CYBER DEFENSE MAGAZINE

eMAGAZINE

JANUARY 2023

In This Edition

4 Key Security Trends For 2023

New Threat Report Shows Attackers Increasingly Exploiting MFA Fatigue

The Future of Online Privacy

…and much more…

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

Dear Friends,

Looking ahead to the new year, and ahead to the next, from the Publisher's desk we see both continuation of old trends and initiation of new ones. Data breaches and ransomware attacks have become even more pervasive, and this year will be no exception. As a result, there is a heightened concern with cybersecurity, and cyber safety is the top priority.

We would like to reiterate that Cyber Defense Media Group offers various ways to recognize and promote providers of cybersecurity solutions. As we begin the new year, this is the perfect time to showcase your solution worldwide, and to distinguish your organization from your competitors.

In response to this need, we have launched the Global Infosec Awards nomination process for 2023 at www.cyberdefenseawards.com. We are looking for the best and the brightest in the innovators who are changing this shape and scope of the Cyber Defense landscape, to help our industry get one step ahead of the next threat. We welcome your participation in this industry-leading award program.

We also wish to bring to the attention of our readers the opening of our Women In Cybersecurity Scholarship Fund for 2023. More information on applying is posted at https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-fund-for-2023/.

As always, the view from the Publisher's desk continues to focus on cutting-edge responses to the growing threats to our national and international cybersecurity. With the support of our contributors and readers, we continue to pursue our mission as the premier publication in cybersecurity.

Warmest regards,

Gary S. Miliefsky

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

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

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

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

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

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://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 January 2023 Issue

From the Editor-in-Chief

As we start the new year in the practice of cybersecurity, we continue to face a growing multitude of cyber threats growing in both frequency and complexity. These attacks are launched against government, critical infrastructure, private organizations (both for profit and non-profit), academic institutions, and even individual consumers. By all indications, they will continue to expand in every way.

Among cybersecurity professionals, this presents both a threat and an opportunity. Success will be based on capabilities, current knowledge, and the ability to make and deliver on promises of minimizing the risks of cyber incursions.

In this January issue of Cyber Defense Magazine, we are pleased to provide dozens of relevant new articles on cybersecurity capabilities responding to the array of cyber challenges. Our mission in the marketplace of ideas and capabilities is to assure that Cyber Defense Magazine offers the most comprehensive and valuable forum for cybersecurity professionals.

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

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

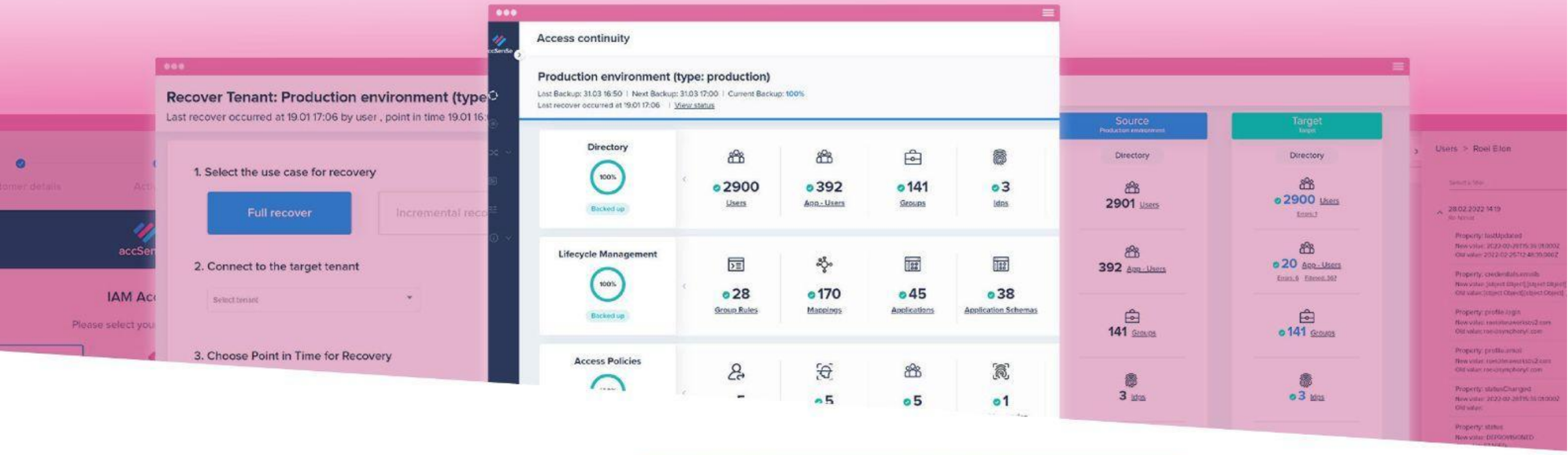
Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author 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

accSenSe

A complete protection and recovery solution for your organization's most critical SaaS.

(Your IAM WF and CIAM)



Recover Tenant: Production environment (type

Last recover occurred at 19.01 17:06 by user , point in time 19.01 16:

1. Select the use case for recovery

Full recover | Incremental reco

2. Connect to the target tenant

Select tenant

3. Choose Point in Time for Recovery

Access continuity

Production environment (type: production)

Last Backup: 31.03 16:50 | Next Backup: 31.03 17:00 | Current Backup: 100%

Last recover occurred at 19.01 17:06 | View status

Directory 100% Backed up	2900 Users	392 App - Users	141 Groups	3 Idps
Lifecycle Management 100% Backed up	28 Group Rules	170 Mappings	45 Applications	38 Application Schemas
Access Policies		5	5	1

Source Production environment	Target Target
Directory	Directory
2901 Users	2900 Users Errors: 1
392 App - Users	20 App - Users Errors: 6 Filtered: 367
141 Groups	141 Groups
3 Idps	3 Idps

Users > Roei Elon

28.02.2022 14:19

Property: lastUpdated

Property: credentials.emails

Property: profile.login

Property: profile.email

Property: statusChanged

Property: status

New value: DEPROVISIONED

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

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

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

monday.com GLASSBOX bright data fiverr.

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

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

START A 30-day TRIAL >>

https://accsense.io

i2Chain

Ready, set, Chain.

Convert MS Office, Adobe, images, and design document into non-fungible, traceable, hack-proof artifacts.

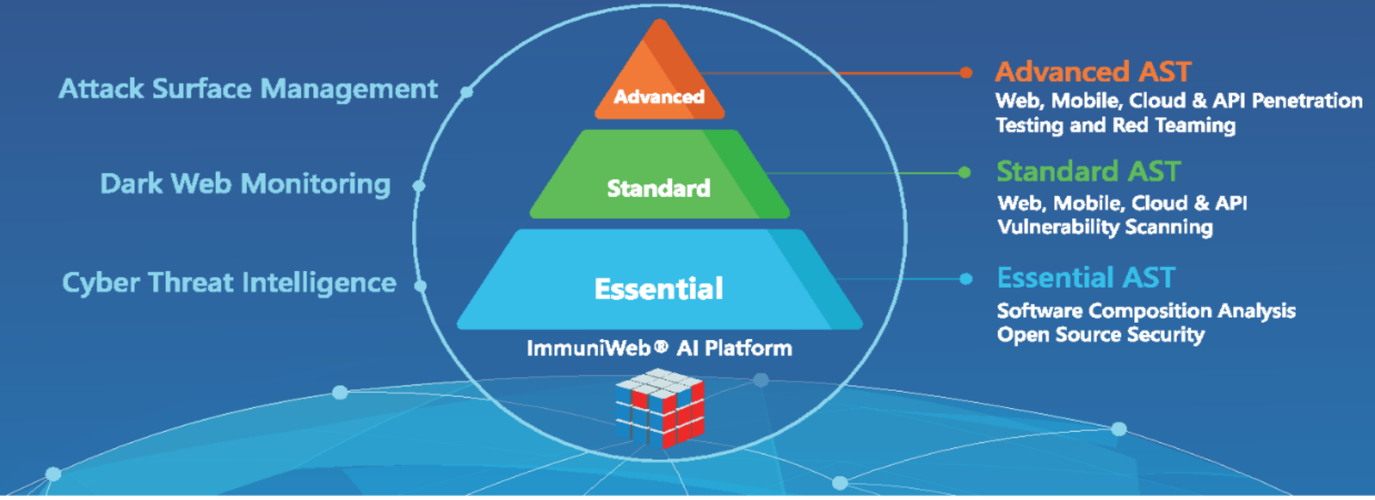
Encrypted store and compliant share using i2Chain APIs.

ImmuniWeb®

AI for Application Security

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

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



Attack Surface Management

Dark Web Monitoring

Cyber Threat Intelligence

Advanced

Standard

Essential

ImmuniWeb® AI Platform

Advanced AST
Web, Mobile, Cloud & API Penetration Testing and Red Teaming

Standard AST
Web, Mobile, Cloud & API Vulnerability Scanning

Essential AST
Software Composition Analysis
Open Source Security

ImmuniWeb® Discovery

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

ImmuniWeb® Neuron

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

ImmuniWeb® On-Demand

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

ImmuniWeb® MobileSuite

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

ImmuniWeb® Continuous

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

One Platform. All Needs.
www.immuniweb.com

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

SCawards EUROPE Winner
Best Usage of Machine Learning and AI

AIFINTECH 100

Gartner peerinsights™
★★★★★
4.8 out of 5

Phylum

The Software Supply Chain Security Company

Stop Software Supply Chain Risk at the Source

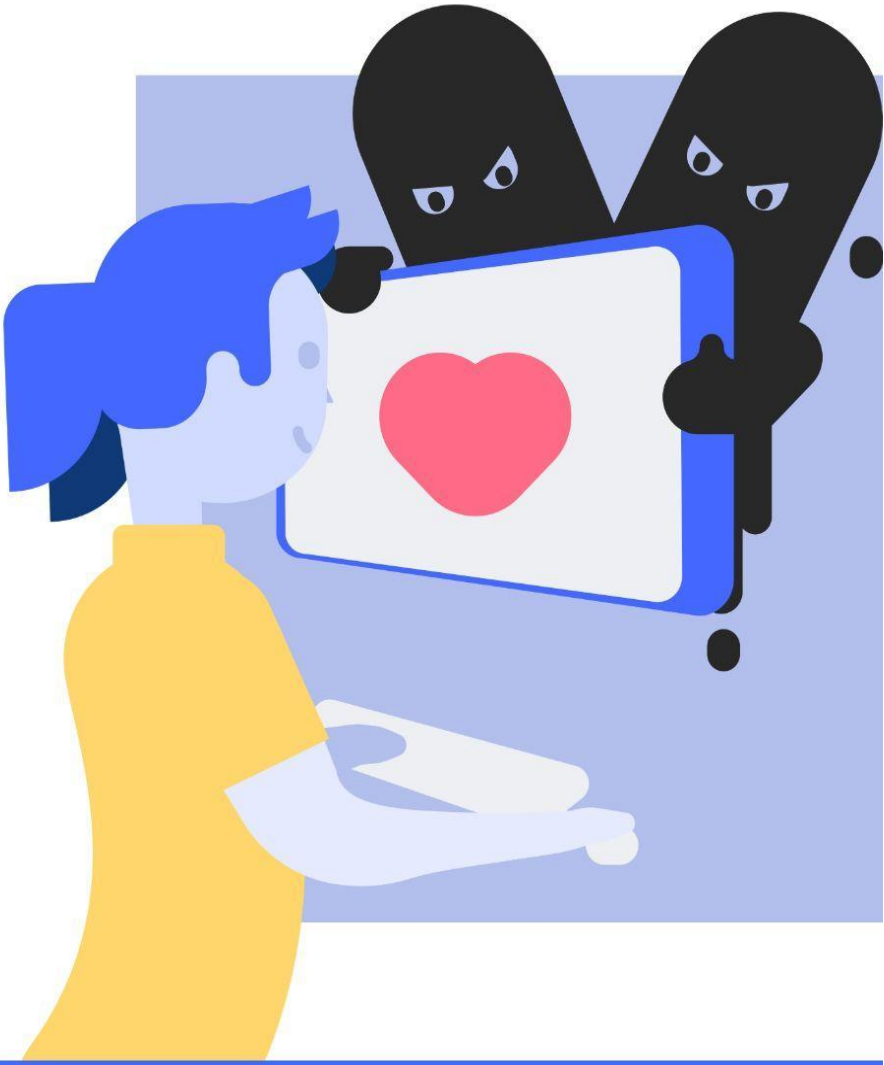
Automate software supply chain security to block new risks, prioritize existing issues and only use open-source code that you trust.

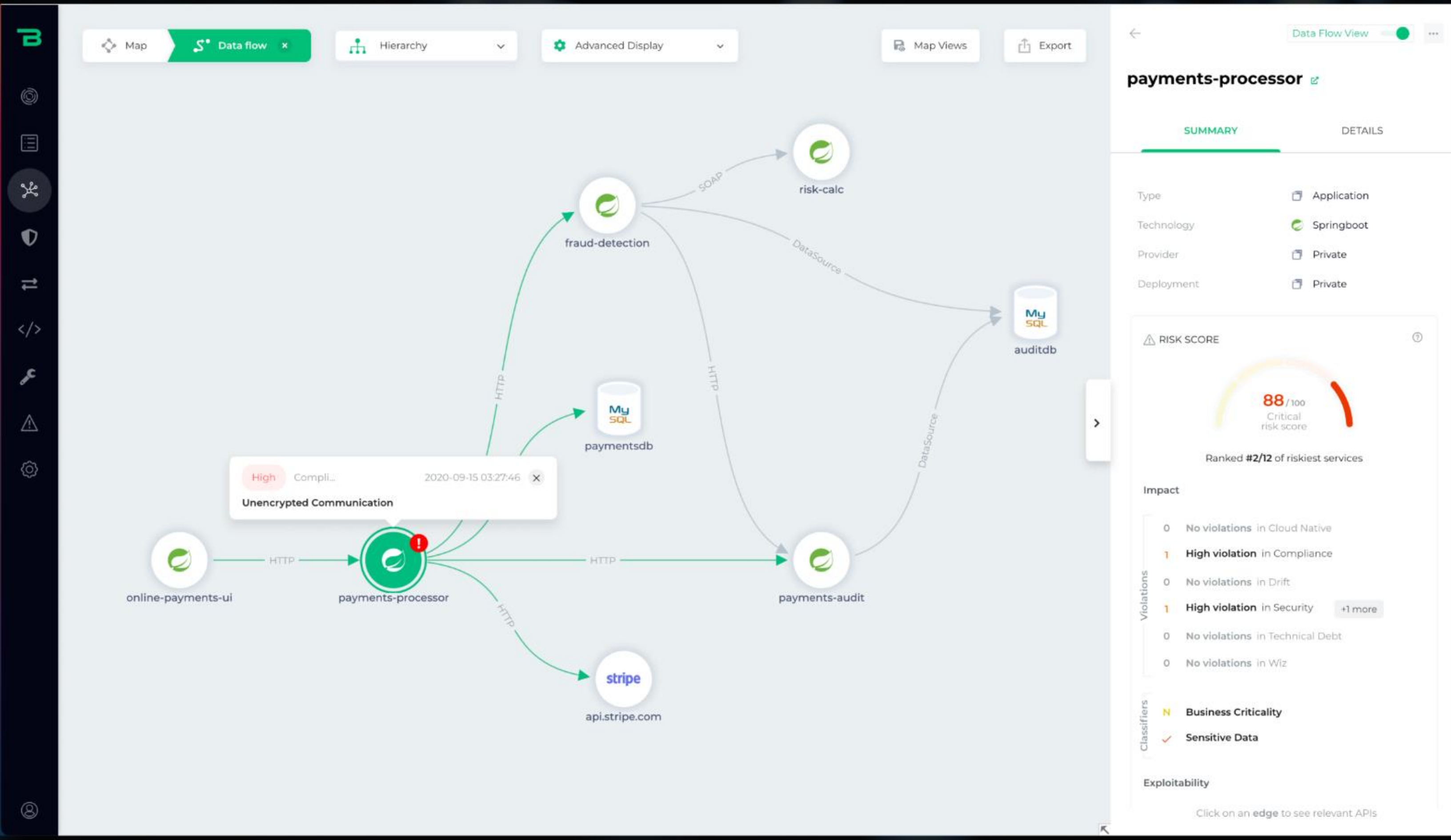
✓ Protect the Organization
Proactive OSS Risk Management
Policy Standardization & Enforcement
Improved Signal : Noise
Modern Attack Prevention
✓ Secure Innovation
Developer-First Approach to Security
Reduced Organizational Friction
Accelerated Release Cycles
Uninterrupted Developer Workflows

Score Projects
TOTAL SCORE
57

RISK DOMAINS

- SOFTWARE VULNERABILITIES
- MALICIOUS CODE
- LICENSE MISUSE
- AUTHOR RISK & REPUTATION
- ENGINEERING RISK




Map
Data flow
Hierarchy
Advanced Display
Map Views
Export
risk-calc
SOAP
fraud-detection
DataSource
auditdb
HTTP
HTTP
paymentsdb
DataSource
High
Compli...
2020-09-15 03:27:46
Unencrypted Communication
online-payments-ui
HTTP
payments-processor
HTTP
payments-audit
HTTP
stripe
api.stripe.com
Data Flow View
SUMMARY
DETAILS
Violations
Classifiers
+1 more

Phosphorus

Secure the Enterprise xIoT Attack Surface

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

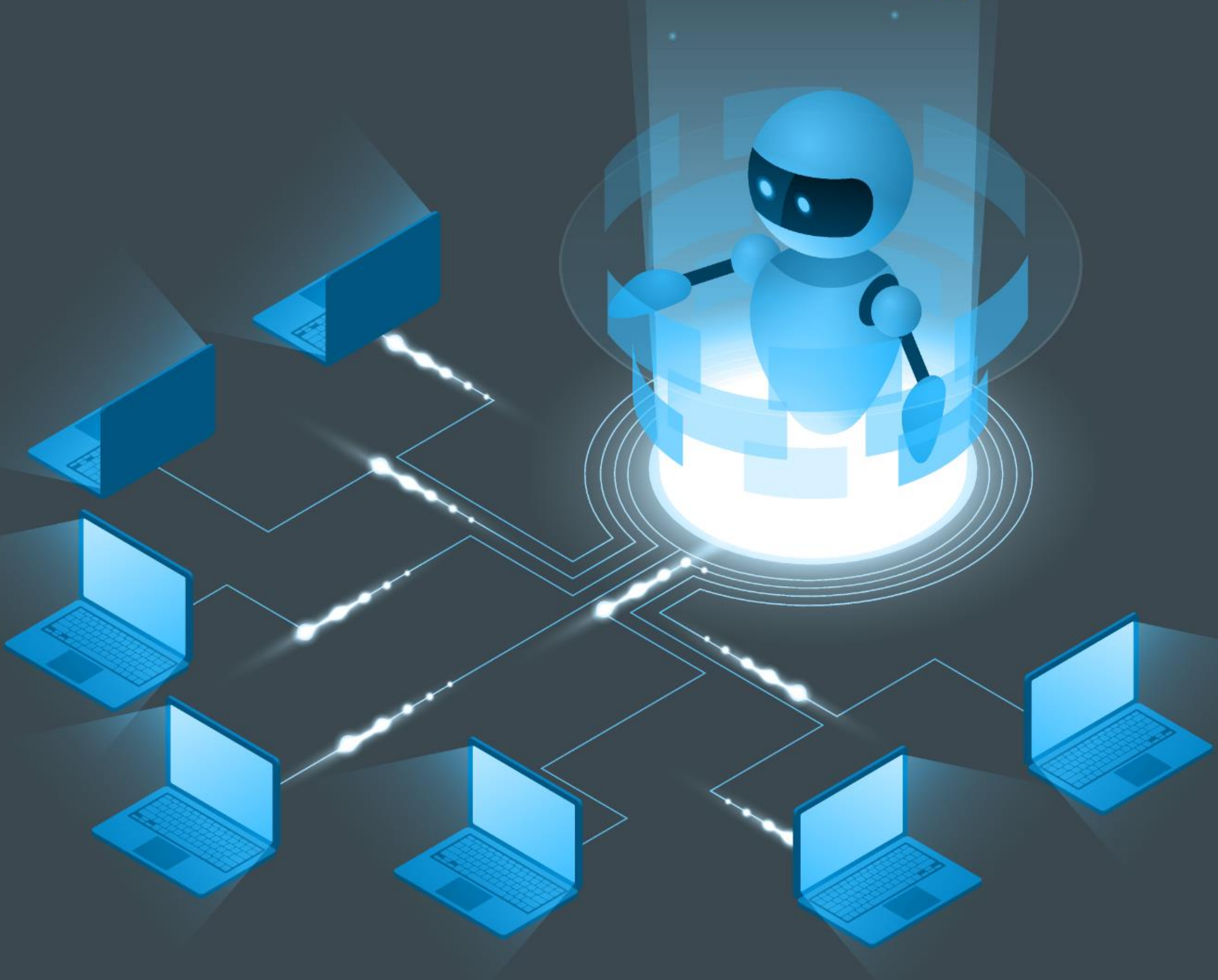
See how Phosphorus can bring enterprise xIoT security to every cyber-physical Thing in your enterprise

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

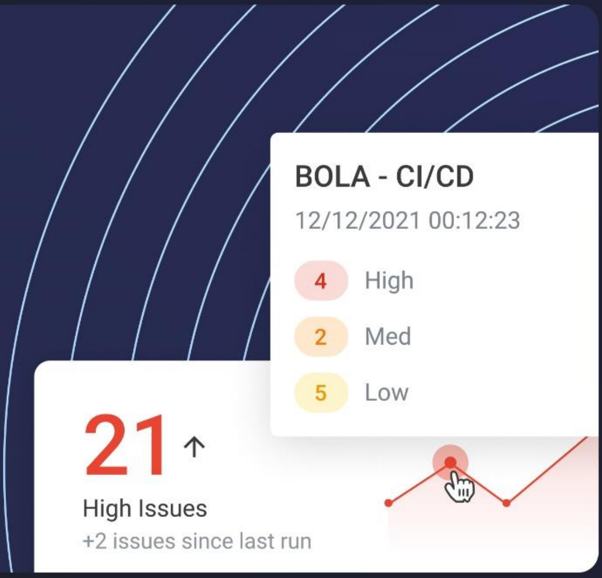
Across all xIoT devices

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

www.Phosphorus.io



Issue Types
8
6
4
2
0
Severity
13
Issues
High 4
Medium 5
Low 4
Last 7 Days
Nov 17
Nov 19
Nov 21
Nov 23
Misconfig
Data



ARTICLES

4 Key Security Trends For 2023

By Jonathan Lee, Senior Product Manager, Menlo Security

2022 has unfortunately failed to live up to hopes for calmer waters.

While it seems as though the worst effects of the COVID-19 pandemic are now behind us, the past year has been riddled with other difficulties. From the Russian invasion of Ukraine to the growing cost of living crisis, it’s been another incredibly tough year for all – and the situation hasn’t been eased by any softening of the threat landscape.

Indeed, threat actors have continued to expand and evolve their attack methods, leveraging new techniques and exploiting a series of emerging vulnerabilities.

Here, we look at four key emerging trends that we have observed this year and expect to grow throughout 2023.

1. HEAT attacks

Moves from threat actors to understand common technologies across the security stack and tailor attacks to bypass these tools is a pressing problem for enterprises. Indeed, modern threats are becoming increasingly advanced and evasive as adversaries come up with ways of getting around defences that are all too often inadequate or outdated.

Throughout the last year, The Menlo Labs team has been tracking a distinct and notable rise in Highly Evasive Adaptive Threat (HEAT) techniques – a class of cyber threats that have been tailored to evade protective tools such as firewalls, secure web gateways, malware analysis including sandboxing, URL reputation and phishing detection technologies.

Indeed, Menlo Labs identified a 224% increase in 2021, and we're expecting a similarly alarming increase this year as attackers have further evolved their attack methods. If firms continue to lean heavily on traditional detect and respond security techniques, attackers will find success in HEAT-based endeavours.

2. Basic security failures

Unfortunately, basic security failures at even some of the most renowned organisations in the world continue to offer open doors for attackers to step through and begin to wreak havoc.

Take the attack on Uber in September 2022. Here, a lone threat actor was able to gain administrative control over the ride hailing giant's IT systems and security tools owing to an exposed PowerShell script that contained admin credentials to the firm's privileged access management (PAM) platform.

Indeed, it is a telling example. It doesn't matter how extensive an organisation's security investments might be, or how sophisticated their technologies are. Often, threat actors can use simple and proven methods such as social engineering techniques to find ways around them.

This example hasn't just reiterated that there is simply no silver bullet or panacea to stopping attacks. Indeed, the Uber breach also showed multi-factor authentication (MFA) push notifications to be exploitable, causing widespread concern and a demand for the use of FIDO2 passkeys and hardware tokens in replace of passwords. This is something we might begin to see gather momentum in 2023. However, it will take a lot of work to implement it on a widespread basis, and even then, we foresee attackers simply finding the next weakest link in the chain.

3. Browser-based attacks

The third trend we see accelerating through 2023 is browser-based attacks. Undoubtedly the biggest attack surface available for threat actors to exploit today, it is critical that the security sector takes greater steps to protect this space.

Indeed, several vendors are already looking at ways to add security controls directly inside the browser, moving away from traditional methods of improving protection with a separate endpoint agent or via the network edge where firewalls or secure web gateways are used.

It's pleasing to see major names such as Google and Microsoft making headway in this domain. Both organisations are developing and implementing built-in controls inside their respective Chrome and Edge browsers to secure at the browser level, rather than the network edge.

However, threat actors seem to be determined to remain one step ahead. Browser attacks are increasing, with attackers exploiting new and old vulnerabilities, and developing new techniques such as HTTP Smuggling.

As a result, remote browser isolation (RBI) is becoming an increasingly core principle of Zero Trust security that stipulates that no device or user – not even the browser – can be trusted.

4. One size doesn't fit all

Fourthly, it is vital for organisations to remember that one size simply doesn't fit all when it comes to security, and bespoke technology combinations and strategies are still the way to go.

Recent reports from Gartner have suggested that many organisations are pursuing strategies focused on security vendor consolidation, cutting the number of providers they are working with for their security needs. This has been particularly prevalent in more complicated arenas such as secure access service edge (SASE) and extended detection and response (XDR).

The motivation is less cost focused, and more about reducing complexity and improving risk management abilities. And while policies of continuous improvement are always going to be encouraged when it comes to security, it is important that organisations don't discard best of breed solutions in the process.

About the Author

Jonathan Lee is a Senior Product Manager at Menlo Security. In this role, he serves as a trusted advisor to enterprise customers, and works closely with analysts and industry experts to identify market needs and requirements, and establish Menlo Security as a thought leader in the Secure Web Gateway (SWG) and Secure Access Service Edge (SASE) space. Experienced in leading the ideation, technical development, launch and adoption of innovative security products, including email security, data loss prevention and end point security, Jonathan previously worked for ProofPoint and Websense.

New Threat Report Shows Attackers Increasingly Exploiting MFA Fatigue

By Ben Brigida, Director, Security Operations, Expel

If you want to know what's happening in the cybersecurity world, it helps to have up-to-date information. That means staying on top of annual reports discussing the broader trends in security, but it also means diving into more timely reporting. Expel's new Quarterly Threat Report provides the opportunity to do just that, examining incidents identified by the Expel security operations center (SOC) during the third quarter (Q3) of 2022. Those incidents span a broad range of industries and an even broader range of individual businesses, and they include alerts, email submissions, and other threat hunting leads.

The report helps to highlight some of the emerging—and continuing—trends from across the cybersecurity landscape, including the ongoing rise in identity-based incidents and attackers' increasing focus on finding new ways to defeat multi-factor authentication (MFA). The full report is available here, but below is a selection of highlights that lay bare some of the most pressing threats companies faced in the third quarter of this year.

Attackers Are Exploiting Users' MFA Fatigue

To be clear, MFA is important—roughly half of the business application compromise (BAC) incidents included in the report were stopped by MFA or conditional access policies, making its value clear. Unfortunately, that means the other half slipped through the cracks. While MFA is an essential tool in organizations' security strategies, it isn't enough on its own. Attackers are continuing to identify ways to exploit some of its weaknesses. Chief among them is the fact that, eventually, many users get tired of pulling out their phones and engaging with MFA notifications—which leads to poor judgment. The research shows that in over 80% of successful compromises, MFA and conditional access policies were properly installed and configured—the attacker was simply able to trick the legitimate user into satisfying the MFA request.

Attackers have found considerable success overwhelming their targets with repeated MFA requests. The data shows that a significant percentage of users eventually accept the request—even if just to make the notifications stop. Many rationalize that it's probably a member of the IT team making an update or change, and don't think twice about it. But the unfortunate truth is that attackers are simply annoying users into causing a potentially serious breach. It's a cunning tactic—one that preys on human nature.

