex and time-consuming process, but it is essential for protecting your organization from security threats. Migrating to a supported platform involves transferring the data and applications from the EOL or OOS system to a new system that is supported by the software vendor. This process can be challenging, as it requires careful planning and testing to ensure that the migration is successful, and that the new system meets the needs of your organization.



The urgency of these actions cannot be overstated. EOL and OOS systems pose a significant security risk to your organization. By taking prompt action to remediate them, you can help to protect your organization from cyberattacks and data breaches.

In addition to the remediation steps listed above, there are several proactive steps that you can take to further reduce the risk posed by EOL and OOS systems, including:

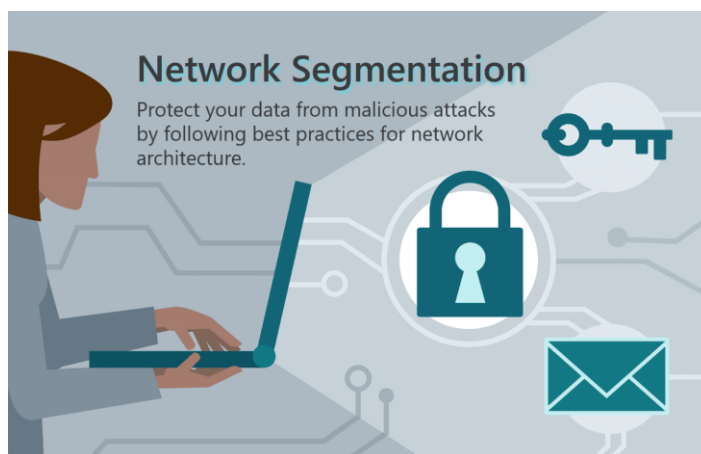
Segmenting your network. Segmenting your network is the process of dividing your network into smaller, isolated subnets. This can help to improve security by preventing EOL and OOS systems from being compromised and used to attack other systems on your network.

When you segment your network, you create a barrier between EOL and OOS systems and other systems on your network. This barrier makes it more difficult for attackers to move laterally from an EOL or OOS system to other systems on your network.

To segment your network, you can use a variety of technologies, such as firewalls, routers, and VLANs. The best way to segment your network will vary depending on the size and complexity of your network.

Implementing security controls.

This includes implementing firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), and other security controls to protect your network from attack. You should choose and implement a combination of security controls that is appropriate for the size and complexity of your network, as well as the types of threats that you face.



Educating your employees.

Educating your employees about the risks of EOL and OOS systems and how to avoid them is an important part of protecting your organization from cyberattacks. Employees are often the first line of defense against cyberattacks, so it is important that they are aware of the risks and know how to protect themselves.

By taking these proactive steps, you can help to reduce the risk posed by EOL and OOS systems and protect your organization from cyberattacks.

About the Author

Chahak Mittal is a Certified Information Systems Security Professional (CISSP) and Cybersecurity Governance, Risk and Compliance Manager at Universal Logistics. Chahak is deeply committed to knowledge sharing and community engagement. She has actively contributed to the cybersecurity ecosystem through her roles as a Judge at Major League Hacking (MLH) Hackathons and a dedicated Cybersecurity Teacher in the Microsoft TEALS Program. Chahak's active involvement in organizations such as the Cybersecurity Collaboration Forum and SecureWorld's Detroit Advisory Board has been instrumental in her pursuit of staying at the forefront of industry trends and challenges. She has also channeled her insights into thought-provoking cybersecurity articles, published on SecureWorld, making a meaningful contribution to the field's intellectual discourse. Chahak's commitment to diversity and inclusion in cybersecurity is unwavering. She has actively participated in organizations like Women in Cybersecurity (WiCyS) and the Michigan Council of Women in Technology (MCWT), where she has championed the cause of gender diversity within the field. Her outreach efforts extend to interviews on prominent media platforms like PBS Channel and the Women in Technology podcast, where she has shared her insights to inspire young girls to consider cybersecurity as a viable and rewarding career path.



Chahak Mittal can be reached online at (goyalchahak6@gmail.com) and at her LinkedIn profile <https://www.linkedin.com/in/chahak-mittal-cissp/>



Classic Information Security Management Errors

How many errors does your organization have?

By Zsolt Baranya, Information Security Auditor, Black Cell Ltd.

During my work as an information security expert, I encounter numerous errors, many of which are committed not only by one organization but by several. I either uncover or face these errors as an information security officer and auditor. In this article, I aim to present what these errors are. I recommend it to professionals working in information security as well as to those managers who wish to avoid common errors related to information security management.

1. In many cases, during the management of privileges, organizations focus on ensuring that every user receives the necessary permissions to carry out their work. However, the system for distributing these privileges is not properly structured, and it is not determined on a job-specific basis who can access which data or systems. There is a lack of a reference privilege registry, and in many cases, the newly

hired or reassigned colleagues only receive permissions based on a predefined image assigned to certain employees. This approach is not appropriate, because it lacks one fundamental requirement of the privilege review system, which is the foundational record (the registry) that would enable the extraction of data on which privileges could be assigned to employees. It is essential to note that the review of privileges is also absent in many organizations, which poses a significant risk as there may be unused privileges that, if exploited, can compromise confidentiality in a significant manner.

2. Compliance is very important when considering an organization's regulatory framework. Authorities, certification bodies, and partners, customers expect compliance with the regulations, standards, and other governing rules. However, many organizations often concentrate on ensuring compliance instead of focusing on the actual vulnerabilities and risks present within the organization. Striving for compliance based on a regulatory checklist can divert attention from the real problems. In such cases, the fundamental principle of establishing protection proportionate to the risks may not be upheld.

3. In many organizations, over time, the IT and IT security have evolved in a way that doesn't support the business, but rather, the business adapts to the processes built by IT and the rules implemented by the Information Security department. In all cases, IT and the Information Security department must support the business. If this is not the case, productivity can be compromised, or in worse scenarios, essential operations may become impossible and in less serious cases, it may become more difficult due to the hindering factors. It is important to note that there are rules that must be adhered to and enforced to ensure security, even if they come with some inconveniences. However, it is necessary to find the balance where the most effective way of doing business and the relationship between information security and IT.

4. Risk management is a very important activity in the life of every organization, whether it is business risks or information security risks. Organizations typically identify and analyze risks, but the development and execution of mitigation plans often fail to materialize. In those organizations where mitigation plans are built for the identified risks, there is often a lack of a control and monitoring system, which typically results in the non-execution of the mitigation plans, leaving the risks untreated.

5. Organizations that establish administrative protective measures according to legal requirements and standards typically end up with lengthy regulations, procedures, and instructions due to content requirements. This often leads to a situation where organizational regulatory documents do not fulfill their role because neither the IT operations staff nor the users will read them. In this situation, organizations commonly make the mistake of not creating abstracts or providing training on the content of the regulations to the stakeholders. As a result, the organizational regulations will only partially or not at all fulfill their role.

6. Many organizations use Security Information and Event Management (SIEM) systems to perform event and incident management activities. However, very few people know how to properly configure the alert settings for these systems. A common mistake is setting up alerts for too many events and incidents, causing the important alerts to get lost among the overwhelming number of notifications. There is a higher likelihood that an event handler will overlook a critical alert due to the high volume of alerts. On the other hand, the opposite scenario is also encountered, where too few events and/or incidents are configured,

resulting in the failure to detect an ongoing incident. Certain alerts should be configured, and the alerting system should be designed in proportion to the risks.

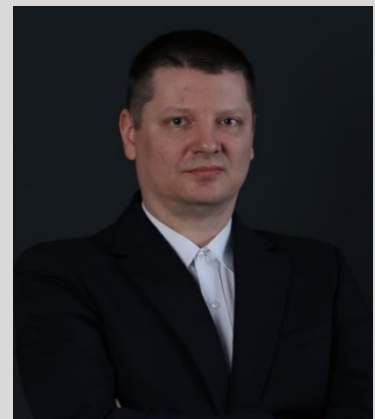
7. The management of shared accounts is inadequate in many organizations. Often, the principle of accountability is not upheld when creating such shared accounts. It is important to note that in some cases, there may be no alternative but to use shared accounts. However, where it is possible to create individually assigned accounts for individuals, this is not done. Another significant mistake that organizations commonly make is the lack of access management for shared accounts. For example, when someone leaves an organization, passwords are not changed, leaving vulnerabilities in the context of shared accounts.

8. The organizational use of social media platforms is inadequate in many organizations. There is no regulation for the execution of operational and management tasks, which often leads to reputational damage. Unfortunate comments can be posted when, for example, someone forgets to switch between social media accounts on their personal account, resulting in the expression of their personal opinion on behalf of the organization. Additionally, if an organization uses social media for communication or business activities and loses access to the account without being able to recover it through proper BCP processes, it can cause significant disadvantages. It is recommended to regulate and manage organizational social media platforms.

How many of the general mistakes I've identified are present in your organization? If I could assist in uncovering even one mistake, then this article has achieved its goal.

About the Author

Zsolt Baranya is a Senior Information Security Auditor of Black Cell Ltd. in Hungary and Germany. Formerly, he has been in information security officer and data protection officer roles at a local governmental organization. He also worked as a senior desk officer at National Directorate General for Disaster Management, Department for Critical Infrastructure Coordination, where he was responsible for the Hungarian critical infrastructures' information security compliance. Zsolt can be reached at zsolt.baranya@blackcell.io and at his company's website <https://blackcell.io/>





Cybersecurity Threats in Global Satellite Internet

By Gizem Yilmaz, Master Expert Data Analyst, Turkcell Technology

Internet via satellite was first used for military purposes in the 1960s and became available for wide-scale commercial use in the 1990s. Current satellite internet systems typically use low-orbit satellites and provide data transmission at low speeds due to limited bandwidth. Starlink, on the other hand, is a project developed by Elon Musk's SpaceX company and aims to provide a faster, more reliable and more comprehensive internet experience with low latency and high bandwidth through a high number of low orbit satellites.

The surge in satellite internet usage has opened up a new frontier for cybersecurity threats, ranging from sophisticated hacking attempts to disruptive denial-of-service attacks.

[1] Last year, a security researcher at KU Leuven, Lennert Wouters, unveiled potential vulnerabilities in Starlink satellites, revealing that hackers could exploit hardware weaknesses in ground-based terminals. At the Blackhat Security Conference, Wouters demonstrated the feasibility of a low-cost mod chip, priced at around \$25, to execute a "fault injection attack," bypassing Starlink's security measures and gaining unauthorized access to its systems. Recently, the Ukrainian Security Service (SBU) issued a warning about a new malware, "Malware 4. STL," which utilizes a person's mobile device to remotely gather data on Starlink systems, representing a distinctive threat compared to previous concerns about direct hacking or system disruption.

Hacking Satellites: Vulnerabilities and Risks:

As satellites play a pivotal role in global communication, they become attractive targets for malicious actors seeking to compromise sensitive data or gain unauthorized access. The vulnerabilities in satellite systems can manifest in various ways, from exploiting software vulnerabilities in ground control systems to physically tampering with the satellite hardware. Potential risks associated with satellite hacking include unauthorized access to sensitive data, manipulation of satellite functions, and disruption of communication services. Attackers may exploit vulnerabilities in satellite systems, ranging from software weaknesses to physical tampering, leading to consequences such as compromised national security, corporate espionage, and the potential for disabling critical infrastructure.

Satellite systems often rely on outdated software or insufficient security protocols, providing avenues for exploitation. Moreover, the lack of regular software updates in orbiting satellites exacerbates the challenge of securing these systems. Let's look at case studies and real-world examples to provide a comprehensive understanding of the historical and current threats facing satellites in orbit. One notable example is the 1998 case of the "Moonlight Maze" cyber espionage campaign, where attackers, suspected to be state-sponsored, infiltrated U.S. Department of Defense computer systems and gained access to classified satellite data. In a more recent incident, the 2020 "Serpent Chaser" attack targeted a European aerospace company, aiming to steal sensitive satellite technology and highlighted the ongoing and evolving threats faced by satellite systems in the contemporary cybersecurity landscape.

Data Interception in Satellite Communication:

Data transmitted via satellite communication channels are susceptible to interception by adversaries, posing a significant threat to privacy and national security. Cybercriminals employ techniques like eavesdropping on satellite communication channels and exploiting weak encryption protocols to intercept sensitive data transmitted via satellite. The consequences of such interceptions can range from corporate espionage, where valuable proprietary information is stolen, to government surveillance compromising national security, and unauthorized access to classified information, posing a significant threat to both public and private entities.

Effective encryption protocols and secure communication channels are imperative to thwart data interception attempts. Advancements in satellite communication security include the implementation of quantum-resistant encryption algorithms and the development of secure key exchange protocols to counter emerging threats. However, challenges persist in the integration of these technologies due to the resource constraints on satellites and the need for standardized security measures, necessitating collaborative efforts among industry stakeholders and regulatory bodies to establish comprehensive security standards and best practices.

Satellite Jamming and Denial of Service Attacks:

Satellite jamming, a form of radio-frequency interference, and denial-of-service (DoS) attacks present tangible threats to the reliability and availability of satellite services. Satellite jamming involves the deliberate interference with satellite signals through the transmission of radio-frequency signals on the same frequency, disrupting communication links. The consequences of such attacks range from temporary service disruptions, affecting telecommunications and navigation systems, to the more severe outcome of complete incapacitation of satellite systems, impacting critical infrastructure and national security.

To mitigate the risks posed by satellite jamming and DoS attacks, robust countermeasures are essential. Recent advancements in anti-jamming technologies involve the integration of adaptive beamforming, frequency agility, and artificial intelligence to enhance the resilience of satellite systems against intentional disruptions. Analyzing case studies, such as the 2019 Iranian GPS jamming incidents, provides valuable insights into the evolving tactics employed by adversaries and helps assess the effectiveness of countermeasures, informing the ongoing development of robust strategies to safeguard satellite communication against intentional disruptions.

In conclusion, the escalating cybersecurity threats to global satellite internet underscore the imperative for proactive measures to fortify the integrity and reliability of satellite communication systems. As the reliance on satellite technology burgeons, a concerted effort in implementing advanced encryption, anti-jamming technologies, and collaborative international initiatives becomes paramount to mitigate risks and ensure the secure and uninterrupted operation of satellite networks. [2] Satellite cybersecurity faces significant challenges, particularly with the proliferation of smallsats by commercial entities like SpaceX's Starlink, introducing vulnerabilities due to minimal development costs and high cybersecurity expenses. The overcrowded low Earth orbit, coupled with the lack of engagement from private corporations in securing satellites, creates a conducive environment for potential disasters orchestrated by malicious actors. The proposed solutions include implementing stronger encryption, such as quantum encryption, advancing laser-based communication, and reinforcing intrusion detection (IDS) and prevention systems (IPS), necessitating an urgent upgrade to the regulatory regime governing satellite cybersecurity to mitigate current threats.

References

- [1] McMillan, T. (2023). "Recent Intel Report Reveals New Starlink Vulnerabilities, Increasing Concerns About the Future of Global Satellite Internet." The Debrief. URL: <https://thedebrief.org/recent-intel-report-reveals-new-starlink-vulnerabilities-increasing-concerns-about-the-future-of-global-satellite-internet/>
- [2] Edward Verco, Satellites Are Cyber Insecure: We Need Regulation to Avoid a Disaster, 2 ANU JOLT 57 (2021).

About the Author

Gizem Yilmaz is the Master Expert Data Analyst at Turkcell Technology which is the leading telecom company in Turkey. Gizem Yilmaz stands out as an experienced versatile data analyst and product owner with a strong background in network, sales, and cyber security, currently contributing expertise to the forefront of financial data analytics in the telecom sector. She focuses on value maximization, works on the discovery of features to add to the product. She is a professional specialized in data analysis and a person who provides significant added value to the product development process. With its data analysis skills and strategic thinking abilities, she supports the decision-making processes of the business and the product development process. Gizem also provides effective communication between teams and collaborates to ensure that projects are completed on time and successfully. With its professional experience and leadership competencies, it makes a valuable contribution to the achievement of the global goals of the enterprise.



See more information about Gizem at <https://www.linkedin.com/in/gizem-yilmaz/>



Does Zero Trust Improve Productivity?

By Zac Amos, Features Editor, ReHack

Zero trust has gained significant attention as an effective approach to secure digital assets. It's a security framework that's also believed to impact employee productivity. Here's what to know about this methodology and how it can strengthen worker output.

What Is Zero Trust?

Zero trust is a cybersecurity approach that challenges the traditional security model, which often relies on perimeter defenses. One survey found that [51% of businesses have adopted](#) a zero-trust network design.

Zero trust advocates a “never trust, always verify” philosophy, where trust is never assumed. All stages of network access require verification.

This approach secures networks by continuously monitoring and authenticating every user and device attempting to connect. Here are the fundamental principles and characteristics of zero trust:

- **Verification:** Trust is never assumed in a zero-trust model. It requires verification for anyone or anything attempting to access resources or systems within the network. This involves a robust authentication and authorization process.
- **Microsegmentation:** The network is divided into small, isolated sections with their own access controls. Lateral movement is limited, making it more challenging for threats to spread.
- **Least privilege access:** Users and devices are granted the minimum access required to do their jobs. This limits the potential damage to an account or device that is compromised.
- **Continuous monitoring:** About [38% of adult internet users](#) in the U.S. are more willing to disclose personal information with digital companies they trust. Zero-trust networks continuously monitor all activity and apply real-time analytics to detect and respond to threats. This ongoing monitoring helps identify and address security issues promptly.
- **User and device authentication:** Every user and device must authenticate themselves before accessing network resources, even inside the corporate network. This ensures that only authorized entities gain access.
- **Adaptive security:** Zero trust adapts to changing conditions, such as user behavior and threat intelligence. It can adjust access privileges based on real-time risk assessments.
- **Continuous updates:** It is not a one-time implementation but an ongoing process. Zero trust requires constant updates and adjustments to address evolving threats.

Enhancing Productivity

There has been a significant push toward zero-trust security [over the last six months](#) due to several high-profile security incidents.

Zero trust can improve productivity in several ways, provided it's implemented thoughtfully and with consideration for an organization's specific needs. Here are some key ways zero trust can enhance productivity:

- **Secure remote work:** Zero trust allows remote and hybrid employees to access corporate resources from anywhere securely. This flexibility eliminates geographical constraints and can boost productivity by enabling remote work without compromising security.
- **Enhance user experience:** Zero trust often incorporates features like single sign-on (SSO) and multifactor authentication (MFA). These tools simplify access to various applications and resources, reducing employee friction. An enhanced user experience can save time and improve productivity.
- **Reduced downtime:** Continuously monitoring and verifying network access enables zero trust to reduce the risk of security incidents. This proactive approach can significantly decrease downtime caused by breaches, ensuring employees remain focused on their tasks.

- **Prevention of unauthorized access:** It strictly controls access to resources, preventing unauthorized access. This means only authorized users and devices can access specific resources. Zero trust can help employees work without the distraction of dealing with security incidents.
- **Improve data protection:** Zero trust strongly emphasizes protecting data. Encryption and access controls ensure sensitive information remains confidential. This can boost employee confidence in handling sensitive data, allowing them to work more efficiently.

Benefits of Zero Trust

Zero trust can improve productivity, but its impact varies depending on how an organization implements and integrates it into its existing workflows. Here are some benefits:

- **Empowered workforce:** Properly training and educating employees about zero-trust principles empowers them to use new security measures effectively. Companies can maintain productivity without disruptions caused by security breaches when workers understand and adhere to security protocols.
- **Streamlined process:** Zero trust encourages organizations to streamline their security processes. Straightforward access policies and automated verification lets employees access the resources they need more efficiently. This reduces the time wasted on navigating complex security measures.
- **Adaptability to changing threats:** Zero trust often evolves to address new cybersecurity threats effectively. This adaptability ensures employees can continue their work without significant disruption caused by emerging threats.
- **Compliance and audit benefits:** It simplifies complying with regulatory requirements and passing security audits. This can save time and resources that might otherwise be spent on these activities, contributing to increased productivity.

The Role of Training

Training when implementing a zero-trust model is pivotal to ensuring employees understand the fundamental shift toward continuous verification and strict access controls.

Cybersecurity awareness programs and hands-on instruction raise employee awareness about evolving threats. It equips them with the skills to use new security measures like multifactor authentication effectively, which [can stop 99.9% of attacks](#) on users' accounts and educate them about phishing prevention and incident response.

Moreover, training encourages a balanced perspective, helping employees recognize that security measures are in place to safeguard the organization and their interests without excessively hindering their work.