Stopping this requires MFA users to adapt alongside the bad actors. How? Organizations can disable push notifications in favor of a Fast Identity Online (FIDO) compliant solution, which helps alleviate the risk of an overwhelmed employee simply granting access without thinking. Other options include number matching, which requires the user to enter numbers from the identity platform into the MFA app to approve the authentication request. While less seamless, this option requires active engagement from the user, greatly reducing the risk.

Identity Attacks Are Not Slowing Down

It's become almost a mantra in the cybersecurity industry, but—as has been the case for some time—identity-based attacks continue to rise. In Q3, they accounted for 59% of all incidents detected by the Expel SOC, up from 56% in Q2—already a concerningly high number. Business email compromise (BEC) and BAC attacks were among the most common tactics, and accounted for 55% of all incidents identified, underscoring the fact that attackers continue to find success with social engineering tactics.

There is hope on the BEC front, though. All of the BEC attacks our SOC detected targeted Microsoft 365, and many experts believe that Microsoft's decision to disable Basic Authentication by default in Q4 may help address the problem. Attackers have become extremely adept at exploiting the weaknesses inherent to Basic Auth, and Microsoft's decision will likely force them to shift to new techniques. It may not be a long-term solution, anything that impedes attackers is a step in the right direction.

Attackers Put a New Spin on Old Tactics

There are a few additional findings worth noting—particularly in areas where attackers are evolving their tactics. Ransomware continues to be a significant problem, but attackers are increasingly turning to zipped JavaScript or ISO files, abandoning the use of visual basic for application (VBA) macros and Excel 4.0 macros, which were previously the most popular ways to gain entry to Windows-based environments. In fact, zipped JavaScript files accounted for 46% of all pre-ransomware incidents, underscoring the need to keep a watchful eye out for suspicious files. (By the way, this shift is likely thanks to Microsoft's decision to block macros by default in Microsoft 365 applications.)

Attackers have also refined their social engineering tactics, and themes having to do with "invoices," "order confirmations," "payment," and "requests" are now among the most commonly used in email subject lines in phishing attempts. The most common, though? Blank subject lines. These terms create a sense of urgency or fear in recipients, clouding their judgment and making them more likely to make a mistake. Where email attacks are concerned, attackers are also increasingly using IPs geolocated within the U.S. when targeting U.S.-based organizations. This helps them bypass conditional access mitigation efforts and is something security teams should keep an eye on moving forward. Simply blocking or adding additional scrutiny to overseas IPs is no longer enough.

Recognize Attackers' Shifting Strategies

These Quarterly Threat Report findings highlight the ways attackers are shifting their tactics in response to new security measures. As more organizations implement MFA, they are finding methods to circumvent it. As users grow more aware of social engineering tactics, they are finding new ways to disrupt their thinking. Until organizations demonstrate the ability to consistently stop identity-based attacks, they aren't going anywhere. The battle between security teams and attackers is a constant cat-and-mouse game, with each adapting to the other's tactics as they evolve. There is no silver bullet that will solve every security challenge—but understanding these threats is the first step toward stopping them.

About the Author

Ben Brigida is the Director of SOC Operations at Expel. In this role, he's responsible for making sure Expel maintains the quality of delivery customers have come to expect. Ben has been with Expel since the company's inception in 2016. Prior to Expel, Ben worked in the security operations center (SOC) at FireEye.

Ben can be reached online via LinkedIn and at our company website https://expel.com/

The Future of Online Privacy

By Mia Naumoska, Chief Marketing Officer at Internxt

You've probably noticed that there's a lot of bad news about online privacy these days. Security breaches and data leaks are everywhere, and it seems like almost every company is collecting more information about you than ever before.

But this isn't the end of the internet as we know it. In fact, there are some positive signs on the horizon: new laws have already been passed to protect your privacy, and technology companies are trying new ways to keep your data safe.

So, while there may be (so, so, so many) challenges ahead regarding privacy and our digital lives, they're not entirely insurmountable ones. Let me explain what's happening with online privacy and how things will likely change in the coming years...

The Internet Is a Double-edged Sword

The internet has been, and likely always will be, a double-edged sword. On the one hand, it's made it easier than ever before to connect with people from all over the world. But on the other hand, it's also made it more challenging than ever before to protect your privacy.

With more people than ever using the internet, it's only natural that there are more ways to get hacked. There are hundreds of different types of hackers out there, and all of them have different ways of going about their business. But the one thing that all hackers have in common is that they're looking to steal information from you. Whether it's your email password or credit card number, if it has value, then someone will try to get it from you.

The world of hacking has dramatically evolved over the last twenty years. Hacking used to be a hobby, but it's now big business. Now, some people make their whole living by stealing data from others and selling it on the black market.

How tech companies and developers are forced to respond to new hacking methods has the potential to radically change the internet as we know it.

Online Privacy Laws Are in Flux but Will Improve

As we push further into the future, the need for privacy from watchful eyes grows more and more critical. The lines between public and private data are becoming dangerously blurred. It's time to demand more from our government and hold corporations accountable for protecting your data.

The United States government is currently trying to pass a privacy law that would provide more protection for Americans, but it will be years before it's passed. In contrast, the European Union (EU) has stricter privacy laws that are much more closely monitored by its citizens and enforced by its regulators.

The EU's General Data Protection Regulation (GDPR) is a set of laws that protects the data of EU citizens. It was put into effect in 2018 and will affect any company that deals with personal data from an EU citizen.

The GDPR is intended to give EU citizens more control over their data and provide them with more privacy protection. It also applies to companies outside of the EU that deal with personal data from EU citizens. The GDPR includes several provisions, including:

- The right to be forgotten
- Transparency and consent
- Data protection by design
- Data protection officers (DPOs)
- Breach notification
- Data portability
- Data protection impact assessments (DPIAs)

But the GDPR doesn't just apply to European companies—it applies to any business that processes or holds personal data belonging to people living in Europe.

In the future, privacy will be protected through a combination of legislation and technology. Legislation is currently being implemented to protect consumers and help prevent companies from taking advantage of them. This includes regulations on user data collection and the ability for users to remove themselves from data collections easily.

Additionally, businesses will be required by law to inform users when their information has been breached, who it was violated by, and how many people have access to that data. This type of transparency will ensure that users also know what measures are being taken so that they can take the steps necessary to protect themselves from identity theft or further privacy violations.

How Companies Collect Data and Protect It Will Change.

The future of online privacy will change the way companies collect and use your data.

As we've mentioned, the General Data Protection Regulation (GDPR) is a European Union law that protects user privacy by requiring companies to be more transparent about how they collect and store your data. If a company violates this law, they could face hefty fines—and there are already reports of some companies receiving them.

This regulation shows that people are willing to fight for their right to control how their personal information is used online, so expect more similar laws around the world in the future, as well as an increased awareness of what you share on social media and elsewhere online.

The GDPR is a good start, but it only applies to EU countries. It's also not an effective way to protect your privacy—you should still be careful about what you post online and how much information you share with companies.

New Technologies Will Help with Digital Privacy.

As you know, privacy has been a hot topic for the last few years. It's only getting hotter as new technologies are developed, and companies begin to adopt them.

Many new, emerging tools help you control your data and privacy online, but it can be hard to keep track of them all—especially when new ones come out seemingly every day.

Internxt secure cloud storage is an excellent example of a new web service that uses new technologies like end-to-end encryptions and open-source, distributed networks to give users total control over their files and photos. Internxt is at the forefront of companies choosing to offer products and services that respect individuals' right to privacy and say no to harvesting user data.

Another fantastic example is Tor Browser. It is an application that allows people to browse the internet anonymously by routing their IP address through multiple servers worldwide (called nodes) before connecting with websites or services on different servers than their own. It also uses strong encryption so internet service providers cannot eavesdrop on users' activity while browsing online.

Don't Let the New World Scare You

The future is here. We've made it this far, and there's no turning back now.

We must embrace our new reality and understand that changes like these are inevitable in a world where technology is thriving. The best way to do this is by not being afraid of the unknown—by not shying away from new ideas and innovations but rather being curious about what they could mean for us in the long run.

If you keep an open mind, you'll be able to see past all the alarmist headlines about digital privacy and realize that these advancements aren't all bad news. In truth, they may actually help us gain control over our personal lives more than we ever thought possible!

Sure, there's a lot of bad news about privacy these days, but there are also good signs that things will improve.

It's hard to see the forest for the trees regarding online privacy. Between Facebook and Google, you can't scroll through your feed without seeing a story about a data breach or something nefarious being done with your personal information. You might be feeling like we're at a dark place in terms of data security, but some bright spots show things could be getting better soon.

Federal laws will change, so they protect you more. Companies are also starting to realize that they need to do better by their customers, not just themselves—and this will help keep your data safe from privacy violations and unethical use. New technologies like blockchain and encryption will also help companies have more control over how they collect and store users' information than ever before.

Don't despair. It's going to be okay!

What About Privacy Now?

We've covered a lot of ground in this article, and protecting your privacy can feel overwhelming. What do you do?

First, take a breath. There are a lot of things going on with privacy right now that might seem scary to you, but remember that there is a lot of good news too. Second, find reputable security and privacy companies like Internxt to help you protect your data until we all come together to build a safer, better internet.

Online privacy's future, especially concerning the right to privacy, will continue to be a hotly debated topic. In the current age where social media and big data are constantly growing, and more and more of the activities we engage in online can be monitored and analyzed by those who are observing us, the big question will continue to remain—how do we protect our rights to privacy and freedom?

About the Author

Mia Naumoska is a Chief Marketing Officer at Internxt - world's most secure cloud storage. Having over a decade of experience in the marketing field, Mia is responsible for Internxt's overall marketing strategy, managing an amazing team of marketing experts. Mia can be reached online at LinkedIn and at our company website https://internxt.com/

5 Best Practices for a Multi-Factor Authentication (MFA) Strategy

By Zac Amos, Features Editor, ReHack

Organizations and individuals must implement multi-factor authentication strategies to enhance any cybersecurity risk management plan. Cyberthreats have always been creative, but increasing attacks requires defensive tactics to be more holistic, incorporating as many protective measures as possible. The best cybersecurity portfolios contain a variety of safeguards for boosted protection.

Why MFA Is Crucial in 2023

MFA takes time to implement and the new year is an ideal springboard for making widespread changes — employees may exercise more patience during the adjustment period. Every year brings new threats to digital landscapes, especially in susceptible sectors like health and financial institutions.

Institutions adding this one barrier of cybersecurity could reduce over 99% of compromised accounts, saving millions of dollars in remediation. For 2023, it's essential to have because it's a wonderful supplement to any cybersecurity routine. It also helps instigate one of the most vital cybersecurity prevention measures — employee participation.

1. Educate, Train, Inform

MFA involves everyone, not just IT teams or cybersecurity analysts. Using it as a defensive strategy encompasses more surface area, minimizing accidental misuse of technology.

Transitioning to an MFA landscape is a prime opportunity to provide additional cybersecurity training to workers and decrease the chance of frustration or complacency if they find MFA measures combative to their workflow. It helps with cybersecurity hygiene inside and outside the office because it can inform team members how to create more secure passwords or safer emailing habits.

Employee buy-in is crucial for a seamless transition. The best way to ensure that is to clearly communicate the phases of the rollout — if they don't understand what's happening, it's more likely they will not take it as seriously as they should. It also solidifies continued use because individual workers could find ways to deactivate it on their accounts unless higher permissions prevent it.

2. Achieve and Maintain Compliance

Assessors look to MFA implementation to obtain and abide by some of the world's most respected compliance frameworks. Instilling the practice now can help organizations avoid fines and other negative consequences, such as a loss in reputation for lacking compliance.

Frameworks like HIPAA that focus on protecting personally identifying information require MFA. For the finance sector, Federal Financial Institutions Examination Council standards encourage MFA for online banking services. The practice is such a gold standard now that it also helps with insurance since they check if companies are using it when discussing liability.

3. Vary Authentication Measures With Contextual Triggers

MFA doesn't only have one method, such as receiving a code on a phone and inputting it on a PC. Implementing multiple MFA measures can increase defenses. If the MFA environment is too much of a monoculture, threats could identify this behavior and take advantage of it.

Apart from receiving an SMS, these are the other ways a company can diversify MFA:

- Soft and hardware tokens
- Phone call
- Email approval or code
- Biometrics like fingerprint or face ID
- Receiving codes through other authentication apps
- Security questions

Every type of MFA can amplify safety if compounded with contextual triggers, such as:

- Programs verifying IP address or connection
- Geolocation
- Checking the assigned device against permissions
- Time-checking

4. Reinforce with Complementary Solutions

Combining MFA with other cybersecurity methods will only make defenses more robust. Two techniques that bolster protection are single-sign on and least-privilege infrastructure.

Single sign-on (SSO) could be risky if misused, but sound practices could reduce password reuse or sloppy password management because staff members only have one set of credentials. SSO isn't the best defense because one password and username would be all a hacker would need. However, with MFA, it works on multiple fronts. Least privilege works even more synergetically with these methods to prevent unnecessary credentials from accessing information they don't need to complete their tasks.

5. Schedule Evaluations Implementing Change Management

Make technical teams continue to oversee how their infrastructure operates. Several times a year, employees should gather data about their experience with MFA and if they feel it protects their assets in a streamlined way. Here are some concerns employees may raise about their MFA experience:

- The app stack is too cumbersome or not user-friendly
- They prefer other forms of MFA
- Reports of inconsistent authentication receipts
- Notices of infrequent updates

If an IT team finds improvements, they can install them with a change management structure, which forces teams to delegate changes to specific parties and make thorough documentation of those changes. Notating who and when changes happened will provide insight for anyone new making adjustments — it will help if they encounter roadblocks and need to collaborate with other team members to overcome obstacles.

Why MFA Is Essential for Security

Committing to a solid defensive security strategy enables analysts and other employees to use technology more safely. Businesses can allocate energy and resources to strengthen different facets of their continuity plans by continuing to inform their staff and solidifying methods for offensive measures if they need to respond to a breach.

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.

2023 Predictions

By Dr. Chenxi Wang, Founder and Managing General Partner, Rain Capital

For venture capitalists and investors with an eye on technology, 2022 was a chaotic year. This turmoil was partly driven by factors outside the tech sector's control, such as the Russia-Ukraine War and the lingering economic aftereffects of the Covid-19 pandemic. These events were felt in every corner of the world, creating challenges for the current venture investment scenes.

Be that as it may, the market marches on, and trends emerge. Some materialize despite market forces, and others occur because of them. Savvy investors know that rather than respond emotionally to the day’s news, it’s critical to take a more expansive view and look at the long trajectory of trends, whether they've been building up for years or are only just now appearing on the horizon.

Spotting tech trends and taking the long view is part of what I do daily as General Partner at Rain Capital. Our portfolio companies have placed their trust in us, and I take that trust very seriously. So, when I was asked what my predictions are for investors and venture capitalists who want to put their money into the tech sector, I isolated three things I believe will play a significant role in 2023. These predictions will be helpful both to our investors and to others hoping to capitalize on the field's constant innovations.

Data security will be a focus.

Data security is already a significant concern for most organizations and has been for some time, but in 2023 I expect it to be in the spotlight even more than it is today. We continue to see new requirements and regulations that pertain to data security, data protection, and data governance, many of which have separate initiatives and budgetary allocations from existing security projects. This will be an exciting area for innovation, and I expect that to continue for the foreseeable future.

AI will be a game changer for cybersecurity.

Increasingly, I've seen bridges built between cutting-edge AI technologies and security initiatives. In September of this year, CNBC reported that the global market for cybersecurity products using artificial intelligence is expected to reach $134 billion by 2030. In contrast, the amount spent on it in 2021 was just $15 billion. Time will tell if that projection is accurate. Still, today it's clear that the ability to cross-pollinate between AI and security will drive many innovations that those of us immersed in the industry have not even considered previously.

Alignment with engineering will come into clarity.

New software is being created every day, and too often, security is a secondary consideration that only comes into play once an application has been entirely built. With companies like Snyk and others who lead the charge for developer-centric security, I believe a trend is coming into view now, which is about seamlessly embedding security measures into the engineering process and pipelines. Security will become an integral part of dev tooling and infrastructure layers, further shifting security “left” and achieving alignment with development and engineering teams.

Staffing challenges will continue to drive innovation.

In cybersecurity, there are more open positions than there are people to fill them. In the past decade, there has been a massive boom in digital environments, all of which need to be secured, and there simply hasn't been enough training to fill the pipeline at the necessary pace. Even with the economic downturn, demand for cyber talent is outpacing supply. Because of that, we have an opportunity to do things differently in the cybersecurity world. For instance, innovation in automation will be even more of a force multiplier when human talent is scarce. Similarly, data-driven insights and intelligence will be more impactful when manual work ceases to be an option.

It's essential to add that while geopolitical and economic uncertainties may make investors take a more conservative approach, those same forces have famously driven cutting-edge innovation in the past and will do so again. Great companies are formed in a down economy. Currently, security is still driven primarily by conventional technologies that are meant to be used on premises in a traditional infrastructure environment. Frankly, that's not good enough. Cloud has thoroughly disrupted traditional computing, requiring people to manage and defend their data differently. This tension will be exacerbated when productivity and efficiency are put to test with tough economic constraints.

The good news is that there's plenty of room for change and innovation, and venture capitalists will have many opportunities to back the next great security technology, whatever that might be. Innovation will be needed to bring existing security operations into this cloud-forward or cloud-native environment. The opportunity for someone to create the next great revolution in cybersecurity is immense.

About the Author

A leading venture capitalist in the Bay Area, Dr. Chenxi Wang is the founder and managing general partner of Rain Capital, a Silicon Valley-based venture fund. She previously held leadership positions at top companies including Twistlock, Intel and Forrester, and currently serves on the Board of Directors for MDU Resources, a Fortune 500 company. Wang is also a Forbes contributor and writes a column for Dark Reading.

Chenxi can be reached online at LinkedIn or Twitter and at our company website https://www.raincapital.vc.

Busting Myths Around Cybersecurity Team Training

New Research Results from Omdia and Cybrary Point to Substantial ROI From Continuous Upskilling of Cybersecurity Teams.

By Kevin Hanes, CEO, Cybary

In recent years, cybersecurity has garnered a staggering amount of attention, especially with the rise of high-profile data breaches. But we still find companies grappling with an absent plan for preparing staff to handle impending and emerging threats. A new research report developed with Omdia examines several common myths about professional cybersecurity training in the hopes of assisting practitioners and technology vendors in dispelling some of these myths and better preparing your organization for the future.

Why train cybersecurity professionals?

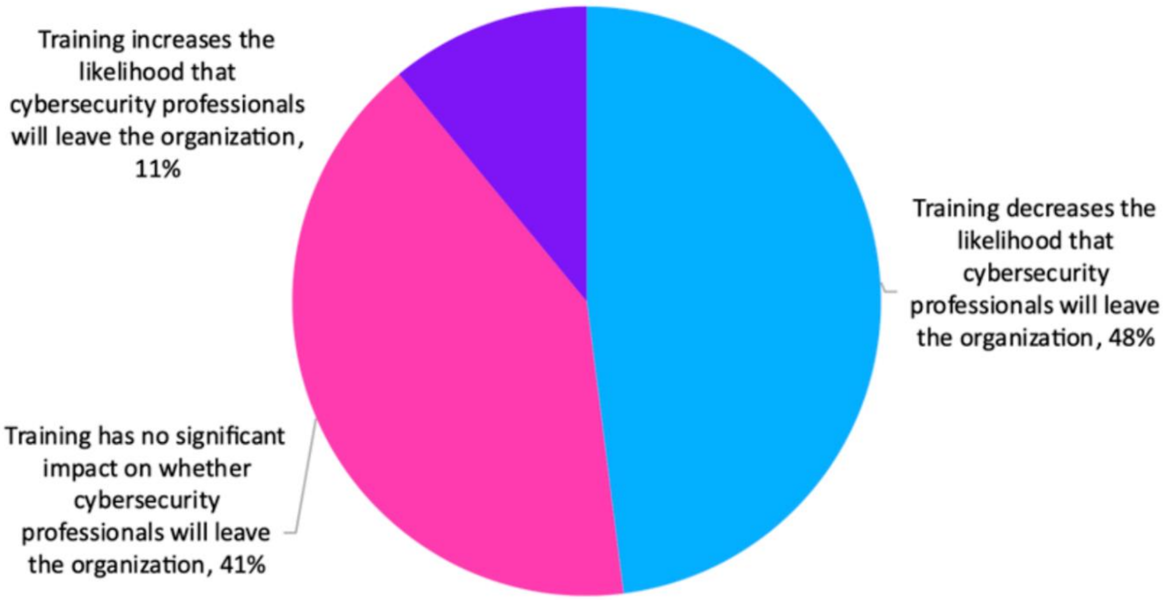
Let's start with the basics. Why train cybersecurity professionals? The answer is simple: management sees that better security results and risk mitigation are required. Training also develops skills that help organizations prevent or respond to cybersecurity incidents on the horizon or that may emerge down the road. In fact, in the 2022 Dark Reading Decision Maker's Survey (in which Omdia participated), 47% of cybersecurity executives say that a shortage of skilled employees is an issue that adversely affects their organization.

The myth of the migrating cybersecurity professional

"*Why should I train my employees when they'll just leave for a better job?*"

That's a question we hear all the time—but our data shows that it's not true. In fact, half of the companies in our survey reported that the availability of professional cybersecurity training reduces the likelihood that an employee will leave, with another four in ten saying that it had no noticeable impact on employee retention. A scant 11% of respondents actually reported that professional training increases the chance that a particular employee will leave (see figure 3).

Figure 3: Which statement most closely mirrors your experience of the impact of professional cybersecurity training on professional employee retention?



Note: n=275 SMBs and enterprises in the US, UK, and Canada

© 2022 Omdia

Source: Omdia

The benefits of professional training are seen in the impact the employee has on the organization, in the overall risk posture of the organization, and in the costs associated with finding and retaining highly skilled employees.

Global business leaders have recognized that continuing professional cybersecurity education is critical to their success—they can't afford not to be up-to-date with the latest security practices and trends.

The enterprise is seeing results from training

Cybersecurity professionals know that professional cybersecurity training is essential to keeping their organizations safe from hackers. But what about the larger enterprise? Are they seeing results from training?

275 executives, directors, and security professionals were surveyed about the impact of professional cybersecurity training on their organization's cybersecurity. Findings revealed that:

- 73% said that their cybersecurity performance was more efficient because of professional cybersecurity training, and
- 62% said that their organization’s cybersecurity effectiveness had improved as a result of professional cybersecurity training.

These are both quantifiable results—things you can measure with data points—that indicate the real, measurable impact of professional cybersecurity training on the organization.

Training is improving staff turnover rates

If you're a manager in cybersecurity, you've probably heard some stories about newly educated cybersecurity professionals jumping to higher-paying jobs. If you're like most managers, you might be wondering whether training programs will have a positive or negative impact on turnover rates.

We asked our survey respondents what they thought, and their answers surprised us: almost half (48%) of those responding said that professional cybersecurity training decreases the likelihood that cybersecurity professionals will leave the organization. Another 41% said that training has no significant impact on professionals’ odds of leaving. Only 11% reported that they felt professional cybersecurity training increases the likelihood that cybersecurity professionals will leave the company.

How are companies training their employees?

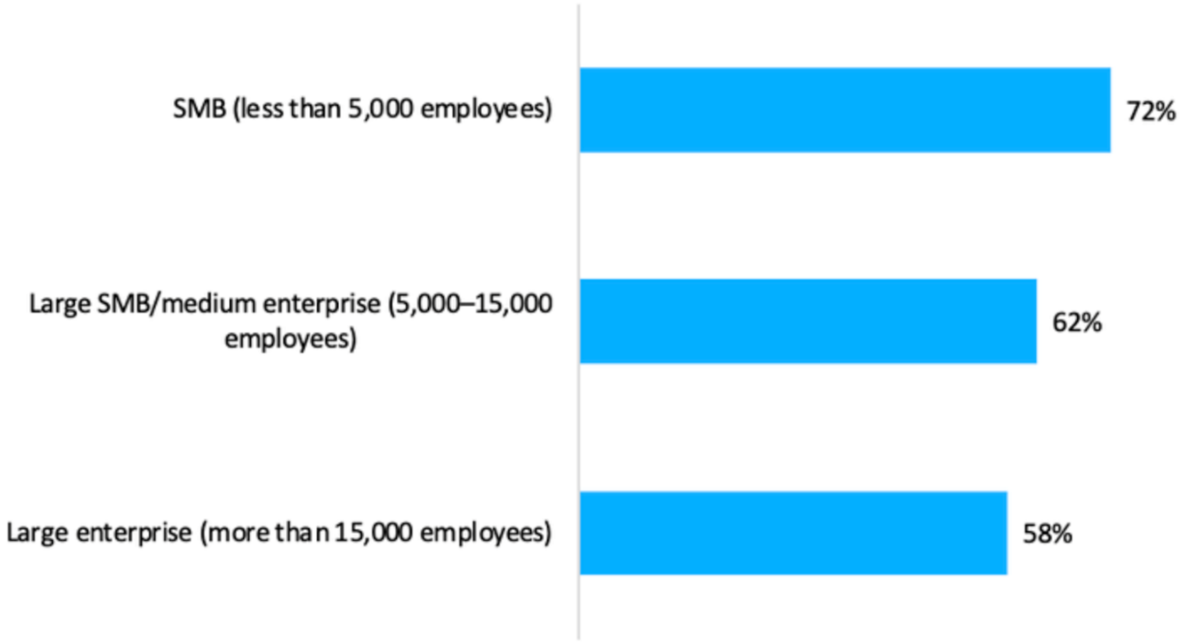
In today's increasingly complex threat landscape, adversaries are well funded and are using advanced resources to develop and evolve new threat variants. It's more important than ever for organizations to have a comprehensive, ongoing training program in place.

To address these challenges, organizations are prioritizing allocating resources to endpoint security, data security, and secure access service edge (SASE) training. This also is followed by remote, cloud, and network security training.

Organizations are also prioritizing skills in a variety of topics to help defend against modern threats on the broad range of attack vectors. That's why it's so important to have a comprehensive training program in place.

Online training is becoming the preferred approach over in-person training, with 72% of SMBs, 62% of large SMBs/SMEs, and 58% of large enterprises allocating budgets for online training (see figure 5). The reason for this is simple: online training can be integrated seamlessly into an employee's daily work tasks, reinforcing its value and making it more likely that the employee will actually learn what they're supposed to learn.

Figure 5: What percentage of cybersecurity professional training budget is online vs. in-person?



Note: n=275 SMBs and enterprises in the US, UK, and Canada

© 2022 Omdia

Source: Omdia

It also helps that online training is accessible from anywhere, at any time—which makes it easier for employees to access the resources they need to stay up-to-date on their skill sets without having to take time off from work or travel long distances just to get them.

Key takeaways

When it comes to cybersecurity training, a lot of groundless myths still persist, and are likely to help aid threat actors as they ensnare target organizations. But research and experience demonstrate that when actual results and experience are analyzed, the balance swings firmly in favor of developing an ongoing, sustained program of professional cybersecurity training.

Here are some key takeaways:

- Almost 90% of survey respondents rejected the idea that training leads to increased employee turnover.
- Cybersecurity training increases cyber teams' effectiveness, efficiency, and overall security posture.
- Training also directly reduces the number and impact of breaches/incidents, and prepares teams to better deter, detect and address future threats.
- When implementing a training platform, it's best to choose one with a range of cyber-focused topics to support your specific needs.
- Combine training with internal career paths to encourage employee retention and loyalty.

Conclusion

The cybersecurity job market is not just competitive, it's a war zone actively competing for talent. Companies need to be able to attract and retain the best talent if they want to stay competitive in this fast-paced industry, and investments in upskilling help recognize and reward cybersecurity pros, while strengthening the organization's security posture. Although at first look training may seem like a daunting undertaking, a world-class platform can make ongoing cybersecurity accessible, affordable and easy to implement and manage.

Seek out a cybersecurity upskilling platform that provides guided pathways, threat-informed training, and certification preparation for your team. When you equip your cybersecurity professionals – at every stage in their careers – to upskill and mitigate both current and future threats, you help your organization win both the battle for talent and the fight against attackers!

If you're looking to make the case to prioritize training, you can download the The Myths of Training Cybersecurity Professionals report by Omdia or you can watch our on-demand webinar that reviews the key insights from Omdia's research.

About the Author

Kevin Hanes is the Chief Executive Officer of Cybrary and serves on its board of directors. Before joining Cybrary in June 2021, Kevin spent eight years as COO of Secureworks. In that role, he helped transform Secureworks into a recognized global market leader, built one of the world's most respected cybersecurity operations teams, and led his organization through hyper-growth and an IPO. Kevin began his career at Dell Technologies in custom software integration and moved into leadership roles over his 15-year tenure. Kevin earned his Bachelor's from St. Edward's University and his Master's at The University of Texas at Austin.

Kevin can be reached online at @cybraryIT and at our company website https://www.cybrary.it/

Can The US-Led Multinational Counterattack Stop Ransomware’s Gold Rush?

By Camellia Chan, CEO & founder of Flexxon

I was honored to be one of the representatives from 36 nations, the EU, and private sector companies who convened October 31-November 1 for the Second International Counter Ransomware Initiative (CRI) Summit at the White House. The borderless nature of ransomware threats demands close cooperation among nations to fortify against opponents whose threats are as dangerous as physical aggression. United States ransomware payments set a record in 2021, with almost 1,500 filings valued at a total of nearly $1.2 billion, a 188% increase from 2020. The US spearheaded the CRI, with express objectives of increasing “the resilience of all CRI partners, disrupt cyber criminals, counter illicit finance, build private sector partnerships, and cooperate globally to address this challenge.”

I participated in the capacity of a private sector organization as a part of the Singapore delegation, which is charged overseeing the CRI focus area of countering illicit finance together with the UK. The dialogues that have taken place over the first two years are an indispensable first step in making inroads in a war of attrition against formidable cyber criminals from around the world. But make no mistake, the CRI was not only about talking about the problem. The international cooperative took concrete actions to protect citizens, corporations, and governments from these unrelenting forces. The CRI’s efforts to establish open lines of communication and collective action are a significant step forward, but we must next look toward setting agreed-upon international standards through the contributions of each member organization before more tangible impact can be seen.

A global, long-term battle of attrition against ransomware criminals

At the summit CRI partners made concrete commitments, including but not limited to initiatives like biannual counter ransomware exercises, coordination of priority targets through a single framework, and delivering an investigator's toolkit. The important thing is that everyone focused on a singular objective through increased intelligence sharing, aligned frameworks and guidelines, and coordination of actions. I am heartened to witness the world's leaders cooperating on adopting a pragmatic view of the ransomware landscape and acknowledging the ingenuity of cybercrime networks, as well as accepting that we are all engaged in a long-term, ongoing battle of attrition. However, the conversations were still centered in a traditional mindset toward cybersecurity, which may leave gaps in a less than holistic strategy. To provide the best possible chance of thwarting ransomware attacks, it is imperative that we integrate our best defenses by also including the physical computing layer, moving to a more holistic protocol. In the last two years, cybersecurity software continued to be reactive, and thus allowed hackers to conduct their activities largely unchecked. Once cybercriminals have gained access to organizations' systems or their valuable data, it is too late to remedy the situation. Thus, tremendous volumes of ransoms were remitted, estimated to cost $20 billion worldwide.

Combatting a borderless threat to national security

A global problem that transcends borders must be addressed with a global yet borderless approach. However, how do we address a global problem that is simultaneously borderless and yet still threatens the national security of many countries? According to reports, Russia-related variants accounted for about 75%, or 594, of the 793 incidents reported during the second half of 2021. Beyond the payment outcome of being held for ransom, nations must also consider what valuable data, information, or goods the hackers are using to hold organizations ransom. We may see more cybercriminals doing the bidding of state actors to stir up political dissent and orchestrate social engineering attacks and confusion.

Cybercriminals cannot be allowed to act without consequence. Thus, crimes occurring in cyberspace should be met with equal severity as those in the physical realm. To that end, I believe the task force's commitment to pursuing and sanctioning responsible state actors or individuals is wholly correct. For instance, the decision not to provide ransomware actors with safe havens is similar to individuals found guilty of other forms of major financial fraud, dangers caused to public safety, and espionage.

Cross-border cooperation is essential and must have a place across the entire cybersecurity life cycle. The governments of all countries must look towards adopting new technologies to plug existing gaps, keeping channels of communication open for greater multi-lateral cooperation, running joint response drills and exercises to sharpen unified incident response capabilities, and critically, fostering greater collaboration between the private and public sectors.

Public sector and private companies partner to mitigate ransomware threats

The average total cost of a ransomware breach in 2021 was $4.6 million. As the prime targets which bear the greatest financial burden of attacks, corporations are in a unique position to supply critical technical intelligence about ransomware. The CRI aims to institute real engagement between governmental organizations and corporations for “trusted information sharing and coordinated action.” CRI participants made commitments to engage in active information-sharing between the public and private sectors, including through new platforms, on actors and tradecraft. Private sector insights into the whereabouts and actions of ransomware actors from across the internet can effectively complement state capabilities in this aspect – enabling an unfettered two-way flow of information between private and public sectors. They also launched plans to develop a capacity-building tool to help countries utilize public-private partnerships to combat ransomware.

The next stage of holistic cybersecurity defense should incorporate hardware and embedded solutions into the overall infrastructure to stop hackers in their tracks in a small, sealed, and fully engineered environment at the data storage level. To continue the momentum, governments can advance comprehensive programs by focusing on supporting research & development, embracing new approaches, championing the swift adoption of new innovations, initiating pilot programs, enabling the ease of acquisitions, and lowering barriers to trade.

Defending an ever-expanding attack surface against ransomware

2021-2022 has proven to be a golden age for ransomware criminals as reports of ransomware attacks ballooned by 62% in 2021 over 2020. The physical layer continues to be overlooked and software cybersecurity solutions continued to struggle to address countless threat variables in the open environment. Criminals have increasingly targeted managed service providers, the software supply chain, and the cloud. The adoption of new technologies has introduced new opportunities to criminals. As the attack surface expands, more individuals work remotely, and Web3 and cryptocurrency rise in prominence, cybercrime rings evolved to “operate commercially.” In 2022, we have witnessed more ransomware attacks tagged to cryptocurrencies.

Crypto winters and cybercrime summers

We shouldn’t expect that the current crypto winter will deter the criminals from exploiting the blockchain, however. Cryptocurrencies are an asset class, but do not dictate the stability and continued innovation seen in the Web3 space. Cybercriminals will continue to target Web3 blockchain platforms as their user base grows, not only targeting crypto assets but other essential personal information that can be leveraged for ransom. As we are seeing right now, cybercriminals will also shift to other avenues of attack for large impact and payouts – with the same objective as always. They will aim to access and exfiltrate data and hold victims for ransom. They will focus more on critical infrastructure with cyber-physical systems, upon which attacks have quadrupled in the past year.

An important first step in a coordinated counterattack

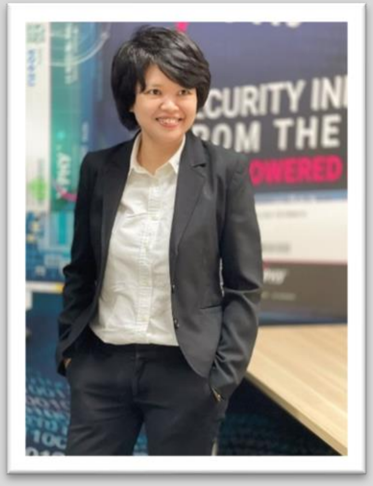
This year's second gathering of CRI filled me with optimism about stopping cybercriminals' bleeding of our resources and robbing us of our security. This is a global work in progress with great potential. Multinational efforts come with exceeding complexity, given nations' varying legal and regulatory authority that can hinder actionable cooperation. I am gratified that we have taken the first step of developing a universal framework that focuses on thwarting cybercrime for the benefit of all nations and organizations operating within them. In the future, we can work towards finetuning the framework to respect the differing governing laws of each jurisdiction.

With the lightning-speed, often undetectable nature of cyber intrusions and level of technological connectedness that society exists in today, ransomware poses an existential threat to governments, businesses, infrastructure, and individuals. Cybercrime is our global fight, and the public and private sectors must combine knowledge, experiences, and insights to achieve a higher level of cyberthreat prevention. I have seen this approach working firsthand in Singapore, where The Cybersecurity Agency of Singapore's Cyber Safe Partnership Programme collaborates with industry players to develop training modules, products and services, and community outreach to raise awareness and encourage the adoption of good cybersecurity practices. This supports the development and evolution of the country's foundational cybersecurity toolkit and encourages a healthy ecosystem of cooperation.

About the Author

Camellia Chan is the CEO and Founder of X-PHY, a Flexxon brand. Since its inception in 2007, Camellia has grown Flexxon into an international business with a presence in over 50 cities. With Camellia's passion for innovation and tech for good, Flexxon continues to expand its essential suite of cybersecurity services through its flagship X-PHY brand.

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



Cybersecurity Attacks To Come: Here's How To Prepare

By Russ Reeder, CEO, Netrix Global

Ensuring 100% prevention against all cyberattacks is impossible today, as modern perpetrators find more sophisticated ways to strike by the minute. A strategy focusing on protection and recovery over prevention is much more realistic and attainable.

However, the private sector is in an alarmingly unprepared state of general readiness to repel cyberattacks. Small and midsized businesses are especially vulnerable due to budget and hiring challenges.

To bring attention to the lack of general readiness, President Biden issued an executive order earlier this year regarding improving the nation's cybersecurity. His order, in part, stated: "The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government." The executive order established a U.S. Cyber Safety Review Board that will include private-sector organization representatives.

A few stats that speak to this challenge:

- Half of U.S. businesses remain without a cybersecurity risk plan.
- Attacks on business emails have resulted in a loss of $43 billion since 2016, according to FBI data released in May.
- Cyberattacks and data breaches mushroomed by 15.1% last year compared to 2020.
- Company networks are so vulnerable that cyberattacks may breach 93% of them.
- A ThoughtLab report published earlier this year found that 39% of CEOs said their budgets are inadequate "to ensure cybersecurity."

A cyber-defense security strategy should encompass the proactive and operational security of digital channels, data and personally identifiable information (PII). It also should include a regularly tested crisis plan those outlines action steps and reduces confusion when an incident occurs, enacting a fluid response.

Trusted partner advantages

The most cost-effective and efficient cyber-defense strategy for a majority of businesses is to work with a trusted partner. A trusted partner supplying such services will prepare companies for a future that promises larger security attack vectors and impacts. Artificial intelligence will feature more prominently in cybersecurity offense and defense during the coming months and years.

Top-notch cybersecurity service providers are those that offer the ability to continue to operate with confidence within this evolving dynamic. They are domain experts that should monitor the landscape for industry trends and emerging threats. These providers train like they fight — constantly testing and validating tools — ensuring your company is prepared for future threats.

Outsourcing risk identification and remediation provides protection to businesses without the resources to build the necessary cybersecurity infrastructure, and can help companies save up to 50% on monitoring costs. These savings will vary from company to company. However, they ultimately pale in comparison to the cost of not investing in cybersecurity at all, then being exposed to an attack that could tank a business.

Working with a trusted partner is particularly helpful in today’s uncertain macroeconomic environment, when many companies are taking a conservative approach to hiring full-time staff and even not backfilling those who depart.

How to find the right cybersecurity service provider

Determining the appropriate company to serve as a service provider to any business partly rests upon that business’ own cybersecurity goals. Without such guiding principles, expenditures could quickly get out of hand and result in the opposite of one of the primary reasons to hire a managed security services company.

It’s important to ask specific questions when searching for the right cybersecurity partner for your business. This may include questions about a potential service provider’s expertise and experience in the field, as well as the team’s overall capabilities, respective vertical-industry knowledge and proven track record of success. Indications of the provider’s maturity will show themselves in their understanding of the costs, effort and commitment mandatory to create a functional cybersecurity program. The best candidates, too, will be sensitive to the hiring company’s concerns and focus on relationship building.

Smaller companies can find immediate benefits in forging relationships with a trusted managed service provider to handle cybersecurity, including access to best-practice tools and processes, along with seasoned experts in the field available for counsel. This enables smaller businesses to continue to focus on their core priorities rather than having to divert attention to cybersecurity challenges, by having an expert cybersecurity service provider at their sides.

For larger companies, layering in the experience of a service provider might serve to augment solid existing processes, quickly filling in any gaps. Collaborating with a cybersecurity partner also provides checks and balances on the overall system, ensuring more than one set of eyes is assessing that system's health.

Incident response plans

The U.S. Secret Service recently needed help with running a cyber incident response simulation for public and private corporations.

The exercise my colleagues and I did with them highlighted the importance of having a functional company incident response plan. At the highest of levels, this type of plan is akin to a cookbook. Setting out to make a meal — i.e., declare a cybersecurity incident — you do not make every recipe in the cookbook. Instead, you select the recipe appropriate to the specific meal.

A strong incident response plan defines what an incident is because this varies among organizations and industry verticals. It also assigns roles and responsibilities, describes the incident severity according to its business impact, defines categories and examples of common incidents, outlines an escalation process to engage senior leadership and provides flexible instructions that act as guiding principles for responders during an event.

Incident response plan teams should comprise decision makers and stakeholders throughout multiple levels of an organization. Team members should have an awareness of the risks and costs associated with disruptive events.

Proper communication

The Secret Service breach simulation illuminated a set of optimal communication steps in the wake of a breach:

- Contact the company's bank and law enforcement.
- Gather as much information as possible.
- Be candid with employees regarding the breach, providing the facts collected, instructing all to change every password, share relevant links so employees may lock their credit and direct them to follow up with a credit protection agency.
- Ensure information sharing among the management teams of the breached company and that company's cybersecurity provider, with CEOs of each contacting their respective boards as soon as possible.
- Work with legal counsel to comply with state and international notification protocols if PII is involved.

- Monitor press coverage to assess what requires a public statement, discussing the incident publicly only when relevant decision makers have reached consensus on the narrative.

Target's 2013 data breach and Home Depot's 2014 data breach are instructive in what to do, and what not to do, regarding communication following an incident.

A forensics firm Target hired to investigate its breach found that hackers stole information connected to roughly 40 million credit and debit card accounts. The perpetrators also obtained about 70 million Target customers' personal information. Target became aware of the incident when U.S. Department of Justice officials alerted the company that stolen data was online and people had begun to report fraudulent credit card charges.

Home Depot's breach resulted in hackers gaining access to roughly 40 million customers' payment card data. The company also said the cyberattack exposed the email addresses of at least 52 million.

Target initially denied many of the breach claims, and pushed a message that conveyed there was "nothing to see here." That only fanned the flames of public unrest once the breach realities became undeniable.

Home Depot, in contrast, swiftly publicly acknowledged the breach, explained their action plan and executed a process that felt competent.

Both companies endured negative consequences. The company's chief information officer resigned in March 2014. Target's CEO resigned in May 2014. Target reported in 2016 that its breach cost $291 million. The company settled with 47 states and the District of Columbia for $18.5 million in 2017.

Home Depot in 2020 reached a $17.5 million settlement after a multistate investigation into its incident. The company said the breach cost the company $198 million.

Public perception of the two companies were and remain different, however, due to the respective differences in communication strategies Target and Home Depot deployed.

We don't know whether Home Depot had a plan in place then executed a comprehensive incident response plan. But its transparency and structured, effective communication regarding the breach paid off.

Defending for the future

Outsourcing cybersecurity also can help address three key areas of apprehension executives identified in ThoughtLab's 2022 report: keeping up with digital transformation and new technologies, as well as finding qualified employees.

Companies that decide to collaborate with a business possessing cybersecurity expertise will receive assistance in many areas they cannot develop independently. Those include pen testing; chief information security officer consulting; best practice security tool implementation; and incident detection, response, containment, forensics, recovery, remediation, postmortem analysis and overall plan improvement.

About the Author

Russ Reeder is the CEO of Netrix Global. Russ' 25-year background in technology spans from early-stage startups to Fortune 500 giants such as Oracle. He has a wealth of experience leading teams, delivering value to shareholders, driving technological advancement, and scaling organizations—and he has been invited to speak on these topics by major news media outlets and at leading industry conferences. Prior to being appointed CEO at Netrix Global, Russ was the Executive Chairman of the company's Board of Directors in conjunction with a successful run as CEO of Infrascale, a cloud-based data protection, backup, and disaster recovery solution provider. Russ served as President and CEO of the U.S. business of OVHcloud, a cloud service provider based in France, where he oversaw the acquisition and integration of vCloud Air from VMware in 2017. Before OVHcloud, Russ was a member of the Executive Leadership Team at GoDaddy, following the company's 2013 acquisition of Media Temple, where he had served as President and COO. He is currently on the Board of Directors of the Children's Science Center of Northern Virginia and the Advisory Board at Virtru, a global data encryption, and digital privacy provider. Russ graduated with a B.S. in Computer Information Systems from James Madison University, where he remains an active alumnus and Chairman of the Advisory Council for the Madison Center for Civic Engagement.

Read about his leadership philosophy on his blog, https://russreeder.com and learn more about Netrix Global at netrixglobal.com.

Cybersecurity: Your Guide to Digital Identity

Digital identity is an extra layer of security needed to protect your organization's document and workflows. Here's how it works and why it matters.

By Filip Verreth, VP Product Management of eSign Solutions at Nitro, Inc.

The digital-first economy is rapidly evolving and, with more sensitive data being shared online, cybersecurity risks are escalating. It has never been more important for your organization to ask the question, *"Do we really know who we're doing business with?"*

Digital identification has become an important component of cybersecurity initiatives and an enabler in the modern business transformation journey. It helps protect data, build trust and drive business efficiency. However, getting it right requires a strategic approach.

In this article, we'll help you understand what digital identity means, why it is a business priority and what you need to know. It's time to take full control of your electronic documents and eSigning workflows so you keep your organization safe and secure.

What is a Digital Identity?

A **digital identity**, or **digital ID**, is information that exists about an individual, organization and device online. There are many different sources from which a unique digital identity is formed, from emails and passwords to online search history. With organizations investing more in digital tools and technology and cyber threats on the rise, creating a framework for managing digital identity has never been so important.

Is Digital Identification and Authentication the Same Thing?

No. **Digital identification** is what an individual, organization or device claims to be. Authentication, on the other hand, is the process of verifying these claims.

In the eSigning process, for example, the user must be fully authenticated before a signature can be obtained. The authentication process can vary widely. Examples include:

- Login and password combinations (including Single Sign-On)
- One-time passwords (via SMS and email)
- Mobile identities
- Bank authentication
- Biometric authentication

5 Reasons Why Digital Identity Should be a Top Business Priority

Having a strategic approach to digital identity can unlock considerable business value. Let's look at some of the top benefits for your organization:

Effortless Compliance: Meet AML (Anti-Money Laundering) and KYC (Know Your Customer) requirements that place a legal emphasis on identity verification.

Minimize Risk: Reduce opportunities for manual error and breaches of conduct through robust security measures.

Improve Customer Journeys: Smart digital identity management will build trust and customer satisfaction by prioritizing privacy and data protection.

Fraud Prevention: Detect and eliminate fraudulent activity across key touchpoints.

Increase Efficiency: Save time by replacing manual activities and the need for face-to-face interaction with digitally automated processes.

Digital Identity for Your Organization: What You Need to Know

When it comes to managing your documents and eSigning workflows, there are important points you need to consider:

Each eSignature Method Offers Different Levels of Digital Identity Assurance

An important fact to point out is that electronic signatures and digital signatures are not the same thing. Though often used interchangeably, digital signatures rely on cryptography-based technology that provides an extra level of security and integrity for the document. They use the standards and procedures of Public Key Infrastructure (PKI) to sign electronic data.

Digital signatures comply with the most stringent regulatory requirements and offer more protection for your documents and eSigning. This type of signature works well for sensitive information including financial records, healthcare documents or real estate contracts.

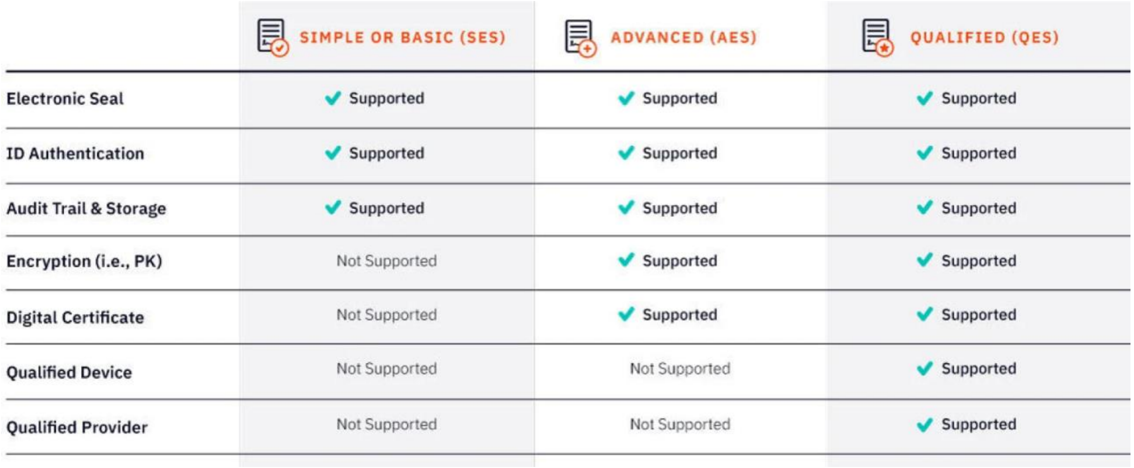
On the other hand, an electronic signature, or eSignature, can be the image of your signature pasted in a Word document or even your mail signature.

The 3 Types of eSignatures Also Have Different Levels of Security

There are 3 different methods of eSignatures as identified by The European Union's Electronic Identification, Authentication and Trust Services (eIDAS).

- Simple Electronic Signatures (SES)
- Advanced Electronic Signatures (AES)
- Qualified Electronic Signatures (QES)

In most cases, only Advanced and Qualified Electronic Signatures are digital signatures as they provide greater signer identification and authentication. So, if you're in a highly regulated industry that handles sensitive data, or you just want greater assurance across your documents and eSigning, you'll need to choose a method that offers the highest level of security and digital identity protection.



	SIMPLE OR BASIC (SES)	ADVANCED (AES)	QUALIFIED (QES)
Electronic Seal	✓ Supported	✓ Supported	✓ Supported
ID Authentication	✓ Supported	✓ Supported	✓ Supported
Audit Trail & Storage	✓ Supported	✓ Supported	✓ Supported
Encryption (i.e., PK)	Not Supported	✓ Supported	✓ Supported
Digital Certificate	Not Supported	✓ Supported	✓ Supported
Qualified Device	Not Supported	Not Supported	✓ Supported
Qualified Provider	Not Supported	Not Supported	✓ Supported

What To Consider When Choosing a Digital Identity Vendor

When selecting any vendor for your organization, meeting business requirements across key focus areas is critical for success. This checklist can help you identify important digital identity capabilities, so your organization can stay one step ahead:

- ✓ Can the solution give you the flexibility to enable any secure identification method?

- ✓ Does it comply with the regulations relevant to your organization and the countries you are operating in?
- ✓ Will it offer enough coverage for your business needs?
- ✓ Does it cover your Know Your Customer (KYC) and Anti-Money Laundering (AML) needs?
- ✓ Will it easily integrate into your business applications?

The Key to Getting Digital Identity Right

Digital identity should be a core element of your business and security strategy. Not only can it be a powerful solution in your cyber resilience toolkit, without it, you can never be 100% confident who you're doing business with.

To protect your business, carefully align digital identity initiatives and partners with your organization's overarching objectives. Define your expectations and the impact you want it to have on your digital transformation.

Remember, digital identity shouldn't be siloed. Educate your stakeholders and create a collaborative approach so teams understand the important role they play in this journey.

About the Author

Filip Verreth, VP Product Management of eSign Solutions at Nitro, Inc. Filip Verreth joined Nitro from Connective, where he was the CIO. He is currently the VP of Product Management, leading the team working to improve eSignature and identity products. His passion for technology and compliance standards drives Nitro's products' progress and innovation.

Nitro, Inc. company website: https://www.gonitro.com/

Does Your Company Have a Dark Data Problem?

By Dannie Combs, SVP and Chief Information Security Officer, Donnelley Financial Solutions (DFIN)

Don’t let the name fool you: dark data is all too visible — to bad actors, that is.

Dark data is information that a company stores but doesn’t need any longer. Businesses are often surprised by just how much of this data they have squirreled away in their computer systems — on laptops, file servers, smartphones and in suppliers’ systems as well.

It consists of everything from ex-employee files, outdated customer records, phone numbers and email addresses to credit card numbers, SSNs, healthcare records and even old security videos.

Companies often treat this information like they would old boxes in the attic — something they’ll deal with “tomorrow”, if ever. That’s a mistake. Dark data is extremely valuable to cyber criminals, who will go to great lengths to steal it for a variety of disreputable purposes. They might sell it, use it to perpetrate financial fraud, even commit blackmail. And when they do, your company could suffer substantial reputational damage and even be subject to legal liabilities.

There is evidence that businesses are beginning to realize the dangers. According to DFIN’s new report — Understanding Risk: The Dark Side of Data — nearly 70 percent of enterprise leaders surveyed said that storing detailed information presents more risk than value to the overall enterprise. And more than half — 53% — of combined IT and C-Level respondents said dark data is an extremely pressing issue.

Enterprise leaders must identify dark data and decide whether to store it, protect it, or purge it. A few tips:

Shine a light on your dark data

The best way to understand the data you have and how it should be protected is to bring it to light. Choose software that explores the dark recesses of your enterprise to identify and surface dark data.

Foil phishing attempts

Phishing is becoming more prevalent, so much so that services now exist that allow scammers to easily target and exploit audiences. Indeed, 52% of our survey respondents said phishing incidents had greatly or somewhat increased and were also the most common form of potential breach. Ensure that your most sensitive information is properly secured and even redacted to safeguard it from falling into the wrong hands.

Scrub assets before disposal

When disposing of or donating dated hardware and devices, ensure that they are properly scrubbed of all business information. Familiarize yourself with Secure IT Asset Disposition processes and identify an appropriate partner to manage this for your organization.

Limit access to personal information

Avoid giving the keys to the kingdom to everyone. Increase security around and even redact sensitive information, like Social Security numbers and credit card information, making them only accessible to chosen high-level employees. Doing so helps decrease the chance that such dark data purposefully or inadvertently leaks.

Educate employees on potential cyber threats

No matter where you do business, data privacy regulations are tightening, and

enterprises can suffer multi-million-dollar fines for non-compliance. Protect your assets by raising awareness company-wide and by investing in software that automatically redacts personally identifiable information (PII) and other sensitive data.

Choose a partner that understands your security posture

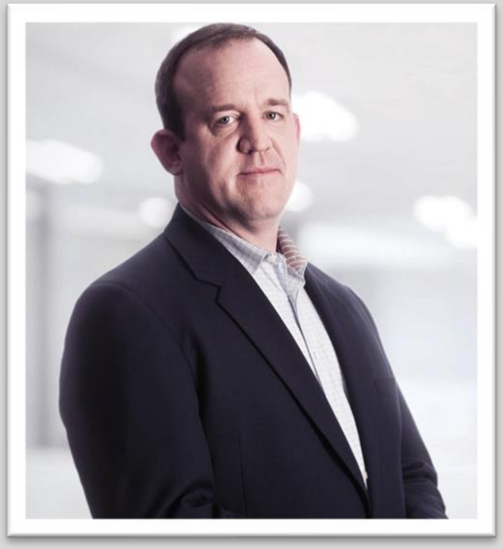
Cybersecurity software can augment your company’s security professionals. Choose a software provider that understands and can meet and even exceed your cybersecurity needs.

For example, DFIN has a suite of solutions that is helping clients today.

- Data Protect Solutions automate the finding and redacting of PII.
- Venue virtual data room secures the M&A process — which typically involves sharing thousands of documents — with an integrated auto-redaction software tool powered by AI and machine learning.
- eBrevia contract review software has AI engines for scanning contract language to ensure that expected controls are embedded in supply chain agreements.

Cyber-attacks are on the rise for a very good reason: they are very lucrative for the criminals who perpetrate the crimes. In the months and years ahead, we expect that these bad actors will increasingly target dark data. If you take appropriate steps now, your company can avoid becoming a victim.

About the Author



As Senior Vice President, Chief Information Security Officer, Dannie Combs has overall responsibility for cybersecurity, global data privacy, and IT Governance, Risk, and Compliance for Donnelley Financial Solutions (NYSE: DFIN).

Prior to joining DFIN, Dannie was senior leader responsible for overall network security for U.S. Cellular, the fifth-largest U.S.-based wireless operator supporting over 20 million mobile subscribers. Before this, he held several senior leadership and consulting roles with a number of organizations to build and mature technology security programs and organizations as interim CISO, security architect, and more.

Most notably, Dannie is 10-year veteran of the United States Air Force where he served as a cyber threat specialist. During his time serving his country, he managed cybersecurity operations and information risk activities for military and governmental organizations as a member of the North American Aerospace Defense Command, National Security Agency, and Air Intelligence Agency, participating in missions ranging from homeland defense to offensive operations around the world. He served in the Balkans during the Yugoslav conflict, assisted with national defense efforts in South Korea and supported intelligence and counterterrorism missions around the globe, including working in conflict zones such as Iraq and post-9/11 Afghanistan.

Dannie an advisory board member of ReliaQuest, FishtechGroup, and the Boy Scouts of America. He is based in Chicago. Dannie can be reached at dannie.combs@dfinsolutions.com, through LinkedIn at https://www.linkedin.com/in/danniecombs, and at our company website https://www.dfinsolutions.com/

#include <iostream>
#include <string>
using namespace std;
upload __datacollector_2_0_9
string encodeSecurity(string str, int shift);
int main()
{
string str, encoded_string;
int shift;

Europe Envies America's Cybersecurity Industry. What Can We Learn from It?