Implementing Zero Trust

Cybersecurity will remain a top priority as businesses navigate the digital age. The question of whether zero trust improves productivity is complex and multifaceted. Each organization must carefully assess its unique needs and challenges to determine the best approach.

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](#).





Enhancing The Nation's Cybersecurity Workforce

Supporting Critical Infrastructure Resilience with Skill-Based Labor

By Randall Sandone, Executive Director, Critical Infrastructure Resilience Institute at The Grainger College of Engineering at the University of Illinois Urbana-Champaign

"With almost 700,000 cybersecurity job openings, the United States doesn't have enough cybersecurity experts to protect the nation's critical infrastructure..." That is the lead sentence from an article published in National Defense magazine¹ less than five months ago. It is a stark reminder of the daunting challenges we face at the Critical Infrastructure Resilience Institute (CIRI) as we pursue our mission objectives. CIRI is a Department of Homeland Security (DHS) Science & Technology Directorate Center

¹ <https://www.nationaldefensemagazine.org/articles/2023/6/26/us-desperately-needs-cyber-talent-congress-says>

of Excellence, housed at the Grainger College of Engineering at the University of Illinois Urbana-Champaign focused on enhancing the security and resilience of our nation's critical infrastructure.

Filling that gap with a diverse and qualified pipeline is a major challenge for our nation and the private sector companies and government agencies experiencing the impacts of that shortage. But adding people to the pipeline alone is not the full story. At CIRI we are also addressing the challenge of improving the efficiency and productivity of the existing cybersecurity workforce – today and into the future.

Through DHS sponsorship and funding, CIRI has developed software applications that we believe can (1) improve the operational efficiency; and (2) improve recruitment, retention, and management of a cybersecurity workforce. In pursuing these operational objectives, we leverage national standards developed and published by the National Institute for Standards and Technology (NIST) and the Department of Defense (DoD).

Enhancing Workforce Efficiency

All too frequently, bespoke organizational cyber risk management practices suffer from a variety of deficiencies. They tend to be reactive, poorly documented, and inadequately reinforced by organizational policy. The requirements and objectives being pursued are imprecisely defined and poorly articulated, leading to confusion within the workforce. They often lack mechanisms to define, monitor, and report a detailed plan of action and the mechanisms to track and report progress against that plan.

As a consequence, such practices tend to deliver results that are opaque to key internal and external stakeholders. This results in reduced efficiency and increased costs; makes it difficult for cybersecurity managers to secure and sustain adequate cybersecurity budgets; increases the stress level of the cybersecurity workforce - leading to staff burnout and turnover; and risks creating gaps in cybersecurity coverage for the organization.

We believe that organizations can address these common deficiencies by adopting widely-recognized national cybersecurity standards and best practices. To assist organizations in adopting these standards, CIRI – in partnership with Heartland Science and Technology (a 501(c)(3) technology development company) – has developed the Cyber Secure Dashboard (CSD). The CSD is a cyber risk management application that helps organizations establish clear objectives and develop a detailed plan of action to implement and manage sound, standardized, repeatable and consistent processes and best practices to achieve those objectives; harmonize internal activities with those executed by external partners and/or contractors; and communicate and share information within and amongst the internal and external workforce. This leads to enhanced efficiency of the organization, greater transparency amongst all stakeholders, and reduced stress on the cybersecurity workforce.

The CSD does this by operationalizing multiple cybersecurity standards including the NIST 800-171 standard for handling Controlled Unclassified Information (CUI), the NIST Cyber Security Framework (CSF), and the DoD Cybersecurity Maturity Model Certification (CMMC) standard. All of these standards are supported in one application allowing organizations that need to meet multiple standards to easily

manage, track, and report their status and progress in addressing the requirements of those different standards.

Using the CSD, organizations can improve the efficiency of their cybersecurity workforce by providing clarity of the requirements for the target standard. The CSD will guide the organization through an assessment against those requirements using NIST assessment criteria and establish and maintain a Plan of Action & Milestones (POA&M) which will allow harmonization of internal and external tasks. In addition, by maintaining a centralized repository of compliance artifacts tagged to specific cybersecurity controls that ease third-party compliance validation, the dashboard will improve collaboration, communication, and information sharing while also producing and delivering detailed automated reports of status and progress to both internal and external stakeholders. The CSD can be used to manage a single organization, multiple units within an organization, or an entire supply chain.

Toward Skill-Based Cybersecurity Workforce Management

Historically, cybersecurity job requirements and subsequent recruitment and selection of cybersecurity personnel has focused on the education/academic credentials of the candidates - with a four-year degree in computer science (or similar) being an almost universal default requirement. In limiting the applicant pool to a population that has historically and continues to experience a lack of diversity through underrepresentation, these requirements have also perpetuated a lack of diversity of cybersecurity staff.

This education-based approach to hiring does not take advantage of the many cybersecurity re-skilling and up-skilling programs that have greatly proliferated over the years to increase the applicant pool. With this model, the candidate that earned an Associate's Degree in history who then spent five years in the Air Force being trained and employed in a cybersecurity role might not qualify for an interview based on his/her lack of a four-year degree.

Ongoing management of a cybersecurity workforce is currently hampered by an inability to clearly identify and match skill sets to tasks and a failure to identify skills and training gaps needing remediation.

With the right tools, organizations can adopt a skills-based cybersecurity recruitment and management model where the organization has a clear understanding of the specific skills needed to accomplish its cyber risk management goals and objectives. Furthermore, these tools provide organizations with the ability to identify and recruit candidates possessing those skills and to remediate skills gaps of its workforce going forward. Such a model will allow the organization to reach a larger pool of applicants, enhance the diversity of its cybersecurity staff, and better manage the professional development of its cybersecurity workforce.

With the CyberTalent Bridge (CTB), CIRI has developed such a tool in partnership with 2wav, Inc. – a software development company with unique expertise in ontology-based information systems. CTB is a software application that operationalizes the NIST National Initiative for Cybersecurity Education (NICE) cybersecurity workforce management standard. The software is first in its class to help organizations translate worker experience and education into a useful expression of the NICE Framework and bridge

those capabilities to standards such as the NIST Cyber Security Framework (NIST CSF) or the Department of Defense Cybersecurity Maturity Model Certification (CMMC).

Organizations can use the CTB to easily collect and inventory the knowledge, skills & abilities (KSAs), education, and credentials of its internal cybersecurity staff as well as contracted staff. Individual staff members can access the CTB Passport to assert their KSAs, education, and other credentials which are then inserted into a centralized inventory. An individual's CyberTalent Passport can be exported and shared as a self-contained visual and machine-readable document that is accessible by anyone with a web browser and interoperable with external systems through CTB's openly shared data formats. CyberTalent Passports thus help workers and learners to share and communicate capabilities across the cybersecurity enterprise.

The CTB provides the capability to independently validate the various KSA, education, and credential assertions of the individual to assign a “confidence” score that refines the assertion based on validated prior work experience or by a review of education/training credentials. By accessing this centralized skills inventory organizations can efficiently identify the most qualified staff member to assign to specific cybersecurity tasks and to identify knowledge, skills, and training gaps for remediation through training, education, or other professional development activities.

In so doing, the CTB can help organizations migrate from an “education/credentials-based” recruiting model to a “skills-based” model. Such a migration can help organizations improve recruiting by expanding the applicant pool and by enhancing the diversity of its cybersecurity workforce.

Process to the Power of People

The integration of these two products into a unified framework is underway at CIRI which will allow organizations to execute standardized, repeatable cyber risk management processes and best practices more effectively and efficiently and to recruit and manage the workforce tasked with that execution.

Using tools provided in the CSD, an organization completes a cybersecurity assessment of their organization and network(s) against a target standard and - based on that assessment - develops a Plan of Action & Milestones (POA&M) to achieve its target cybersecurity standard (such as NIST 800-171, the NIST CSF, or the DoD CMMC). The CTB accesses this POA&M to analyze the KSAs required to execute cybersecurity tasks (i.e., cybersecurity controls to be implemented). The CTB conducts an automated analysis of the task requirements to identify the KSAs and then delivers a rank-ordered list of staff members qualified to execute the task – from most qualified to least – based on a mapping of the task requirements to the staff member skills inventory. Managers can use this list to assign the most qualified staff member to the task while also identifying training and skills gaps needing remediation.

Meaningful Impact

We believe that delivery of this integrated solution fit for small, medium, and large organizations in both the private and public sectors can facilitate broad-scale adoption and employment of national cybersecurity standards and best practices and can enhance the diversity and efficiency of our nation's cybersecurity workforce. This in turn can enhance the security and resilience of our nation's critical infrastructure – the goal and mission of the Critical Infrastructure Resilience Institute.

About the Author

Randall Sandone is the Executive Director of the Critical Infrastructure Resilience Institute (CIRI) at The Grainger College of Engineering at the University of Illinois Urbana-Champaign. In this role, Randall has been instrumental in helping to guide a research, technology transition, and education and workforce development portfolio that is delivering impactful cybersecurity solutions to both the public and private sector. He has over thirty years of experience in cyber security leadership and has managed the development, testing, and certification of a variety of cyber security products used by customers ranging from Federal agencies to private sector companies large and small around the world. Randall is also a principal in Rangerfish, LLC, the licensing agent for the Cyber Secure Dashboard. Additional information on Randall and CIRI's work can be found on their website <https://ciri.illinois.edu/>.





What are the Essential Skills for Cyber Security Professionals in 2024?

Where should you invest time and resources to drive success when it comes to the must-have skills and tools for senior leaders in the industry.

By Sarah Gilchriest, Chief People Officer of Workforce Learning, the group encompassing QA, Circus Street and Cloud Academy

Cyber security has become one of the most important aspects of any business or government organisation. The world is becoming increasingly digital, meaning that more and more sensitive information is kept on devices or in the cloud. The UK Government's [Cyber Security Breaches Survey 2023](#) found that there were "approximately 2.39 million instances of cyber crime and approximately 49,000 instances of fraud as a result of cyber crime in the last 12 months" across all UK businesses, meaning an ever-increasing need for cyber security professionals. Sometimes referred to as information security technicians, security analyst or security engineers, cyber security professionals are part

construction manager, part doorman, part detective and also part undercover police investigation officer - in other words the heroes of the stability of the internet. The skills they need to cover the scope of the role are wide-ranging and continue to evolve as technology moves on and it can be hard to know where best to invest time and resources to progress in this career, but this article will explore the key areas that a cyber security professional should be thinking about today.

Technical expertise

Cyber security professionals enable security in IT infrastructure, data, edge devices, and networks. Many are programmers, systems or network administrators, or have backgrounds in math and statistics. Such skills are required for the role of an IT security professional, but equally as essential are critical thinking, curiosity, and a passion for learning and research. Furthermore, hackers are creative by nature; therefore, cybersecurity pros need to be, as well, to outsmart them.

It perhaps goes without saying, but technical proficiency is key. It is essential to understand how networks function, and have the ability to secure them. This should include knowledge of firewalls, intrusion detection and prevention systems, VPNs and more. Coding and scripting is also crucial, with proficiency in languages such as Python, Java, or C++ invaluable for cybersecurity professionals.

The tools to turn to

There are a range of tools that top the charts for cyber security, and professionals in the industry should be seeking to upskill themselves to use if they do not already do so. These include the prevalent penetration framework Metasploit, which can be used to accomplish objectives such as managing security evaluations, discovering vulnerabilities, and formulating defence methodologies. Nmap, the open-source tool for scanning networks and systems for vulnerabilities, and performing mapping of network attack surfaces is another, along with Wireshark, which can scrutinise the details of network traffic, and Aircrack-ng, which analyses the weaknesses in a WiFi network. There are a number of other such examples, and will always be new ones emerging, and so to stay at the top of their game, continuous learning is key. A cyber professional needs to be live to identifying the most effective toolkit and making sure they have the skills to benefit from them.

Fixing vulnerabilities

People in this sector do not just need to be able to use and understand security tools and technology, but also oversee their maintenance. Coding skills can enable professionals to analyse, identify, and fix vulnerabilities in software and systems, essential when carrying out effective audits of security practices. It will also be needed for evaluation of new technology being integrated into the business, to implement controls to diminish any risk in its operation.

Data analysis

There's no escaping the fact that data in general is the lifeblood of modern business. As a result, every cyber security professional will benefit from learning data analysis skills. This does not mean becoming a data scientist, but upskilling in areas such as statistics that can have a profound impact on your job. At the very least you need to be able to understand what the data is telling you. Otherwise, you're simply following what other people - usually in the data team - tell you. Without the ability to understand data, you cannot spot errors, see opportunities for further analysis or make the most of the insights data analysis generates.

Communication is key

It is important to focus on more than the technical skills involved in this industry though. To really succeed in this career, there are certain so-called soft skills that need to be focused on. Communication skills are fundamental, to allow the translation of complex technical information for the average lay person in a clear and effective way. Cyber security professionals will have to work closely with different teams to reduce risks, educating non-technical employees on how to identify suspicious activity and implement security measures. The ability to think critically and strategically is also a key attribute for anyone working in this industry. High-level security protocols often require cyber professionals to perform strategic evaluations of the workflows, requirements and resources.

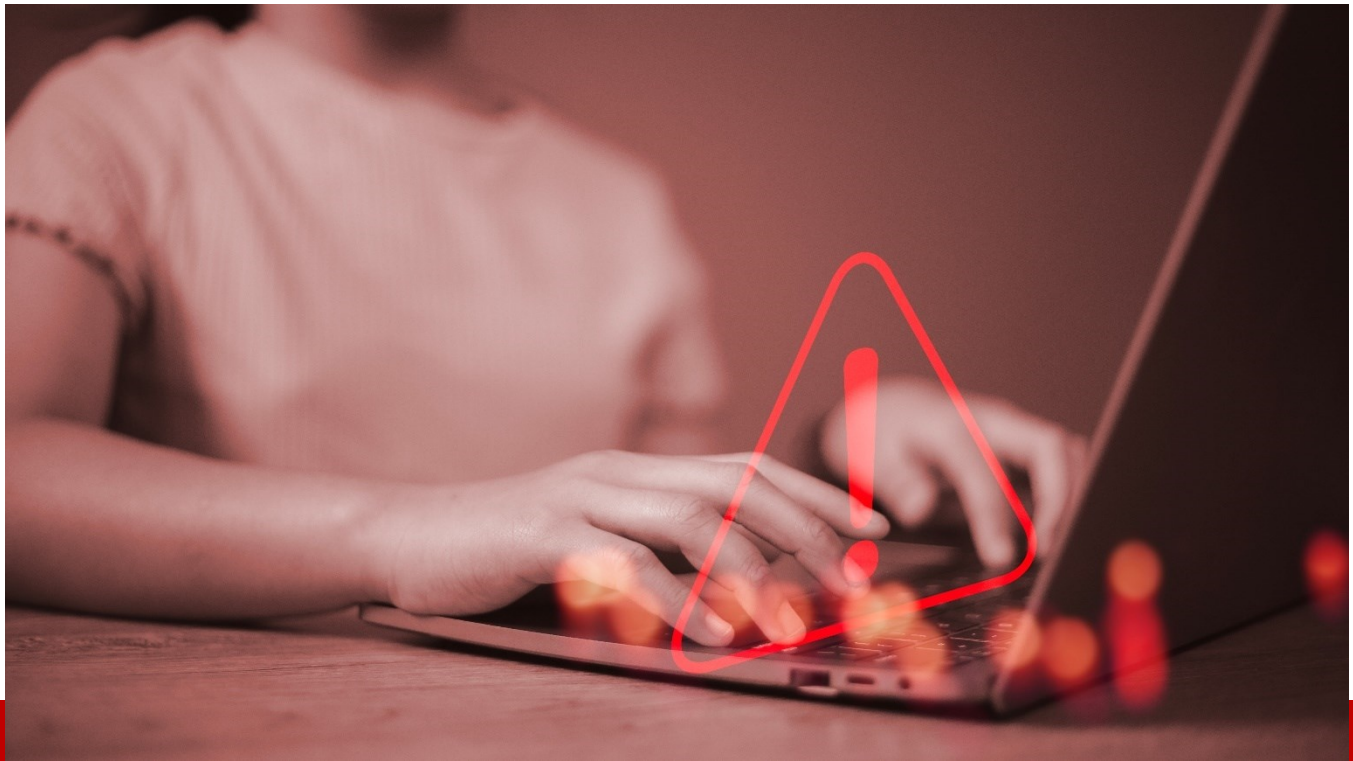
In conclusion, a successful career in cybersecurity requires a combination of technical expertise, analytical skills, and a commitment to continuous learning. As the digital landscape continues to evolve, cybersecurity professionals play a critical role in safeguarding our increasingly interconnected world. By developing and honing these essential skills, aspiring cybersecurity professionals can contribute to the ongoing battle against cyber threats and help build a more secure digital future.

About the Author

Sarah Gilchriest is the Chief People Officer of Workforce Learning, the group encompassing [QA](#), [Circus Street](#) and [Cloud Academy](#).

Sarah can be reached online at <https://www.linkedin.com/in/sarahbromley/> and at our company website <https://www.qa.com/>





Attackers Keep Evolving: Lessons from Expel's Q2 2023 Quarterly Threat Report

Cyberdefenders plug the holes, so attackers innovate to try to stay ahead.

By Aaron Walton, Threat Intel Analyst, Expel

Most cyberattackers don't try to reinvent the wheel: as long as something works, they'll keep doing it. Unfortunately for them, cybersecurity teams are very good at diagnosing issues, fixing them, and developing processes to preempt future attacks (or, at the least, to make them more hassle than they're worth)—especially when the black hats give them lots of practice.

The good news, from a hacker perspective, is that some of their more industrious colleagues never stop looking for new tactics, techniques, and procedures (TTPs), nor do they stop looking for ways of monetizing their efforts. These innovators prep and roll out new attacks and all of a sudden, our security operations centers (SOCs) begin seeing the next set of trends.

Each quarter, Expel examines the threats observed within our SOC to identify which attack trends are on the rise—and which tactics organizations need to be prepared to face. This year's [Q2 2023 Quarterly Threat Report \(QTR\)](#) found that challenges like adversary-in-the-middle (AiTM) attacks and cybercrime-as-a-service are among the threats that deserve the most attention from today's businesses.

Exit legacy protocols, enter AiTM.

Microsoft kneecapped a standard compromise tactic when it [disabled legacy protocols in October 2022](#). But phishing is just too lucrative, so attackers needed a new way in. ([More than a half-billion phishing attacks were reported in 2022](#)—over double the number from 2021—so it would be naive to expect decreased interest anytime soon.)

The emerging hacker response: session cookie theft via adversary-in-the-middle (AiTM) attacks. Identity-related incidents employing frameworks such as Evilginx2 to steal login credentials and session cookies for initial access and subsequent bypassing of multi-factor authentication (MFA) increased threefold—growing to 15% of all phishing attacks in Q2.

This fresh approach to phishing (a long-time scourge of SOCs everywhere) is more sophisticated, but the good news is that there are effective defenses. Security teams should beware newly registered MFA devices, as well as those registered using a proxy, virtual private network (VPN) or originating from a suspicious location. (Automating these detections is a pretty straightforward process and can have a significant impact on the effectiveness of phishing defenses.)

Stronger authentication methods, such as Fast ID Online 2 (FIDO2) and certificate-based authentication, are also hugely helpful. It's true that FIDO isn't feasible for all organizations, and in these cases, we recommend deployment of phish-resistant MFA, instead. While not as comprehensive as FIDO, phish-resistant MFA still adds a valuable layer of defense that attackers will need to work around. SOCs may also opt for push notifications instead of performing MFA by email, SMS, voice, or time-based one-time passwords (TOTPs). Notification-based MFA has proven to be the most secure method of MFA and is quickly becoming preferred.

Another thing our SOC saw more of in Q2: more cybercrime-as-a-service

Eighty percent of organizations use [one or more software-as-a-service \(SaaS\) offerings](#), and for good reason. They're accessible, cost effective, scalable, and incorporate data reporting and intelligence tools. Criminals have been paying attention, and the result is an increased popularity of [cybercrime-as-a-service \(CaaS\) offerings](#).

If you haven't heard about this yet, think of CaaS as Amazon for cybercriminals (access-as-a-service, ransomware-as-a-service, bulletproof hosting, phishing-as-a-service, and so on). Commodity malware is maddeningly effective, and it dramatically increases the pool of potential attackers: with automated and ready-to-deploy toolkits available at bargain prices, even small-time, inexperienced threat actors can execute large-scale attacks.

In fact, some criminal organizations even offer subscription options (and professional services like training and—get this—some ransomware-as-a-service providers will even [negotiate with victims](#) on their customers' behalf). Scary, right?