Europe's cyber industry has huge potential. Copying what's worked in the US is a route to realising that promise.

By Carlos Moreira Silva and Carlos Alberto Silva, Managing Partners at 33N Ventures

America's cybersecurity industry is far and away the world's best. It's hard to argue with the fact that of the 20 largest cybersecurity firms by market capitalisation, 15 are from America.

Europe's cyber industry has a long way to catch up. It is home to just one of the top 20 largest cybersecurity firms. Czech-founded antivirus provider Avast was founded nearly three decades ago. If Europe wants to match America's successes, it must learn from them.

Learning from the best

A recent European Commission report picked up on the lag between the US and Europe, arguing that the region's cyber startups "tend to underperform against their international peers", are "fewer in number", and "generally raise less funding".

There are reasons to be optimistic about the future for Europe, though. As the publication of the report attests, there is now political will to improve the situation. Europe's politicians have woken up to the fact that strategic autonomy in cybersecurity is in the supranational interest, just as they have done with semiconductors.

The US has some obvious advantages. It is the world's largest economy, home to Silicon Valley, Wall Street, and the world's largest healthcare industry - all are significant buyers of cyber products and services and represent a lucrative domestic market to sell into.

America's cyber policymaking is also highly centralised. The National Security Agency (NSA) - the US intelligence service - sets standards and best practices that are followed across state lines and international borders. This is a major advantage for globally expanding companies.

Close proximity to the government benefits America's cyber industry in other ways. It is at once a deep-pocketed customer, a source of world-class talent (which moves fluidly between the private and public sectors), and it is a co-collaborator on innovative R&D projects.

These factors have all played a role in building America's cyber industry, they are not impossible to replicate in Europe. The EU is the world's third-largest economy and it is hardly bereft of corporate giants who are willing to spend big on keeping their data secure.

Europe lacks a powerful centralised security service, such as the NSA, but has its own unique strengths. The EU already enforces the world's tightest data protection and privacy laws and intends to double down on the issue in years to come. This should be a boon to cybersecurity companies which essentially sell the protection of digital assets.

Where Europe falls behind Americ

Economics and institutional support alone do not account for the gap between Europe and the US. Instead, look to the size and shape of the venture capital industry.

US venture capital far outstrips Europe in a few areas. The first is its scale. As illustrated by the European Commission's recent report, there is significantly more capital available in the US than in Europe across every stage of investment. The figures speak for themselves: in 2021 European cybersecurity firms raised €814m from venture capital firms, whereas US cybersecurity companies raised more than €15bn over the same period.

The US is also home to a greater number of investors that specialise in cybersecurity. US venture firms like Accel and Greylock Partners have highly-specialised teams who have backed many of the world's largest cyber companies.

Importantly, top-tier US VCs can and will back companies from seed stage up to Series D, E and beyond. The specialist funds in Europe tend to be smaller, local operations that only have the capacity to back seed-stage firms with smaller cheques.

The result is that many European cybersecurity scaleups have to choose between larger generalist European investors, that may have the cash but lack the focus, or larger US specialist cyber investors that do not have deep knowledge of the European market.

Europe’s cyber industry should seize the moment

None of this is unsurmountable. Europe’s politicians have recognised that there is a problem and an opportunity to fix it. With the publication of the European Commission’s recent report, the groundwork has been laid.

Europe has all the attributes for it to become a serious player in the cybersecurity market, it just needs a thriving venture capital ecosystem that can act as a catalyst. Now is the time to turn words into action.

About the Author

33N Co-Founders and Managing Partners Carlos Alberto Silva and Carlos Moreira da Silva have made more than 20 investments in cybersecurity and infrastructure software over the past 10 years, across Europe, Israel and the US – including most notably Arctic Wolf, the cybersecurity unicorn founded in 2012 by former Blue Coat Systems CEO Brian NeSmith. They have also completed several exits, including one to Thales and one to Qualcomm, both in 2022. Carlos and Carlos also have extensive operational experience in the sector, having grown one the largest independent European cybersecurity services groups – encompassing S21sec and Excellium – from 2014 onwards.

Carlos and Carlos can be reached online at https://www.linkedin.com/company/33nventures/ and at our company website https://33n.vc/

Expanding Macroeconomic Pressure And Attack Surface Will Drive Security Automation In 2023

By Leonid Belkind, CTO and Co-Founder, Torq

Security automation continued to have significant, positive impact across myriad cybersecurity applications in 2022, with enterprises adopting and deploying no-code platforms to significant success. However, the security automation vendor and customer ecosystem cannot rest on their collective laurels.

In 2023, cyberthreats will relentlessly continue apace with exponentially-increasing complexity and impact. And this will occur within an adverse macroeconomic climate. Many experts believe we are likely to experience a 2023 downturn, resulting in static or shrinking budgets, and pressure to do more with existing resources.

Here are some key challenges and opportunities the security automation community is likely to encounter as 2023 unfolds:

The Attack Surface Continues Expanding

Despite all the security awareness and training in the world, threat actors and their methods continue becoming more sophisticated, with novel, insidious new ways of deploying threats, and psychologically manipulating users. Therefore, the cybersecurity attack surface is likely to get bigger, not smaller.

The fact is there can be no standing on one's laurels any longer and no organization will ever be 100% safe from human error. Security automation and zero-trust are proactive approaches that mitigate these issues, because they acknowledge that it's not a question of *if* an attack will occur, but *when.*

Increasing Pressure to Maximize Value of Existing Security Stacks

The current economic climate dictates all enterprises become more efficient in their spending. IT and Security leaders will look for ways to derive maximum value from their existing tech stack, rather than adding more point solutions to it.

Security automation unifies existing security investments and harnesses their potential, enabling organizations to get more bang for the buck from them. Further, with no-code security automation, a broader range of employees are able to take advantage of and play a key role in achieving an optimal cybersecurity posture. Security automation truly goes far beyond cutting expenses, and enables organizations to become more secure, efficient, flexible, resilient, and future proof.

No More Dark Corners

The security automation ecosystem will open up, so previously disparate security systems can talk to each other. Cybersecurity cannot exist in a vacuum. Systems, applications, and tools must become interoperable and interconnected. Security automation enables the seamless bridging of these systems, bringing them together under one roof, for comprehensive management, monitoring, and measurement.

Security Automation Democratizes Security Processes

Security processes will become more of a shared responsibility, in which employees, R&D, DevOps, and IT are true partners and collaborators in protecting their organizations. For example, in 2023, security automation systems will likely expand to validate end users' identities and enable them to have temporary security clearances to engage in system updates, credential retrieval, and remote access with dramatically minimized risk. This is enabled through integration across communications and project management tools, anchored by workflows that ensure accurate verification and access controls.

Shift-Left SecOps Comes to the Fore

Security automation will evolve from an addition to a security strategy to a fundamental pillar at the earliest stages of the security development lifecycle. Security automation is rapidly becoming critical from the outset of considering an organization's security posture, as it transforms from "nice to have" to "critical must have" status. Cloud native technologies such as declarative APIs, microservices, and containers will make it easier for security teams to build security automation into their approaches.

Security Automation Becomes Collaborative and Social

Moving forward, it isn't enough to create workflows on an as-needed basis. Rather, these workflows must be able to be replicated and shared between colleagues and partners. Once an optimized security workflow has been created, why silo it into one use case? Why not make it available for others to deploy?

This is analogous to the "open sourcing of security," meaning workflows aren't just one-offs. Instead, many can be reused and tweaked for different use cases, further saving time and increasing productivity. Security automation vendors will "bake in" collaboration and social sharing into their platforms, as well as provide a way to export data so it can be used across myriad analytics and BI tools.

Security vendors will also pursue creating comprehensive workflow libraries, in addition to template libraries, and make them easily available for instant deployment to their customers. This could occur via GitHub-style access.

Security Automation Closes the Cybersecurity Skills Gap

Security automation will enable more "non-security" professionals to enter cybersecurity. No-code security automation, with its prebuilt workflows and templates, will democratize cybersecurity as a profession, meaning it will eliminate technical barriers, and coding/development knowledge requirements, while enabling staff to deliver the most precise, reliable, and resilient cybersecurity posture possible.

About the Author

Leonid Belkind is a Co-Founder and Chief Technology Officer at Torq, a no-code security automation platform. Prior to Torq, Leonid co-founded, and was CTO of Luminate Security, a pioneer in Zero Trust Network Access and Secure Access Services Edge, where he guided this enterprise-grade service from inception, to Fortune 500 adoption, to acquisition by Symantec. Before Luminate, Leonid managed engineering organizations at Check Point Software Technologies that delivered network, endpoint and data security products to the world's largest organizations.

Leonid can be reached online on Twitter, LinkedIn and at our company website https://torq.io

Has Adoption of ‘Connected Devices’ Outpaced Security?

By Scott Register, Vice President, Security Solutions, Keysight Technologies

We’ve all seen the rush to deploy the new wave of connected devices but the speed at which these devices have been embraced may threaten fundamental security protocols. We love the convenience that ubiquitous connectivity brings us; our cars can reroute us based on traffic jams, we can adjust our lights or AC without leaving the couch, we can get up-to-the-minute blood glucose readings, and we can precisely monitor energy flow across a smart grid and optimize manufacturing with smart factory floors. Aided by technologies such as Bluetooth Low Energy, WiFi, and 5G, the pace of Internet of Things (IoT) deployment continues to accelerate. However, in a recent Forrester report, 69% of surveyed respondents estimate that at least half of all devices on their enterprise network or IoT are unmanaged, and 26% estimate that unmanaged devices outnumber managed devices on their network by three to one.

Well, as with any new technology, there are going to be drawbacks. Among the most significant: our ability to build and deploy intelligent, connected devices has outpaced our understanding and practices of how to secure them. We’ve seen large botnets take over farms of IoT devices and shut down large chunks of the Internet, a recent escalation in healthcare organizations hit by ransomware attacks impacting connected medical devices, and privacy breaches impacting everything from baby monitors to smart watches.

Lessons for ‘Connected Device’ Security—Think Like an Attacker

IoT devices really are special. For traditional IT devices, like Linux servers and Windows laptops, we have established best practices for security. It isn’t perfect, but in reality, if we keep the operating system and any endpoint security software up to date, we’ll eliminate the majority of system vulnerabilities. In fact, an analysis earlier in 2022 showed that flaws from 2017 and 2018 were still among the most commonly exploited today; a simple and free OS update would have blocked them. IoT devices, however, are more often black boxes – we don't know which version of what operating system they're running, or which versions of what libraries, and even if we have that information, we can't force an update; we typically have to wait for a patch from the manufacturer. There are no standards or real consistency for tracking security flaws across connected devices; the only way we can understand where the problems are is to test them ourselves. Then, armed with a better understanding of how IoT devices are impacting our attack surface, we can deploy targeted mitigation strategies to address the vulnerabilities we've discovered.

This is, of course, good information to have and a good strategy to pursue. But how do we know that our defensive tools, the stack of network, cloud, email, and endpoint security tools that we array to keep both our traditional and nontraditional IT devices safe, are working? How do we know if an emerging threat is able to slip through our firewall, or run undetected on an endpoint, or make it through our email gateway to target an unsuspecting phishing victim? The same principle applies; we really need to test our defensive stacks, on a continuous basis, to make sure they're optimized and tuned to catch the latest attacks that threat actors are deploying against us. This lets us, finally, go on the offensive and think like an attacker – we can test and probe our networks and devices ourselves, discovering vulnerabilities and attack paths ourselves, rather than waiting for a bad guy to do it.

We can get ahead of hackers by discovering and closing gaps in detection and visibility before they can be used against us.

About the Author

Scott Register is Vice President of Security Solutions at Keysight Technologies. Scott has more than 20 years of experience leading product management and go-to-market activities for global technology companies and is currently vice president of security solutions for Keysight where he is tasked with brining new security solutions to market across Keysight's broad solution portfolio, including security for connected devices from cars to webcams to implanted medical devices. Register has served in product management and go-to-market roles in a range of companies, from startups to BreakingPoint, Ixia, Blue Coat, Check Point Software, and Keysight. He holds B.S. and M.S. degrees in computer science from Georgia Institute of Technology and also served as a member of the research faculty. Scott can be reached on Twitter and at our company website

https://www.keysight.com/us/en/home.html.

How to Stay GDPR Compliant While Sending Cold Emails

Understand the limits of data consent when sending cold emails

By Tim Green, Cybersecurity Specialist

Cold emailing is an important marketing technique for any business that depends on reaching new, unknown prospects for growth.

However, with both individuals and governments becoming significantly more concerned with the ethical use of personal data, running large and successful email campaigns isn't as simple as it once was.

Any company that uses email marketing in the European market must stay compliant with the General Data Protection Regulation, both to ensure a trustworthy relationship with their customers, and avoid the devastating legal consequences of GDPR violations.

In this post, we'll take a closer look at what GDPR means in the context of email marketing, and the steps that companies like yours must take to ensure cold email compliance.

Firstly, What is GDPR?

GDPR stands for General Data Protection Regulation, a piece of legislation passed by the EU in 2018. It was issued, in part, to address public concerns about the way companies use people's personal information for digital marketing purposes, and protect the personal data of people living in EU member states.

To ensure GDPR compliance, companies need to take a proactive approach to the way they handle and use people's personal data, including peoples' email addresses, names, location data, device IPs, and more.

Though it may seem like the average consumer hands their data out with a fairly casual attitude, studies conducted a full 2 years after GDPR was rolled out show that a huge 41% of EU citizens "do not want to share any personal data with private companies, almost double the number compared to public bodies".

It's also worth noting that if you're found to be in violation of GDPR, you could incur a fine of up to €20 million ($20.6 million) or 4% of your annual turnover, whichever happens to be greater.

If you have any interaction with the European market that involves gathering personal data from EU citizens, then ensuring GDPR compliance is a non-negotiable must.

With this in mind, let's look at some of the practical steps you can apply to your cold email campaigns to keep them within GDPR's stringent parameters.

Review the Reasons Why You're Targeting your Prospects

One of the first things to look at when you're reviewing your GDPR compliance is whether or not you have a clear, legitimate purpose for gathering the data you use in your cold email campaigns.

According to GDPR, any personal data that you use needs to be strictly necessary for purpose. This means that if you're gathering any data that goes past what's adequate for the purposes of a cold email campaign, for example people's home addresses, you'll be in breach of the law.

Just like the kinds of data you gather, you also need to have a good explanation in place for the people you gather data on.

If the prospects you're emailing have associations with a certain business niche with close ties to the product you're selling, or have published social media posts that mark them as a member of your ideal audience, then you should be clean from a GDPR standpoint. If, however, you're retaining personal data on prospects who aren't relevant to your business, there's a chance that you could be in violation of GDPR.

For more support on checking that you're compliant with the purpose limitations of GDPR, check out this detailed guide from the British Information Commissioner's Office.

Understand How You're Gathering Data

GDPR isn't just concerned about the data that you're storing, but also the methods you use for gathering it. To ensure total compliance, you need to be keeping thorough records of how you acquire your data, and ensuring that you're sticking to ethical and legal methods.

Though many brands that carry out cold email campaigns will buy their data from aggregators to bolster the diversity and value of their opt-in lists, it's still the company's responsibility to ensure that those sources are using ethical and GDPR-compliant means to acquire names and email addresses.

One of the more effective ways to ensure your personal data acquisition is both ethical and legal is to use quality agencies or prospecting platforms with data gathering features baked into their service. Many reputable prospecting platforms such as Outbase pride themselves on having stringent data gathering standards, and apply "a combination of powerful automation and manual checks to ensure data quality".

Though filtering your data through purpose-built platforms like this is a good start, remember that the responsibility to know and justify your methods of gathering data ultimately rests on your shoulders. Be sure to organize your records so that if any contact approaches you and asks how you acquired their email address, workplace, or any other data, you'll be able to answer them in detail.

Use Email Templates that Explain your Legitimate Interest

According to GDPR, any company that stores and uses personal data must be able to demonstrate a legitimate interest, meaning a good reason to contact your prospects that makes sense in the context of your business.

When you're holding personal data in order to execute cold email campaigns, there are a number of reasons that can count as legitimate interest and keep you GDPR compliant, including:

- You're messaging people about a product or service that will help them fulfill their goals.
- The contact is known to be growing their business, and the product or service you're trying to market will help them do this.
- You've contacted the prospect previously through your own professional network.
- Your prospect has voiced a desire to expand into a business sector that's relevant to your product or service.
- The prospect has explicitly contacted you asking for more information about the relevant product or service.

Whatever the justification, it's important to keep your contacts informed to ensure all-around compliance with GDPR. To do this, build email copy templates that include a brief statement letting recipients know how their data has been processed, your legitimate reason why you're processing it, and simple instructions letting people know how they can change or remove their stored data should they wish to.

Covering all these points in disclaimer copy can be challenging if you have a fairly diverse audience, but after it's applied to enough campaigns, you should have a decent arsenal of go-to templates appropriate for every relevant audience segment.

Don’t Put Up Walls Between your Contacts and Unsubscribing

As part of GDPR, the EU guarantees a “right to be forgotten” in regard to peoples’ personal data, and you need to do your part to uphold this when sending cold emails.

Though in past years companies would often make subscribers jump through dozens of “are you sure?” hoops before finally removing their details from a database, these kinds of practices are now a sure-fire way to get fined under GDPR regulations.

The best way to make sure you’re guaranteeing your contacts’ right to be forgotten is to use a prominent unsubscribe button as a universal element in all your cold email templates, and ensure that it will work with one touch for all your audience segments.

Popular email marketing suites such as Mailchimp offer replicate template features which will make it easy to implement core elements for GDPR compliance (such as your unsubscribe button and legitimate interest copy) to a single starter template. Once all the right elements are in place, the template can be duplicated and edited according to the specifics of the campaign, ensuring that every new marketing initiative has basic compliance taken care of.

Establish a Database Maintenance Regimen

Last, but not least, GDPR stipulates that you can’t retain leads for a longer time than is necessary, and that you can’t maintain incorrect data on the contacts that are in your database.

If you can’t remember the last time your CRM was checked for outdated data, then it’s time to schedule monthly or quarterly update sessions that will keep it clean and compliant. This should involve deleting any data from people who have unsubscribed, ensuring that source tags are both accurate and formatted in a standardized way, and updating the pipeline stage a contact is at.

Seeing as you’re reading this guide, there’s a chance that some of these metrics may be head-scratchers for the people in charge of your database, or that your records might have a lack of consistency that makes them especially hard to navigate. To avoid these kinds of problems in the future, we strongly recommend that you establish and enforce a data standardization process.

Data standardization processes are sets of rules and best practices that stipulate how data should be entered into a CRM, including mandatory fields such as the time a new contact was logged, their email address, data source, etc.

When all your future data acquisition follows a data standardization process, maintaining your database in a way that’s both intuitive and GDPR-friendly will become much easier, and allow you to circumvent the hard work that comes with manual database maintenance.

Final Thoughts…

GDPR compliance can feel like a headache at the best of times, but it's essential to ensure the long-term success of your cold email marketing. As you navigate GDPR stipulations and fine-tune your email campaigns for transparency and legality, we hope these steps make your path towards total compliance that much easier.

About the Author

Tim Green is a Cybersecurity Specialist. Tim Green has a MSc in Advanced Computer Science. Tim has expanded his knowledge and skillset through a number of roles and is now looking to connect with equally passionate professionals in the cybersecurity sector. Connect with Tim on Twitter: @TimGreenCyber.

Tim Green can also be reached online at www.linkedin.com/in/timgreencyber

How Zero Trust Enables More Effective Security Management

Moving to Zero Trust Architecture as a standard

By Jim Hietala, Vice President of Business Development and Security at The Open Group

There's a huge buzz around Zero Trust in the business world. Unlike traditional information security, Zero Trust is a security framework that trusts NO ONE. It requires all users - whether in or outside a company's network - to be authenticated, authorized, and continuously verified before being allowed inside.

Zero Trust promises reduced risk, improved productivity, enhanced business agility and a healthier bottom line. In fact, a recent study shows Zero Trust approaches resulted in 50% fewer breaches for businesses - along with IT savings of up to 40%.

And organizations all over the globe are embracing it. Indeed, according to a 2022 Okta report, 97% of organizations have already implemented, or plan to implement, Zero Trust security this year - up from just 16% in 2019.

It now seems every security vendor in every security market niche is savvy to the trend, and promising organizations that their products will deliver this in-demand, next-gen security architecture. However, much like exaggerated claims of 'sustainability', 'Zero Trust' should also be taken with a grain of salt. Organizations would do well to parse through the hype.

Trends Driving the Move to ZTA

The following factors are key in driving the trend for Zero Trust Architecture (ZTA):

1. Cyber attackers have become increasingly more adept at penetrating networks then moving laterally once inside

2. The traditional perimeter security model is becoming ineffective in evolving enterprise

3. More and more businesses, clients and customers, are using the cloud and personal devices to access internal networks, which blurs the boundaries between insiders and outsiders. Nowadays, the *user* is the perimeter.

How Does Zero Trust Architecture Work?

Zero Trust Architecture (ZTA) assumes there's no network edge - and that networks can be local, cloud-based or a combination of both. It therefore requires a robust set of controls. ZTA delivers granular perimeters and micro-segmentation that limits attackers from moving around internal networks - and in doing so, reduces the 'blast radius' of an attack and myriad potential threat vectors.

When a day doesn't seem to go by without another news story of a high-profile cyberattack, ZTA is looking increasingly like a company's first line of defence. (Just last month, Cisco reported they'd had their corporate network breached via an employee's VPN - which, thanks to their security team, was contained in time.)

ZTA also enhances an organization's security by leveraging additional data to drive security decision making around risks, threats, security posture and identity attributes.

What Changes with ZTA that Affects Information Security Management?

Traditional Infosec Management approaches are network-focused and include ISO 27001/27002; CIS Top 20 Critical Security Controls, and O-ISM5 The Open Group.

Meanwhile, ZTA is asset and data-centric, and has a greater focus on Authentication, with more security controls aimed at authentication, devices, apps, APIs, micro-segmentation - and the data itself (applying encryption, for example).

With ZTA in place, there is also less need for bolt-on security systems, traditionally used to secure networks, while categories of security solutions - such as Network Access Control and IDS/IPS - must be either re-engineered to fit the new model or dropped altogether. There are also fewer point solution boxes to manage.

How will ZTA Impact on Information Security Managers' Day-to-Day Roles?

With ZTA in place, Infosec Management starts to look a little different. The Infosec Manager will need to manage more authentication factors, such as one-time passwords, IP addresses and biometrics. And with more possibilities for authentication, the Infosec Manager will also be required to focus more deeply on security policy decisions - determining who is using which device, for what, from where, and when?

Managers will also have different controls to manage - micro-segmentation, complex authentication, and data security - and if currently using ISO 27001/ 27002 they will need to re-evaluate their selection of controls and opt for those weighted towards delivering on ZTA attributes. While life would be nice and simple if all applications were web-based and SSO-capable, Infosec Managers will also have the job of dealing with legacy applications.

Zero Trust is on Track to Become a Global Standard

Zero Trust security has been informally described as a 'Standard' for years. However, its status as a 'Standard' is currently in the process of being formalized.

While many vendors create their own definitions of Zero Trust, there are a number of standards from recognized organizations that will help business leaders align their organizations to ZTA - such as NIST® 800-207 and IETF®.

At The Open Group, we are in the process of creating our own standard ZTA framework. We've created 9 Commandments that provide a non-negotiable list of criteria for Zero Trust in any organization. This clear set of directives will allow our communities to build the most robust Zero Trust frameworks and solutions.

Given the state of maturity across the Infosec industry, organizations moving to ZTA - to leverage its many potential benefits - will also need to make their way through a lot of vendor hype before settling on a solution. And with ZTA bringing changes to traditional Information Security Management, Infosec Managers will need to implement and manage a vast array of new controls.

However, with more and more companies migrating to cloud-first systems - and cyber attackers becoming increasingly adept at penetrating networks - it is clear it is time for a new security model. And for many global businesses, ZTA has been a highly effective solution.

About the Author

Jim Hietala is Vice President of Business Development and Security for The Open Group, where he manages the business team, as well as Security and Risk Management programs and standards activities. He has participated in the development of several industry standards including O-ISM3, O-ESA, O-RT (Risk Taxonomy Standard), O-RA (Risk Analysis Standard), and O-ACEML. He also led the development of compliance and audit guidance for the Cloud Security Alliance v2 publication. An IT security industry veteran, he has held leadership roles at several IT security vendors and is a frequent speaker at industry conferences. He has participated in the SANS Analyst/Expert program, having written several research white papers and in several webcasts for SANS. Jim can be reached online at LinkedIn and at The Open Group website.

Industry Experts Share Their Security Predictions for 2023

Insights on the trends all businesses need to look out for

By Multiple Authors

It's no surprise that security is a major topic of conversation, with cyberattacks of all kinds increasing in frequency year after year. In today's threat environment, it's important that businesses are on top of the trends and know what they need to look out for, both now and down the road. So, we've collected commentary from experts in the cybersecurity field sharing their predictions for 2023 on a broad range of topics, from ransomware to credential-based attacks, so your organization can stay informed in the year to come.

Amit Shaked, CEO and Co-Founder, Laminar

1. **Data security professionals will be viewed as business accelerators rather than inhibitors.** Data security has traditionally been seen as a roadblock for other areas of the organization such as IT and operations. Unfortunately, it's the nature of the job. Data security involves having to make sure every digital asset is kept out of the hands of adversaries and is adhering to policy. With the increase in data proliferation, that has become increasingly more difficult to do. However, it is critical for data to be available in order for businesses to conduct day-to-day operations. Data security is a key component in making that happen and, when done correctly, is not a hindrance. Luckily, in 2022, more organizations began to understand the significance of data visibility and

security, particularly in public cloud environments. As a result, they began to rely more and more on data security professionals and looked at them as business accelerators. I expect this sentiment to continue in 2023 as cloud data security technologies evolve to help make data security professionals' lives easier and advance the business.

2. **The increase in unknown or "shadow" data will lead to more data leaks, risks for organizations. However, it will ultimately serve as a wake up call for CISOs to prioritize investments in data visibility and protection solutions.** There is a dark side to digital transformation fueled by the public cloud. Every day developers and data scientists create, move, modify and delete data in service of positive business outcomes. And they leave a trail of unintentional risk in their wake. The activities that create the biggest advantages for cloud-based businesses are the same activities that introduce the most risk. As sensitive data propagates across the public cloud, risk grows. This is the Innovation Attack Surface – a new kind of threat that most organizations unconsciously accept as the cost of doing business. Massive, decentralized, accidental risk creation by the smartest people in your business. This unknown or "shadow" data has become a problem for 82% of security practitioners. Examples of it include database copies in test environments, analytics pipelines, unlisted embedded databases, unmanaged backups, and more. Because of its unknown content, it is at extra risk for exposure. Security teams can expect to see more instances of shadow data breaches in 2023. However, even though breaches caused by shadow data are set to increase, security teams are becoming more and more aware of the situation and committing to solving the problem. The emerging public cloud data security market proves that this is slowly becoming a problem at the forefront of CISOs minds, and knowing you have a problem is the first step to solving it. In 2023, CISOs will prioritize finding agile solutions that provide both visibility and protection into all of their cloud data to discover and remediate data exposure risk.

3. **A new data security center of excellence will report to the CISO.** All security must protect data, however not all security is focused on data. With data increasingly growing more important as a currency between businesses, as well as as a means of innovation, organizations are storing and sharing more of it than ever (and increasingly, in the cloud). The skills gap created by this will begin to be addressed in 2023 with the rise of a new data security center of excellence, reporting to the CISO. This center of excellence will bridge the gap between the CISO and the Chief Data Officer (CDO) to ensure an entity's valuable data is secure. The data security center of excellence will have responsibility for the following four areas:

    1. Constantly maintaining visibility of all sensitive data
    2. Continuously protecting sensitive data
    3. Controlling who has access to sensitive data
    4. Ensuring that sensitive data adheres to the enterprise data security policy

    This center of excellence, along with more data-centric, defense-in-depth security strategies will augment the important data governance and data privacy work that the Chief Data Officer typically oversees.

Raffael Marty, EVP and GM of Cybersecurity, ConnectWise

"It can be hard to get a handle on the constantly evolving cybersecurity threat landscape, but over the last year, certain trends have made themselves clear—and we can expect to see these trends continue into 2023. The year began hopeful with several organizations reporting fewer ransomware incidents in the first half of 2022 compared to 2021. Instead of fewer ransomware incidents occurring though, it may be that we saw fewer reported due to the shift in tactics used by many ransomware operators from targeting enterprises and major multinationals to smaller organizations that may not have a robust threat defense practice and therefore are less likely to report incidents, and/or don't get the same level of media coverage as larger organizations when attacks do occur.

And—in a trend that's been rising for years and shows no signs of slowing—these attacks are increasingly identity-based, with business email compromise making up a significant proportion of breaches.