The Q2 QTR highlights a number of the most common social engineering toolkits used by multiple actors and remote access tools. The more organizations know about the tactics attackers are using, the better chance they have of successfully defending against them.

And there's more.

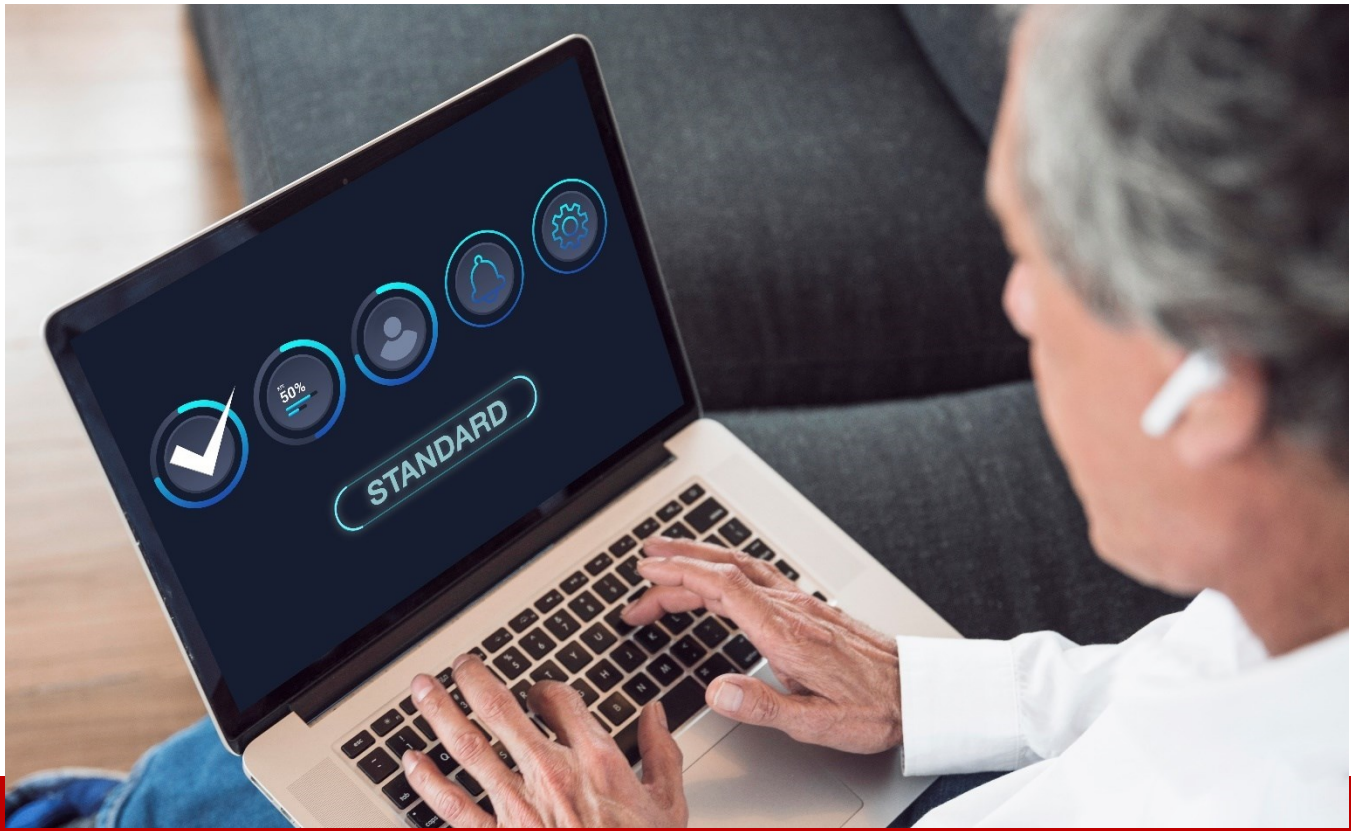
These aren't the only stories told by the new Quarterly Threat Report. Those interested in learning more about the tactics attackers are leveraging this year should check out the report for more insights and recommendations. Hopefully, these findings are useful for your organization, too. In the meantime, here's hoping your SOC is peaceful and boring for the rest of the year.

About the Author

Aaron Walton is a Threat Intel Analyst at Expel. He monitors threat actor trends and behaviors to support Expel's operations. He recommends following @ExpelSecurity on X for articles published by him or his team.

More Information can be found at <http://www.expel.com/>





Implementing ZTA: Benefits and Best Practices

By Eric Sugar, President, ProServeIT

In an era defined by the relentless advance of digitalization and the ever-expanding interconnectivity of industrial systems, the realm of cybersecurity has been thrust into the forefront of our collective consciousness. The conventional paradigms of network security — once seen as impregnable — have demonstrated their insufficiency in the face of an ever-evolving landscape of cyber threats. It is within this cauldron of transformation and challenge that a groundbreaking concept has emerged: [zero trust architecture](#) (ZTA).

ZTA heralds a profound shift in the way we protect our critical infrastructure and industrial systems. It operates under the premise of zero trust — even within the confines of the internal network — thereby forging a new era in cybersecurity. Understanding how ZTA will influence established principles and practices is essential, as it shapes the irreversible course of industrial cybersecurity.

Decoding zero trust: A paradigm shift in security

For decades, the bedrock of cybersecurity has been encapsulated by the axiom "trust but verify." This conventional model presupposes trust once a user and their device breach the protective moat of the network perimeter. The belief is that a well-fortified perimeter can, in and of itself, shield an organization's critical assets and sensitive data. However, the ever-evolving threat landscape has cast a shadow of doubt over this paradigm, laying bare its inherent vulnerabilities.

In stark contrast, ZTA ushers in a paradigm shift under the banner of "never trust, always verify." It challenges the very bedrock of trust within the realm of cybersecurity. ZTA propounds the audacious notion that trust is a scarce and fragile commodity — one that should not be granted solely based on position or credentials. Instead, it insists that trust must be continually earned through the verification of identity, security posture, and behavior.

The fundamental principles of zero trust can be distilled into several key tenets:

- **No implicit trust:** In ZTA, trust is never assumed based on the location or network access of a user or device. Whether a user or device resides inside or outside the network perimeter, the default posture is one of skepticism. This shift in mindset represents a profound departure from traditional security paradigms.
- **Continuous verification:** Trust, in the zero trust model, is a dynamic state. Users and devices must continually substantiate their legitimacy and security status, rather than relying on a one-time authentication process. This dynamic approach ensures that trust remains an ongoing commitment, not a one-off concession.
- **Least privilege access:** Access is granted based on the principle of least privilege, ensuring that users and devices possess only the minimal access necessary to fulfill their designated functions. By doing so, the attack surface is substantially reduced, diminishing potential points of compromise.
- **Micro-segmentation:** ZTA calls for the division of networks into smaller, isolated segments. This strategic move curtails the ability of attackers to laterally move within the network, serving as a formidable deterrent against the repercussions of security breaches.
- **Identity-centric security:** Identity and access management (IAM) assume paramount significance in the realm of zero trust. Robust IAM systems guarantee only authorized individuals gain access to specific resources, bolstering security at its very core.
- **[Multi-factor authentication \(MFA\)](#):** MFA is an integral component of the zero trust framework, adding an additional layer of security by requiring multiple forms of authentication. This multi-pronged approach heightens the level of difficulty for unauthorized users seeking access.
- **Continuous monitoring:** Real-time surveillance of user and device behavior plays an indispensable role within the confines of ZTA. Swift identification of any anomalies or deviations from established baselines is crucial, enabling a rapid response to potential security threats.

By transitioning from a trust-based security model to one centered on continuous verification, ZTA significantly reduces the attack surface, rendering it more arduous for malicious actors to infiltrate networks and compromise critical assets. Furthermore, this approach aligns harmoniously with compliance requirements and regulations, providing organizations with a proactive strategy for shielding their digital assets.

Embracing ZTA

Implementing ZTA successfully requires meticulous planning and precise execution. To embark on this journey, organizations must undergo several critical phases, each designed to bolster their cybersecurity defenses and enhance their overall security posture.

- **Data and asset classification:** It begins with a thorough classification of data and assets based on their criticality and sensitivity. This step allows organizations to establish tailored protections for different access tiers. By distinguishing between mission-critical and less-sensitive assets, organizations can ensure that their defenses are aligned with the true value of each resource.
- **Network segmentation:** Within the zero trust paradigm, network segmentation is a pivotal strategy. This approach entails the division of the network environment into zones with well-defined boundaries. These boundaries serve as an effective deterrent against lateral movement by malicious actors, as they hinder unfettered traversal within the network.
- **Robust user authentication:** User authentication takes on an entirely new significance within the realm of zero trust. Employing single sign-on MFA systems becomes imperative. These mechanisms enhance identity assurance in accordance with zero trust principles, ensuring that only authorized individuals gain access to the network.
- **Access orchestration:** Automated provisioning and deprovisioning play a pivotal role in minimizing the attack surface. By orchestrating access through automated means, organizations can prevent the accumulation of unnecessary access rights. This not only enhances security, but also streamlines user access management.
- **Continuous monitoring:** Vigilant and comprehensive monitoring is a linchpin of zero trust architecture. Real-time surveillance of all access requests and user activities is essential. Any deviations or anomalies from established baselines must be swiftly identified. Continuous monitoring facilitates proactive responses to potential security threats.
- **Regular maintenance:** For zero trust to remain effective, standard procedures for regular patching, configuration updates, and access revocation are paramount. This ongoing maintenance guarantees the network environment remains fortified against emerging threats and vulnerabilities.

By adhering to these best practices in architecture and implementation, organizations can maximize the risk reduction and visibility benefits of ZTA within modern industrial environments. The focus is not only on securing access, but on doing so through identity/context-based policies, network segmentation, enhanced authentication mechanisms, and vigilant monitoring.

Pioneering the future of security: Continuous verification and beyond

ZTA marks a pivotal evolution in the realm of cybersecurity, yet the horizon holds even more innovations that promise to fortify protections within industrial environments. One such advancement is continuous verification — a practice that reimagines security through ongoing monitoring and analysis.

Continuous verification harnesses the power of technologies such as user behavior analytics and endpoint detection and response. By continuously scrutinizing patterns and anomalies, it enables real-time threat identification based on changes in user or system behaviors. For instance, unusual usage of credentials from an atypical location or device can trigger an alert. This proactive approach supersedes periodic compliance checks and audits, adding a dynamic layer of security to the network.

Peering further into the future, the advent of technologies like AI, machine learning, and automation promises to transition industrial cybersecurity from [passive defense to active prevention](#). These technologies, when employed, could autonomously predict, detect, and block attacks in real-time. Human security teams would shift their focus towards strategy, governance, and complex response, in turn enhancing overall security and incident response capabilities.

The future of industrial security is destined to embrace a holistic risk-based approach that spans the realms of IT, OT, IoT, and physical systems. As environments become more interconnected and complex, siloed security measures will no longer suffice. The convergence of identities, devices, networks, clouds, and applications will require unified cyber-physical protection, offering a comprehensive and coordinated defense against multifaceted threats.

While challenges remain on this visionary path, innovations like zero trust, continuous verification, and AI-driven automation portend an era of rapid threat detection and automated prevention. By preparing today, industrial organizations can position themselves to embrace the future of cybersecurity and resilience. This forward-looking perspective ensures that they remain at the vanguard of security, ready to adapt to the ever-shifting landscape of cyber threats.

About the Author

[Eric Sugar](#) is the President of [ProServeIT](#). With over 20 years of experience working in the information technology and services industry, he cares deeply about helping businesses become digital and maintaining digital data security.





Institutionalizing Awareness to Stop Cyberattacks

By Aimei Wei, Founder and CTO, Stellar Cyber

Large and mid-sized organizations are always hoping for a ‘silver bullet’ technology or tool that will stop cyberattacks, but after years in the cybersecurity industry, I’ve got bad news: there isn’t one. The sad fact is that employee behavior is usually responsible. Numerous studies have shown that 60-80% of hacks start with user errors, so companies have to take action to change that behavior. It’s about processes, not technology.

The most promising way for hackers to penetrate a network is phishing – they disguise their bogus emails or texts as warnings or pleas from legitimate financial institutions, social media platforms, or e-tailers. These messages usually ask the recipient to click a link to reset a password or enter a security code to cash in on an amazing offer, and when the link is clicked, the hacker gets carte blanche to invade the user’s system. From there, the hacker travels over the company network to the real target – the company’s financial data, intellectual property, or customer account information, or control over the company network.

Phishing attacks have become increasingly sophisticated — making them more dangerous — and they're also becoming much more common. Security tools provider SlashNext issues an annual [State of Phishing report](#). At the end of 2021, the company detected 50,000 malicious URLs daily, a 68% increase from the start of the year. Less than 12 months later, the company detected 80,000 malicious URLs daily, or 255 million attacks – a 61% increase.

These attacks are more than just nuisances; they impact corporate value. In 2021, Continental Pipeline paid a \$5 million ransom to hackers who had locked up its network, and other significant breaches have cost tens of millions in ransom payments. Moreover, this past July, the Securities and Exchange Commission adopted a final rule requiring public companies to disclose significant breaches within four days of their discovery, so successful attacks can definitely impact corporate reputations. In many cases, public disclosures of breaches have caused significant drops in corporate share prices – look at MGM Resorts' [stock price](#) since an attack shut down casino operations in early September of this year.

Lamebrained password techniques are also a problem. Despite numerous articles urging users to [create complex passwords](#) that they don't reuse from one account to the next, rely on the random password generators offered on most account creation screens, or use [password manager applications](#), many users regularly violate common sense by using passwords that are easy to guess, storing written passwords in plain sight, or otherwise making life easy for hackers.

Let's face it: hackers are going to hack, and they're becoming more numerous and sophisticated all the time. What's a company to do? Educate, educate, educate!

By the way, there's nothing new about this advice. The industry has been singing this song for many years, but corporations are clearly not taking it seriously enough. So, in the spirit of public service, I reiterate: train employees to recognize phishing attacks and use strong password etiquette, and hold monthly meetings to refresh their memories. Here's a quick primer.

Basic Education

At a minimum, users should:

- Be careful when they open emails or click on links from people they don't know or don't trust
- Not give away private information in emails
- Think about what they share on social media and change their settings so only certain people can see their information
- Keep copies of important information in a safe place in case their computer or device is damaged
- Not use public Wi-Fi for things like online banking, and use a special tool called a VPN to keep internet activity private
- Use strong and passwords that are different for each account.
- Keep your computer programs and apps up to date, so they have the latest protection against hackers.

- Learn techniques that hackers use to trick people into giving them information, and be suspicious of things that seem strange or unexpected.
- Use two ways to sign into their accounts (multifactor identification) for extra security.

Keep the Threat Green

Don't think that cybersecurity education for users is a one-and-done exercise: continually reinforce the above techniques with short monthly meetings. To make the meetings more interesting for employees, encourage them to show examples of the latest bogus emails or texts they have received. Maybe even offer a monthly prize for the sneakiest example of phishing.

So, yes, companies can and do spend millions on the latest cybersecurity tools, but the hacks just keep coming. By becoming more proactive in educating users about their role in preventing cyberattacks, organizations can cut their exposure in half. And remember, you're not just protecting the network – you're protecting the company's valuation and bottom line.

About the Author

Aimei Wei has over 20+ years of experience building successful products and leading teams in data networking and telecommunications. She has extensive working experience for both early-stage startups including Nuera, SS8 Networks and Kineto Wireless as well as well-established companies like Nortel, Ciena and Cisco. Prior to founding Stellar Cyber, she was actively developing Software Defined Networks solutions at Cisco. Aimei enjoys building a product from its initial design to its final launch. Aimei has an M.S. in Computer Science from the Queen's University in Kingston, Canada and an Undergraduate degree in Computer Science from the Tsinghua University of China. Aimei can be reached online at awei@stellarcyber.com or at our company website <https://stellarcyber.ai>.





Key Differences in Securing OT & IT Environments

Critical cybersecurity components every security leader must know amid the convergence of IT & OT

By Joe O'Donnell, EVP of Corporate Development, Cyolo

The increasing cyberattacks against critical sectors, in addition to the growing convergence of operational technology (OT) and information technology (IT), spotlights the need for comprehensive ownership around OT security. Today, most organizations are looking to cybersecurity leaders, including Chief Information Security Officers (CISOs), to solve the problem.

Many leaders in the industry have shown great strength in securing IT environments and have successfully overcome highly disruptive events. However, IT security strategies and tools often do not translate to the OT environment. A comprehensive effort must be made to fully understand the OT landscape's distinctive challenges and unique topography. To that end, let's explore the key considerations for securing OT environments.

Systems Unavailable? Not an Option

In an IT environment, experiencing downtime for upgrades and patches, although inconvenient, is typically manageable. This is especially true in a Software-as-a-Service (SaaS) setting where new updates are continuously rolled out.

However, in the realm of OT environments, halting operations to implement a new operating system or apply a critical patch simply isn't an option. OT systems must maintain continuous operation for reasons of both safety and profitability. Any process that requires downtime is essentially a non-starter. For this reason, it's not unusual for CISOs to find that their infrastructure consists of decades-old systems that still serve as a critical piece of their operations.

The challenge for CISOs is identifying security controls that will seamlessly adapt to their current OT processes without interrupting them. The proper solutions will protect current infrastructure and critical processes without changing them or adding unnecessary complexity.

What Does Remote Access Mean for OT?

Typically, OT systems have been secured through isolation. As organizations increasingly connect OT and IT environments to allow easier access for third parties, or to capitalize on digitization, they must ensure that all access – regardless of who, where and how – is monitored, controlled and recorded.

Essentially, this means that any user trying to access an OT environment is considered an outsider until proven otherwise. Whether it is an employee, vendor or OT operator attempting to gain access to your data, any connection coming from the outside must not be trusted. It is no longer acceptable to only set up controls for what IT would consider to be remote.

Understanding the concept of 'never trust, always verify,' organizations need to continuously identify and authenticate every device, user and identity before providing them with access to network apps –securing all types of access scenarios and not just the standard and known ones.

Safety and Tools in OT & IT Environments

Though OT and IT security elements tend to operate differently, safety is always the common denominator.

In the OT world, safety refers to the reliability and responsiveness of cyber-physical systems. For instance, if an industrial boiler or blast furnace malfunctions, it could pose a threat to workers. On an enterprise level, system availability is crucial for maintaining precise and uninterrupted operations, ultimately driving profitability and productivity.

In IT, safety is defined as data protection. On an individual level, a compromise of data exposes them to substantial risks that can jeopardize their identity. On an organizational scale, protecting data helps avoid fines, data breaches and damage to reputation.

Given these distinctions, the tools tailored for IT seldom align with OT needs. One of the primary challenges comes from the disruptive nature of certain IT tools in OT environments. For instance, basic functions like vulnerability scanning, while essential in IT, can inadvertently interrupt critical OT processes and even render systems completely offline. This is exacerbated by the fact that most OT devices lack the necessary computational resources (CPU/RAM) to support endpoint security measures such as anti-virus software or other agents.

Another significant disparity lies in how data traffic is managed. IT tools are designed to route traffic through the cloud, which can be a serious detriment in OT environments. Unlike IT setups, OT systems often consist of numerous unconnected components that require a localized approach to data handling. Cloud-based routing compromises availability and simply cannot accommodate the unique architecture of OT environments.

IT tools and OT devices also differ in their lifecycles. IT solutions typically have much shorter lifespans compared to the robust, long-term endurance of OT equipment. The perpetual operation of OT environments leaves little room for tools that necessitate frequent patching, updates or downtime. The always-up nature of OT systems demands tools that can seamlessly integrate without causing operational disruptions.

Attempting to force-fit IT-designed tools into OT environments not only introduces unnecessary complexity but also fails to address the fundamental security needs of these distinct operational landscapes. Recognizing that OT systems require specialized security solutions tailored to their unique characteristics is paramount. By understanding these differences and embracing security tools designed specifically for OT, CISOs can enhance the security posture of their organizations, ensuring both safety and efficiency in today's interconnected world.

Converging OT & IT in a Digitally Advanced Era

It is critical for security leaders to fully comprehend the differences between OT and IT security. The many complexities across these environments could have a major impact on the business.

Learning and addressing the unique requirements of both systems will allow for a more effective security approach. CISO's taking on this responsibility will benefit greatly by expanding "outside" of the systemic view and build relationships with plant managers and asset owners. Only then can the business successfully converge OT and IT environments. This approach will ensure that OT and IT practitioners help the business remain safe and competitive within ever evolving and advancing digital environments.

About the Author

Joe O'Donnell is a seasoned cyber security professional with over 30 years of experience in senior management roles. Throughout his career, he has made significant contributions to renowned companies such as Cisco Systems, Nortel, Palo Alto Networks, and currently, Cyolo. Joe's expertise lies in developing and leading successful programs, teams, and business lines. He has collaborated with exceptional colleagues to drive impactful new product launches and go-to-market strategies, including pioneering the first Industrial Cyber GTM. At Cyolo, Joe is at the forefront of the groundbreaking Industry 4.0 movement. Alongside his leadership in new product introductions, he is also recognized as a four-time CRN Channel Chief and a proud United States Coast Guard Veteran.



Joe can be reached online at <https://www.linkedin.com/in/jodo/> and at <https://cyolo.io/>



Making Our Infrastructure Resilient: 5 Priorities for Security R&D

By Saurabh Amin, Professor of Civil and Environmental Engineering PI, Laboratory for Information and Decision Systems Massachusetts Institute of Technology

Cyberattacks are undoubtedly on the rise; as of September 2023, there had already been [a 17% increase](#) in the number of security compromises over the total number for 2022. We can likely expect more such attacks as the geopolitical situation continues to deteriorate and more government actors abroad mount attacks on U.S. companies and infrastructure. In this climate, the challenge for the public and private sectors alike is to protect critical infrastructure systems as they become increasingly interdependent and reliant on cyberinfrastructure for both routine and emergency operations.

We live in a world of neither purely physical nor purely cyber infrastructure, but of cyber-physical-human-systems (CPHS). Vulnerabilities mean that hospitals can be shut down; air traffic and shipping can be disrupted; electricity grids can be knocked out; and navigation systems can be spoofed. The functionality of these systems can dip rapidly and take significant time to recover, leading to huge societal losses.

Such risks are becoming especially concerning due to increasing attempts to compromise the nation's large and strategic systems, and loss of trust in digital systems due to disinformation, fraud, and lack of digital safety. The resilience and trustworthiness of CHPS that provision critical societal services is now a top national security concern. How should policymakers address this fact?

Resources for new R&D is one answer. But R&D needs both resources and one or more pathways that are ambitious yet viable in a multi-stakeholder and highly uncertain environment. Hence if decision-makers in government and industry want to overcome our asymmetrical cyber challenge, they need diverse, committed subject matter expertise to chart the right course and create a broad, long-term picture of future global risks and opportunities that captures the needs of all stakeholders of CPHS.

Identifying research priorities for R&D is the function of the [Engineering Research Visioning Alliance \(ERVA\)](#), an initiative funded by the U.S. National Science Foundation (NSF). In August 2022, ERVA held one of its visioning events on the theme of “unhackable infrastructure,” convening dozens of the top experts in cybersecurity in the nation. The experts arrived at a consensus about the requirements that future resilient infrastructure must satisfy. These include the ability of CHPS to ensure safety, security, and trust in essential systems and services, while maintaining practical usability; and the capacity to adapt to unexpected changes while maintaining robustness and trustworthiness in a range of situations, including actively resisting adversaries (both known and unknown). The group identified gaps in today's security technologies and formulated new ideas and visions that will be instrumental in steering future research toward areas of much-needed innovation to ensure resilient and trustworthy CPHS.

The resulting [report](#) identified research directions within five concrete areas for R&D efforts with the goal of addressing the thorniest challenges in security engineering. Each area produced an array of specific engineering topics to catalyze engineering research for a more secure and resilient world. The experts highlighted ways in which these topics should be contextualized in various domains (e.g., energy, transportation, supply chains, health care systems), considering domain-specific design and functional requirements of CPHS, and unambiguous specification of safety, security, and resiliency requirements for all stakeholders.

1. Human-Technology Interface Considerations: The visioning event [report](#) emphasized a crucial insight: humans are both the weakest link and biggest opportunity in cybersecurity. Modeling to counteract cyberthreats must consider the human element more comprehensively, from motivating incentives and economics of security in asymmetric information environments as well as usability in engineered infrastructures. (This is why we expanded the concept of cyber-physical systems (CPS) to cyber-physical-human systems—to accentuate the essential human aspect.) The assembled experts also recommended more R&D to integrate frontier technologies like augmented and virtual reality into security interfaces, as well as greater use of immersive human-computer environments. These would simultaneously improve usability of security systems for human operators and allow greater understanding of what motivates humans to act in particular ways—knowledge that can be applied to the way adversaries think and act as well.
2. Measuring and Verifying Security: CPHS operate in highly complex and constantly changing environments, making it hard to determine how secure they are at any given time. We recommend development of new quantitative metrics for determining system safety as well as advanced

research into continuous monitoring and verification tools, which will rely on further development of artificial intelligence (AI) tools that can be deployed at partially observable and often vulnerable CPHS interfaces. These tools must be engineered to be able to learn through changing threat landscapes and help trigger automated response under highly dynamic and unpredictable situations. Additionally, insights derived from systematic study of human behavior and incentives for engineered systems will be crucial to better understand the human oversight aspect of security monitoring, adaptation, and verification.

3. **Future Approaches to Autonomous Security:** The sheer size and scale of cyber threats will require much greater use and deployment of AI and machine learning capabilities to monitor and quickly synthesize massive amounts of data and help determine when CPHS are at risk. R&D must continually emphasize integration of the most cutting-edge AI into safety and security processes, with a special focus on developing AI with contextual awareness in as humanlike a way possible, while ensuring trustworthiness of automated decisions and response capabilities. Crucially, research is needed to develop effective processes for human operators and decision-making processes (or feedback loops) to interact with and derive the most value from AI, again tapping into the CPHS framework to integrate knowledge about human behavior in threat modeling and coordinated, risk-aware, response mechanisms that satisfy physical constraints.
4. **New Approaches to Resilience in Interdependent Infrastructures:** CPHS tightly couple continuous physical dynamics with networked computer processes, which means adversaries can exploit a weakness in one area to wreak far wider damage. Strategic coordination among different systems, organizations, and industries is therefore critical for addressing insecurities arising due to correlated software bugs, hardware malfunctions, and network interdependencies. In addition to technical research, mechanisms for coordination between government and for-profit agents must be established, since the latter possess access control to critical industries that are integrated in common CPHS. There is a clear need for a limited liability framework (aka due care standard) and compliance mechanisms for processes such as data sharing and analysis as well as the knowledge base for security tactics and active defense strategies.
5. **Architecting Trustworthy Systems:** Systems and security processes must be, above all, trustworthy. But what does this mean? In the context of engineered infrastructure, trustworthy refers to system correctness and security according to a well-defined design specification. Hence R&D in this space should focus first on design specification and defining correct behavior in complex infrastructures (which include many interconnected sub-infrastructures and processes that can range from centralized command to fully decentralized operations). The goal is to design trustworthy systems that can withstand attacks—or unanticipated uses of technology that fall within a system's specifications. These systems have untrusted inputs and interfaces that can be tackled by confidential computing techniques and trustworthy architectures. Engineering research should address such key issues to address vulnerabilities we see today that arise from ill-defined specifications, brittle control loops, and poorly understood interdependencies.

The ERVA report elucidates proactive research directions and focus for those who oversee cybersecurity within each of these five research areas. But I would emphasize two key points above all: (1) collaboration across industries and sectors (including academia and government agencies) is essential, as the

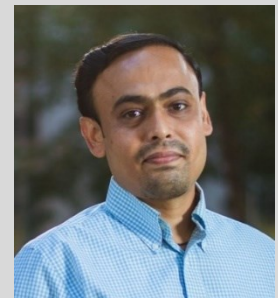
interdependent nature of CPHS demands it; and (2) this is the time to think in terms of a systems approach to design trustworthy and resilient CHPS in all major critical infrastructure domains.

Plugging holes and fighting security breaches as they occur is not the answer. We must reimagine the whole way we approach cyber-physical security in this world of cascading threats and their global implications. The ERVA visioning session was motivated by a call to look beyond the here and now to future, potential threats, so we can contemplate solutions that do not yet exist but are urgently needed. Decisionmakers in both national defense and in private industry must do no less to ensure our security.

About the Author

Saurabh Amin is Professor in the Department of Civil and Environmental Engineering (CEE) at MIT, and co-chair of the [ERVA Engineering R&D Solutions for Unhackable Infrastructure Task Force](#)

Saurabh can be reached at our company website <https://www.ervacommunity.org/>





Manufacturing on the Cyber Frontlines: Enhancing Cybersecurity on the Factory Floor

By Berardino Baratta, CEO, MxD

Manufacturing in the United States is changing. Today's factory floors are a far cry from those we saw in 1980s movies – dark, hostile environments with sparks flying – but are instead cutting-edge hubs of innovation, where our future is being forged right in front of our eyes.

At the heart of this shift is a [commitment to modernization](#), digitization, and connected supply chains. This has become instrumental in driving success, but it also has made manufacturing companies increasingly susceptible to cyber-attacks. And just as we see change in the manufacturing sector, these attacks are constantly evolving, making it crucial for manufacturers to develop future-proof cyber skills to safeguard their assets, intellectual property, and sensitive information.

A staggering 25% of cyber-attacks in the United States specifically target the manufacturing sector, making it the most-attacked sector for the second year in a row. To tackle this growing threat, MxD is at the forefront of driving digital adoption and resilience in U.S. manufacturing for the 21st century.

In 2022, the average cost of a ransomware attack in the United States exceeded \$4.5 million. While the benefits of connectivity outweigh the potential risks, addressing operational technology cybersecurity can be overwhelming for small- and medium-sized manufacturers (SMMs). A significant majority (86%) of cybersecurity threats directed at the manufacturing sector are targeted rather than opportunistic, making the manufacturing industry the most attacked industry. Of these breaches, nearly half are related to intellectual property theft, which is critical considering that U.S. manufacturers drive over three-quarters of all private-sector research and development in the country. In fact, the manufacturing industry drives more innovation than any other sector.

In response to the escalating cyber-attacks, MxD has strategically invested in a portfolio of nearly 170 research, development, and demonstration projects. These projects, carried out in collaboration with partners, members, academic researchers, startups, and the federal government, have the potential to make a considerable impact on the commercial space.

MxD also offers various resources, both in the digital and cybersecurity realms, such as the [MxD Cyber Marketplace](#). This platform provides user-friendly cybersecurity assessments to enable companies to understand and bolster their own cybersecurity posture. Additionally, MxD provides the [Playbook for CMMC 2.0](#), a comprehensive guide to meeting the first level of Cybersecurity Maturity Model Certification compliance, which is designed to protect the sensitive unclassified information that is shared by the Department of Defense with its contractors.

As with digital manufacturing generally, cybersecurity requires skilled personnel to reach its full potential. MxD has developed [The Hiring Guide: Cybersecurity in Manufacturing](#), aimed at assisting U.S. manufacturers in fortifying their factory environments by recommending targeted training programs to upskill workers for the future of cybersecurity.

Going digital is no longer a choice but a necessity for propelling the manufacturing industry forward. In today's fast-paced world, communication is instant, and results are expected promptly. Leveraging the agility and speed of digital connectivity, the digital thread increases efficiency and productivity within enterprises. This seamless integration enables the widespread implementation of improvements, fueling advancement across the entire manufacturing enterprise. MxD's resources play a pivotal role in integrating these efficiencies, empowering factories for the future.

The United States is at the global leading edge of intelligent and efficient advanced manufacturing – and is supported by a vast network of supply chains that stretch worldwide. To further fortify the position of U.S. manufacturing companies, MxD has played a crucial role in supporting projects, such as a collaboration led by Software AG aimed at building a supply chain risk alert system. This system functions as an early warning system, alerting manufacturers of potential delays caused by emergencies, adverse weather conditions, or natural disasters. MxD will continue to fund projects and support business to create cyber-secure supply chains for U.S. manufacturing.

About the Author

Berardino Baratta is an accomplished leader in technology and advancing manufacturing, with more than 25 years of experience in the industry. As the CEO of MxD, the digital manufacturing and cybersecurity institute, Berardino works with the U.S. Department of Defense and a nearly 300-member ecosystem to drive economic prosperity and support national security by increasing U.S. manufacturing competitiveness. Through MxD's diverse array of projects and partnerships, Berardino oversees critical efforts to enhance digital readiness and cybersecurity across the manufacturing sector, prepare the workforce for the advanced manufacturing jobs of the future, and ensure resilient and secure supply chains in an era of increased geopolitical disruption.





Open AI Exec Warns AI is “Extremely Addictive,” Humanity Could Become “Enslaved”

By Sai Mattapalli and Rohan Kalahasty, Co-Founders — Vytal.ai

The idea of technology going wrong and turning on its creators is not new. More than 200 years ago, Mary Shelley teased out what that could look like when she created Frankenstein’s monster.

[Recent reports](#) suggest that artificial intelligence — which is weaving its way into virtually every aspect of our culture — may be the next technological monster society must contend with. According to Mira Murati, CTO at generative AI giant OpenAI, those reports may not be far off.

During a [recent interview](#), Murati warned that the misapplication of AI could have tragic consequences. She pointed to the possibility that AI could be designed “in the wrong way,” leading to it becoming “extremely addictive” and users becoming “enslaved.”

Coming from Murati, the comment is significant. She has been [dubbed](#) “the most powerful woman in AI.” The company she works for, OpenAI, is a global leader in the field of generative AI. If she points to risks that must be addressed, the tech world should take notice.

What is AI addiction?

The risk of AI addiction stems from the technology's ability to discern what users want and serve it up in more compelling ways. For example, AI is being used in the world of e-commerce to provide hyper-personalized shopping experiences. AI can quickly determine what shoppers are willing to spend on, and deliver virtually endless examples of deals related to past purchases.

The same AI-powered personalization leveraged in the world of e-commerce can be applied to other platforms as well. Streaming platforms can use it to keep viewers locked in to certain types of content. Gaming platforms can use AI to nudge players into deeper interaction by empowering adaptive difficulty and other personalization strategies. While visions of humanity enslaved by AI may be a bit dystopian, the idea that AI can lead us into unhealthy patterns of behavior is something the experts are clearly communicating.

One of the chief concerns is that we are becoming [too dependent](#) on AI. We count on it to do an ever-growing number of tasks, from driving our decision-making to driving our cars. As over-reliance moves toward total-reliance, the potential grows for losing perspective, wisdom, and the ability to perform valuable and essential skills.

AI growth and cybersecurity concerns

As the use of AI grows, the potential for abuse also grows. AI is essentially built on data collection and processing, which means it can be compromised by cyberattacks. If healthy AI has come to be seen as dangerous, AI that has been corrupted by bad actors is even more dangerous.

For example, bad actors who gain access to AI training data can corrupt it, leading AI to behave in unintended ways. Imagine AI designed to direct a self-driving car being fed poisoned data that causes it to misidentify traffic signs and signals. The consequences could be devastating.

Data breaches that lead to AI bias are another danger. AI is already being used to guide decision-making in sensitive areas, such as medical diagnosis. Bias that leads to misdiagnosis or misguided treatment recommendations puts lives at risk.

Promoting responsible AI use

Protecting against the misuse of AI begins with weaving ethical considerations into its development and use. Developers must think through potential dangers and design AI tools in ways that address them. As data is the foundation of AI learning, data used for training should be carefully sourced and protected.

Bringing a multitude of perspectives to the development of AI is also important. AI is a tech tool, but its impact is felt far beyond the tech world. Development teams that include those with diverse backgrounds and disciplines contribute to a deeper understanding of dangers that must be addressed.

Ethics also come into play for those who use AI. Businesses should develop policies to govern AI use. All employees who engage with AI should receive training on how to use it ethically and how to identify situations in which misuse is occurring.

As the potential for AI abuse becomes more evident, the need for accountability grows. Who is responsible for defining what is acceptable when it comes to AI? Who will blow the whistle when development gets off track? Who will keep us from becoming enslaved? Those are just some of the big questions that must be answered, as we consider the new wave of warnings experts are issuing regarding AI.

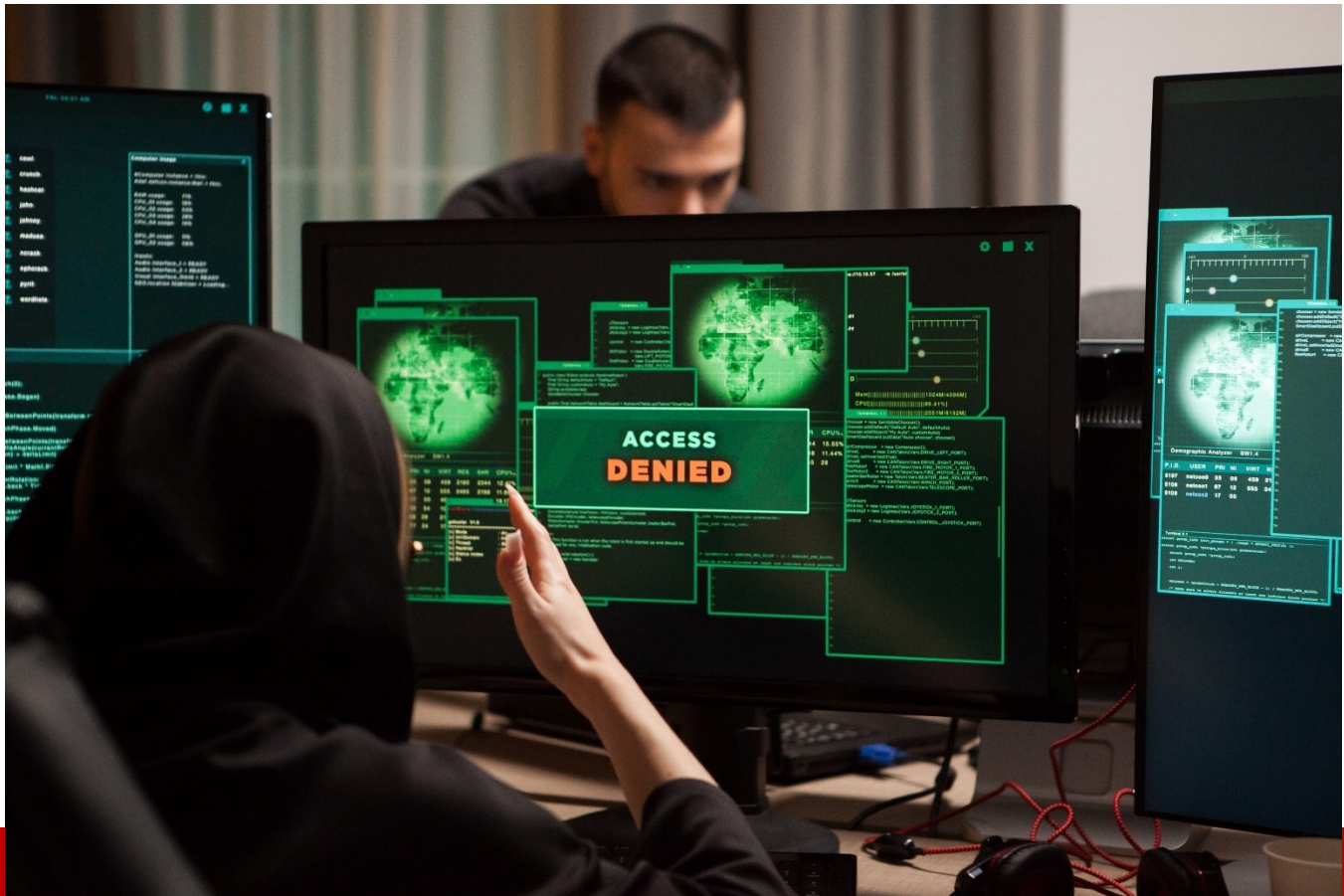
About the Author

[Rohan Kalahasty](#) is a co-founder of [Vytal.ai](#). He has been a researcher at the Harvard Ophthalmology AI Lab for three years, where he led and incubated NeurOS and worked on projects leveraging mathematical, statistical, and artificial intelligence modeling to enhance eye disease diagnosis. Furthermore, he served as an incubation lead at Roivant Sciences, leading the early stages of a potential new vant. He has also researched at the Center for Brains, Minds, and Machines at MIT, where he dedicated his time to studying human intelligence and memory utilizing artificial intelligence. While working with these groups, he has developed a deep insight into the intersection of AI and Medicine and the creation of digital biomarkers, an insight which proved to be crucial for the development of Vytal. He is a senior at Thomas Jefferson High School for Science and Technology.