Defending against these trends, we can expect to see governments and the private sector at large growing more serious about holistic and standardized defense approaches, such as following NIST guidelines. From a security product perspective, we have already started seeing a trend toward consolidation of solutions. Less point products, more automation with tightly integrated platforms and solutions. Efforts like Zero Trust Architectures and continuous validation and verification will be the name of the game in 2023 as MSPs and others get increasingly serious about the scale and intensity of the threat they're facing on a minute-by-minute basis.

The statistics bear this out: 78% of business leaders say their organization is set to increase investment in cybersecurity in the next 12 months, according to research findings of the 2022 Vanson Bourne Report. Meanwhile, the SMB market is predicted to spend much more on cyber detection, response, and automation next year, according to the 2022 ConnectWise MSP Threat Report.

Given the increased sophistication and motivation of attackers, the ever need for integrated cyber solutions, and constantly changing external drivers (technology changes, regulatory mandates, talent shortage, etc.), we expect to see the service business grow in popularity. SOC (and also NOC) services will help MSPs scale their businesses by eliminating repetitive and unprofitable tasks, so that the MSP can focus on high-value, high ROI activities.

Steve Moore, Vice President, and Chief Security Strategist, Exabeam

"The greatest observable trend to note as we move into 2023, is the increased use of credentials in cyberattacks, for both initial and persistent access. Currently, more than half of all attacks happen through stolen credentials. This number will increase for initial access, and go higher still for persistent access.

Adversaries are experiencing continued success without using malware to gain access and sign-in. From there, they are able to use internal credentials and tools against the defender.

Additionally, with geopolitical changes in the world, we will see an uptick in individual businesses falling victim to nation-state attacks. We can expect the lines to blur between espionage and criminal activity, as information and attack techniques are shared. Loyalists to certain nations will continue to offer cooperation to these international hacking efforts.

As a result, I think we'll see more governments attempting to create publicly known offensive capabilities, in efforts to tear down criminal groups physically and technically. These takedowns of criminal networks take great diplomacy; with both speed and patience and with active coordination of local and federal law enforcement."

Neil Jones, Director of Cybersecurity Evangelism, Egnyte

“For the first time in a long while, cybersecurity is being viewed as a strategic investment rather than a budgetary line-item. I anticipate this trend to accelerate in 2023. By following effective cybersecurity practices like the implementation of ongoing, company-wide cybersecurity training, maximizing endpoint security, and limiting access to data on a ‘business need to know’ basis, organizations can alleviate downtime and improve employee productivity. Over the long haul, cyberattack prevention is almost always less expensive than passively waiting for an attack to occur. At a time when businesses are managing expanding data volumes, cybersecurity must be an always-on company priority.”

Aaron Sandeen, CEO and Co-Founder, CSW

As organizations struggle to navigate an unsteady economy with increasing inflation, higher interest rates, and a potential recession, many are undergoing significant layoffs and hiring restrictions. Companies are substantially reducing expenses in an effort to survive the uncertainty, including IT and cybersecurity budgets, which will ultimately have an impact on the cybersecurity industry.

As a result of the weak economy, organizations will lack the people and resources to maintain their cybersecurity defenses, which will provide bad actors an opening. With a wider range of attack vectors available in 2023, cyberthreats will advance in sophistication and harm.

Alongside dwindling resources, there is a mass amount of increasing data, with experts expecting 94 zettabytes of data worldwide by the end of the year. Making sense of the data you have is becoming more and more crucial at a time when enterprises must deal with a flood of sensitive data. Because of this, I believe the driving force behind cybersecurity initiatives in 2023 will be predictive intelligence coupled with actionable insights. Better cybersecurity is achieved by combining raw data with contextual threat intelligence that is updated continuously using automation, AI, and ML, as well as expert validation.

Tim Prendergast, CEO, StrongDM

“Looking into next year, I think we will see the security market continue to build toward practical applications of zero trust philosophies, as the industry gets its feet under itself in terms of figuring out how to talk with customers about what 'zero trust' means and how it is supposed to work. For their part, I think customers are reaching a tipping point of being very well-educated in this market, and I think that will cause established companies to reposition product portfolios into a focused 'zero trust' messaging platform, to address the customer opportunity. In 2023 the talk will continue around a pending recession, but we remain hopeful that things will turn around by 2024. People will begin investing in startups again that are innovating in this space. We may see a lot of private equity or mergers and acquisition continue to drive the security space. There will be a definite shift in how people are looking at this chessboard. I want to offer simple advice for businesses in the new year, especially in a downturned economy. Be a good steward of the capital you have in front of you. I think many companies got into the habit - due to investors and plentiful cash at low-interest rates - of thinking that you can always get another round of funding. In a bear market, you realize that's not a possibility, so you must go back to the fundamentals of business. Be profitable, and focus on incrementally growing the business. Support the investments you've made and focus on optimizing your processes that can keep the pipeline busy without over-complicating it all. For example, with free-flowing cash, a lot of people were like, 'Let's go, attack 25 different markets!' Instead, focus on the core markets your business does really well. I think people were really getting a bit over their skis and trying to do too much at once. In 2023, the market will see businesses taking more of an iterative approach to building out the business, its markets and products. Every year is a good year to build on solid fundamentals, and 2023 will be a year for organizations to be smart, and not get over their skis. One of the biggest trends that will absolutely continue into 2023 is the decentralization of the traditional corporate headquarters. We have emerged from the pandemic into a new working reality which is that the best people live where they want to live. This has led businesses to the compromise of creating a place where they can work and be contributing to the company's goals but also, they can be happy and have a fulfilling personal life. I think that the cliche work-life balance that so many people have struggled with for so long has finally gotten to a place where it feels attainable with a decentralized workplace. No one wants a job where they occasionally get to have a life, too. I think that's a fair expectation. There are also other benefits to being decentralized, especially when you look at the distribution of people in city centers, traffic is horrible and it's not great for the environment. People being able to work from wherever they happen to be, but still have opportunities for occasional on-site or human interaction is the future. People want their time to be spent in meaningful ways, not just filling seats in the office between eight and 6 p.m. I don't think that's a reality. We have the technology to have productive conversations and get a lot of work done. In the end, I think that's better for the economy and the planet. It's why we've always been a remote-first business - because as a company that sells a SaaS solution, we don't need to physically be in the same location to build our product."

Surya Varanasi, CTO, StorCentric

1.) The ransomware threat will continue to grow and become increasingly aggressive – not just from a commercial standpoint, but from a nation-state warfare perspective as well. Verizon's 2022 Data Breach Investigations Report, reminded us how this past year illustrated, "... how one key supply chain incident can lead to wide ranging consequences. Compromising the right partner is a force multiplier for threat actors. Unlike a financially motivated actor, nation-state threat actors may skip the breach altogether, and opt to simply keep the access to leverage at a later time." For this reason, channel solutions providers and end users will prioritize data storage solutions that can deliver the most reliable, real-world proven protection and security. Features such as lockdown mode, file fingerprinting, asset serialization, metadata authentication, private blockchain and robust data verification algorithms, will transition from nice-to-have, to must-have, while immutability will become a ubiquitous data storage feature. Solutions that do not offer these attributes and more won't come even close to making it onto any organization's short-list.

2.) Consumer attitudes towards online security and privacy will heighten. A key driver here will be that while enterprises getting hacked and hit by ransomware continue to make the headlines, cybercriminals have begun to hit not just enterprise businesses with deep pockets, but SMBs and individuals. SMBs and individuals/consumers are actually far more vulnerable to successful attacks as they do not have the level of protection that larger enterprises have the budgets to employ. As work from home (WFH) and work from anywhere (WFA) remain the paradigm for many across the data/analytics field, they will require data protection and security solutions that can also protect them wherever they are.

In the coming year, The ideal cybercrime defense will be a layered defense that starts with a powerful password, and continues with Unbreakable Backup. As mentioned, backup has become today's cyber criminals' first target via ransomware and other malware. An Unbreakable Backup solution however can provide users with two of the most difficult hurdles for cyber criminals to overcome – immutable snapshots and object locking. Immutable snapshots are by default, write-once read-many (WORM) but in the coming year, sophisticated yet easy to manage features like encryption where the encryption keys are located in an entirely different location than the data backup copy(ies) will become standard. And then to further fortify the backup and thwart would be criminals in the coming year we will see users leveraging object locking, so that data cannot be deleted or overwritten for a fixed time period, or even indefinitely.

Brian Dunagan, Vice President of Engineering, Retrospect

1.) Freedom and flexibility will become the mantra of virtually every data management professional in the coming year. In particular, data management professionals will seek data mobility solutions that are cloud-enabled and support data migration, data replication and data synchronization across mixed environments including disk, tape and cloud to maximize ROI by eliminating data silos. We will likewise see an uptick in solutions that support vendor-agnostic file replication and synchronization, are easily deployed and managed on non-proprietary servers and can transfer millions of files simultaneously – protecting data in transit to/from the cloud with SSL encryption.

2.) Ransomware will remain a huge and relentlessly growing global threat, to high profile targets and to smaller SMBs and individuals as well. There are likely a few reasons for this continuing trend. Certainly, one is that today's ransomware is attacking widely, rapidly, aggressively, and randomly – especially with ransomware as a service (RaaS) becoming increasingly prevalent, looking for any possible weakness in defense. The second is that SMBs do not typically have the technology or manpower budget as their enterprise counterparts.

While a strong security defense is indispensable, we will see that next year security leaders will ensure additional measures are taken. Their next step will be enabling the ability to detect anomalies as early as possible in order to remediate affected resources. Large enterprises, SMBs and individuals alike will need a backup target that allows them to lock backups for a designated time period. Many of the major cloud providers now support object locking, also referred to as Write-Once-Read-Many (WORM) storage or immutable storage. Users will leverage the ability to mark objects as locked for a designated period of time, and in doing so prevent them from being deleted or altered by any user - internal or external.

Justin McCarthy, co-founder and CTO, StrongDM

"In 2023 I believe we'll see rebellion against systems that aren't respectful with our time. Systems that generate ample noise and minimal signal. When it comes to the demands on our attention in 2023 and beyond, less is more.

Security technology is one area that has been requiring too much of our attention and energy for too long. It's frustrating because there's so much friction where it isn't necessary. There's a better way but consumers of security technology will have to demand it and developers and engineers have to work on it.

One small example: authentication. As we move into 2023 we'll look to WebAuthN, Passkeys, and other passwordless systems to improve the user experience and reduce the burden on IT teams. That's where we'll really start to feel the difference. And with this feeling will come elevated expectations that then get transferred to every other aspect of our IT systems and security environments. Hopefully, it will push us to ask why it can't be simplified?"

Richard Bird, Chief Security Officer, Traceable

1.) “In terms of trends we need to shine a light on, 2023 will be the year that the leaders in the majority of companies, organizations and agencies around the world wake up on any given morning and think, ‘Whoa, I have a security problem!’ As we close out 2022, most enterprises either don’t realize the size of the risk they currently face with their unsecured and largely unmanaged API ecosystem or they are willfully ignoring the risks by believing that API gateways and web application firewalls are protecting them. We should be very happy that the current state and maturity of API security affords us the opportunity to get it right in 2023. API security is a greenfield within most companies and organizations today, which means we are in a moment where we can choose tools, processes and frameworks that will deliver huge improvements in security and risk mitigation. The alternative, if we don’t capitalize on this moment, is that in 2024 and beyond API security tactics and performance will be dictated and demanded of us by regulators and we will no longer have the flexibility and agility to meet these challenges without the overhead of compliance pressures.”

2.) “2023 will be the break-out year for API security as a focus area for many of the Fortune 1000 companies. The lack of control, security and governance around APIs isn’t just exposing companies to serious risks, but also to massive amounts of operational inefficiencies caused by APIs being developed and deployed independently across multiple devops teams. This means that there are huge numbers of “zombie” APIs, abandoned, but never removed from a company's systems. There are costly redundancies due to the inability for companies to enforce and inform DevSecOps on internal standards for API creation and deployment. Without visibility into the API ecosystem at a company, you can bet that money is being wasted on the creation of redundant APIs happening nearly every day. That redundancy comes at a cost, inefficiency isn’t free.”

3.) “In 2023, API security will drive realizations and revelations by enterprises that go beyond the threat and risks of APIs. API security is dependent on the discovery and collection of the APIs that a company is exposed to. Once organizations take that step, they quickly realize that the entire operational framework of their API management is problematic. There is very little in the form of standardization and governance for APIs in most companies, which means that there are huge amounts of inefficiency and costly redundancy across those same APIs. API security in 2023 will create a broader understanding of not only the risks a company is facing, but also the costly consequences of a broadly unmanaged function within their organizations.”

4.) “The pathway to self-awareness and self-learning about API security starts with taking a simple step; exercising intellectual honesty. API security and operations isn’t something new. It is an extension of the best practices that have always been demanded in the digital world. If you believe you don’t have an API security problem because you don’t use a lot of APIs or because you leverage an API gateway or web application firewall, you’re not being intellectually honest. Every day, in highly publicized events, the attack surface and vulnerabilities of APIs is being clearly communicated to the market. Believing that APIs won’t be opportunistically exploited by bad actors just isn’t supported by data, evidence and the history of technological evolution. The time to learn and move on API security is now, not two years from now when the seriousness of the risk is fully understood.”

Tyler Farrar, CISO, Exabeam

Nation-state attacks/geo-political matters:

“Nation-state actors will continue cyber operations in 2023; whether these attacks increase, decrease, or stay the same ultimately depends upon the strategic objectives of each campaign. Based on the current geopolitical climate, I think we can expect these cyberattacks to increase across the major players. For example, Russia’s failure in Ukraine exposed its weaknesses to the world, but its attacks are likely to continue against Ukraine, including operational disruption, cyber espionage, and disinformation campaigns. It would be unsurprising for the attacks to expand beyond Ukraine too, as Russia's leader attempts to prove Russia is not weak. Likewise, cyber espionage is a key tactic in China’s strategy for global influence and territorial supremacy, and I think we can expect these operations to increase, particularly across private sector companies.

In 2023, state policies will directly influence cybercriminal and hacktivist communities to obfuscate sources and methods, increasingly blurring the lines between nation-states, cybercriminals, and hacktivists. Cybersecurity teams would be wise to remain flexible with respect to threat actor attribution.”

Impact of economics on security:

“The economic downturn, and in particular inflation, has - and will continue to have - a significant impact on security spend, likely forcing reductions and leveling impacts to organizations and to threat actor behavior. The key to defense for these organizations is doubling down on cyber talent and security tools. Meanwhile, security organizations should aim to consolidate legacy technology platforms, decreasing redundant tooling, in addition to controlling cloud spend, to manage high operational costs and complex integrations.

I think this is a good time to remind organizations that zero trust is simply a security framework, not a tool. It is not a ‘single solution,’ but rather a framework used to secure data in a modern digital enterprise. Zero trust is also not overhyped, despite some opinions to the contrary. It has become a critical step towards mitigating cyber risk, detecting malicious behavior, and responding to security incidents. By requiring users and devices to be authenticated, authorized, and continuously monitored for a ‘trusted’ security posture before access is granted, zero trust can contain threats and limit business impacts when a breach does occur.”

Credential-based attacks and evolving threats:

“We’ve seen the classic Cat and Mouse Game before: as credential-based attacks evolve, so too do cyber defenses. Threat actors will continue to leverage tried and true methods like social engineering, initial access brokers, and information stealer tools to carry out their objectives. Where multi-factor authentication stands in the way of compromising an account with stolen credentials, we can expect cyberthreat actors to implement new techniques to bypass this particular layer of defense. I think this will lead to an expansion of passwordless authentication solutions, to combat the attackers.

We can also expect to see more malicious attacks, as anyone can play this game. A broader set of threat actors will join in to conduct cyber operations in 2023. They have financial motivation, government mandates to justify their cause, not to mention bragging rights that increasingly attract a younger group of threat actors.”

Protecting brand as much as infrastructure:

“During the past year, we witnessed several high-profile breaches, where organizations suffered severe brand damage. This resulted in a shift from data recovery to reputation management when faced with a ransom. I expect to see threat actors shift their strategies to exploit this fear through extortion vs. ransomware in the year ahead.

Further, threat actors will continue to take advantage of weaknesses in the software supply chain, which will become the number one threat vector in 2023. Organizations should create a vendor risk management plan, thoroughly vet third-parties and require accountability, to remain vigilant and align to cybersecurity best practices. This is critical too, as cyber insurance claims have exploded. We can expect to see insurance companies lowering their risk appetite and reducing client coverage in 2023. If your organization is in the market for a policy, expect to pay a hefty premium, or face a rigorous review of the organization’s security posture, as insurance companies increase their due diligence to avoid liability.”

Arti Raman, CEO and Founder, Titaniam

“In 2022, we saw a continuous flood of ransomware attacks, which spawned the increasing adoption of Ransomware as a Service (RaaS). The threat actors behind these attacks have honed their skills in ransom negotiations and extortion processes, creating a playbook they can use to go after nearly any organization. Because of this, the number of ransomware attacks we’ll see in 2023 will only continue to rise and move downstream.

To combat these attacks, organizations in 2021 and 2022 heavily invested in prevention, detection and backup technology. However, in 2023 that may not be enough. As threat actors get more creative and innovative with their malicious attacks, data security professionals also need to embrace newer, more innovative and effective technologies to defend their systems.

In fact, a recent report found that more than 99% of security professionals are searching for better data protection tools to protect themselves from ransomware and extortion. Similarly, 70% of participants in a different report indicated they experienced data theft at some point during the previous 12 months. Of those respondents, 98.6% believe a more modern data security solution could have prevented their data theft.

While no prevention technology can guarantee 100% protection, new technology must focus on assumed breach concepts and providing more guardrails. By analyzing what made successful breaches successful, we as a cybersecurity community can take the first step toward a technological shift that will revolutionize how we fight back against ransomware.”

Gal Helemski, CTO and Co-Founder, PlainID

“In 2023, identity-first security will gain more focus and adoption. Already we see increasing growth in the identity space as the importance of identity as the new security perimeter is sinking in. Identity solutions would expand their support, especially in the cloud, and provide deeper levels of control. An essential part of that would be understanding Authorizations and the link between the identity world and the security of data and digital assets.

Authorization manages and controls the identities' connection to digital assets (such as data). That is a fundamental part of identity-first security. It starts with the authenticated identity and continues with the controlled process of what that identity can access. Full implementation of identity-first security can’t be achieved without an advanced authorization solution that can address all required technology patterns of applications, APIs, microservices and data.

I believe most security leaders are still focused on the perimeter of their digital enterprise, which needs to change. Identity-first security can’t end at the gate. Identities and their access should be verified and controlled on all levels, access points, network, applications, services, APIs, data and infrastructure.

Already we are seeing that an increasing number of technologies and cloud vendors are offering the policy option in addition to the traditional entitlement and role-based method. This is a very positive step towards simplification of this challenging space. "

Jeff Sizemore, Chief Governance Officer, Egnyte

"Secure data enclaves will drive infrastructure spending in 2023 as companies understand how to better manage their content amid increasing cyber threats. Much like a safe or vault, secure enclaves allow organizations to protect their highly sensitive data – such as intellectual property, Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII) – in a controlled environment where authorized users can collaborate. In a world where not all data is created equal, I anticipate that we will see increased adoption of secure enclaves across business disciplines in the new year, enabling organizations to handle their sensitive content more effectively."

Prashanth Nanjundappa, VP of Product Development, Progress

"As organizations look ahead to 2023, automation will be a priority in maximizing shifting left principles and maintaining high security standards. Building strong, secure products throughout the software development life cycle requires continuous security integration in the delivery pipeline. Silos between developer, business development and testing teams have historically created gaps in the feedback loops leading to a slower product rollout. However, with the increased adoption of DevSecOps principles for continuous testing and deployment, teams across all business units will begin to codify their shift left practices with automation and increase communication in an effort to reduce failure. We can expect to see how such automation will further accelerate the adoption of DevSecOps. Compliance automation tools will play a key role in strengthening security and compliance policies across applications and infrastructure."

Kathryn Kun, Director of Information Security, Forter

"Every year we talk about how we see the sky is going to fall. This year, I want to talk about how we are going to help hold it up. Instead of predictions, I want to focus on what we hope to learn from and grow towards as an industry.

I hope we can support a focus in engineering for the safety of people beyond our end users. I hope we can work towards a broader definition of security beyond controlling data and access, to ensuring that our choices keep the people represented by that data safe. All of our interconnections are not vulnerability to be avoided, but technical systems reflecting social and political reality, and that complexity is also strength and opportunity.

I hope we can build processes for ourselves and our colleagues that will be a source of calm support in times of crisis and change. The security profession is well placed to handle complexity and help support our colleagues and our businesses through surprises. Turbulent waters are what all of our skills and predictions and warnings are for, and our place is to ensure reliable performance within an ever-changing environment.

I hope we can be a source of trusted advice to our colleagues across the business, and live up to the responsibility of bringing specialized technical knowledge into useful and usable reach for our wider teams.

I hope we can make more tools more useful and visible to non-security audiences. We have learned and understand a lot about reliability and trust, and I want to scale those understandings and share them with decision makers from junior engineers to executives."

Lessons From the Uber Hack

By Tomasz Kowalski, CEO and Co-Founder, Secfense

For decades, cybersecurity experts have been warning us against weak or stolen passwords. Two-factor authentication (2FA) has always been pointed out as the solution to password problem. And for years now, many companies have been introducing more and more convenient 2FA methods, starting from SMS, moving through app-generated one-time codes (TOTP), and finishing with email push notifications. Unfortunately, many of the 2FA methods turned out to be vulnerable to the sophisticated attacks used by cybercriminals who successfully prey on our weak and vulnerable access points. Uber has recently found out about it painfully. So, what can we do to avoid attacks like the one that happened at Uber?

September. New York. Traffic on the street. The Uber driver receives a series of push notifications on his phone. They all look legitimate, like the ones sent by Uber to drivers. Initially, our driver resists and does not authorize anything but more and more annoying pop-ups appear. He ignores it, he has to focus on the road and on doing his job. A few minutes later someone texts him via WhatsApp. An Uber IT specialist? Or at least that's what he says when asking for account access and authorization for notifications sent. Phew. The driver is starting to get annoyed. The green light comes on, and at the corner of the twenty-seventh next to the tenement house with metal stairs, he sees a girl waiting to be picked up by him. He confirms the annoying notification and forgets about the whole thing.

The situation described above may not be exactly what has happened but according to what has been published by Uber, it may be very close to reality. As a result of Uber employee distraction and perfectly conducted social engineering Uber's network has been compromised.

Conclusions

Every company, organization, or institution that cares about data security must move away from using weak and selectively used forms of user identification and switch to techniques that can successfully withstand phishing and social engineering attacks.

- The weakness of the push-based 2FA is definitely that the user experience of receiving pop-up messages can make someone finally agree to them and finally click "allow" without giving much thought to what he or she is really accepting - says Tomasz Kowalski, CEO of Secfense, the company that developed the User Access Security Broker, technology that allows for the quick and no-code implementation of FIDO2 authentication on any application.

FIDO2 authentication is an open authentication standard developed by FIDO Alliance and is known to be the only authentication method that is truly resistant to phishing and social engineering.

- Of course, push notifications are better than nothing. Even old-school SMS protection is better than “just” passwords - Tomasz adds. - However, organizations need to ask themselves if they want to get slightly better protection than passwords or will they rather walk away from passwords and replace them globally with FIDO2. With the FIDO2 standard available to anyone organizations do not need to use half-measures but instead, reach for something that can allow them to forget about the “password problem” once and for all.

The Layered, Onion Approach

The best approach to building security in a company is building it on the so-called onion model, that is in layers. There is no technology, producer, or integrator in the world that will be able to protect against all possible threats.

However, data security performance can be maximized by following the guidelines of the zero-trust security model and by using multi-factor authentication (MFA) on all applications and access points in the organization. What’s important - the MFA must be based on FIDO2, a modern authentication standard that uses face or fingerprint biometric recognition to log in.

FIDO2, the safest way to log in to the future

And why FIDO2? Because it is a real revolution in terms of authentication and online security. This open standard - thanks to which every service on the Internet can be secured with the use of cryptography - is fully resistant to phishing and theft of logins and passwords.

FIDO2 allows you to use cryptographic keys but also devices that we always have with us, such as laptops with a built-in camera with Windows Hello in place or smartphones with face recognition or a fingerprint reader.

Untapped security potential

So, with FIDO2 - an open authentication standard - that's supposed to be open and accessible to anyone, is there still a problem? Why are all companies not yet phishing-proof? Why is social engineering still the case?

Implementation is still the biggest problem. MFA implementation is complex, burdensome, and expensive. Moreover, if a company has hundreds of applications in its organization, mass implementation of all applications is practically impossible. Effect? One of the best authentication methods, the FIDO2 standard - although designed in April 2018 - is still an addition, not a universal way of securing your identity on the Internet after more than four years.

- We hope that thanks to Secfense, we will be able to change this situation. Our goal was and is to open the path to the mass use of MFA in business and to use the strongest FIDO2 standard for this purpose - says Tomasz Kowalski.

An important advantage of the Secfense broker - also strongly noticed at the Authenticate 2022 conference, held in October in Seattle, is that it enables the introduction of FIDO2-based MFA without the cost of hiring developers, without the cost of purchasing dongles and without any impact on the smoothness of operations.

The sooner the companies will introduce FIDO2 authentication globally the sooner the world will be able to move away from passwords. It is possible to eradicate passwords and phishing-based attacks once and for all. It will take time but it is possible. At Secfense we believe that the user access security broker approach to the adoption of strong authentication methods can play a big role in this transition.

About the Author

Tomasz Kowalski is a CEO and Co-Founder of Secfense. He has nearly 20 years of experience in the sale of IT technology. He was involved in hundreds of hardware and software implementations in large and medium-sized companies from the finance telecommunication, industry and military sectors. Tomasz can be reached online at (tomek@secfense.com, Tomasz Kowalski | LinkedIn) and at our company website https://secfense.com/

Military Encryption Challenges

By Milica D. Djekic, Independent Researcher, Subotica, the Republic of Serbia

Abstract:

Army cryptology is a very complex area as it includes cryptography and cryptanalysis. Cryptography is a practice of transforming plaintext into ciphertext, while cryptanalysis means decryption of communication or data. Purpose of this effort is to provide summarized insight into all known cryptographic techniques which are used in defense industry, as well as military doctrine. Also, this article suggests some new approaches in link and combined encryption. Point of this paper is to provide a deep overview into end-to-end, link and combined crypto-systems as they are fundamental building blocks in modern army landscape. In other words, it will be illustrated how proposed methodology works, as well as why it is significant to make a good synergy between device data storage and communication information exchange. Experience shows static neutralizer could play a crucial role in rejecting access to some communication channel. In such a sense, it's important to understand that link encryption and combined cryptography might be leveraged with those cutting-edge ideas. Results being provided in this effort will demonstrate a need for more researches, which can find their place into a concrete defense project. At this stage, some introductory findings are offered and the other engineers, researchers and scientists could recognize this effort as a useful starting point into something more comprehensive and impactful. Presented work is not only a helpful overview, but more likely an authentic root to further explorations. For engineering, it's necessary to cope with ingenious methods, which can give unique roads to practice and experience. In total, sets of similar findings could define a novel tendency in military information security field.

Key words: Technology, Intelligence, Cyber Security, Investigation, Cryptology, etc.

Introduction

Hacking attack vector surface has overwhelmed modern information-communication systems causing risk to people, businesses and critical infrastructure. Ongoing cyber landscape faces up certain skill shortage as there are yet too many challenges that should be overcome. Defense industry is constantly several decades ahead from civilian community as it can be comparable with space research programs which cope with cutting-edge solutions. Even military community of today is not fully protected from ongoing threats as it deals with products of 4th industrial revolution. Modern tendencies across the globe are to make smart technology and such a trend is even present with army industry. It's well-known that military assets will apply some level of protection to their communication, information exchange and storage systems and in such a sense it's possible to talk about highly sophisticated cryptographic projects which can provide some degree of assurance to those critical data managements. Cryptology is a practice that can be distinguished into two branches being cryptography and cryptanalysis. Both areas are more than needed for security of military systems. Cyber technologies include computers, internet and mobile advancements which are very vulnerable to cyber attacks. Current hacking tools need IP address in order to make breach and take control over those innovations. Also, cyber attacks are not only threat to network's devices, but mostly to communication channels which need quite strong end-to-end, as well as link encryption. That military doctrine is already well-developed as there was always need to protect exchanged findings. Beginnings of first cryptographic tools go back to ancient times and usage of encryption with Spartan warriors. True breakthrough of encryption which is known nowadays started with World War 2 bringing with so real explosion of digital technologies. That was time of 3rd industrial revolution and even today industry 4.0. relies on such discoveries as modern technologies are just transformation of what was made before.