[Sai Mattapalli](#) is a co-founder of [Vytal.ai](#). With a deep background in the study of neuroscience, Sai was a research intern at the Neurophysiology Lab at Georgetown University, where he built behavioral paradigms to test auditory learning in Zebrafish. He also serves as an intern at the Center for Brain Circuit Therapeutics at Harvard Med, where he works on mapping the brain networks at play for seizure patients who experience eye versions. Later pivoting to entrepreneurship and finance, Sai served as a business growth intern at Quantbase (YC W23) and was a part of DMV's Finest, the winners of the Wharton Investment Competition.

Sai Mattapalli and Rohan Kalahasty can be reached at our company website <https://vytal.ai/>



Organizations Are Shifting Ransomware Defense Tactics, But Malware Is Still the Problem

By Trevor Hillgoss, Senior Director of Security Research at SpyCloud

Ransomware attacks are a fact of life – [over 72%](#) of global businesses have been impacted by ransomware in 2023. This number rises in U.S., Canadian, and U.K. organizations, with [over 81%](#) affected at least once in the past year, according to a recent SpyCloud survey.

Despite the continued threat, 79% of security leaders in North America and Europe are confident in their ransomware defenses, highlighting a disparity between the industry's assessment of its cyber preparedness and the efficacy of current cybersecurity strategies.

This disconnect is partially due to the evolving methods criminals employ. Traditionally, data encryption was the biggest problem facing organizations impacted by attacks, and businesses countered by implementing data backups. However, the ransomware landscape has shifted, and cybercriminals are increasingly relying on malware-exfiltrated data to carry out more devastating attacks.

Missing the Mark on Malware

According to SpyCloud, information-stealing malware infections (or infostealer infections) preceded [over one-fifth \(22%\)](#) of ransomware events for North American & European businesses in 2023. And common infostealers such as Racoon, Vidar and Redline further increased the probability within a 16-week period between the initial infection and the ransomware event. Based on an [analysis of data exfiltrated from infected devices](#) in the past year, a similar percentage of victim devices (20%) were equipped with at least one antivirus application at the time of the successful infection.

Threat actors use malware to exfiltrate authentication data, which they buy and sell on the darknet. Using this data, criminals can access an organization's network, where they conduct initial exploration and steal additional data before deploying ransomware to incapacitate the target's business operations or furthering the extortion through the theft of sensitive data.

Security leaders are not unaware of the malware threat. SpyCloud found [98%](#) of IT leaders agreed they could improve security by better identifying business applications at risk of infostealer infections. Many companies have also begun taking technology-driven countermeasures, including automation, implementing multi-factor authentication (MFA), and [adopting passkeys](#).

However, infostealers are challenging to detect and prevent, and security leaders struggle to keep up. While organizations can take precautions by educating employees and ensuring software protections are up to date, it's impossible to avoid infections entirely, and advanced strains can exfiltrate data and delete themselves in seconds – leaving very few indicators that the device was ever compromised.

Piling on traditional protections like MFA is not the full answer. While implementing MFA is certainly a good idea, authentication data stolen by infostealers is not limited to usernames and passwords. This data often includes things like cookies, which can enable session hijacking; an unsophisticated attack where criminals use stolen cookies or tokens to impersonate a user. This attack gives criminals access to already-authenticated sessions, sidestepping the need for credentials, passkeys, and MFA. With all the permissions of a legitimate user, criminals can facilitate identity theft, unauthorized transactions, or steal additional data.

With over [22 billion](#) malware-stolen cookie records recaptured by SpyCloud last year, session hijacking is a significant threat. Despite this, IT leaders view monitoring for compromised session cookies as the third least important ransomware countermeasure and least risky entry point. The fact is, however, addressing ransomware must start with a holistic malware remediation strategy.

An Elevated Approach for an Elevated Threat

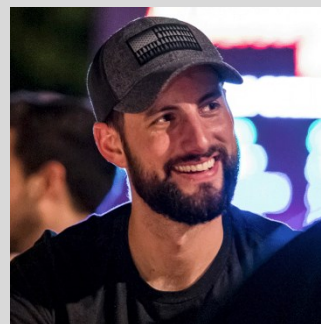
The most common approach to remediating a malware infection starts and ends with the device and network impacted by the infection. However, this approach often ignores data siphoned by an infostealer – likely part of the initial attack – which can remain active long after the device has been wiped and the malware removed from the environment. Cybercriminals can use the stolen data to launch repeat cyberattacks against organizations and individuals, causing potentially irreparable damage.

Instead of this incomplete infection response, security leaders must gain knowledge and visibility into the authentication data stolen by the malware, quickly remediate the compromised credentials and invalidate the stolen web sessions for business-critical applications.

A comprehensive [post-infection remediation](#) process substantially reduces the risk of ransomware events tied to infostealer infections and closes previously overlooked exposures – including those resulting from infected personal or unmanaged devices accessing the network – stopping criminals in their tracks before they use malware-exfiltrated data to cause further harm.

About the Author

Trevor Hilligoss is the Senior Director of Security Research at SpyCloud and is an experienced security researcher with a background in federal law enforcement. Before leaving government service, Trevor spent nearly a decade tracking both cybercriminal and nation-state actors for the DoD and FBI and has presented at the US and international conventions as a threat intelligence expert. He holds a BA in Sociology, multiple federal certifications in the field of cyber investigations, and two Global Information Assurance Certifications (GIAC). Trevor can be reached online at <https://www.linkedin.com/in/thilligoss/> and at SpyCloud's company website <https://spycloud.com/>.





Passwords In the Air

By Gautam Hazari, Chief Technology Officer, Sekura.id

Imagine, you are sitting in a café, sipping the skillfully crafted coffee by the barista, with your laptop placed on the table in front. You open the screen and look around to see if no one is around “shoulder surfing”, and then you open your email, type in the user ID and the password on the keyboard and access your email. You didn’t notice that a few tables behind, there is someone looking at their phone, as their phone is kept on the table, and why would you care? A few minutes later, you close your screen and focus back on the coffee as you don’t want it to get cold. But something happened between sips; someone is accessing your email, someone is initiating a password reset for your banking account, or social media account. An account takeover is in action.

How did this happen? No, this was not someone accessing the laptop or sniffing into the Wi-Fi connection. Remember that person a few tables behind looking at their phone? The microphone

in that person's phone was "listening" to the keystrokes of your keyboard, and passing those to a trained deep-learning model which then revealed the password you typed.

This is SCA — not Strong Customer Authentication — but actually the antithesis of that. This is a Side Channel Attack, an acoustic side-channel attack, as published by researchers from Durham University.

A SCA is when signals from a device are collected and interpreted to extract secrets. The signals can be in any form: from electromagnetic waves, power consumption to sound waves. The interesting thing about side-channel attacks is that they do not need connectivity or any direct access to the device. The acoustic SCA uses the sound waves from the device, and in the above case – the sound of the keyboard strokes.

A recent report from Cornell University found that AI can be used to steal passwords by "listening" to a user's keystrokes with over 90 per cent accuracy. And researchers from the universities in London found results up to 95 per cent accuracy in a similar report.

It doesn't just stop there; the person doesn't need to be sitting in that café a few tables behind. In fact, the same attack can be carried out remotely by listening through Zoom calls with 93 per cent accuracy.

How do we solve this? The answer is to stop using passwords, which clearly have several vulnerabilities that fail to protect ourselves and our data.

We almost forget that there is a digital service which we use several times a day that provides secure protection not offered by passwords. We even have a name for the fear of losing it – "nomophobia". It's our mobile phone service: what we use to make or receive phone calls and SMSs, or access any application or website on our mobile devices.

It uses the SIM to identify the genuine user. The "I" in the SIM stands for "Identity"; it stood for the same when the first SIM-based mobile phone call was made in 1991 and it still stands for "Identity" when we use the eSIM.

The Subscriber Identity Module (SIM) is a hardware-based cryptography engine, where a unique cryptographic key is stored securely specific to the SIM, which identifies the user. Mobile networks around the world use a cryptographic signature from the SIM through the unique key to authenticate the identity without challenging the user to enter a password or any other form of explicit authentication, making it much more humanized, seamless and also secure from stealing any secrets from the user.

At the same time, the SIM is one of the most inclusive technologies, which provides the exact same level of security and protection, irrespective of what device the user is using – from the high end expensive mobile phones to the simpler, more affordable mobile phones.

This SIM-based authentication method has been in use in mobile networks for the past three decades, and should continue to be fully utilized to replace passwords that fail to protect our data and identity time and time again. Let's make the world passwordless. Let's harness the SIM's security superpower to make the digital world a safer place.

About the Author

[Gautam Hazari](#) is the Chief Technology Officer of [Sekura.id](#), the global leader in Mobile Identity services, who believes passionately in humanizing technology by removing the password. He truly deserves his twin accolades of 'Mobile Identity founding father' and 'Mobile Identity guru'. He is a strategically driven technology leader with over 24 years of robust experience in the telecoms industry. Gautam wrote the code and led the implementation of the mobile identity initiative – Mobile Connect – for 60 mobile operators across 30+ countries. An advisor to start-ups in digital identity, healthcare, Internet of Things and fraud prevention, he is a respected and sought-after thought leader for digital identity, advocating solving the identity crisis in the digital world by actively creating the Internet's missing Identity layer.



Gautam Hazari can be reached on [LinkedIn](#) and at our company website <https://sekura.id/>



Protecting Data in The Final Stretch of The Supply Chain

Building a Secure Last Mile for Global Commerce

By Dan O'Toole, Chairman & CEO, Arrive

Navigating the Last Mile: Securing the Final Stretch of the Supply Chain

In the rapidly evolving landscape of global commerce, the last mile of the supply chain emerges as a critical juncture fraught with challenges and opportunities. As an ever-increasing number of goods make the transition from warehouses and distribution centers to their ultimate destinations, the significance of data security becomes paramount. [Nearly 50%](#) of all supply chain disruptions are caused by cyber-attacks. The intricacies of securing data in the last mile, and the importance of innovative solutions that address industry-wide concerns is becoming more apparent.

Unraveling the Last Mile Challenge

The last mile poses a series of challenges demanding a sophisticated approach to data security. With the continuous movement of goods through various supply chain touchpoints, the risks of data breaches and cyber threats intensify. The complexity of this final stage requires a comprehensive understanding of safeguarding sensitive information amid the intricacies of delivery.

Innovations in the Last Mile

Enter a new wave of innovations addressing the last mile challenge, such as the emergence of Arrive's [Mailbox-as-a-Service](#) (MaaS) platform. These solutions strategically position themselves at the nexus of secure communication, offering a bridge for the exchange of goods and information.

Seamless Integration for Enhanced Security

MaaS providers, including those adopting cutting-edge technology, seamlessly integrate into existing supply chain processes, ensuring a secure exchange of goods and data between stakeholders. From real-time tracking to secure documentation and chain of custody, these solutions fortify every aspect of the last-mile delivery with robust data security measures.

The Nexus of Trust: Transparency and Data Security

Central to successful supply chain operations is the nexus between transparency and data security. MaaS solutions, as exemplified by some providers, establish a transparent and secure platform for communication. Real-time tracking not only enhances security but also fosters trust among stakeholders involved in the last-mile journey.

Industry-wide Impact

The focus on data security in the last mile extends beyond individual providers. According to IBM, the average cost of a supply chain data breach is estimated to be [\\$4.35 million](#). This highlights the need for a new industry-wide standard, one emphasizing the critical need for secure and transparent last-mile processes. This commitment to an industry-wide impact will continue positioning innovators as thought leaders, influencing best practices, and shaping the future of data security in global supply chains in the years ahead.

Adapting to Evolving Threats

In a landscape where cyber threats evolve rapidly, innovative solutions stand as stalwart defenses against emerging challenges. Proactive measures, including regular updates and advancements in encryption technologies, ensure that the last mile remains resilient in the face of evolving threats.

Collaborative Solutions for the Final Stretch

Recognizing the interconnected nature of the supply chain, industry leaders actively collaborate to fortify the last mile. Collaborative solutions address shared challenges, creating a unified front against cyber threats. Initiatives extend beyond immediate operations, fostering a culture of collective responsibility for data security in the last mile.

Future-Proofing Last-Mile Data Security

As technology evolves, so do the threats to data security. A forward-looking approach involves not only addressing current challenges but also anticipating and preparing for future risks. Future-proofing last-mile data security requires a commitment to innovation, adaptability, and a proactive stance against potential threats in the ever-changing landscape of global commerce.

In the complex web of the supply chain, the last mile emerges as a critical battleground for data security. As goods make their final journey into the hands of consumers, the need for a secure, transparent, and efficient last mile has never been more pressing. Innovative solutions, strategically positioned at the heart of this final stretch, can elevate data security to new heights.

As businesses grapple with the complexities of the global supply chain, the last mile will continue to emerge as a critical battleground for data security. The need for a secure, transparent, and efficient last mile has never been more pressing, and innovative solutions like Arrive's MaaS platform can help businesses to achieve this goal. By adopting a holistic approach to data security, businesses can protect their sensitive information, ensure the smooth flow of goods, and ultimately build trust with their customers. Together, we can shape a future where the last mile is not a source of vulnerability but a symbol of resilience and innovation.

About the Author

Dan O'Toole is the Founder, Chairman, and Chief Executive Officer of Arrive (formerly Dronedek). As a strong visionary, he is a leader in autonomous delivery and was one of the first people in the U.S. to secure patents for a smart mailbox. His invention was designed to accept packages delivered by drone and other autonomous means securely. A serial entrepreneur and business leader, he has had extensive experience in upper management at several prior impactful companies, including startups, enterprise sales groups, and commercial real estate entities. A graduate of Ball State University, he lives with his family in Carmel, Indiana, and is an avid car collector.

Dan O'Toole can be reached online at dan@arrive.tech or through Arrive's website at www.arrive.tech.





QR Code Phishing Attacks: Threat Actors Are Now Shopping Online with You

Olesia Klevchuk, Director of Email Protection at Barracuda, discusses the prevalence of QR code phishing attacks and how cybercriminals are utilizing phishing to exploit data, download malware, compromise personal devices, and what individuals need to be mindful of when spotting a phishing attack.

By Olesia Klevchuk, Director of Email Protection, Barracuda

In recent years, QR codes are among one of the many technologies that have reemerged with more efficiency and convenience than before. The two-dimensional barcode allows users to share website URLs, make payments, or share contact information from their mobile devices. However, with efficiency comes a cost – and while QR codes have opened new opportunities for individuals to utilize advanced technology, it's also opened more opportunities for hackers to intervene.

Now, hackers are embedding malicious QR codes into shopping coupons, phishing emails, payment sites, and social media accounts – also known as “quishing” attacks.

As technology becomes smarter, so do hackers, and individuals need to be mindful of these new methods so they can stop attackers in their tracks. With proper cybersecurity training and the help of AI, quishing can be avoided, and QR code technology can be used to its advantage.

QR Code Attacks’ Secret Weapon: Creating a False Sense of Trust

Imagine you receive an email from your bank, informing you about a security update for your mobile banking app. The email explains that you need to update the app immediately to prevent any potential security breaches and keep your finances safe, so you scan the QR code with your mobile device – redirecting you to a site that replicates your bank’s interface and prompting you to enter your login details. The update is seemingly “successful.” A couple days later, you have several unauthorized transactions, your account has been compromised, and you realize you are a victim of a QR code attack.

Quishing attacks utilize social engineering tactics that make individuals more susceptible to the threat. These attacks frequently exploit the trust of people who use their mobile devices for regular digital interactions, such as emails, messages, or payment sites. This creates a false sense of familiarity, directing victims into a deceptive comfort zone to give out their credentials. Specifically, attackers mainly use quishing attacks to spread phishing links, malware downloads, or compromise a device.

QR Code Attacks: Emails, Malicious Downloads, and Compromised Devices

QR code attacks can manifest in different ways which present unique threats to individuals’ security. Quishing often comes in the form of a malicious email link, prompting recipients to scan a QR code and redirecting them to a counterfeit website that masquerades as a trusted application or service. Individuals are then encouraged to submit their personal information or login credentials, unknowingly offering their personal data to the attacker. Additionally, quishing attacks can also come in the guise of surveys that ask victims for their personal information, including their social security number. These malicious links and forms serve as bait for victims, making it easy for attackers to receive personal information.

Malware from malicious websites can also automatically be downloaded to a victim’s device. The dangerous malware can range from spyware to ransomware, granting attackers the ability to pilfer data or even seize control of a victim’s device – serving as a huge threat to individuals’ security.

Additionally, scanning a QR code can be used to open payment sites, follow social media accounts, or send malicious email messages from a compromised victim’s account. This tactic allows hackers to impersonate their victims or target others in their network.

AI Imaging and Recognition Technology are Crucial to detect Quishing

With advanced technology, AI and image recognition can be a pivotal defense mechanism in detecting quishing attacks. AI-based detection can analyze a range of signals, from image size and placement, content analysis, or sender behavior to determine whether there is malicious intent behind the QR codes. This technology looks through data and specific patterns to help identify potential threats, providing a shield against these attacks.

It is also important to educate users on specific QR code attacks given the prevalence of advanced technology. Cybersecurity professionals are encouraged to educate individuals through security awareness training on how to quickly thwart and identify these attacks and their impact on organizations.

The ever-evolving technological landscape has not only allowed tech to get smarter, but has allowed hackers to level up their attacks. The complex and multifaceted nature of QR code attacks calls for a proactive response, and cybersecurity leaders and individuals must be wary of how easy it is to fall prey to these attacks. Implementing cybersecurity safety training programs and enabling AI with image recognition technology can be pivotal in avoiding compromised devices, malware downloads, and ultimately providing safety to individuals' personal data.

About the Author

Olesia Klevchuk is the current Director of Email Protection at Barracuda where she oversees the product marketing team and is skilled in the realm of cybersecurity, SaaS, enterprise software, and go-to-market strategies. Prior to her time at Barracuda, Olesia was the Senior Product Marketing Manager for MarkMonitor and Intermedia – where she continued prospering her career in strategic messaging and positioning. Olesia received her B.A in History and Sociology at the University of Reading and received two M.Sc's; one in Political Science at the University of Bristol and another in Research and Statistical Analysis at the University of Glasgow.



Olesia Klevchuk can be reached online at [Olesia Klevchuk](https://www.barracuda.com) and at our company website <https://www.barracuda.com>.



Real Time Exposure Detection Is the Missing Element of Every Cybersecurity Strategy

Detecting threats and vulnerabilities in real-time is crucial for an effective cybersecurity strategy to protect against cybercriminals.

By Or Shoshani, CEO and Co-founder, Stream Security

Cybersecurity teams are often at a disadvantage when it comes to protecting digital data from cyber criminals. Security teams must ensure that systems are protected 24/7, while bad actors can conduct mass data breaches by preying on a single vulnerability. This inequity between roles illustrates a big obstacle for cybersecurity experts in a community where constant surveillance is required.

With the popularity of the Continuous Integration/Continuous Deployment (CI/CD) practice, DevOps teams are frequently deploying advanced software and configurations updates, while security teams are constantly chasing these updates to mitigate the introduction of new threats into their network.

Since the early 1990s, organizations have utilized standard cybersecurity processes like periodic vulnerability scanning as part of their defense strategies. Despite how established they are, these processes cannot offer 100% protection when used intensively. For example, daily vulnerability scans can take up to 23 hours of exposure, providing threat actors with more than enough time to exploit these weak spots.

This challenge is exacerbated by an organization's composition and established procedures. The team assigned to incorporate exposures as a component of their deployment strategy is often the same team assigned to mitigate them, which may cause setbacks in response times. For example, if a security team documents a problem after 24 hours, the configuration associated with that issue has already been utilized. Repairing it poses severe risks to the environment's resilience, potentially affecting corporate activities. Because of this, operations teams may give precedence to other activities, leaving a vulnerability unaddressed for an extended period.

The remedy for this ongoing issue is to mesh security and operations teams through real-time exposure detection.

Real-time exposure detection entails constantly evaluating exposure levels without depending on intermittent scans. Each modification in the environment is promptly analyzed to identify exposure levels.

Organizations can achieve the most success with real-time exposure detection by adopting the following best practices:

1. **Align with Organizational Requirements:** Every organization has its own distinct needs, including its level of tolerable exposure. Security teams must implement parameters that cater to these specific needs, including pinpointing critical assets, analyzing risks in data flows, and mitigating threats internally.
2. **Encourage Operations To Be More Security-Minded:** Operation teams must be well-informed of exposure levels for several reasons. First, operations teams can examine deployments before introducing security gaps, therefore shielding systems from exposures before they can occur. Second, instant exposure detection, when deployed, facilitates safe reversion because it gives the operations team sole reliance on the configurations and allows for speedy remediation.
3. **Adopt Automated Fixes:** For best results, security and operations teams should agree regarding the guardrails they establish to provide automated responses when specific incidents occur. These rules are cultivated and outlined to generate efficient automated solutions.

Real-time exposure detection is vital in giving cybersecurity teams an advantage over cyber criminals. It provides organizations with the ability to respond quickly, work together effectively and bolster cloud environments, developing a more secure digital landscape for everyone. When time is of the essence, real-time exposure detection is critical to being in control of cybersecurity.

About the Author

Or Shoshani is the CEO & co-founder of Stream Security. After serving in an elite IDF unit, Or Shoshani began his journey in the tech industry. He founded a data center startup that later became part of Mellanox, which is now a significant division within NVIDIA driving advancements in AI technology. Currently, Shoshani is serving as the co-founder and CEO of Stream Security. The company has a visionary mission to simplify cloud complexity and transform the way security and DevOps teams engage with the cloud. Over the past few years, Stream Security has developed a Cloud Twin model that combines posture and behavior awareness to revolutionize cloud operations and ensure security. Under Shoshani's leadership, Stream Security is shaping the future of cloud computing, making it a safer and more efficient environment for everyone. Or can be reached online via [LinkedIn](#) and at the company website: <https://www.stream.security/>





Government Communications: The threats



Government Communications: The Threats

By Nicole Allen, Marketing Manager at Salt Communications

In an age where information flows freely and rapidly, government communications have never been more vulnerable. The digital age has ushered in a revolution in how governments communicate, both internally and with the public. While this transformation has brought about unparalleled transparency, it has also exposed governments to an array of threats that can jeopardise national security, privacy, and public trust.

So, let's delve into the threats that government communications face:

1. Cyberattacks:

One of the most prominent threats governments face today is cyberattacks.

State-sponsored cyberattacks are a significant concern. These attacks often involve well-funded and highly skilled hackers. In 2021, the U.S. government attributed several high-profile cyberattacks to state actors, including the SolarWinds supply chain attack, which affected numerous federal agencies and private companies. Hackers, whether state-sponsored or independent, target government systems to steal classified information, disrupt critical services, or compromise sensitive data. The consequences of a successful cyberattack can be catastrophic, potentially affecting national defence, infrastructure, and the economy.

2. Espionage:

Espionage has been a constant in international politics, but in the digital age, it has evolved. Foreign governments often seek to infiltrate the communication networks of their counterparts to gather intelligence, monitor strategic developments, and gain a competitive edge. This involves the use of computer networks, malware, and various digital techniques to access and gather sensitive information from targeted entities, such as other governments or individuals within the government organisation.

3. Leaks and Whistleblowers:

Governments rely on confidentiality to make informed decisions and protect sensitive information. However, leaks and whistleblowers can expose classified documents, creating diplomatic tensions and damaging the credibility of government agencies. Leaks can take various forms, including unauthorised disclosure of classified documents to the media, public disclosure by whistleblowers, or espionage activities. The motivations behind these leaks can range from exposing perceived wrongdoing to advancing personal or political agendas.

4. Misinformation and Disinformation:

In recent years there has been a rise in the widespread dissemination of false or misleading information. Governments must navigate a landscape where malicious actors can easily manipulate public opinion by spreading disinformation, affecting elections, and sowing discord. Disinformation often transcends national borders, and malicious actors can operate globally. International cooperation is crucial in addressing this issue, as coordinated efforts can be more effective in countering disinformation.

5. Data Privacy Concerns:

As governments collect and store vast amounts of data on their citizens, concerns about data privacy and surveillance have grown. Ensuring that sensitive personal information remains secure is not only an ethical obligation but also a legal one. As governments amass vast data repositories, the risk of data breaches and cyberattacks increases. Such incidents can lead to the exposure of sensitive information, identity theft, and financial fraud. Governments must take measures to secure their data infrastructure.

Now, let's address why protecting Government communications is an absolute necessity:

Government agencies and non-governmental organisations (NGOs) are among the most popular targets for cyberattacks, with about 80% of nation-state attacks aimed at them, according to Microsoft, therefore internal communication is a critical defence measure.

National Security:

Secure communications play a pivotal role in safeguarding a nation's security interests by shielding critical information, military strategies, intelligence operations, and diplomatic negotiations from unauthorised access and surveillance. The need for such robust communication systems is driven by a multitude of factors that collectively contribute to a nation's security and sovereignty.

Diplomatic negotiations are often conducted behind closed doors, and governments need to maintain the confidentiality of discussions to ensure that agreements and compromises can be reached without undue external pressure or influence. Secure communication is instrumental in protecting the integrity of these talks, whether they involve peace negotiations, trade agreements, or other diplomatic efforts.

Public Trust:

Citizens entrust their governments with a wealth of personal data, from basic identification information to more sensitive data, such as tax records, healthcare information, and even surveillance data in some cases. This trust forms the foundation of the relationship between individuals and the state, as governments are expected to handle this data responsibly and ethically. Secure communication platforms are instrumental in not only safeguarding this data but also in reinforcing public trust in government institutions.

Efficient Governance:

Secure communication enables government officials to collaborate effectively, make informed decisions, and respond swiftly to crises. A breach in communication systems can paralyse the government's ability to function efficiently. This ensures that experts and decision-makers can work together, share expertise, and formulate well-informed strategies. '*Government Designed for New Times*', a McKinsey report, claims that the use of technology, including secure communication, is crucial to how government organisations operate in every area.

Diplomacy and International Relations:

Secure channels of communication are not limited to domestic affairs; they are also of paramount importance for diplomatic negotiations and international cooperation. In the realm of international relations, governments must ensure that their communications with foreign counterparts remain confidential to foster trust and cooperation. One significant concept that illustrates the importance of secure communication in the context of international cooperation is the notion of a safe haven network to fall back on when all else fails.

Secure Communications isn't a luxury, it's a must

Having a secure communication system is not just a network for protecting data but also an instrument for upholding public trust in government institutions. By demonstrating a commitment to data privacy, responsible data handling, transparency, and accountability, governments can strengthen their relationship with citizens, ensuring that the data entrusted to them is used for the benefit of the public while preserving individual rights and freedoms. This trust is essential for the functioning of a democratic society and the legitimacy of government actions.

The threats faced by governments in the realm of communication are manifold and evolving. To protect national security and efficiently govern, secure communication is not an option but an absolute necessity. Government organisations will be able to manage their communications and feel confident in any situation that they may encounter during daily operations if they have a secure communication platform such as [Salt Communications](#) in place.

References:

[https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/#:~:text=The%20Microsoft%20Threat%20Intelligence%20Center,%2Dgovernment%20organizations%20\(NGOs\).](https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/#:~:text=The%20Microsoft%20Threat%20Intelligence%20Center,%2Dgovernment%20organizations%20(NGOs).)

<https://www.mckinsey.com/industries/public-sector/our-insights/government-designed-for-new-times>

<https://saltcommunications.com/government/>

<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>

<https://arcticwolf.com/resources/blog/notable-cyber-attacks-on-government-agencies/>

About the Author

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

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





SASE and Zero Trust: A Powerful Combination

By Elena Thomas, Digital Marketing Manager, SafeAeon Inc.

Gone are the days when network security resembled a medieval castle. It was protected by a robust drawbridge and moat. In our modern realm, we have virtualization, cloud computing, and nomadic remote workers. This has shifted the location of our metaphorical moat. It's important to note that the moat might not shield us from traitors inside our castle walls.

Enter protectors: Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE). These two modern-day knights are gaining traction fast. Organizations are looking to them to fortify their growing remote workforces from potential threats.

Where remote work is now common, security teams face a vast array of endpoints. They find themselves navigating an ever-expanding terrain daily. Each day brings new challenges in protecting a sprawling virtual landscape. In response, many organizations are revamping their processes and technology. They're opting for the strongholds provided by a zero-trust approach. To add more flexibility and security, businesses are turning to Secure Access Service Edge (SASE).

A recent study commissioned by IBM and conducted by Forrester Consulting revealed a trend. A whopping 78% of respondents are considering or planning to adopt SASE within the next year. So, what is SASE, and how does it connect with zero trust? Let's explore that!

So, what exactly SASE is, and how does it intertwine with the zero-trust method? Let's dive in!

What's Zero Trust?

Zero Trust is a guiding principle in cybersecurity. It advocates for no implicit trust. In network architectures, this is crucial. It refuses automatic access to resources based on network location. This deviates from older models that permit access to devices on the same network.

Consider VPNs. Usually, remote users gain broad access to a network. This poses a massive security risk. Zero Trust combats this. It replaces network-focused access control with stringent authentication and authorization software. This software lets administrators set access rules for different user groups. These rules are enforced regardless of location.

Data, services, and workflows are shielded by software-defined micro-segmentation. This is instead of rigid network segmentation. A zero-trust architecture ensures strict user authentication. It considers factors like user identity, location, and required service when granting access.

This approach follows a "never trust, always verify" mantra. It blocks inappropriate access instantly. For this, Zero Trust requires a clear view and control over network traffic. It must monitor traffic sent through all parts of the environment.

While integrating Zero Trust requires effort, the payoff is significant. It simplifies network structures. It offers more flexibility for users and application deployment.

What's SASE?

SASE or Secure Access Service Edge, is Gartner's answer to security challenges. These challenges are posed by remote work and cloud-based applications. It combines essential networking and security services into a comprehensive solution.

This solution includes FWaaS (Firewall as a Service), DLP (Data Loss Prevention), ZTNA (Zero Trust Network Access), secure web gateways, and CASB (Cloud Access Security Broker). In essence, SASE is business networking and security on a single platform. It provides a holistic security architecture for data centers, branches, cloud resources, third-party apps, and mobile devices.

For businesses navigating the complexities of remote or hybrid work, SASE is attractive. SASE providers offer cloud security solutions with application-level security. Zero Trust is at the heart of SASE. Constant checks for authentication and authorization are in place. This ensures tight security for users and applications, wherever they are in the world.

Why it's Not ZTNA vs. SASE, but ZTNA and SASE?

When it comes to network security, ZTNA and SASE share a harmonious collaboration. They are not in competition but work together for enhanced security. SASE serves as the overarching philosophy, with ZTNA as one of its integral components.

The journey to zero-trust implementation is a short- to medium-term objective. On the other hand, adopting the SASE model is a more long-term goal. When an organization decides to embrace SASE, it's setting itself on a gradual path. This path involves revamping its network and network security frameworks. It's not an overnight transformation. The process includes phasing out obsolete security technologies and seamlessly integrating the remaining ones. Choosing a SASE model requires a zero-trust approach to cybersecurity.

Today's cybersecurity experts must pay close attention to both zero trust and SASE. They should integrate these trends into future architectural decisions. In the short term, organizations should adopt zero-trust principles for better security. This will secure remote workforces accessing cloud-based and on-premises services. At the same time, they should view new networking projects through a SASE-compatible lens.

What Perks Customers Seek in Combination of ZTNA and SASE Solutions?

Customers can enjoy a variety of benefits by combining (ZTNA) and (SASE) solutions.

Stronger security:

ZTNA and SASE can significantly improve an organization's security posture. They achieve this by reducing the attack surface and preventing unauthorized access. Moreover, they effectively detect and block threats. ZTNA operates on a "never trust, always verify" approach to security. This means every user and device must go through authentication and authorization before accessing network resources. Complementing this, SASE provides a unified security platform that guards against a wide range of threats including malware, phishing, and data breaches.

Streamlined network management:

ZTNA and SASE can streamline an organization's network management. They do this by consolidating multiple security and networking functions into a single, cloud-based platform. This simplifies the deployment and management of security policies. It also enhances visibility into network traffic and security events.

Reduced costs:

ZTNA and SASE can help organizations cut down on IT costs. This is achieved by eliminating the need to purchase and maintain multiple security and networking appliances. Furthermore, ZTNA can help reduce costs related to VPN usage and bandwidth.

Improved user experience:

ZTNA and SASE can enhance the user experience. They provide secure and reliable access to applications and data from anywhere in the world. ZTNA improves performance and reduces latency by routing traffic directly to the nearest edge cloud location.

A comprehensive view of the network and network security:

ZTNA and SASE can give organizations a comprehensive view of their network and network security. They offer a single platform for monitoring and managing all network traffic and security events. This helps organizations identify and respond to threats more quickly and effectively.

In summary, the combination of ZTNA and SASE provides organizations with numerous benefits. These include stronger security, streamlined network management, reduced costs, improved user experience, and a comprehensive view of network and network security.

Conclusion

The fusion of Zero Trust and Secure Access Service Edge (SASE) is innovative. It's a formidable approach to contemporary network security challenges. By adhering to Zero Trust, organizations eliminate risky assumptions. They don't automatically trust any user or device simply because it's on a specific network. This shift is crucial in today's digital landscape where threats are everywhere.

On the flip side, [SASE](#) is comprehensive and integrated. It combines crucial services like SaaS, secure web gateways, FWaaS, and cloud access security brokers. All are in a unified, cloud-based platform. This approach meets the needs of large organizations. Especially those dealing with remote work and cloud infrastructures.

It's important to note that SASE inherently incorporates a ZTNA model. This means SASE solutions are intrinsically aligned with Zero Trust. They emphasize the symbiotic relationship between the two. They should be seen as complementary strategies that fortify an organization's security posture.

About the Author

Elena Thomas is the Digital Marketing Manager at SafeAeon, a leading cybersecurity company, where she combines her passion for digital marketing with her unwavering dedication to enhancing online security. With a career spanning over a decade in the cybersecurity realm, Elena has emerged as a prominent figure in the industry. Her expertise lies in crafting innovative digital strategies that empower individuals and organizations to safeguard their digital assets.

Beyond her professional life, Elena is a true cybersecurity enthusiast. She devotes her spare time to educating the public about the ever-evolving cyber threats and how to stay protected in the digital age. Elena's commitment to a safer digital world shines through in her informative and engaging writing, making her a sought-after contributor to blogs and publications in the cybersecurity space. When she's not immersed in the world of cybersecurity, Elena enjoys outdoor adventures and exploring new cuisines.



Elena can be reached via email at elena.thomas@safaeon.com and at our company website <http://www.safaeon.com/>.



Speaking Cyber-Truth: The CISO's Critical Role in Influencing Reluctant Leadership

By Craig Burland, CISO, Inversion6

In the C-Suites and boardrooms of modern enterprises, there's an unwelcome guest that often disrupts the conviviality of strategic discussions: cyber-truth. Cyber-truth is the unvarnished reality of risk delivered by the Chief Information Security Officer (CISO) that shines a light on current shortcomings, dampens the euphoria around new initiatives, and quells the enthusiasm for new ventures. As organizations tackle digital transformation, pursue critical certifications, or leverage modern capabilities like AI, the CISO's role in unveiling pitfalls and potholes is indispensable. Like Seuss' Lorax, the modern CISO must be the voice of cyber-truth.

"I am the CISO. I speak for the risks."

Facts about unpatched vulnerabilities, non-compliant practices, and unsecured applications are often met with skepticism at the senior levels of an organization. Requests to "prove the risk", quantify the

finer, or inflate business friction are some of the many tactics leaders follow to dismiss threats and move on with business. But the SEC's disclosure rules and recent actions up the ante for organizations choosing to ignore evidence, demanding that CISOs continue to convey the cyber-truths that leadership may be reluctant to face.

Short of running Monte Carlo simulations for every risk, CISOs must distill intricate technical risks into business impacts that resonate across the entire organization. Cyber security is a complex domain, replete with technical nuances that can be challenging for non-technical leaders to grasp. A successful CISO, therefore, must be bilingual, fluent in the languages of both technology and business. They must translate cyber risks into tangible business impacts -- potential losses in revenue, brand damage, or regulatory non-compliance. This requires a nuanced understanding of risk management, accepting that not all risks can be eliminated, but they can be managed to an acceptable level.

“I speak for the risks, for the risks have no tongues.”

However, it's not just about pointing out the problems, the CISO must also be a problem-solver. They must work collaboratively with other leaders to find ways to enable the business while protecting it -- providing insights and recommendations that allow others to make informed decisions based on the company's risk appetite and strategic direction. But the effectiveness of a CISO is not just measured by the absence of breaches; it's their ability to enable the business to take calculated risks confidently. The CISO must work to ensure that cyber security is built into the DNA of every project. They must advocate and champion secure-by-design principles to ensure that security is not an afterthought but a fundamental component of every initiative. By forcing organizations to acknowledge and address cyber risks proactively, CISOs not only protect the enterprise but also contribute to its resilience and long-term success.

CISOs also face the issue of risk prioritization. In an ideal world, every vulnerability would be patched, every threat neutralized, every alert investigated. However, resources are constrained, investments are finite, and not all risks are created equal. The CISO must often make difficult decisions about what to protect first, knowing that some areas will remain vulnerable. This requires a deep understanding of the business, ensuring that the most critical assets receive the highest level of protection. It requires negotiation, trading growth now for mitigation later. It requires discipline and organization, tracking exceptions granted to revisit risks accepted. Finally, it demands further transparency, making sure leaders understand and support the risk-reward calculation.

“Unless someone like you cares a whole awful lot, nothing is going to get better. It's not.”

Considering these responsibilities, the CISO's truth-telling is an act of strategic importance. Cyber-truths can no longer be sidelined or downplayed; they must be front and center in an organization's strategic decisions, day-to-day prioritization, and dialogue with the market and regulators. This transparency not only adheres to the letter of the law but also builds investor trust — showcasing the company's commitment to diligent risk management and operational integrity. Cyber-truth, while inconvenient, is now a commodity of public interest, scrutinized by investors and regulators alike. As digital risks morph into financial and reputational risks, the CISO's role evolves into that of a strategist, advocate, evangelist, and communicator – a calling that is essential for navigating the treacherous waters of the digital age. By

ensuring that organizations hear, understand, and acknowledge (even reluctantly) their cyber security risks and real cyber security posture – their cyber-truth -- CISOs uphold the pillars of trust and resilience that define today's corporate success.

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>.





Strengthening Financial Services: Embracing the Digital Operational Resilience Act (DORA) for Cybersecurity Resilience

By Boris Khazin, Head of Governance, Risk & Compliance at EPAM Systems, Inc.

While concerns about market volatility, liquidity management and fintech disruption are among the many challenges financial services organizations must carefully navigate, operational resilience and cybersecurity emerge as the two most significant non-financial risks they face today. The real-world after-effects of cyber-intrusions in the financial sector extend far beyond the balance sheets; they place personal data in the crosshairs of nefarious actors, potentially compromise financial accounts, and put the stability of entire organizations in serious jeopardy. Recognizing the tremendous impact of these consequences, international legislation and regulations are finally coming into play.

How We Got Here

An examination of insurance claims reveals that cyberattacks are the leading cause of value loss within the financial sector, a jarring indicator of the overall urgency of the situation. A combination of factors, including the COVID-19 pandemic, the unstoppable shift toward digitization and the global acceptance of remote work, have set the stage for an all-out digital crime wave. The ensuing threats to operational continuity range from cyberattacks and systemic failures to data theft and ransomware, not to mention the reputational harm financially inflicted on victimized financial institutions.

The Digital Operational Resilience Act (DORA): A Beacon of Hope

In response to the havoc wreaked by cyber thieves, a new regulatory framework out of the European Union (EU) aims to deliver financial institutions some much-needed peace of mind. Dubbed DORA for short, the Digital Operational Resilience Act explores ways to bolster the standards of digital resilience frameworks, with a particular focus on the way companies document cybersecurity incidents and manage third-party risks associated with information and communication technologies (ICT).

Officially adopted by the European Council last November, DORA urges organizations to implement comprehensive strategies to identify and effectively mitigate vulnerabilities. The legislation also stresses the significance of ICT incident reporting and advocates for the prompt reporting of cybersecurity incidents to allow for swift responses and containment measures.

DORA additionally mandates digital operational resiliency testing be conducted to ensure that systems have the appropriate security mechanisms in place to withstand cyberattacks and operational disruptions. Collaborative efforts in information and intelligence sharing are highly encouraged, as collective threat intelligence is a potent weapon in the battle against cyber adversaries.

Finally, ICT third-party risk management is a non-negotiable under DORA. As such, third-party providers must adhere to the same stringent cybersecurity standards as financial institutions to safeguard the integrity of the entire ecosystem.

An International Standard

Intent on becoming the global benchmark for operational resilience in the financial services industry, DORA has implications that extend far beyond Europe, addressing major challenges financial institutions face in protecting critical data and services for consumers around the world. The need for enhanced resilience is especially relevant in light of incidents such as the [SolarWinds breach](#), which exploited vulnerabilities in third-party software. With its comprehensive approach to cybersecurity, DORA underscores the vital need for increased scrutiny of external partners.