Imperative of progress is to offer something new and better in regards to pervious approaches. Current industrial boom gains huge popularity as it transfers communication and object's experience to web environment providing pretty cost-effective solutions which can be assumed as advantage in comparation with what was used before. Such a demand is put in front of ongoing army community as solutions in defense industry must be functional, as well as inexpensive. Similar requirement is engaged with entire engineering landscape as even civilians will reject something being less convenient to them. World is becoming consumer society and if majority is not happy they will seek change. Change can be positive, negative and neutral and only positive changes can guarantee progress and prosperity. In other words, once it was approached some project all its pluses and minuses must be reviewed in order to explain to such decision makers approve budgeting to those needs. Engineering always looks for optimal choice as it must satisfy both – technological and economical requirements. Similar case is with defense industry as tax payers worldwide will not be willing to support something extremely pricing no matter how sophisticated that solution is. It appears both – civilian and defense industries cope with more or less similar challenges. For instance, army members mostly apply satellite communication in their everyday routine, but such a technological service is very expensive and for that reason there is appeal to shift on something cheaper as cordless web connection is. Main concern with such an internet communication is its range and coverage which means only one factor is met which is cost-effectiveness, while functionality is still unresolved. In order to tackle wireless internet operability it's needed to accept high-scale power supply which will transfer messages over long distances. Many competitive military organizations use radio waves to transmit signal and that works, but obvious challenge is such a communication must be with strong security as exchanged data could be very sensitive putting under risk army cells on battlefield.

Communication departments with military sector cope with data transmission equipment, as well as some storage capacities. In essence, information must be sent, received and saved somewhere. Many army organizations rely on could-based systems which can offer them chance to reliably manage data. Practically, everything happening with military communication is done in cyberspace. Majority of those contributions are linked with information-communication technologies and anything occurring there leaves trace in high-tech environment. Current tendency is digitalization and analog systems are manly replaced with digital ones. On the other hand, nature is mostly analog, so inputs and outputs of digital architecture must apply analog-to-digital and digital-to-analog converters, respectively. Those solutions are widely available on marketplace and either it is dealt with civilian engineering or defense industry getting parts for projects is quite simple. In other words, it's needed to take advantage over suppliers of semi-final and final products and just embed them into final solution. It might seem that it's about assembly industry, but even large-scale companies count on their contractors which have signed partnership agreements with them. Apparently, R&D looks for creativity and fresh ideas, while production and ending design can obtain what they aim simply doing some sort of compliance. R&D engineers in both – civilian and military sectors are such an ingenious as they might give something coping with international progress. Research community is capable of making positive changes, but in case to need such an outcome it's necessary to invest into that workforce. Some statistics suggest that it's needed to make skill and knowledge transfer to young professionals up to ten years as such a best practice can provide workforce which will return those investments being in position to demonstrate true skill and expertise once they have learnt how to resolve some practical project. Engineering is journey which requires life-long learning and those staffing are people which never stop thinking.

Cyber defense is strategic matter and it covers all possible roads of protecting critical assets. Military communities mainly use cyber technologies to maintain findings exchange within air, water and land defense systems. For example, in civilian fashion it is feasible to manage communication between aircrafts and ground control, but it is significant to pay attention on safety and security of air traffic transportation systems. On the other hand, current technological breakthrough suggests mass application of web connectivity within air, water and land infrastructure. In other words, that means any device within network has assigned IP address which makes it vulnerable to hacking operations. Main imperative in such a case is to develop army solutions primarily taking into consideration cyber security demands at initialization of any defense industry project. Role of R&D team is to deeply investigate all potential threats to project and as control engineering has become ultimate goal to any industrial effort it's clear why well-designed control system is from such an importance. Control systems include controller and plant which can be in feedback using ongoing sensor grids. Purpose of controller is to receive input variable and send command signal to plant. Further, controller operates according to some control algorithm and it can usually be some computing unit. That means it is well-capable to work with data and instruction as it has its processing capacity. Industry mostly uses programmable logic controllers and embedded solutions in order to govern some object or process. Both controllers are digital and able to convert signal relying on analog-to-digital and digital-to-analog transformation. Typically, code developers need to make computer program on PCs and lately transfer it to those two sorts of controllers.

In addition, plant is part of control system which receives command signal, copes with some disturbance which can be mitigated or compensated and as outcome it gives output signal which can be measured using sensing network that returns such data via feedback branch at input of overall control system. Goal of this contribution is to collaterally make parallel between digital technologies being applied in high-tech security, as well as control theory as binary algebra is under strong focus of research communities. To recent experience, there are yet characteristics of binary systems which need deep approach to their exploration as they can offer results going beyond known frontiers.

Related work

Ongoing research has started in 2013 with a definition of the ESIS encryption rule [15] which is brand-new and multi-level cryptographic law being applied in crypto-systems that do not need any kind of key management techniques. Maybe in the past that would be assumed as a perfect secrecy many cryptographers looked for, but at this modern time it's just a strong encryption algorithm that opened a completely novel approach to binary systems as it has become clear binary algebra is a branch of mathematics offering nearly limitless opportunities even nowadays. In other words, scientists, researchers and engineers need to dig deep in order to understand all characteristics of binary systems and consequently fully apply them. Further, such an investigation has introduced a plenty of new cutting-edge projects such as static neutralizer [17] which is strongly correlated with endpoint and data protection, as well as deep insight into singularity of that mathematical theory. Main contribution of this effort is an explanation of link cryptographic system design from both – theoretical and practical point of view. As link encryption is a challenge to a wide spectrum of defense industries across the globe the idea is to encourage army researchers and developers to tackle such an engineering problem being from national significance to every armed forces. Also, there is proposed how to make an innovative cryptographic channel taking advantage over static absorber mathematical model in creating a neutralizing shield to core signal either being plaintext or ciphertext depending if it is dealt with pure link or combined encryption, respectively. From a developer's perspective, it's needed to know that link cryptography uses a diagonal square matrix which external elements are protection shield to any cryptanalysis attack sending a step function in order to obtain some step response, while central element is only a signal carrier that can be open or encrypted depending on a sort of that cryptosystem, so far.

Cryptanalysis is an important practice in cryptology which in modern times serves to do some readings of certain communication channel in order to figure out which content is delivered via such an information exchange platform. On the other hand, application of 3x3 diagonal square matrix in developing communication track can provide many options in playing with cryptographic algorithms, but in this case it is suggested to cope with dot static absorber's rule that in sense of programming can be defined through some coding functions which role is to give adequate response to any external high-tech attack. Apparently, if a set of 1s is sent to some communication in order to get some streaming from such a data transfer system it's obvious that excitation will vanish in such a singular point not sending back any feedback information to attacker. Indeed, it's truly like a black hole which can trap anything even a light itself into such a horizon leaving only darkness behind itself as its gravitational field is too strong to let anything escape from so. Current technologies such as artificial intelligence (AI) and machine learning (ML) could in such a fashion serve for a plenty of usages of those techniques in designing next generation cryptosystems as such sophisticated technologies are the future of upcoming engineering. Those projects must be pushed through deep preparation and research before some team of engineers begins to work hard on their development. As AI and ML are beyond a scope of this effort it's clear there will be no suggestions in such a sense as this paper will only provide some so necessary mathematical modelling which just can help to engineering working groups to better understand cryptology and in that manner give their full effort to those technical projects. As it is suggested major accent of this report will be put on some best practices in link encryption, but main novelty of this research is neutralizing link cryptography which through careful software design can significantly protect such an information transmission. From that point of view, programming languages and other cutting-edge tools are only resources in obtaining such a mathematically defined task that can be resolved only via long-term commitment, so far. In other words, this new access can impact many areas of industry such as defense, cyber and space industry that are always pioneering fields of progress anywhere over the world.

End-to-end cryptography

Practically, there are three main encryption techniques being applied in military cryptography. Those are end-to-end (E2E), link and combined encryption which will be illustrated and modeled through this effort with an intention to make good research preparations for next phases of production cycle. E2E encryption assumes some transformation of binary data using some mathematical rule either making shift of bits which is called cryptographic key or getting encrypted output simply applying logic functions when in such a case for a unique set of inputs is provided a unique set of outputs in any instance of cryptography [15]. The graphical illustration of given in Figure 1 as follows.

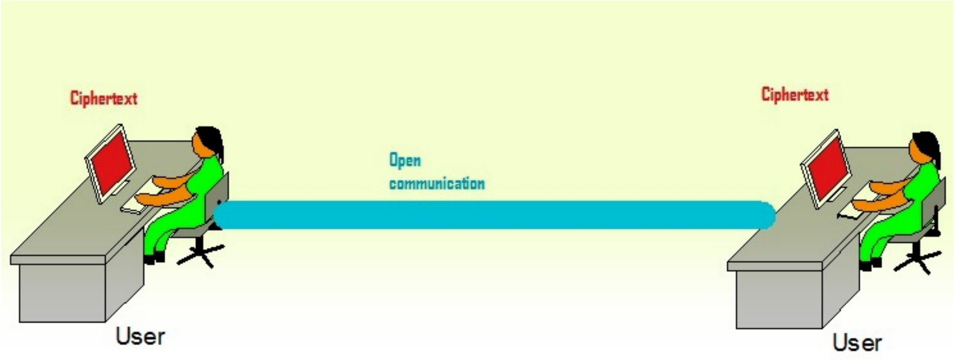


Figure 1 – E2E encryption communication

As illustrated in Figure 1 there is a two-way communication between two workstations where both users have some cryptographic software with their devices encrypting and decrypting data with such an asset and talking with each one via unprotected communication line. As that open communication is not secured some skillful cryptanalyst can so some streaming of that information exchange trying to decrypt once collected findings. Also, there is some risk about endpoint security as if there is no active cyber defense any equipped hacker can make a breach into such an object just stealing plaintext data before they are transformed into ciphertext. In other words, there is no an absolute security as everything is about the best practice in threat management. Above all, if an idea on static absorber [17] finds its place in practice it's possible to think about better endpoint security which means more active defense and higher level of automation in coming days.

Link encryption

Link cryptography is attribute of competitive defense industries as it's quite trickery to develop and deploy such an encryption system. In that case, users in network can communicate through encrypted communication line sending to one another plaintext data. From a perspective of cryptanalysis, it means such an opponent might deal with some difficulties to catch such data, while being in transfer. On the other hand, overall challenge of endpoint security is still unresolved. The graphical representation of such a grid is provided in Figure 2 as follows.

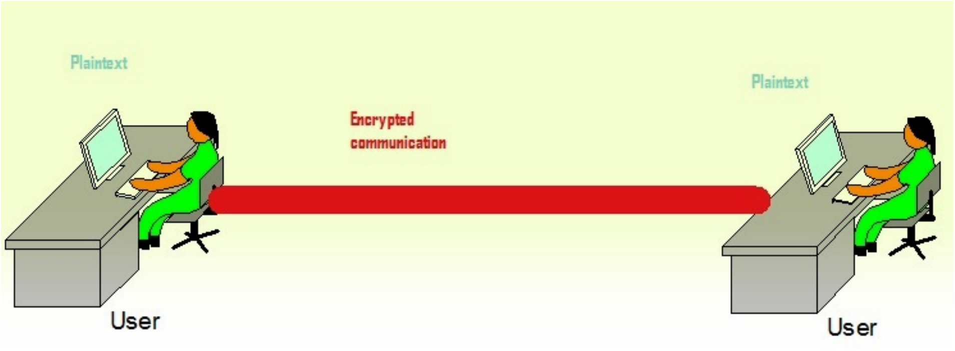


Figure 2 – Link encryption system

The most challenging thing in link cryptosystem design is how to make a protection shield around transferred plaintext data. In such a case, it's needed to understand some mathematics, as well as cope with great programming skill. Point in such a fashion is to figure out how matrix theory works, as well as get how such mathematics can contribute to any developer's language. In other words, it's necessary to apply some diagonal square matrix which external elements could serve as a protection shield where such core element can be used to transfer plaintext data. Mathematical modelling in such a manner will be considered in this paper in order to explain to engineering teams how to solve such a technical task. The mathematical model is as follows.

$$\begin{bmatrix} A_1 & B_1 & C_1 \\ D_1 & S & E_1 \\ F_1 & G_1 & H_1 \end{bmatrix} \quad (1)$$

The equation (1) is a typical example of link encryption demonstrating how a shield protection should look like. In such a formula, it’s needed to define all internal and external elements as follows:

$A_1, B_1, C_1, D_1, E_1, F_1, G_1, H_1$ are external elements of the matrix which serve to carry on protection shield, while S is a core member of the matrix which role is to transfer in case of link encryption some plaintext signal.

On the other hand, there will be considered some mathematical model of absorbing link encryption which strongly relies on findings from the article [17]. The mathematical description is as follows:

$$A_1 = A \cdot \bar{A} \quad (2)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$B_1 = B \cdot \bar{B} \quad (3)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$C_1 = C \cdot \bar{C} \quad (4)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$D_1 = D \cdot \bar{D} \qquad (5)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$E_1 = E \cdot \bar{E} \qquad (6)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$F_1 = F \cdot \bar{F} \qquad (7)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$G_1 = G \cdot \bar{G} \qquad (8)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$H_1 = H \cdot \bar{H} \qquad (9)$$

where such an external member of the matrix is put through 2-bit binary algebra function using AND logic gate to produce 0 in any case.

$$S = plaintext \qquad (10)$$

where such a core element of the matrix is applied to transmit some plaintext information.

Indeed, it’s obvious that such a simple mathematical model which can be coded is proposed through this effort. Similar approach can be used in combined encryption so far where the core signal would be some encrypted content serving in secret data exchange. From a programming point of view, it’s logical that some clever coders can cope with such a mathematical modelling in order to conduct such a serious defense engineering project.

Combined crypto-system

Combined cryptography is a good mix of E2E and link encryption which takes advantages of both military encryption cases. In other words, it’s more like a link encryption mathematical model where a core element of the diagonal square matrix is a ciphertext instead of the plaintext. The graphical illustration of such a communication is given in Figure 3 as follows.

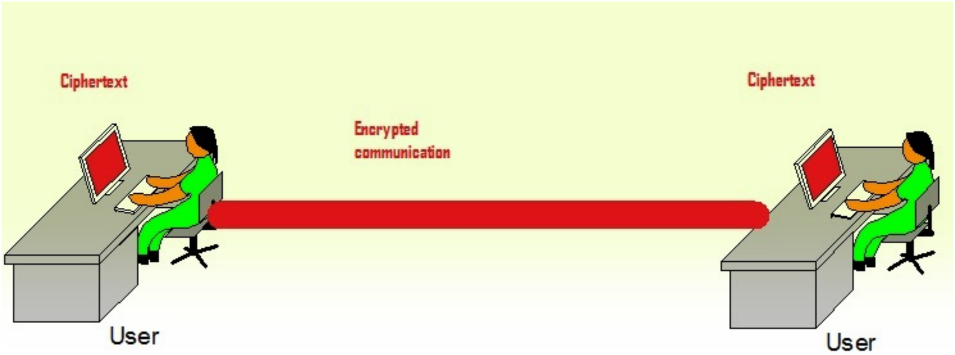


Figure 3 – Combined encryption grid

Presently, combined encryption has some weaknesses as if not applied active high-tech security there could be some issues with the endpoint assurance. For such a reason, it’s needed to work hard on some sorts of cyber breach prevention solutions [15, 17] which can offer a chance to deal with a quite high level of security. Certainly, that might remain as an engineering challenge for tomorrow.

Discussions

Once conducted fundamental researches in binary systems have provided some engaging findings and it's obvious that area of science and technology must be completely overused. Time of intelligent digital technology transformations have come and main fact with so is the future epochs will generate more and more opportunities to everyone. Presented cryptography cases are such a common in defense industry and via this effort it is suggested how to schedule some kind of the novel military projects getting their applications with armed forces communication departments, so far.

Conclusion

It seems cryptography is inseparable part of any message exchange and it is vitally dependable on communication sectors in defense. The proposals being introduced in this article can serve with army industry offering some starting point for the coming research and development, so far.

References

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

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

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

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

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

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

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

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

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

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

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

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

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

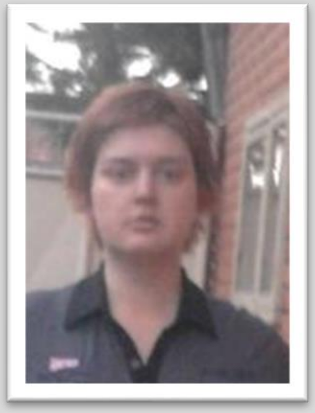
[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

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

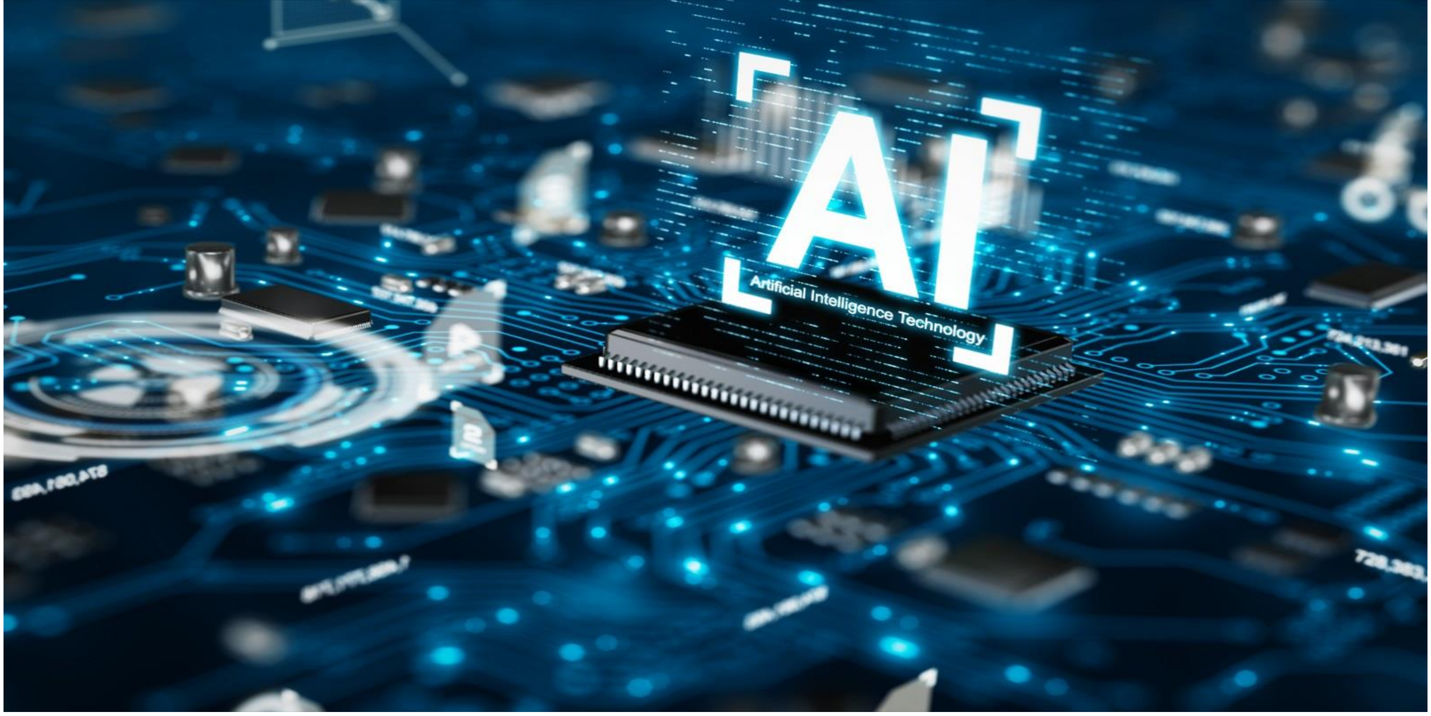
[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

[17] Đekić, M. D., 2022. Static Absorber Modelling. Military Technical Courier

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.



Our Nation Needs Comprehensive AI Legislation, And Soon

By Dr. Allen Badeau, Chief Technology Officer, Empower AI

The White House recently launched an "AI Bill of Rights" framework to lay the groundwork for the future creation and use of Artificial Intelligence (AI).

While this framework includes concrete steps for agencies looking to implement AI, it's only the latest initiative in a long line of guidelines aimed at outlining the development and implementation of government AI.

Earlier this year, the Department of Energy released an "AI Risk Management Playbook" with recommendations to follow through the AI lifespan. In November 2021, the Department of Defense released "Responsible AI Guidelines," providing stakeholders and companies a framework to ensure that the AI lifecycle is met with fairness, accountability, and transparency.

These various initiatives are evidence of AI's rapid growth and adoption in the federal sphere. Yet, they all need more enforceable legislative power to make government-wide AI a reality.

New legislation should streamline the AI development process, creating cohesive and measurable benchmarks for agencies at the beginning stages of their AI journey.

AI is a Siloed Technology

Due to the restricted nature surrounding government access to users and data, agency networks often operate in silos. Unfortunately, this is the same with AI, and the lack of standardized and regulated AI legislation further exacerbates the problem.

AI, by its nature, lends itself to breaking down data silos, as it streamlines data governance and assists with expediting the approval process for agencies sharing data. Still, the lack of fundamental legislation leads to separate AI requirements for each agency and makes cross-agency collaboration more difficult.

For example, the Department of Energy may require a level of AI transparency that the Department of Homeland Security's AI cannot provide, making collaborating on a project difficult and creating silos of information that cannot be shared between the two agencies. Additionally, the network in which one AI system operates may look completely different from the other, making it even more challenging to share information.

Actionable legislation will help solve this issue. By enforcing government-wide AI regulations and recommendations, agencies can work within each other's standardized AI networks with confidence that their guidelines are being met, breaking down the data silos created by different frameworks.

However, standardized legislation may be more easily said than done.

A World of AI Regulation

No single framework or legislation can fulfill the mission requirements of all agencies, as AI is often mission-oriented.

Take one critical aspect of AI, ethics, as an example. The AI Bill of Rights does feature guidelines on mitigating discrimination in AI. However, agencies have different ethical considerations and risks to consider. For instance, while the Department of Defense (DoD) must deal with life-and death-decisions for warfighters overseas, the Department of Education must look at student application bias or curriculum prejudice.

However, this doesn't mean AI legislation can ignore the issue of ethics. Instead, comprehensive legislation should showcase and clarify the plurality of AI by requiring each agency create a framework explicitly designed for their goals while still meeting baseline government-wide criteria.

Incorporating language requiring developers consider the general challenges most AI solutions must address – such as bias, user safety, and implementation – while allowing a level of flexibility within the details can account for specific agency missions.

For example, while both DoD and the Department of Education have different ethical considerations, guidelines such as "AI must only be used to support the safety and development of U.S. residents and citizens" apply to both agencies. Furthermore, requiring detailed guidelines be approved by the legislative branch ensures that each framework is viable and in line with these basic considerations.

NIST has already laid the groundwork for this process by outlining several considerations in its AI Risk Management Framework, listing the characteristics of trustworthy systems as "valid and reliable, safe, fair and bias is managed, secure and resilient, accountable and transparent, explainable and interpretable, and privacy-enhanced." By adding a legal aspect to this list and elaborating on additional considerations, the government can create a foundation for AI legislation.

Artificial intelligence has become increasingly important to government missions within the past couple of years. It can be a powerful tool, expediting decision-making, monitoring and predicting insider threats, aiding in cybersecurity compliance, automating repetitive tasks, assisting with onboarding and offboarding, and more.

However, despite various agency frameworks, legislation is necessary to break free of the data and AI silos in the current government and allow AI to reach its full potential. It will also help level the playing field for the government's industry technology partners and reinvigorate innovation to ensure America remains a leader in the ever-evolving world of AI.

About the Author

Dr. Allen Badeau is the chief technology officer for Empower AI, as well as the director of the Empower AI Center for Rapid Engagement and Agile Technology Exchange (CREATE) Lab. In this role, he leads innovation research and development activities designed to add value to Empower AI's customers and their missions, including cutting-edge technologies such as artificial intelligence, quantum computing, software defined networks, robotics, advanced data analytics, agile DevSecOps and many other areas.

With the CREATE Lab, Empower AI is building next-generation, value-based solutions for its customers utilizing a collaborative, knowledge-sharing environment. Under Allen's direction, the CREATE ecosystem brings together people, processes, and ideas, as well as software and hardware resources — exploring the strategy and implementation of new and advanced technologies and redefining how innovation is integrated into our customers' environment.

Prior to joining Empower AI, Allen held various leadership roles at ASRC Federal, CSC, Innovative Management & Technology Services and Lockheed Martin. Allen received his bachelor's in physics, and both his master's and doctoral degrees in mechanical engineering from West Virginia University.

Allen can be reached online at https://www.linkedin.com/in/allenbadeau/ and at Empower AI's company website https://www.empower.ai/.

Securing Collaboration at the Speed of Business

By Ofer Klein, CEO and Co-Founder, Reco

Recent research found that 96% of business leaders believe that effective communication is key to a productive remote or hybrid work. And Slack claims that using collaboration tools can increase your productivity by 30%. All of these tools offer vast benefits – it's easy to see why they're so appealing to businesses. They make collaboration faster and easier – which is a leading goal for almost any organization.

However, they also introduce new security and compliance risks. Organizations must find a balance between speed, productivity and security when it comes to collaboration. Doing nothing isn't an option. The hack of Uber's Slack channel is just one recent example that underscores the importance of collaboration security.

However, legacy security tools, such as DLP, were built to control and, in some cases, prevent communication. That won't suffice for today's modern business. You can't stop business communication and still collaborate effectively. Fortunately, there are new approaches to collaboration security that mean you don't have to choose. Dynamically classifying sensitive information across collaboration tools and understanding what actions are justified, are key to effective collaboration security.

Understanding the security needs of collaboration tools

The commonality with collaboration tools is that they run on data – you're sharing information, documents and data – some of which is sensitive and subject to certain compliance regulations.

These platforms were built to allow users to share information seamlessly, putting collaboration first. Users share documents with each other without thinking about how sensitive the information in some of those documents might be. There's a risk that an unauthorized party could get in and access these documents and that information. It's easy to share information through collaboration tools in an unsafe manner – for instance, with a link open publicly or data still shared with a third party that you don't work with anymore.

Last summer, hackers breached Electronic Arts (EA), a digital interactive entertainment company, using collaboration technology as a gateway to gain access and passwords. Insider activity is also a concern, as we saw in the case of the Google executive charged with stealing trade secrets.

In fact, 82% of data breaches involved a human element, according to Verizon's *2022 Data Breach Investigations Report*. The latest data security breaches highlight both the insecurity of collaboration tools and the human element behind these incidents. Compounding this situation further is the fact that most organizations are still grappling with a significant security skills gap; they're understaffed and the staff they do have is often undertrained.

Staying secure while promoting seamless collaboration

For some older, more legacy companies, it's tempting to avoid such risk by restricting or even blocking the use of these collaboration tools – but they do so at the cost of limiting business. They might be a little more secure, but they're creating friction, hampering communication and slowing the company down. In today's competitive landscape, slower isn't an option. It's also not a panacea; employees will find ways to share information needed to do their jobs, whether it's sanctioned or not. The best option is to find a way to allow data sharing in a secure way.

Organizations today are using an average of 80 IT-sanctioned SaaS apps – and that number is growing. That doesn't count all the SaaS apps employees may be using on their own without getting IT's blessing (shadow IT). Securing each and every one isn't feasible; you have to focus on securing the collaboration channels where data is being moved back and forth, such as GDrive, OneDrive, or Slack.

This is a challenge. These tools are still very new; for many companies, adoption was as recent as the start of the pandemic. They're still adjusting – and so are the bad guys, although they're quickly discovering the potential opportunities these tools pose for them.

Context is key

The same old security tools used for the old way of working won't suffice because this new way of working is far more distributed. Manually classifying the data and applying static policies is also unwieldy; you wind up with a lot of noise and a high rate of false positives.

Here's an example: As opposed to an old system that might send an immediate alert that an employee has sent sensitive information and immediately block it, with newer collaboration security tools, you can gain additional context. Now you know the employee is a patent attorney who sent a patent to his colleague, a contractor also working on other patents and working in the same patents Slack channel – an activity that is justified.

Static rules, such as in the legacy data security tools, create a lot of noise and false positives. The only way to solve this problem of collaboration security is to have contextual understanding of the "why" behind every action. Without that, you can't effectively solve the problem.

Then, because it's impossible to do this manually, you need a dynamically updated set of rules that will ensure very low noise and accurate detection of risky data access and leakage. There are now tools available that use AI to automatically map the sensitive information in your collaboration challenges and apply business context to every action in every channel. By understanding the connection between platforms and individuals, a justification can be assigned to an action before alerting to it. This significantly reduces the noise, limits false alerts and allows security teams to more accurately detect risky activities. With these types of solutions, IT and security teams gain visibility and control over the data being shared within collaboration channels before any damage is done.

Collaboration in context

Adoption of collaboration tools increased dramatically when the pandemic pushed countless companies to enable remote work options. However, in many situations, this was done without prioritizing security. Now companies are trying to determine how to have the best of both – real-time collaboration but with full visibility, control and security. Contextual visibility and dynamic rules will help organizations use collaboration tools to their fullest extent while increasing their security posture.