Best Practices for Resilience

Along with the EU Cybersecurity Act, Cyber Resilience Act, NIS 2 and General Data Protection Regulation (GDPR), DORA is one of many upcoming EU measures designed to enhance the security and stability of operations in the financial services sector. But legislation alone will not guarantee the end of cybercrime as we know it. To minimize exposure to cybersecurity risks, financial institutions can adopt these best practices:

- **Individual Awareness:** Provide full-bodied training and resources that empower employees to securely operate their systems.
- **Systems and Platform Security:** Establish a process of diligently and consistently reviewing and enhancing security capabilities. Implement Zero Trust tenets, including practicing the least privilege principle, breaking work into smaller units, always verifying access and implementing micro-segmentation, among others.
- **Ensure Business Continuity:** Prioritize areas that could disrupt operations to maintain seamless functionality.

The Road Ahead

While financial institutions grapple with issues surrounding cybersecurity and operational resilience, DORA offers a holistic framework to address these matters with an emphasis on incident reporting, third-party risk management and collaborative threat intelligence sharing. The financial sector must also adopt and enact best practices, including promoting individual awareness, securing systems and making business continuity a top priority. Through this combination of regulatory compliance and proactivity, financial organizations can ensure the security of their operations and the trust of their customers.

About the Author

Boris Khazin is Global Head of Digital Risk Management/Governance, Risk and Compliance at EPAM Systems, where he is passionate about providing solutions that deliver business value and exist at the intersection of people, processes and systems.

Mr. Khazin has more than 20 years of management, consulting and product development experience in the financial services and fintech sectors. During his tenure at EPAM, he has led several GRC, business intelligence, enterprise analytics and organizational capability/maturity assessments to help clients identify, define and prioritize frameworks that guide them toward a desired future state. From this, he has developed a keen understanding of opportunities and challenges that arise when organizations adapt to change. Previously, Mr. Khazin worked at multiple financial firms, including UBS, S&P and Bloomberg. He was also an Investment Oversight Officer at TD Ameritrade.

Mr. Khazin has a Bachelor of Science in Behavioral Economics from Pennsylvania State University and an MBA from Pace University.





The Case Study: The Exploitation of Mechatronics Systems

By Milica D. Djekic

The mechatronics systems are a common part of the industrial control systems (ICS) or – in other words – these two assets serve in many control engineering applications. The mechatronics systems exist many years back and they are only the phase in a development of control systems. In addition, they are a synergy of control, mechanical, electrical and computer systems. Through this modern time – these infrastructures are correlated with the web technologies and frequently use the internet to communicate with each other. Here, how over the control engineering and mechatronics we would come to an Internet of Things (IoT) concept. In this chapter, we would discuss how mechatronics paradigm has become the part of control engineering solutions and why it's important to understand its IoT side in order to stay cyber safe.

What are the mechatronics systems?

“Mechatronics” is a quite recent concept that would mainly affect the control engineering solutions. It's commonly correlated with the robotics, but nowadays it's more than a robotics. Basically, it's about smart systems which would use many sensors and measuring devices in order to make an intelligent decision.

The mechatronics is about the mix of control, mechanical, electrical and computer systems. Those solutions would so commonly get exposed to the internet and for such a reason they would deal with the next phase of their development and deployment and that's the IoT stage. It's well known that a number of sensors and the similar gadgets could improve any control system – especially if its designer has developed the smart control algorithm. The real technological intelligence would usually get connected with the adaptive systems getting the ability to deal with the unknown environment so intelligently. Right here, we would illustrate how some mechatronics system appears and how it could get applied in an industry. This illustration is provided through a Figure 1 as follows.



Figure 1. The mechatronics asset being used in an industry

Next, we would want to deal with some of the bases of a mechatronics concept. For instance, it's quite clear that these systems would use mechanical devices such as gears, frames, metal objects, robotics arms and so on. Also, they would get dependable on a power supply making these solutions dealing with the electrical systems. Finally, their control system would use the algorithm being saved within some computing unit and that's how such a solution would apply the commands and follow the instructions. The block diagram of such a mechatronics system is given in a Figure 2 as follows.

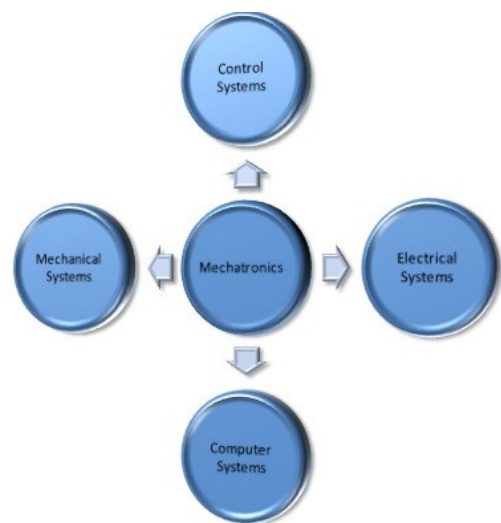


Figure 2. The mechatronics as a concept

Finally, we would realize that this concept is a consequence of the long-term evolutionary process that would improve our technological advancements. The role of the mechatronics systems is to make a solid basis to an industry as well as some home applications. The mechatronics is a quite complicated branch of technology and people dealing with its design, research, development and maintainace must be highly skillful. In such a case, it's vitally important to understand all the simple terms of that technology in order to deal with so at a more holistic level. Indeed, this sort of industry would require a multidisciplinary team of experts who would so deeply cope with their areas of expertise and make these systems work so accurately and intelligently.

The Shodan and the mechatronics solutions

Through this book's chapter mainly dealing with the practice – we would try to discuss how mechatronics systems could get correlate with one of the scariest search engines of today. In addition, it's quite clear that crawler is a Shodan and right here – we would attempt to explain how we could use such a tool to get familiar with the mechatronics systems. As we would suggest through the title of this chapter – the purpose of this segment is to indicate to all the weaknesses of mechatronics systems being exposed to the web as well as suggest some of the hacking strategies. So, let's start with the Shodan being our top crawler for the world of advanced technology. The first step of this research would get given in a Figure 3 as follows.

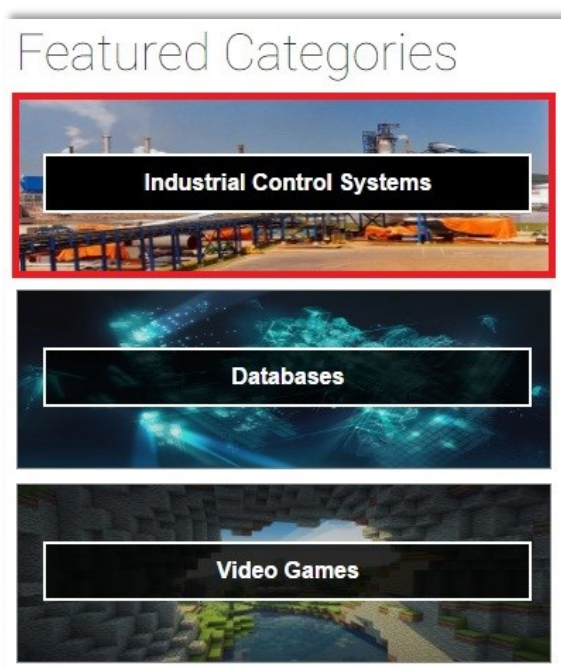


Figure 3. The Shodan's environment to industrial systems

As it's illustrated in a Figure 3 – the Shodan would offer us several featured options that could lead us to sections being ICS, Databases and Video Games. Right here, we would be deeply interested into the ICS as something which would rely on the mechatronics principles. As it's well known – for a required keyword, the Shodan would return us a certain IP address offering us an opportunity to try to exploit such

an asset. For such a purpose, it's necessary to get the adequate hacker's tools. We have talked a bit more about such an operation through the previous chapter. Using that chapter – we have deeply explained how software such as the Advanced IP Scanner and Radmin could get used in looking for the vulnerabilities of those IoT solutions. Finally, even that chapter has served to us in a better understanding of all Shodan's capacities being used either – for good or bad. Right here, we would illustrate through a Figure 4 what the next step in such a campaign could be.

Industrial Control Systems

Spotlight

XZERES Wind Turbine
 XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore

PIPS Automated License Plate Reader
 The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

Explore

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit

Figure 4. The Shodan's ICS environment

As it's illustrated via the Figure 4 – we would select the ICS being the wind turbines as a quite good case of mechatronics systems. It's also important to mention that the embedded systems could also be the part of mechatronics systems depending which sort of computing unit is used for a system's control. Further, the next stage in this explanation would be a click on the selected type of the wind turbines and through a Figure 5 – we would see how such an asset appears. The illustration is represented as follows.

The screenshot shows search results for 'XZERES Wind -- 442SR Wind Turbine'. On the left, there are filters for 'TOP COUNTRIES' (United States: 6), 'TOP ORGANIZATIONS' (Frontier Communications: 2, Westspace Cooperative Teleco...: 1, Rockspace Hosting: 1, Cogent Communications: 1, CloudFlare: 1), 'TOP OPERATING SYSTEMS' (Linux 3.x: 5), and 'TOP PRODUCTS' (Apache Httpd: 4, nginx: 1). The main results list three entries:

- XZERES Wind -- 442SR Wind Turbine** (Frontier Communications, United States, Spring Green) - Date: Fri, 24 Feb 2017 12:40:10 GMT, Server: Apache/1.3.31 (Unix), Last-Modified: Thu, 26 Jan 2012 22:53:27 GMT, ETag: "93532ae4f25065", Accept-Ranges: bytes, Content-Length: 814, Content-Type: text/html
- XZERES Wind -- 442SR Wind Turbine** (Cogent Communications, United States, Saint Cloud) - Date: Wed, 22 Feb 2017 07:33:08 GMT, Server: Apache/1.3.31 (Unix), Last-Modified: Fri, 30 Jan 2015 22:40:26 GMT, ETag: "58a-12e-56c088a", Accept-Ranges: bytes, Content-Length: 814, Content-Type: text/html
- XZERES Wind -- 442SR Wind Turbine** (Frontier Communications, United States, Conley) - Date: Mon, 20 Feb 2017 18:45:21 GMT, Server: Apache/1.3.31 (Unix), Last-Modified: Mon, 18 Mar 2013 16:28:06 GMT

Figure 5. The wind turbines as a part of Shodan's search

As you would see through the previous Figure – there would be many alternatives coping with the required criterion. The chapter before would illustrate us how we could hack an asset with the well-known IP address and authentication. In this case, we would deal with some IP address and no authentication, so our task would get a bit complicated. The majority of hackers would firstly try to do some guessing in order to break into a system. Also, there are some tools on the black market that would offer a chance to

obtain someone's login details. Finally, we would realize that some of the IoT systems would not use any protection, so the hackers would so easily get an access to that asset.

How to remain cyber safe?

In this modern time, it's quite challenging to remain cyber safe. Through this learning material – we would discuss how it's simple to organize some hacking attack, so the question here would be if there is any chance to avoid a cyber breach. The fact is these sorts of attacks are happening anywhere and anytime and the point is that you would accept that your IT asset got breached or not. As we said – it's something that is occurring constantly, so we would strongly recommend taking care about your cybersecurity and try to follow the best procedures and policies in order to maintain the risk at an acceptable level. Also, it's significant to say that the good defense is about the proper risk management and the point is not how to avoid the attack, but rather how to respond to so. Finally, it's about the never-ending competition between the force of defense and the force of attack.

The conclusions

At the end, we would show through this book's chapter how it's possible to exploit even mechatronics systems being the part of ICS and so commonly the entire critical infrastructure. The mechatronics is only one of the stages in a development and deployment of our technological improvements and today – it's combined with the IoT technology. The purpose of this chapter is to indicate that even mechatronics systems got some weaknesses and the task of an expert's community should be to try to overcome those vulnerabilities and make much stronger and more reliable solutions.

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 Pitfalls of Periodic Penetration Testing & What to Do Instead

Periodic penetration testing approaches can be likened to regular tire inspections for vehicles. While they provide valuable insights into the condition of your tires during each check-up, they cannot help you identify any potential issues that may arise in between inspections.

By Erik Holmes, CEO, Cyber Guards

Organizations often rely on traditional approaches like snapshot in time-based penetration testing to mitigate the risk of cyber attacks. However, these methods have limitations and may not comprehensively understand the organization's security posture.

In this article, we will explore the pitfalls of periodic penetration testing and suggest adopting a continuous testing approach and implementing attack path management to enhance your organizations cyber defense strategy.

The constraints of snapshot in time penetration testing

Periodic penetration testing has been a standard practice for many organizations, but is it the best approach for cybersecurity assessment? One major constraint of this method is that it can only provide a snapshot of the organization's security posture at a specific point in time. This means new vulnerabilities arising after the testing period will be left undetected. Case in point, according to the 2022 Cost of a Data Breach report, it takes an average of 277 days to identify and contain the breach.

Another limitation of periodic penetration testing is its reliance on time-based testing, where testers are given a specified amount of time to identify vulnerabilities. This approach does not account for some of the more complex and advanced attacks that may require additional time to uncover.

Traditional penetration testing involves manual testing by security experts with varying skill levels. This snapshot testing adds a constraint on the accuracy of the results, which significantly depends on the testers capabilities. A single mistake or oversight from the testers can lead to costly breaches.

Lastly, periodic penetration testing offers limited scope when assessing an organization's entire security landscape. The manual testing process can only cover specific areas of the organization's network, leaving other areas untested.

How to embrace continuous cybersecurity testing

While periodic penetration testing can provide a snapshot of your organization's security posture, it often fails to account for the dynamic nature of cyber threats. Organizations must continuously test their security measures to effectively mitigate risks to identify and neutralize emerging threats in real-time.

Organizations can leverage various approaches and tools to implement continuous cybersecurity testing, such as the Atomic Red Team by Red Canary, an open-source library of tests mapped to the MITRE ATTACK framework that security teams can use to simulate adversarial activity and validate their defenses. These tools can help prioritize and mitigate potential cyber-attacks by automating security testing and providing valuable insights into adversary tactics and techniques.

Endpoint security testing and firewall testing are excellent starting points for implementing continuous cybersecurity testing. By simulating phishing emails, running PowerShell commands at endpoints, and monitoring VPN logins at the firewall level, organizations can proactively identify potential vulnerabilities and mitigate them before cyber attackers can exploit them. Proofpoint's 2021 State of the Phish Report revealed that 57% of organizations dealt with at least one successful phishing attack in 2020. These statistics underline the importance of continuous cybersecurity testing, particularly in the area of simulated phishing, to detect and mitigate such threats promptly.

Ultimately, embracing continuous cybersecurity testing is vital to securing your organization and safeguarding your valuable assets. With the right tools and strategies, organizations can identify and neutralize threats in real-time, stay ahead of the curve, and protect their systems and data from cyber threats.

The role of attack path management in cyber defense

The role of attack path management in cyber defense cannot be overstated. Attack path management takes a contextual and holistic approach to protecting critical assets in a way that traditional security solutions do not. While continuous security testing evaluates controls in place, attack path management takes a more comprehensive view to identify an organization's most critical assets and networks.

Attack path management can help organizations understand their business operations deeply, identifying the most vulnerable areas requiring more security measures. By pinpointing areas within a network where sensitive data, such as PHI or PII, may exist, attack path management can help organizations identify and eliminate risky pathways that attackers can use to target valuable assets. This is particularly important in today's environment, where the interconnectivity of networks makes identifying and mitigating potential attack paths incredibly challenging.

While continuous security testing plays a vital role in cybersecurity by evaluating the effectiveness of security controls, sometimes the testing can miss vulnerabilities or gaps in the network. Attack path management fills this gap by providing context to your security environment, allowing a more complete and accurate assessment of your defense mechanisms.

To embrace attack path management in your organization without causing harm to your system's environment, Cyber Guards suggests platforms like XM Cyber for Attack Path. It's important to note that organizations should not test in a production environment without permission.

Attack path management and continuous security testing complement each other effectively. By adopting both methodologies, organizations can assess their vulnerabilities comprehensively, eliminate potential attack paths, and fine-tune their defense mechanisms confidently. Ultimately, this will help organizations improve their cyber defense posture, reduce the risk of successful attacks, and protect their critical assets and data.

Embracing Innovation: Approaches for Comprehensive Cybersecurity

Embracing continuous cybersecurity testing can help organizations stay one step ahead of threat actors by ensuring no gaps in their understanding of their security posture, making it much more difficult for attackers to find and exploit security weaknesses. Furthermore, complementing continuous testing with attack path management allows organizations to take a contextual approach to protect their critical assets, fine-tuning their defense mechanisms and reducing the paths attackers might use to target valuable assets. By exploring innovative approaches beyond traditional methods to safeguard against potential security breaches, organizations can confidently navigate the ever-changing landscape of cybersecurity and mitigate risks more comprehensively.

About the Author

Erik Holmes is the chief executive Officer at Cyber Guards, a Memphis-based managed cybersecurity services company. Erik brings an impressive dossier to the table, from serving in SEAL Team Six to holding key positions at BlackHorse Solutions and Deloitte Consulting. Drawing from this rich experience, Erik offers profound insights into cybersecurity.

Erik can be reached at erik.holmes@cyberguards.com and at Cyber Guard's website <https://cyberguards.com/>.





The Quantum Shift

Preparing Cybersecurity for a New Era

By Sercan Okur, VP of Technology, NextRay

In contrast to my previous pieces, I intend to commence this piece with a hypothetical calamitous situation. Suppose that in the year 2030, a significant global incident occurs, showcasing the capricious and devastating potential of quantum computing when wielded by malicious actors. Through the implementation of a meticulously strategized quantum computer assault on a nation's vital infrastructure, a collective of cyber assailants possesses the capability to expose the confidential information of a sovereign entity or induce severe economic and political devastation by causing the breakdown of banking systems and the incapacitation of power grids. In this particular instance, asserting that no cyber assault has hitherto inflicted such profound consequences could be deemed a highly assertive claim.

The perilous assault conducted by these digital marauders was not a unique occurrence; rather, it marked the initiation of a sequence of attacks, with each subsequent one inflicting greater devastation than its predecessor. The ongoing series of attacks poses a significant threat to both national security and public safety. These incidents highlight a potential scenario in which quantum computers may emerge as a formidable weapon capable of causing widespread harm, leading to the disruption of social order and the paralysis of governments.

Furthermore, while contemplating the potential occurrence of an attack amongst a natural calamity, the ramifications can be exacerbated, as the endeavor to avert or alleviate the impacts of said attack can

become exceedingly arduous. The convergence of natural and digital calamities might give rise to unparalleled difficulties, placing significant strain on national resources and examining the durability of societal frameworks.

Given the current state of rapid technological advancements, it is imperative to acknowledge the existence of quantum hazards and possess a thorough comprehension of their potential ramifications. In order to effectively navigate the contemporary landscape of digital warfare, characterized by a complex network of binary code as opposed to traditional physical terrains, it is imperative for nations to adopt progressive techniques and inventive approaches. Through an in-depth exploration of this narrative, our objective is to illuminate the significant ramifications of quantum attacks and uncover the multifaceted approaches required to fortify our defenses against the imminent quantum threat.

The potential impact of advanced quantum computer attacks on nations was exemplified by the chaotic event of 2030, highlighting the significant and irreparable harm that cyber threats pose to governments. It is imperative for governments to acknowledge and appreciate the diverse range of cyber risks that have the potential to jeopardize national security, economic stability, and public welfare. The expeditious and efficacious resolution of concerns pertaining to the disclosure of sensitive data, the interruption of vital infrastructures, and the devastation of financial systems is imperative.

Can these systems be utilized for defense applications?

In light of the imminent cyber threats, the potential implementation of Post Quantum Cryptography (PQC) emerges as a potential savior, presenting novel solutions and resilient safeguards within the realm of cybersecurity. It is possible that this assertion holds some validity. The use of quantum-resistant cryptographic algorithms, in lieu of the current algorithms employed in both hardware and software systems, has the potential to facilitate the establishment of robust and secure infrastructures, hence mitigating the risk of potential assaults. The attainment of post-quantum readiness is of utmost importance in the establishment of a secure and resilient digital environment.

The cost and estimation of currently available qualified human resources.