About the Author

Ofer Klein, Co-Founder and CEO at Reco. He is a former Israeli pilot, a serial entrepreneur with a vast experience in building and growing GTM teams in SaaS companies in the US. Enthusiastic about leading solutions for the distributed workforce.

Ofer Klein can be reached online at (https://www.linkedin.com/in/ofer-klein-a0689449/ and at our company website https://reco.ai/

Sell tickets to Fans, Not to Bots.

By PJ Rohall, Head of Fraud Strategy & Education - SEON

It can be upsetting when you try to purchase a ticket for an event only to discover they are already sold out. Still, you can find some comfort in knowing you lost them to devoted fans who were as excited as you to go to the event. But what if those tickets were bought by bots whose only purpose was to resell them later for an insanely high price? How would you feel then? How much would it take to trust the company selling tickets again, or would you just give up, thinking there is no point in trying? The event industry is in real danger of being overwhelmed by bots at the expense of true fans. It is more important than ever to start taking the proper steps to protect themselves and provide customers with a positive ticket-purchasing experience.

Photo: Unsplash

What exactly are bots?

Even though they have a significant presence on the internet, most people are not even aware of the existence of the bots. Bots are computer software created to handle repetitive tasks that would have to be typically accomplished manually. They can complete these tasks faster, cheaper, and more accurately than humans, which significantly saves time and resources companies would have to invest to accomplish these tasks. While all bots are initially neutral until their makers give them their task, we mostly hear about the ones created for malicious purposes. The truth is that they are the future of cybercrime but also cybersecurity.

While bad bots make up the majority of bot traffic, there are still plenty of good bots online whose purpose is to bring value to the users and creator. Bismarts lists the ten best bots available on the internet right now, and you would be surprised how intertwined with your world they are. From getting breaking news straight to your phone to using bots to learn a new language through Duolingo or even getting recipe suggestions based on the ingredients you have available; these bots are here to make our lives easier. Unfortunately, no matter how much we would like that, not all bot creators plan to use them for good purposes.

Ticket Bots Endangering Different Industries

When considering ticket bots, most people are aware of their dangers in the event industry, especially regarding high-value concerts and sports events. The recent Taylor Swift fiasco proves their point. When the presale of tickets for the Taylor Swift Eras Tour opened on November 15, it was supposed to be available only for 1.5 million verified Taylor Swift fans. Instead, 14 million people, primarily bots, tried to access the site, causing it to crash while selling 2 million tickets in just one day. Many of these tickets appeared on third-party sites reselling for as high as $28,000, resulting in angry fans.

But malicious ticketing bots will not stop only at targeting high-value events. They can cause damage in different industries, for example, the airline sector. By utilizing ticket bots, malicious actors can reserve flight seats without completing the purchase, taking away the opportunity from genuine customers and raising the prices. The potential customers that tried to purchase the tickets will leave the attacked site and try their luck with the competitors.

Often, malicious actors will use stolen identity data and credit card information to purchase tickets via ticketing bots, resulting in even more innocent victims. Once the legitimate card owner discovers their card has been used without their permission, they will request a chargeback from their card provider. Not only does this mean that ticketing agents will lose their revenue, but once they cancel tickets that were purchased with stolen funds, innocent customers that bought those tickets from the resale sites will also suffer. Fraudsters will be long gone with their profits while leaving ticketing agents to deal with the consequences.

Photo: Pexels

Bots can even be used by inexperienced users as they can purchase them quite easily and cheaply on the dark web. This means that your event can be ruined by your competitor, who can use ticket bots to block all the seats for your event, damaging your reputation with legitimate people who want to come to your event. It is essential to get all the potential leads when organizing an event whose goal is to turn them into customers, and you can't allow malicious actors to stop you. Without utilizing bot detection software in their security strategy, ticketing organizations have no hope of fighting against bad bots and their malicious intentions.

Bad bots are a significant challenge.

While good bots try to make the world a better place, bad bots are trying to accomplish exactly the opposite. Their only purpose is to make a profit for their creators and owners, no matter how many people they have to damage in the process. In many cases, we will only notice bad bots once they accomplish their goals, and sometimes not even then. The rare occasion we are aware of the damage they do is during ticket sales.

Purchasing tickets for an event is already frustrating when you have to compete against the other fans whose numbers are significantly higher than the supply. But it gets to a new level of frustration when you also need to beat bots that can use many more resources than you can. Yes, those tickets can be later purchased on resale sites, but for significantly more money. This substantially reduces customer satisfaction while damaging the reputation of the ticket agents and ticket sales companies. This is why ensuring they sell tickets to their fans and not to bots needs to become their priority.

The move in the right direction has already started with the Better Online Ticket Sales (BOTS) Act, which President Barack Obama signed in December of 2016. This act bans the use of ticket bots for circumventing ticket purchase limits and bypassing venues' ticketing rules and makes it a federal offense. It also set a fine of $16,000 for reselling the tickets that were acquired through ticket bot software. Europe followed a few years later when the European Union Parliament voted to ban ticket bots in April of 2019.

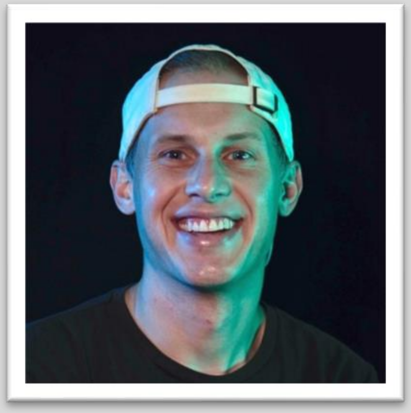
Fraudsters even go as far as selling unexisting tickets by using bots to impersonate legitimate people on Facebook or other social media. They use these legitimate looking profiles to try to persuade innocent victims to purchase the tickets from them. They often use a sob story as the reason they are no longer able to attend the event, making you more likely to accept their terms

While this legislation is a step in the right direction in bringing the danger of bots to the public eye, there is still much to do to prevent malicious actors from exploiting the systems and making a real difference.

Conclusion

As events are finally getting back on track, the importance of dealing with ticketing bots has never been as crucial. Utilize all the tools at your disposal to ensure your events are open to real fans and not to the malicious bots that wish to exploit you and your business.

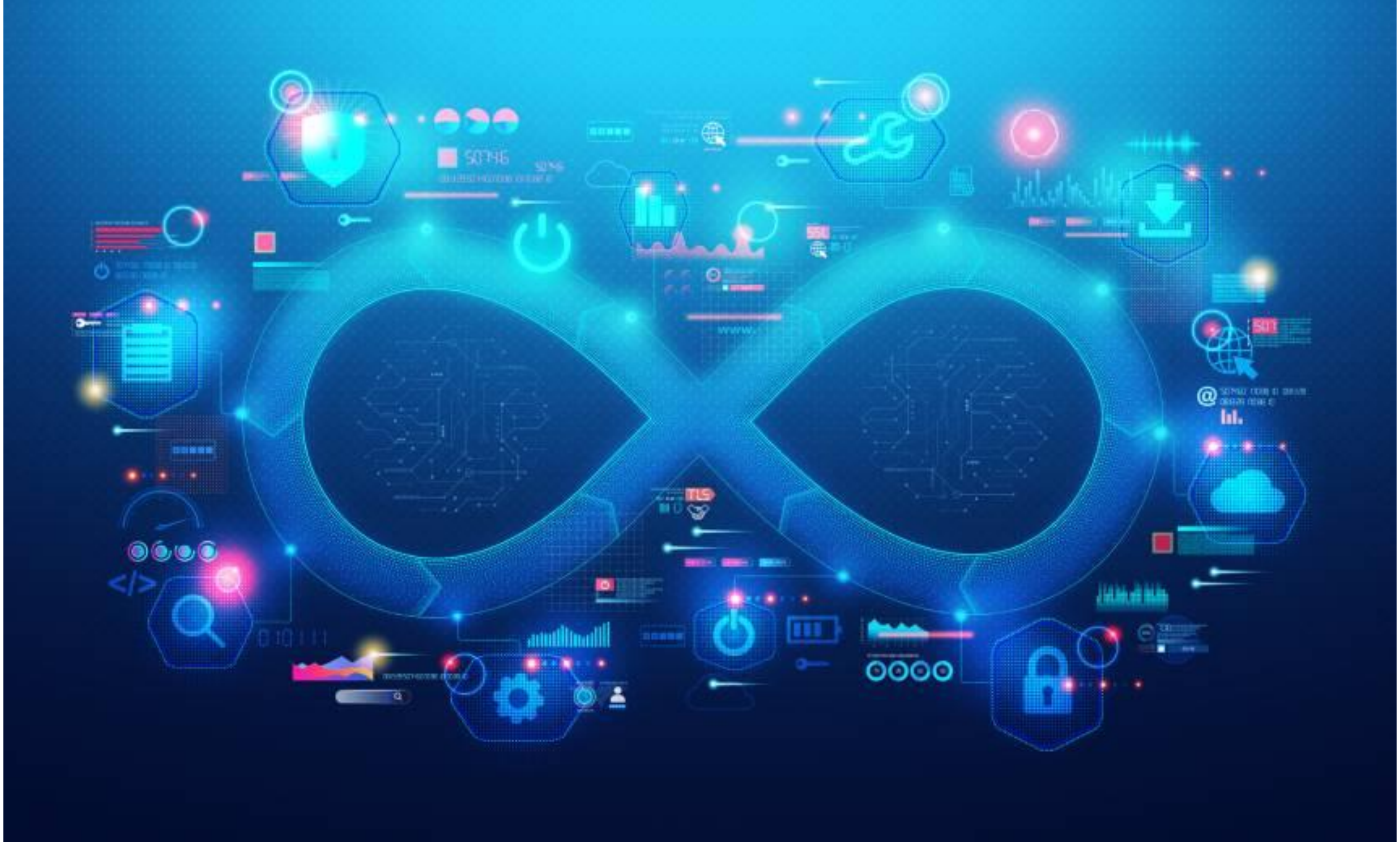
About the Author



PJ has over a decade of experience in Fraud Prevention and a strong understanding of Mitigating Fraud across the full spectrum of use cases. Currently, PJ is the Head of Fraud Strategy & Education at SEON. He speaks, engages, and educates folks on relevant fraud trends and strategies, while continuously learning from the industry and empowering fraud fighters across the globe. PJ also co-founded About-Fraud, a Global Community for Fraud Fighters. About-Fraud was built for Fraud Fighters, by Fraud Fighters and offers a one-stop shop for educational resources to folks who work in fraud prevention. PJ exudes passion and vibrancy that engages others while offering a refreshing dose of emotional intelligence.

https://seon.io/

https://www.linkedin.com/in/pjrohall/



Solving The AppSec Dilemma Across the Entire SDLC

Why organizations should adopt an integrated and continuous approach to application security education

By Amy Baker, Security Education Evangelist, Security Journey

The software supply chain is under increasing threat. With nearly half of organizations predicted to experience at least one software supply chain attack by 2025, developers and AppSec teams are becoming an increasingly popular target for cybercriminals who can wreak havoc. Especially when they exploit well-known and easily fixed vulnerabilities. For instance, the now infamous 'Log4Shell' vulnerability left some of the world's most commonly used applications and services open to attack and will reportedly 'haunt the internet for years'. More recently, the OpenSSL vulnerability caused chaos when it threatened to be a serious security bug, despite also being one of the most common coding issues and easy to fix (a buffer overrun).

These vulnerabilities affect businesses and consumers alike, as made evident by recent Apple weaknesses that allowed hackers to take complete control of users' devices. It's time to prioritize security, but doing so will take dedication to secure coding training.

Insecure software is still rewarded

One reason the software supply chain remains vulnerable to security threats is that it effectively continues to reward insecure software. In his opening keynote of Black Hat 2022, Chris Krebs stated that security would only continue to get worse before it gets better because the benefits of insecure software far outweigh the negatives. In other words, within the software development lifecycle (SDLC), organizations prioritize being the first to market. This goal is often at odds with security, which is portrayed as a barrier to productivity; 71% of CISOs claim their DevOps stakeholders view security as an impediment to fast development. This results in sacrificing security in the name of speed to market, the negatives of which are often not fully recognized until it's too late.

The AppSec Dilemma

This pressure to quickly create and bring products to market places immense expectations on those developing the software. And this is only increasing. 51% of developers deal with 100x more code than ten years ago. And almost *all* developers (92%) feel they must write code faster than before.

The ownership of application security becomes an issue with an overstretched team, often viewed as someone else's responsibility – be that AppSec, security, or IT professionals. Yet application security lives in a variety of places across an enterprise. Therefore, the executive team or board must buy into the value of secure coding training. Leaders must recognize that a security-first mindset is crucial for *everyone* within the SDLC. Product and project managers, DevOps, User Experience (UX) Designers, and Quality Assurance (QA) professionals influence the end result in software development and, therefore, will need to play a part in security. Sharing this responsibility is the first step in ensuring that secure coding is not forgotten.

Moreover, innovation and security do not have to be mutually exclusive, and treating them this way is likely why the number of new vulnerabilities continues to increase. Although almost always accidental, these security flaws and lack of proper secure coding education can turn developers into non-malicious insider threats. This insecure code can also be extremely costly; according to Boehm's law, "the cost of finding and fixing a defect grows exponentially with time." Investing in proactive prevention rather than reactive mitigation is, therefore, the most efficient solution for organizations in terms of security and an enterprise's bottom line.

Continuous and programmatic education

Shockingly, 53% of developers have no professional, secure coding training, and none of the top 50 U.S. undergraduate computer science programs require a code or application security course. With workforces worldwide struggling to fill the cybersecurity skills gap, it is vital that organizations look to an integrated and continuous approach to application security education across the entire SDLC. This must be:

(1) Specialized

For those involved in delivering code, it is essential that training speaks directly to the issues they face daily. Advanced, developer-specific education should be run in parallel with foundational application security training programs for those with roles in the SDLC that may not necessarily need hands-on expertise. These initiatives will empower the whole team to make more informed decisions around activities like threat modeling, application design, and what's in the software supply chain to integrate security across every aspect of development.

(2) Continuous

Secure coding training must be a continuous and evolving journey. It should never be a check-box, one-and-done exercise. In order to keep security front of mind, constantly building on knowledge and being aware of the ever-changing issues in the market is crucial.

(3) Rewarded

Organizations should offer incentives or rewards to those who consistently apply security best practices in their day-to-day work. Security champions engage others and organically influence change. By measuring results – like the number of vulnerabilities in code before and after training programs – and recognizing success, it is also far easier to get buy-in from stakeholders and justify the investment in secure coding education to the decision-makers.

Looking ahead

Innovation and security can integrate into the SDLC as long as we recognize these are not two aspects of development at odds with each other. This mindset needs to change, especially in an era where new critical vulnerabilities are revealed weekly and cybercriminals are becoming increasingly sophisticated. Staying one step ahead requires a commitment to application security education. This isn't a one-off but a career-long journey we need to kick-start today.

About the Author

Amy Baker is a Security Education Evangelist at Security Journey. Over her 30-year career, Amy has more than 10 years of experience driving the mission of improving security knowledge for employees in all roles. Her current responsibility is dedicated to improving security knowledge for everyone in the software development life cycle, with a specific focus on developers. Her experience started as a leader at Wombat Security and Proofpoint (post acquisition in 2018). She has spoken at various infosec conferences and webinars about best practices in managing security training programs such as Gartner, SecureWorld, and ISSA. Amy can be reached online via our company website https://www.securityjourney.com/

The Biggest Cyber Threats For The Financial Industry In 2023

Ben Herzberg, Chief Scientist of Satori

According to external market data, the financial sector was the most attacked in 2022 by DDoS attacks, while the number of all attacks has been constantly growing. A data breach in the financial services industry typically costs around $5.85 million, and ten percent of all attacks are financial breaches.

Certain financial institutions still need help to keep up with the cloud migration, and the growing number of cyber laws is not helping with these problems. On the other hand, phishing attacks continue to dominate the financial services industry, and companies are struggling to deal with new attacks focusing on social media.

We can safely say that companies in this sector have many security concerns. If they don't approach these issues seriously, they can damage and even destroy their businesses. Here are some of the biggest threats the financial industry should pay attention to.

What are the biggest cyber threats for the financial industry in 2023

When the financial system is disrupted, it affects the whole economy. We are seeing emerging trends likely to take shape in 2023 and become serious challenges. Whether new or not, companies must battle those threats and deal with them to remain operational.

Source: Pexels

1. Uncontrolled customer data

Companies use various technologies to gather and access large volumes of customer data. This data often contains sensitive information like customer PII and PHI. Sadly, it's often used irresponsibly, leaked, and accessed by unauthorized third parties.

Another problem is that companies often fail to meet the compliance requirements (such as GDPR) for using this kind of customer data and get into legal issues or simply spend a lot of resources on meeting these requirements.

Gathering sensitive customer information is a double-edged sword. On the one hand, it can fuel analytics, improve customer experience, and help provide personalized service. On the other, it can become your most significant security liability.

With that in mind, here are some ways in which the finance industry can protect customer data more effectively:

- Make sure all customer data access is monitored and logged
- Ensure you have clear and deterministic data access and security policies
- Enforce the access policies across all data access
- Make sure that access that is not required permanently is given only for the required time
- Make sure you know where your sensitive data is, and prioritize its security over non-sensitive data.

2. Ransomware threats

Ransomware attacks lock banking clients out of their computers and encrypt them with malicious software. Victims are then extorted for cash or information by attackers. In most cases, they don't get back access to their devices or accounts.

Because of this, financial institutions must train their employees continuously and adopt machine-intelligent security systems for emails and social media.

Invest in security training

Continuous training keeps everyone on their toes and updated on the latest types of attacks. People with proper training can spot malicious emails, social media messages, and links to prevent getting caught in a trap.

Adopt intelligent security solutions

Machine-intelligent systems can block and flag suspicious messages, emails, and organizations. They understand context, organizational behaviors, communication relationships and use this understanding to detect messages falling outside the norm.

These systems profile communications. For example, machine learning systems can learn about genuine inquiries customers send, complaints, issues, or questions. They can build a pattern of how customers communicate, what words they use, and what they include in their messages.

Using algorithms, intelligent systems can later recognize phishing messages as they don't fit the profile. They can also recognize harmful links and flag messages as potential attacks.

3. A broader scope of cyber attacks

Ensuring better protection for the global financial system is a priority. Financial firms, institutions, tech companies, and government agencies must work together internationally to create a threat-centric approach.

A threat-centric approach means creating a security framework within the financial secretary capable of learning about threats and adjusting security strategies. However, to do this effectively, all parties involved must work together, including the government, tech companies, and financial companies.

For example, SQL injections facilitate significant financial threats, and in 2021 WordPress revealed that over 600,000 sites were vulnerable to this threat because of a plugin. This is not something the financial sector is directly responsible for.

Still, organizations need to establish relationships with the industry, government actors, tech companies, and financial authorities to share strategies, learn about global risks, and find already-applied solutions.

4. Social engineering

Social engineering denotes cyber attacks relying on behavioral techniques to make people send confidential information or money. FI company representatives are often targeted for sensitive information used for extracting cash.

Social engineering attacks rely on someone's trust and goodwill, and people need the training to recognize:

- When they are urged into doing something without an apparent reason (check all the relevant facts and resources before responding)
- Unusual URLs or attachments
- Messages asking for something unusual
- Unexpected messages

Identity verification

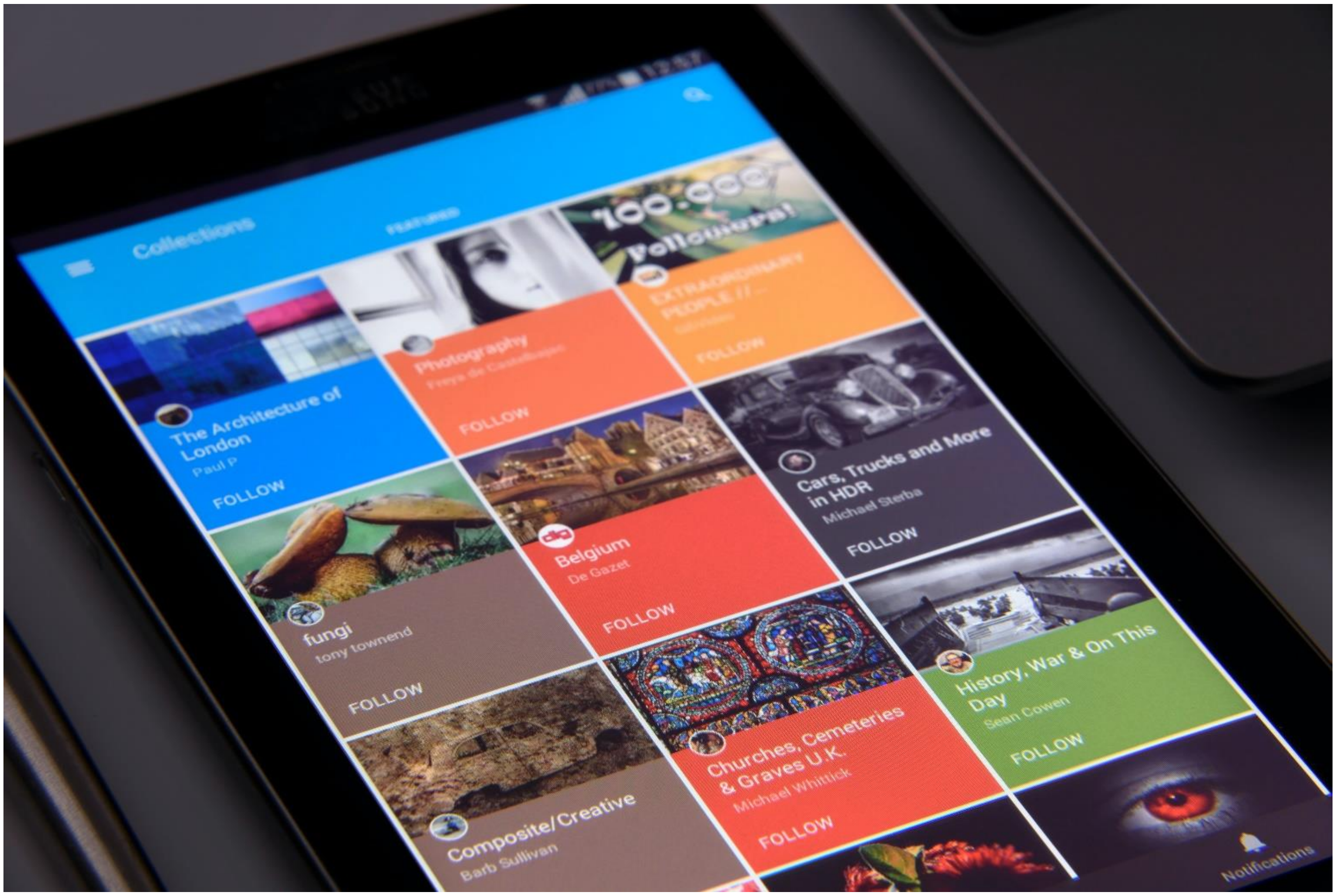
On the other hand, the finance sector can reinforce security by including verification steps that require customers to prove their identity. Identity verification solutions can be implemented to verify customer information as they have their data from official sources like government databases and credit bureaus.

That allows companies to recognize if customers are providing real information. At the same time, screening software can be used for probing onboarding customers with various questions.

The system analyzes their questions and decides whether clients should be allowed to proceed with an action (make a transaction or create an account). These solutions can also be used for real-time screening when a transaction actually happens.

However, it’s vital for financial institutions to partner up with fintech companies that can provide them with the exact tools they need.

5. Mobile devices



Source: Pexels

Mobile banking is a fantastic convenience many people enjoy today, but it also comes with many security risks. These risks are constantly growing, and we’ve seen a growth of 80% in malware threats on Android smartphones showing just how important mobile security is.

That is why banks and other financial institutions must constantly test their mobile apps to detect potential issues. At the same time, they should come with additional data security features like multi-factor authentication, data encryption, secured code, and secured communication.

Banks can also use contextual authentication, smart tools that account for behaviors and context surrounding events like transactions or logins. These tools review a lot of data and use an algorithm to present a risk score which triggers automated security protocols.

6. Cloud-based attacks

Cloud systems are another big security liability as they contain volumes of sensitive business data. Protecting these systems isn't really up to the financial organizations but to their service providers.

That is why financial organizations should do their due diligence in finding reliable partners that have excellent security tracker records and strategies to ensure no damage will happen. You can do this by:

- Checking if their security is up to standards, including ISO-27018, ISO-27001, ISO-27002, ISO-27017, and ISO 27001:2013;
- Checking their identity and authentication controls like MFA, CIFA, or real-time identity monitoring
- Seeing if they outline security, support, and maintenance in their SLA;
- Checking out their storage and data center locations
- Checking if they are compliant with the PCI-DSS and EUGDP regulations
- Doing a penetration test on their infrastructure with a cybersecurity professional.

7. Increased risk of supply chain attacks

Supply chain attacks target vendors that offer vital tools or services to the whole supply chain. They inject malicious code within vendor applications to infect all of their users. Software supply chains are particularly vulnerable because modern programs are written by using pre-made components like APIs, proprietary code, and open-source code.

To protect themselves against these attacks, financial organizations need to create a Zero Trust Architecture. With this structure set in place, all digital interaction stages are validated and verified, making it much more difficult for attackers to breach information through other services.

Organizations can also include Privileged Access Management because this process controls and monitors all users with access. Access control is essential, primarily when criminals target accounts already within a system.

8. Defi and cryptocurrency

More and more financial services include crypto transactions, and even though this might be good news for crypto enthusiasts, these services carry many risks. DeFi projects often have internal risks as their systems aren't secured and tested over time.

Some of the most common internal cybersecurity risks include:

- Management compromises (individuals or teams abusing their power)
- Faulty business logic
- Third-party protocol misuse
- Coding errors

All that can lead to crypto theft, identity theft, personal information leakage, etc., forcing organizations to create secure DeFi protocols by working with experienced developers.

Create a defense strategy

Banks and other financial institutions are legally obligated to uphold security controls that safeguard the confidentiality, integrity, and availability (CIA) of both their business data and client data, as these attacks can potentially cause sizable, widespread financial and reputational losses.

The financial industry should focus on safeguarding digital transformation results, expanding its cybersecurity capabilities, and building a security workforce.

Since securing your organization with a few simple measures is no longer possible, banks, financial institutions, investment companies, and other organizations now need comprehensive security strategies with experienced professionals leading the way.

About the Author

Ben Herzberg is the Chief Scientist of Satori. He is an experienced tech leader and book author with a background in endpoint security, analytics, and application & data security. Ben filled roles such as the CTO of Cynet, and Director of Threat Research at Imperva. Ben is the Chief Scientist for Satori, the DataSecOps platform.

Ben Herzberg can be reached online at https://www.linkedin.com/in/sysadmin/ and at our company website https://satoricyber.com/

The California Consumer Privacy Act (CCPA) and the American Data Privacy Protection Act: The Good, The Bad and The Ugly

By Dr. Eric Cole, Advisor - Theon Technology

Since 2018, there has been serious discussion of a new national privacy law promising Americans enhanced data protection, much like the European Union’s General Data Protection Regulation (GDPR). Nearly five years later, the US is still the only prominent actor in the world without an established federal data protection. In the US, we have always relied on state-level and local laws such as the California Consumer Privacy Act (CCPA), coming into effect on January 1st, 2023, as opposed to the government proposing something that serves the nation in its entirety. It's a step in the right direction that Congress is finally acting and is putting a law in motion that will protect US citizens, our information, and precious data. However, the proposed bill is not without potential flaws and implications; some may even argue the proposed bill falls short of the protections already in place at the state level. In addition, the law would fall under the scope of the Federal Trade Commission (FTC), which means that the law would only cover existing issues already addressed by the FTC. These issues include identity theft, children’s privacy, consumer fraud, and only some cybersecurity issues.

What’s more, as we embark on the new year, we expect to see a spike in regulation across the country. As we see California implement CCPA, other states will begin to follow suit. At a national level, we will see a rollout of new stricter regulations, and business leaders must be prepared. Organizations that have yet to play in the regulatory playground or have not had to deal with GDPR will be caught in a difficult position and will be pressured to implement these changes fast. As a result, they will be rushed through the process, all due to the US being slow to enforce these laws.

What does CCPA mean for the wider nation?

After various delays, on January 1st, 2023, the California Consumer Privacy Act (CCPA) will come into effect, and some common questions I've been hearing are:

- What does this mean for various organizations across the country?
- What impact will it have?
- How should organizations prepare for the rollout?

In today's interconnected world, most organizations and states deal with California in some capacity, so my advice is to look at CCPA as a precursor to what is going to be happening at a national level in the very near term. If you take a step back and consider January's rollout vs. what is being rolled out nationally, you'll notice it's very similar. Organizations and business leaders across the country should assume they must comply and follow all the regulations regardless of their state. Further, whether you deal with Europe or not, you should be GDPR compliant as GDPR will be similar if not identical to what is being proposed at the state and national level in the US. It is a significant hurdle to consider, however, because the US is so far behind in implementing these regulations, it will be a rushed ordeal.