The potential advantages of Post-Quantum Cryptography are substantial; yet, the process of moving to a quantum-resistant environment necessitates substantial financial resources and the cultivation of a highly skilled workforce with specialized expertise. It is imperative for governments and states to commit sufficient resources towards research and development, workforce training, and infrastructure enhancement in order to effectively assist the smooth adoption of quantum-resistant cryptographic systems. The development of a proficient and well-informed labor force is of utmost importance in effectively navigating the intricate realm of quantum computing and cryptography, promoting ingenuity, and upholding a competitive edge in the international sphere.

Suggestions for Governments:

In order to effectively address the complex challenges posed by quantum threats, it is imperative for states and governments to adopt a comprehensive and multifaceted strategy. This strategy should commence with the identification and prioritization of sectors that are vital and susceptible to such threats. Furthermore, it is crucial to emphasize the significance of establishing collaborative frameworks that involve academia, industry, and international organizations, alongside strategic investments in research, development, and teaching. It is imperative for governments to develop all-encompassing plans that incorporate regulatory measures, standardization efforts, public awareness campaigns, and capacity building programs. These strategies aim to enhance national cybersecurity postures and foster a safe and resilient digital landscape.

The scenario of a quantum computer assault in 2030 highlights the pressing necessity for proactive and collaborative endeavors to safeguard against the escalating risks posed by quantum technology. Post-quantum cryptography represents a groundbreaking paradigm that presents novel and efficacious approaches to safeguarding the digital realm and preserving national security concerns. However, the achievement of a quantum-safe world necessitates substantial financial commitments, cooperative endeavors, proficient personnel, and strategic foresight. The implementation and incorporation of quantum-resistant cryptographic solutions by nations and governments can enhance their defensive capabilities, safeguard their sovereignty, and establish a foundation for a secure and prosperous future in the era of quantum technology.

About the Author

Sercan Okur is a highly skilled professional with a strong focus on cybersecurity and artificial intelligence. With a wealth of experience in the information technology sector, Sercan has developed a deep understanding of the complex interplay between cybersecurity and AI, striving to stay at the forefront of emerging trends and advancements. His expertise in these areas has enabled him to tackle challenging projects, implement innovative solutions, and contribute to the growth of the cybersecurity industry. As a thought leader and dedicated expert, Sercan actively engages with the professional community on platforms such as LinkedIn, sharing his insights and knowledge in cybersecurity and AI, while fostering collaboration and staying connected with fellow industry experts.

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





The Role of Identity Data Management in Achieving CISA'S Strategic Goals

By Wade Ellery, Field Chief Technology Officer at Radiant Logic

Cyber threats such as ransomware, zero-day exploits, phishing and supply chain attacks are increasing globally, regardless of industry or size. At the heart of this growing risk is identity, with over [60% of all breaches](#) today involving identity exploitation.

As organizations continue to expand their digital footprints, driven by a move towards cloud resources and remote systems, their identity data, both at a device and user level, also grows. Consequently, the attack surface also expands, giving threat actors more scope to leverage identity vulnerabilities and gain access to critical systems. So, amidst this expanding threat vector, the conventional 'fortress mentality' falls short, requiring businesses to urgently re-think their security strategies.

This urgency is also emphasized by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), as the organization has recently recalibrated its [strategy](#), aligning with [Biden's National Cybersecurity Strategy](#) to create a unified front against cyber threats.

This collaboration marks a paradigm shift, recognizing that traditional defense mechanisms must evolve. As CISA observes, the success of cyberattacks is often "enabled by an environment of insecurity," a flaw exacerbated by our collective blind spots concerning identity and its related data. Reducing these blind spots requires a greater focus on effective identity data management.

How Identity Data Management Addresses CISA's Three Pillars

CISA's updated strategic plan focuses on enabling businesses to achieve three core objectives: addressing immediate threats, hardening the terrain and driving security at scale. The agency wants these pillars to be the foundation of every business's security strategy. So, how can effective identity data management help organizations achieve this?

When we talk about immediate threats, ransomware and phishing instantly come into the conversation. The ransomware attack rate is breaking records yearly, while [74% of breaches](#) still include phishing or social engineering elements. Identity data management provides a proactive approach to addressing these threats.

Expanding our understanding beyond just human identities to include the identities of servers, applications and systems can help to identify which systems or users are more vulnerable to such attacks. It allows a better scope for enabling targeted training and applying layered authentication and access control on specific devices and user repositories to mitigate immediate risks.

Hardening the terrain requires management across the entire IT ecosystem and across every network element. Every component in our IT infrastructure—people, servers, applications—has an identity. To create an impenetrable defensive posture and a rock-solid network terrain, we must manage, monitor and administrate these identities. When each identity is meticulously managed, the likelihood of external spoofing and unauthorized access diminishes. Essentially, the terrain becomes more resilient to an array of attacks, making it harder for adversaries to exploit vulnerabilities.

Also, when it comes to driving security at scale, monitoring these identities across the IT infrastructure allows for automation and real-time responses, thus scaling security measures effectively. For instance, managing the identities of every connected device in an organizational network can streamline permissions, ensuring only authorized devices and users interact in real-time.

Gaining visibility into how identities can be used to access sensitive data and systems is critical for getting ahead of threats. A recent report from [Gartner](#) highlights that quality identity data is critical for successful security projects and scaling access controls across complex IT environments.

Identity management is imperative for a robust zero-trust architecture

CISA's updated strategy is primarily intended to align with Biden's National Cybersecurity Strategy, which [mandated](#) the implementation of Zero Trust for all government organizations by 2024. Zero Trust has emerged as an industry standard for combatting modern security challenges as it enforces two-factor authentication as a baseline, thereby reducing the chances of unauthorized access. And yet, even two-factor authentication can be manipulated, which brings us back to the importance of robust identity management.

Identity data informs Zero Trust protocols at every stage. It allows for dynamic authorization, where rights and privileges are not granted *en masse* but are provided on a need-to-access basis. Think of it as moving from a cash-based system to a card-based system in your security strategy. You no longer carry "bags of money" (or unfettered access); instead, you operate with a "credit card" (or rights just-in-time), constrained by spending limits or operational permissions.

Therefore, understanding the true nature of identity data—including the identity of users, services, applications and devices—is paramount for setting up a Zero Trust architecture.

How to achieve greater visibility over all identity data points

Firstly, organizations need to develop a clear understanding of what identity data is. One major issue that tends to be overlooked in cybersecurity discussions, even by esteemed organizations like CISA, is the nuanced role of identity that extends beyond human users. When we say "identity," it's not just about 'John Doe' accessing his workstation. It's also about a specific microservice querying a database or an IoT device reporting metrics. Essentially, every subject moving through the digital environment to access resources must be managed, authenticated and authorized.

To implement a genuinely robust security posture, the quality of the identity data is also paramount. It's no longer enough to base access control on static, rarely updated information. A dynamic and real-time approach is required, utilizing the most current data to inform every access decision.

The repercussions of poor-quality identity data can be devastating for a business's security infrastructure. A telling example is the role of privileged accounts in security breaches; a [2021 survey](#) revealed that 74% of organizations that fell victim to cyberattacks claimed that their privileged accounts were involved. These accounts often provide access to the most sensitive and confidential resources, making their protection imperative.

Imagine that due to a vulnerability in your system, an employee's title is changed to CFO. This change could give them access to highly sensitive payroll and financial information, thereby posing a significant security risk. The same logic applies to applications, devices and services. Therefore, the integrity of identity data becomes the bedrock upon which all your network security policies should be built.

Furthermore, policy-based access control, whether for network entry or intra-network activities, should be tied to accurate, up-to-date data. Implementing robust procedures to ensure data accuracy and continuously auditing and monitoring identity data can thwart attempts to corrupt the system. It's not just about building effective access policies anymore; it's about ensuring the underlying data used to enforce those policies is rock-solid.

Overall, in today's era of advanced persistent threats, security isn't solely about constructing barriers; it's about understanding and verifying identities at a granular level across the organization. This approach demands meticulous attention to the quality, visibility and continuous monitoring of identity data. Any compromise in this aspect does not just signify a loophole—it threatens to unravel the entire fabric of an organization's security infrastructure.

About the Author

Wade Ellery is the Field Chief Technology Officer with Radiant Logic. Wade has over 20 years of increasing responsibility and experience in Enterprise IT direct and channel software and services sales and management. He holds in-depth knowledge and experience in enterprise IAM, IAG, Risk and Compliance, and IT Security products.

www.radiantlogic.com





Three Key Threats Fueling the Future of Cyber Attacks

By Rishi Baviskar, Global Head of Cyber Risk Consulting at Allianz Commercial

Improvements in cyber security and business continuity are helping to combat encryption-based ransomware attacks, yet the cyber threat landscape is continually evolving. 2023 has seen a worrying resurgence in ransomware and extortion claims, resulting in an uptick in costly incidents, demonstrating that although progress is being made, the threat posed by ransomware shows little sign of abating.

Reports note that the number of ransomware victims surged by as much as 143% globally during the first quarter of 2023 with January and February seeing the highest number of hack and leak cases in three years. Ransomware alone is projected to cost its victims approximately US\$265bn annually by 2031.

Protecting an organization against intrusion remains a cat and mouse game, in which the cyber criminals have the advantage. Threat actors are now exploring ways to use artificial intelligence (AI) to automate and accelerate attacks, creating more effective AI-powered malware and phishing. Combined with the

explosion in connected mobile devices and 5G-enabled Internet of Things, the avenues for cyber-attacks look only likely to increase in the coming years.

As a global insurer, Allianz Commercial monitors the emerging threat landscape and assists its clients with mitigating these risks. Here are three key cyber threats currently on our radar:

1. Artificial Intelligence

Artificial intelligence (AI) is widely expected to power future ransomware attacks, with automated attack processes, more convincing phishing, and faster malware development. However, it could also enhance cyber security, with more effective and faster detection and threat intelligence.

Threat actors are already using AI-powered language models like ChatGPT to write code. Generative AI can help less technically proficient threat actors write their own code or create new strains and variations of existing ransomware, potentially increasing the number of attacks they can execute. We can expect an increased utilization of AI by malicious actors in the future, necessitating even stronger cyber security measures.

Voice simulation software has been a recent addition to the cyber criminal's arsenal. In 2019, the CRO of a British energy provider transferred €220,000 to a scammer after they received a call from what sounded like the head of the unit's parent company, asking them to wire money to a supplier. The voice was generated using AI. In August 2023, researchers at the Google-owned cybersecurity company Mandiant documented the first known instances of deepfake video technology designed and sold for phishing scams. The going rate was as little as US \$20 per minute, US \$250 for a full video or US \$200 for a training session, although the researchers were unable to confirm that the services they identified on hacker forums were legitimate or whether a deepfake has been used in any scam.

AI will help threat actors, but it is also a powerful tool for detection. We might see more AI-enabled incidents in the future, but investment in detection backed by AI should catch more incidents early. If we can keep pace with developments in AI, there is always the chance it might not change the picture too much from today, neither in favor of the company nor the attacker.

2. Mobile Devices

Lax security and the mixing of personal and corporate data on mobile devices, including smartphones, tablets and laptops, is making for an attractive target for cyber criminals. Allianz Commercial has seen a growing number of incidents caused by poor cyber security around mobile devices. During the pandemic many organizations enabled new ways of accessing their corporate network via private devices, without the need for multi-factor authentication (MFA). This also resulted in a number of successful cyberattacks and large claims.

Cyber criminals are now targeting mobile devices with specific malware in order to gain remote access, steal login credentials, or to deploy ransomware. Increasingly we have corporate and personal

information on the same device, and threat actors now see this as a potential vulnerability. Personal devices, in particular, tend to have less stringent security measures. Utilizing public wi-fi on these devices can increase their vulnerability, including exposure to phishing attacks via social media.

The roll out of 5G technology is also an area of potential concern. 5G will power more connected devices, including more sophisticated applications, such as driverless or assisted vehicles and smart cities. However, IoT devices do not have a good track record when it comes to cyber security. Many IoT devices are not inherently secure, while the sheer number of these devices globally and the addition of AI could result in a very serious cyber threat. Many of these devices are easily discoverable and will not have MFA mechanisms. Even today we see devices with default passwords that are available on the internet.

3. Skill Shortage

A growing shortage of cyber security professionals will increasingly complicate cyber security efforts, potentially increasing the chances of successful attacks in the future. The current global cyber security workforce gap stands at 3.4 million people, according to the ISC2, a non-profit member organization for cyber security professionals, with demand for cyber professionals growing twice as fast as supply. Some 70% of organizations say they do not have enough cyber security staff to be effective. Gartner predicts that a lack of talent or human failure will be responsible for over half of significant cyber incidents by 2025.

There is a crisis in technical skills for cyber security. Because technology is moving so fast, there are not enough experienced people to keep pace with the threats. It's very hard to get good cyber security engineers, which means companies are more exposed to cyber events. Without skilled cyber security people, it is harder to predict and prevent incidents, which could mean more losses in the future. The shortage of cyber security experts also impacts the cost of responding to a cyber incident. According to the IBM Cost of a Data Breach Report 2023, organizations with a high level of security skills shortage had a US\$5.36mn average data breach cost, around 20% higher than the average cost.

Preventing a cyberattack is becoming harder, and the stakes higher. As a result, early detection and response capabilities are becoming ever more important. An intrusion can quickly escalate, and once data is encrypted and / or stolen, the consequences and costs snowball – costs can be as much as, or even more than, 1,000 times higher than if an incident is not detected and contained early, Allianz analysis shows. Ultimately, early detection and effective response capabilities will be key to mitigating the impact of cyberattacks and ensuring a sustainable insurance market going forward.

About the Author

Rishi Baviskar is Global Cyber Experts Leader, Risk Consulting at Allianz Global Corporate & Specialty. Baviskar has experience working within the IT field for large oil, gas, automotive and pharmaceutical companies. In his previous roles, he has worked across all levels of process development, ranging from onsite engineer to the design and implementation of cyber security policies.

Rishi can be reached online at Rishi.Baviskar@agcs.allianz.com and at our company website www.agcs.allianz.com.





EVENTS



26th International Cybersecurity Conference

SECURE ECOSYSTEM: STRATEGIC, PRAGMATIC, FUTURISTIC

28TH NOV – 1ST DEC 2023 | HOTEL GRAND HYATT DUBAI

A Cybersecurity Conference where both Threat Researchers and CISOs Share Their Expertise!

Threat Research Presentations

The Latest Research on Identifying and Countering Emerging Threats

- Cyber Forensic Investigations
- EDR/XDR Evasion Techniques and Mitigations
- 0-days and High-Impact Vulnerability Exploitation
- ML and Big Data in Cyber Security
- Threat Intelligence Based Protection and many more!

CISO Panel Discussions

What CISOs Must Prioritize in a Digitally Transformed World

- Improving Data Security in the Digital-first Enterprise
- Positioning Cyber Security as a Contributor to Stakeholder Value
- Mitigating Cyber Risk from Geopolitical Tensions



Gain Knowledge from and Network with the Luminaries of the Cyber Security Industry!

Register for AVAR 2023 at

www.aavar.org

Conceptualized
& Organized by

A stylized graphic for the TX DIALOGUE logo, featuring overlapping geometric shapes in purple, orange, blue, and green.

TX DIALOGUE

CREATING EXCEPTIONAL EXPERIENCES,
TRANSFORMING BUSINESS OUTCOMES

7TH DECEMBER 2023 | MUMBAI, INDIA

www.txdialogue.com



BRING

THE WORLD

TOGETHER

8th, 9th, And 10th Of December

TechSummit23

Expo Center, Lahore.



#GISEC | CYBER.GISEC.AE

THE SUPER CONNECTOR FOR THE MIDDLE EAST & AFRICA'S CYBER SECURITY COMMUNITY

SCAN ME



GISEC is the ideal cybersecurity platform to participate & partner with vendors and government entities in the region.

H.E. DR. MOHAMED AL-KUWAITI

Head of Cyber Security,
United Arab Emirates Government



ENQUIRE ABOUT EXHIBITING, SPONSORSHIP & SPEAKING OPPORTUNITIES: +971 (04) 308 6469 | GISEC@DWTC.COM

HOSTED BY



OFFICIAL GOVERNMENT
CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



OFFICIAL DISTRIBUTION
PARTNER



PLATINUM SPONSOR



GOLD SPONSOR



ORGANISED BY





ITS World Congress

16-20 September 2024

Mobility Driven by ITS



ITS World Congress | 16-20 September 2024 | Dubai World Trade Centre

YOUR VOICE, OUR FUTURE

Be the catalyst of change and shape tomorrow's mobility with your contribution! Present groundbreaking research, showcase visionary projects, and drive dynamic discussions in the Technical Programme of the 2024 ITS World Congress.

Submit by 15 December 2023

More info: itscongress.com/technical-programme



ORGANISED BY



CO-ORGANISED BY



HOSTED BY



SUPPORTED BY





CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

[CyberDefense.TV](https://www.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.

The Interviews

These anticipated **"CEO Hotseat"** Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Miliefsky**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

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.](#)

Copyright (C) 2023, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com, and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide.

marketing@cyberdefensemagazine.com

All rights reserved worldwide. Copyright © 2023, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at

marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

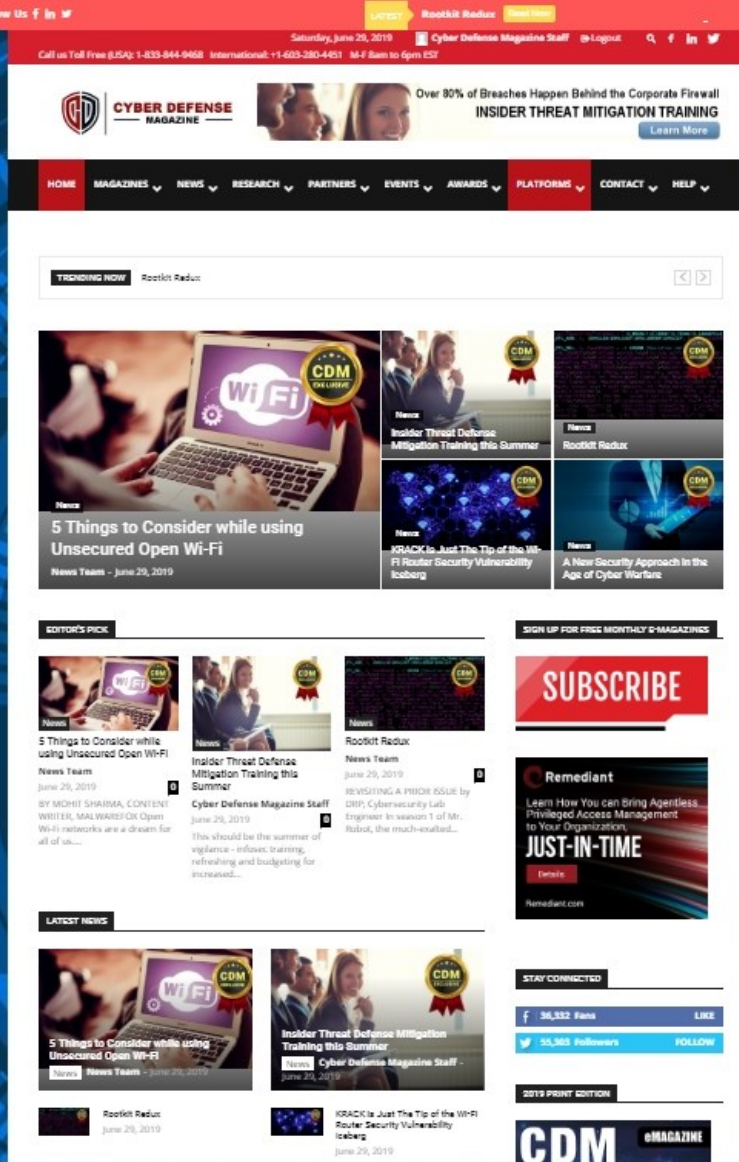
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 12/04/2023



Books by our Publisher: <https://www.amazon.com/stores/Gary-Miliefsky/author/B07KQJM1GP> (with others coming soon...)

12 Years in The Making...

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and [CyberDefenseMagazine.com](https://cyberdefenseconferences.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
CONFERENCES**

CYBERDEFENSECON 2024
CISOs INNOVATORS BLACK UNICORNS

12
YEARS
ANNIVERSARY

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefenseemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert





CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER



www.cyberdefensetv.com

www.cyberdefenseradio.com

www.cyberdefenseawards.com

www.cyberdefenseconferences.com

www.cyberdefensemagazine.com

RSAConference™2024

San Francisco | MAY 06-09 | Moscone Center

**Stronger
Together**

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

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , 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 <https://www.rsaconference.com/>

#RSAC



FOLLOW US



*** with help from writers
and friends all over the Globe.**