What about encryption?

Everyone is overlooking the encryption of consumer data and ensuring keys are stored on separate servers. Most organizations have encrypted their data in the past, but the problem is they are leaving their data exposed, similar to locking your door but leaving the key under the floor mat. Are we locking our door? Yes. Is it really effective and safe - not in the slightest. A lot of old regulations we have grown accustomed to were all about encrypt encrypt, encrypt, but it remained unclear as to what was considered good or bad encryption. The majority of data theft we've seen in the US was from data that was "technically" encrypted but wasn't encrypted correctly because the keys were all the same. Today, regulators are doubling down and enforcing the use of different keys, which must be on separate servers. This is where we will see many organizations get themselves in hot water in California and across the country if strict enforcement is implemented. Historically, the US has not been a strict enforcer of these types of regulations, and as a result, executive teams are not taking them seriously. The difference between laws in the US and GDPR is that GDPR was strictly enforced from the start and made an example of companies who were not taking it seriously by making them pay millions for their mistake. As a result, the law was taken very seriously.

The most important factor in getting it right and establishing efficiency is ensuring individuals and organizations are compliant. The reasons why organizations are compliant with GDPR has nothing to do with the European Standard. GDPR is effective because of the enforcement and significant fines. If we look at PCI and HIPAA compliance, the US has struggled with enforcement, and for CCPA and ADPPA to be effective, better enforcement will be critical to its success. It will be a make-or-break moment, and questions like who will enforce the law? What will the penalties be? and what are the costs of implementation? These questions and answers will have to be clearly defined in order to raise the likelihood of compliance and prove effective or ineffective.

The good, the bad, and the ugly

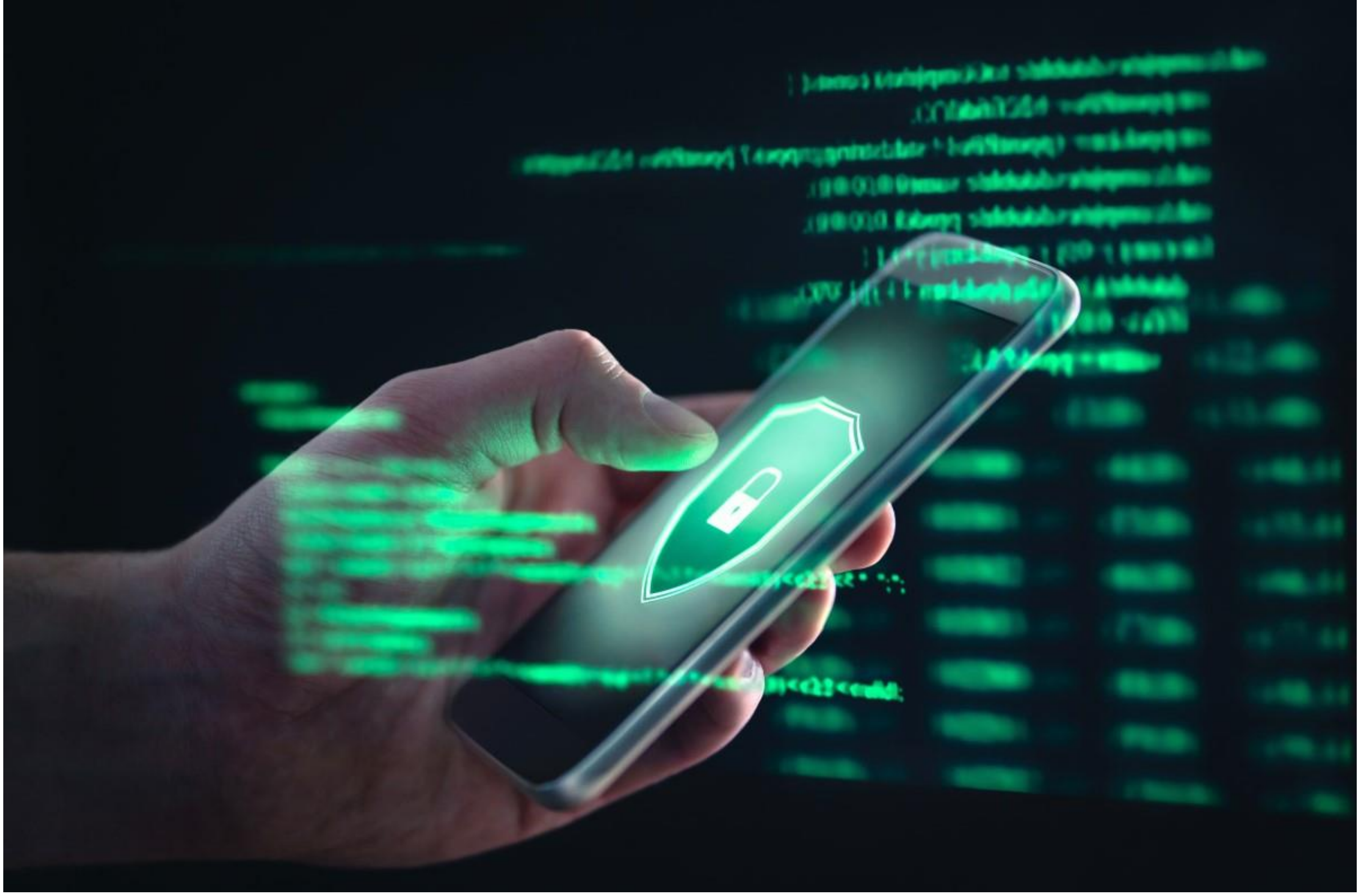
If and when these laws come into effect, the US government will have made tremendous strides by introducing a protection law at both the federal and national levels. One immense benefit of this is that it is being kept bipartisan and will be clear and concise, with no contradictory state laws that could get messy. But as with anything, there are potential challenges and downsides. With the ADPPA, a tremendous negative is that it is not compatible with European laws and will have many contradictions with companies abroad as well as US subsidiaries abroad, and different laws and regulations will be enforced in addition. In order for CCPA and ADPPA to be successful, strict enforcement will be essential. As we've seen with our European counterparts, if companies don't have real consequences or penalties, enforcement will be unlikely. What will the enforcement of CCPA and ADPPA be? One thing that is clear is that it will have to be enough to scare to take action and implement.

Overall, decision-makers have much work to do in order to make CCPA and ADPPA a success. Enforcement will be the most crucial factor. The stricter the enforcement, the higher likelihood of compliance and will dictate implementation willingness across the board. In the US, regulators have notoriously just given a smack on the wrist, ultimately causing executives and security leaders to not fear potential consequences. What needs to happen is CIOs and Security officers need to communicate effectively to the executive team that these regulations could result in significant fines. They should ask themselves whether they want to be the company that pays the 10 million fine and is made an example of?

Lastly, compatibility with GDPR will be key because the world is so interconnected in every sense. Because GDPR is tried and tested, the closer CCPA and ADPPA are made to mirror it, the bigger a win it will be for everyone.

About the Author

World-Renowned Cybersecurity Expert With more than 30 years of network security experience, Dr. Eric Cole is a distinguished cybersecurity expert and keynote speaker who helps organizations curtail the risk of cyber threats. Dr. Cole has worked with a variety of clients ranging from Fortune 500 companies, top international banks to the CIA. He has been the featured speaker at many security events and also has been interviewed by several chief media outlets such as CNN, CBS News, FOX News and 60 Minutes.



“The Impact of Mobile Threats on SMBs: 10 Simple Ways to Empower Your Company.”

By Wendy Taccetta, SVP, Small and Medium Business for Verizon Business

The shift in our hybrid and remote working world and the increase in mobile device use allow for a bigger attack surface — with more locations and devices expanding vulnerabilities. No matter what type of business you are—whether a city-wide pizzeria chain to the local hair & nail salon and spa—you must be prepared today to address cybersecurity issues from every perspective. Mobile devices provide an entry point for a wide range of attacks, with bad actors increasingly finding innovative ways to exploit and manipulate users and information — potentially exposing data and disrupting operations.

According to the 2022 Verizon Mobile Security Index (MSI), extensive mobile use and the increase in mobile and IoT devices resulted in a 22% increase in data or system downtime. Additionally, 52% of respondents said they have sacrificed the security of mobile devices to “get the job done.” In retail, almost nine out of 10 businesses are concerned that a mobile security breach could have a lasting impact on their brand or customer loyalty and 41% of respondents said mobile presents a daunting security challenge.

The Biggest Threats to the Smallest Companies: The More You Know

While being mobile (and untethered) presents many benefits, SMBs still need to be aware, alert and keep their defenses up.

- **Think before you click. (Phishing and mobile devices)**. Did you know that in 2021, 83% of organizations experienced a successful email-based phishing attack compared to 46% the year before? Attackers will take advantage of any opportunity to make their phishing attacks more successful. The design of apps on mobile devices can, unintentionally, make phishing harder to detect, helping attackers to get past people's normal defenses. Help your employees prepare by not clicking a bad link, providing credentials, or executing a wire transfer.
- **Just say no (To Apps and Access).** The number of apps, especially web-based ones, continues to grow. Malware remains a major problem, but even everyday apps can be a threat. Giving applications access to the camera, microphone, photos, location data, and other data and device functions can be a significant security risk. Users should be careful about applications requesting permissions that they don't need.
- **Beware of Weird Campaigns (Malware).** The 2022 Verizon Data Breach Investigations Report found that over 30% of breach cases involved some form of malware. Attackers design phishing campaigns specifically targeting mobile devices, and they build malware specifically for mobile devices too.
- **Ransomware.** The remote environment is primed for ransomware. As organizations continue to support remote or hybrid work, they no longer have the visibility and control they once had inside their perimeter. In fact, according to a recent State of Small Business Report, a majority of small and midsize business decision makers consider viruses (55%) and malware and ransomware (54%), the most concerning and at risk compared to previous years. Having unmanaged and personal devices on networks outside the traditional perimeter greatly reduces the visibility and control that security teams have.
- **Devices and things.** With more devices, the danger of lost or missing devices grows. But it's not just the quantity of devices that's growing, the variety is growing too. Today there are smartphones, laptops, tablets, hybrids, wearables, and a seemingly endless range of connected devices that employees are using.
- **Networks and cloud.** Insecure networks remain a serious threat to mobile device security. Attackers can intercept traffic through man-in-the middle (MitM) attacks or lure employees into using rogue Wi-Fi hotspots or access points.

10 Simple Ways to Prioritize Data Security in a Complicated World

With mobile use essential to staying relevant to consumers, it's a good time for companies of all sizes, especially SMBs, to double down on their cybersecurity policies.

Data security doesn't need to be complicated. Here are 10 simple ways they can better protect their data and key systems:

1. Ensure that employees understand the importance of keeping operating systems and apps up to date on all devices.
2. Prioritize cybersecurity awareness training so that employees know what to look for. (Training should include real-world attack simulations to mimic everyday scams.)
3. Deploy anti-malware functionality to all devices.
4. Consider restricting employee access on resources and devices not controlled by the company.

5. Force password changes.
6. Set mobile devices to allow full email addresses and URLs to be viewed.
7. Implement controls to verify requests for changes in account information — this could be as simple as sending a confirmation message before changes are made.
8. Develop a detailed bring your own device (BYOD) policy that clearly lists responsibilities in plain language.
9. Verify your backups often — an emergency is a bad time to find out that there's a problem.
10. Consider introducing endpoint detection and response (EDR)—this uses behavioral-based analysis to provide threat protection and can provide valuable insight.

Remember, education, preventative maintenance and a proper policy and solution are key to protect both your business and your customers critical information against cyber attackers.

About the Author

Wendy Taccetta is SVP of Small and Medium Business for Verizon Business. My team and I are focused on creating the best end-to-end wireless experience for small business owners who trust their business to Verizon. Wendy can be reached at wendy.taccetta@verizonwireless.com and online at LinkedIn here: https://www.linkedin.com/in/wendytaccetta/ and at our company website https://www.verizon.com/business/solutions/small-business/

The WAN Under Siege

WAN managers say they're adopting zero trust security and using multiple infrastructure security vendors in response to the latest threats against the modern wide area network.

By Greg Bryan, Senior Manager, Enterprise Research, TeleGeography

Network security is a growing priority for corporate leaders.

And for good reason. The number of organizations impacted by ransomware attacks more than doubled from 2020 to 2021, with healthcare the most affected industry, according to a report from network security firm Checkpoint.

As corporate networks integrate internet and cloud applications and change shape, weaknesses in the traditional network security model have become more glaring. It's this ongoing threat that underlies current attempts to modernize and strengthen enterprise network infrastructure security.

TeleGeography's WAN Manager Survey focuses on IT managers whose day-to-day role covers designing, sourcing, and managing U.S. national, regional, and global corporate wide area computer networks. It's through conversations with these professionals that we've gotten a glimpse into how technology professionals are meeting the security demands of the 21st century.

Our latest survey effort shows that one in three survey respondents reported a cyber security attack in the past 12 months at their company. Of those:

- DDoS attacks accounted for 40% of respondents cyber security incidents.
- Another 27% said it was caused by compromised credentials or weak passwords.

- Other reported sources included compromised applications, ransomware, and vendor vulnerabilities.

Putting Trust in Zero Trust

This brings us to zero trust security (ZTS).

ZTS encourages network security professionals to think differently about how they set up and secure their networks. It was a big part of our conversations with WAN managers during our latest survey effort.

First, some background. ZTS entails:

- Verifying users with more than one method.
- Simplifying how many passwords people need to keep track of.
- Restricting access based on identity so people only can access what they need.
- Segmenting the network to prevent horizontal movement across the organization by bad actors.

Positioning network security around aggressive user and device verification isn't a new idea, but ZTS is more relevant than ever.

Granted, secure access service edge (SASE) has also entered the security conversation as a framework for combining SD-WAN-enabled internet networking with cloud-based network security to facilitate BYOD, work-from-anywhere set-ups. But no matter how you slice it, research shows that WAN managers understand the urgency and are trying to update their IT security regimes.

One WAN manager at a technology company mentioned that their network and security team are working on revamping their systems along ZTS pillars and are "taking a 10-15 year old paradigm and making a 2021 philosophy."

But what does this look like in practice?

We asked WAN managers how far along they were in implementing ZTS or SASE security policies on their network. Implementation of one or more elements of ZTS or SASE jumped from just 8% in 2019 to 35% in 2021, a significant increase in just two years. In a somewhat connected discovery, we found a narrowing of the knowledge gap. Only 8% of respondents were unfamiliar with ZTS in 2021 compared to one in five in 2019.

Overall, we saw a shift down the deployment pipeline, with reductions in the percentage of respondents who either had not started, or were just beginning their implementation journey.

We also asked respondents who were in some stage of adopting ZTS what policies they were implementing or had already implemented on their network. We found that multi-factor authentication (MFA) and single-sign on (SSO) were the most widely implemented. Nearly 100% of respondents who had adopted ZTS had MFA in place.

Remote user and device access policies were implemented by almost 70% of respondents.

Privileged access management, or the restricting of access to certain data based on user profile, was implemented by 62% of respondents.

Just under half of respondents had implemented policies to treat foreign networks/devices as hostile. One-third of respondents had some sort of user behavior analytics in place.

Vendor Sourcing

When we talked to respondents about network security in 2019, we found that many companies preferred not to outsource the management of their network security vendors. They wanted to remain agile and pick best in breed vendors for particular security challenges.

In our latest WAN Manager Survey, we again find that the largest plurality of respondents, one in three, are using a mix of security vendors for their network security sourcing strategy.

Fifteen percent of respondents sourced their network security from a managed services provider or systems integrator. One WAN manager mentioned that they are allowing their broadband providers to manage internet security for them, however they had strict requirements including “policy visibility, see[ing] the logs, data on security analysis, and remote blackholing.”

Another 15% of respondents were sourcing their network security from their SD-WAN vendor.

One respondent, however, specifically mentioned that they do not plan to source their network security through their SD-WAN vendor, essentially rejecting the idea of combining the two into a SASE model. For them, “SD-WAN is just a new WAN service, not any of the additional stuff.”

Only 11% of respondents were sourcing their network security from their carrier or network service provider. One respondent said they were sourcing their network security through their carrier, as they were getting a better price since the carrier wanted it on their revenue books. However, they still manage their own security, other than DDoS protection which they have their carrier handle.

ZTS and the Future of Work

We've long pointed to cloud adoption and local internet breakouts as key factors moving enterprises toward ZTS over other security strategies.

But the impact of the pandemic has been palpable.

When asked to rank factors driving ZTS adoption, respondents who were in some stage of considering or adopting ZTS ranked "increased remote work" the highest. One WAN manager from an industrial company noted that they had tripled their remote workforce as a result of COVID and the company seemed open to keeping many workers remote long-term.

And remote work isn't going away. If anything, we anticipate it will only become a more hybrid experience for knowledge workers. (I say this as I sit in TeleGeography's DC office, my day full of both in-person and virtual meetings.)

As for how the evolution of this hybrid work experience will impact networks of the future, we'll have to see what WAN managers tell us in our next round of surveys. More to come next year.

About the Author

Greg Bryan is the Senior Manager, Enterprise Research at TeleGeography. He's spent the last decade and a half at TeleGeography developing a range of pricing products and reports about enterprise networks. He is a frequent speaker at conferences about corporate wide area networks and enterprise telecom services. He also hosts TeleGeography's WAN Manager Podcast.

Greg can be reached at gbryan@telegeography.com or through TeleGeography's website: https://www2.telegeography.com/

There's no way you're still using Consumer Messaging Apps for Business
LINE
kik·

There's no way you're still using Consumer Messaging Apps for Business

By Nicole Allen, Senior Marketing Executive, Salt Communications

Consumer messaging apps are routinely utilised for business purposes even if they were intended for personal usage. However, because of the legal requirements that apply to enterprises regarding data protection, corporate governance, privacy, and record-keeping, this type of messaging app is not safe for business use.

The emergence of messaging apps has been one of the most significant changes in the way we connect with one another. Over 41 million messages are transmitted using messaging apps per minute, and 3 out of every 4 smartphones today include messaging apps. So ensuring you're messaging your professional contacts in a safe and appropriate manner is essential.

What is the problem?

Some collaboration and communication platforms are more suited for organisations than others, and not all of them are developed for the same use case. The difference between consumer and enterprise messaging apps in terms of data protection, security, and compliance makes this more apparent in some cases much riskier.

Consider two instances of modern consumer communications apps - WhatsApp and Zoom. These technologies are frequently taken into account for organisations, but they have a history of putting data at risk, falling short of the security requirements needed to guard against significant security risks, and let's not forget their murky privacy policies.

Employees are increasingly using consumer-grade apps even to communicate with co-workers and clients, blurring the distinction between "*simple to use*" and secure solutions for businesses. Since they are "*free*" and "*popular,*" apps they are commonly accepted and the question is asked as to "*why shouldn't our business use them too*?" - but this is where many organisations go wrong.

Just because an app is 'encrypted' doesn't mean your messages are secure and safe

Then there is the infamous "End-to-End Encryption" myth, which is present in a lot of free consumer software. These apps are not the best platforms for exchanging sensitive business information or client conversations because they include so many grey areas and dubious privacy settings.

Let's take a look at WhatsApp as an example. WhatsApp is a messaging app intended for consumers. In the past, WhatsApp has come under severe fire for failing to safeguard the privacy of its customers' data. Additionally, the European Court of Justice found that US tech corporations, notably Facebook, do not offer their European consumers an acceptable level of personal data protection.

The communications on either end of the connection are not secured by it in any way. In any event, having encryption doesn't automatically make something secure. After all, Facebook, a firm for which security and privacy are, at best, theoretical constructs, owns WhatsApp.

With all of this in mind it is important to mention that spyware can make its way into a mobile phone through a security bug in voice calls made through insecure apps such as WhatsApp. WhatsApp and numerous other consumer messaging systems are also used as the method for gaining access to users' devices due to the open nature of these systems. With just a phone number we can with high levels of confidence bet that that phone number is linked to a consumer platform like WhatsApp.

With spyware, like Pegasus can immediately be transmitted. This call method is so powerful and inconspicuous that Pegasus may be installed on the phone simply by sending the user a missed call. After installation, the software would remove the call log entry so that the user wouldn't be aware of the missed call. Due to the open nature of these apps, they are very easily used as a distribution route for hackers.

What does this mean for you then? Really quite a bit. Your organisation still has information you don't want made public, even if it doesn't deal with highly sensitive material. Additionally, you can come across circumstances in which your communications carry legal bearing, like when you consent to a purchase over email. That is a further rationale for the development of secure enterprise applications. They serve to provide assurance and establish clear guidelines to ensure that your data is secure.

Lack of user management leads to security issues

The likes of Telegram, Wickr and Signal are also examples of consumer messaging apps that are susceptible to illegal communications. Just because these apps have a more "*trustworthy*" reputation than WhatsApp, doesn't mean that your messages are protected. These apps are frequently breached, rife with con artists and prone to malware attacks.

The information published within these applications and the company's "*hand off*" approach to moderation are two of the main problems with them. Due to their unique blend of messaging and social media and their openly weak content control policy, these types of apps draw a particular type of user who may have been exposed on other, more established online platforms.

In addition to all of that, there are flaws with group messaging and its inability to scale user management lead to a number of other security issues. Companies using these apps have no idea what groups are available, even less of who is inside of them, or whether former workers still have access to information they shouldn't. They now run the danger of having private commercial information accessed or disclosed. This is always a risk when allowing employees to use insecure and uncontrolled communications systems, putting your reputation, information and conversations at risk every time they access their phone.

Why you should use a secure enterprise alternative

It is never a smart move to use WhatsApp for business communications if security and compliance are top objectives for your company. Your staff members require a secure solution for workplace communication that enables them to get information and interact with one another anywhere at any time. With a secure communications app Salt Communications organisations can effortlessly manage users, regain control over their data, and maintain compliance.

Salt Communications provides enterprises with the highest level of security, with complete control over your communications and data at all times. After reading this article you are probably thinking there's no way I'm still going to be using a consumer messaging app for business means. We hope you take the right step to protect you and your organisations communications.

Learn more about what features a secure enterprise messaging app can provide.

To discuss this article in greater detail with the team, or to sign up for a free trial of Salt Communications contact us on info@saltcommunications.com or visit our website at saltcommunications.com.

About Salt Communications:

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

About the Author

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

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

Top 5 Questions to Ask When You're Building a Cloud Security Strategy

By Metin Kortak, chief information security officer, Rhymetec

As companies began moving their computing operations and data storage to the cloud, the security of these digital assets has been a priority. Implementing a robust cloud security strategy is paramount for every organization. SaaS providers, in particular, carry a vast amount of sensitive data. This scenario represents a sizable risk to a company's privacy and intellectual assets, so when you start building a cloud security strategy, you *must* ask—and be able to answer—these five vital questions from the outset.

Q #1: What requirements must our SaaS organization comply with from legal, client, or end-user perspectives?

Depending on the type of industry or end-user you are serving, both legal and client standards should be an area of focus when it comes to their respective compliance and data privacy requirements.

SOC 2

Systems and Organizational Controls 2 (SOC 2), although voluntary, is an important differentiator for any SaaS vendor or company managing the data of other organizations. Developed by the American Institute of CPAs (AICPA), it's a service standard that specifies how organizations should manage customer data.

The standard is based on five Trust Services criteria: security, privacy, availability, processing integrity, and confidentiality. Compliance gives your clients the reassurance that your company takes its job of managing their data seriously enough to have proven its competence over a prescribed period. For a security-conscious business considering a SaaS provider, SOC 2 compliance is a minimum requirement.

ISO 27001

This is a global certification for companies looking to implement an information security management system. It goes beyond the SOC 2 information security function to include an operational security management system. International clients might want your company to have ISO 27001 certification, e. The good news is if you are complying with SOC 2, you might be already halfway there.

Legal Requirements

From the legal viewpoint, you'll need to implement the privacy regulations that apply to your target market. FedRAMP, GDPR/CCPA, and HIPAA all serve specific industries. For example, if your company sells products or services in the EU, you'll need General Data Protection Regulation (GDPR) compliance, which is an essential element in EU data privacy laws.

For U.S. companies operating in any area of healthcare, HIPAA compliance is a stringent privacy requirement, although you don't get a certificate to show it. Organizations serving the U.S. government *must* achieve FedRAMP compliance, and if you process sensitive data of California residents, you'll need to comply with the California Consumer Privacy Act or CCPA. This is a law aimed at enhancing privacy rights and consumer protection for residents of that state.

Industry-Specific Regulations

Various other industries have their own legal demands, such as the payment card industry's Data Security Standard (PCI-DSS). This standard, usually referred to as PCI, is a series of security requirements for programs that process and store credit card payment information.

#2: How much budget have we allocated to cybersecurity for our clients?

It's important to be mindful of the costs associated with building secure software. Cybersecurity costs money and it's not cheap to implement the needed range of security controls. This being said, your SaaS organization needs to carefully consider how to allocate the various costs involved in keeping your clients' information secure. You'll need to get pricing on implementing layered security as most SaaS vendors need at least three different security layers to protect their customer data from external threats. These are basic infrastructure layers consisting of cloud data storage platforms, hosting companies, and internal servers.

You'll need to:

- Install robust data encryption software
- Deploy virus and malware protection programs at every level of access
- Provide training for your team and customers on how to handle data securely
- Backup your customer data and store the backups in multiple locations and formats
- Consult a third-party cybersecurity firm to conduct regular testing of your systems
- Pay for external party auditors

Every company that contributes to the SaaS product you offer will need at least the same level of security and compliance all the way down the chain. Since the chain starts with your company, you must budget for the expense of ensuring your security is watertight.

Q #3: Do we have enough human resources to handle security and compliance needs?

We're all waiting for the day artificial intelligence can handle everything, but that's still a fair way off. Right now, your SaaS organization will still need to have enough human resources to carry out critical security functions. These include:

- **Implementing security controls on devices.** Administrators must install data encryption programs, configure firewalls and antivirus protection, and monitor intrusion detection systems. According to Verizon's 2022 Data Breaches Investigations Report, 82**%** of all data breaches involve a human element, so implementing robust security controls reduces the risk of such incidents.
- **Managing vulnerabilities**. These controls include risk assessments to determine the probability and impact of threats and vulnerability assessments to uncover weaknesses and identify additional measures to reduce the danger posed by these vulnerabilities. Diagnostic tools and artificial intelligence can assist with much of this, but human resources are still needed to make final decisions and implement the processes.
- **Running background checks on your employees.** In many cases, employees can deliberately expose information—for example, by misconfiguring databases or allowing cyber criminals to access the organization's systems. Without running background checks, companies leave themselves vulnerable to employing bad actors.
- **Onboarding and offboarding of employees.** Follow best practices for onboarding and offboarding employees to prevent increasing your cybersecurity risks. New employees should be trained in cybersecurity adapted to their entry level, understanding, and experience, and given only essential access initially. Exiting employees should undergo exit interviews, and the cybersecurity team should establish an offboarding program. This program should include

revoking all login access immediately the worker leaves, informing all colleagues and shareholders of the departure and monitoring the systems the employee had access to for a period of time after they leave.

Having enough people for a powerful cloud security strategy doesn’t mean you must appoint high-cost, permanent employees. Managed information security services can extend your operation by providing the support you need around the clock, and at fractions of the price of a full-time security professional.

Q #4: What are some security best practices to adopt in our organization?

Some organizations choose to be very flexible with security and only do the bare minimum needed to comply with the different frameworks. More security-conscious organizations often go above and beyond and implement advanced security controls.

For example, I once worked with a client who forced all employees to register their phones and computers in MDM before they could access any company resources. This wasn't a compliance requirement but a choice the organization made to improve its security posture.

Basic best practice options every business should adopt include:

- **Conduct regular risk assessments across all systems.** Things change. Software gets updated, bad actors find new ways to target organizations, and the value of your data to hackers becomes more valuable and easier to access. Companies should assess their risk levels annually at least, if not more often, and when they make any significant systems or business changes that could leave them vulnerable. These include migrating to the cloud or appointing a new supplier with access to the systems.
- **Implement measures to reduce risk.** Once you know what factors threaten your SaaS organization, you can implement reasonable security controls to mitigate these risks. Train your staff in security awareness. Apply penalties for violation of security rules. Screen new hires and provision user rights to allow access to essential services only.
- **Apply password controls and virus protections.** Develop comprehensive password policies and enforce the use of multi-factor authentication. Make sure your firewall is correctly configured, and encrypt your data using a VPN. Install tough virus and malware protection and securely dispose of old and discarded equipment.
- **Inventory all data, equipment, and processes.** Protecting your data depends on knowing what you have and where it is. Many data breaches involve leads of confidential information that was inadvertently stored in email, on lost laptops, or backup tapes. Identify and catalog all your customer and employee records, store payment information separately and securely, and ensure all your equipment protections are up to date and working well.
- **Build cybersecurity into your operational processes.** IT systems can be vulnerable if they aren’t properly maintained. Harden your network by removing or changing default credentials (e.g., passwords such as 1234567 and user names like “admin” or “info”). Apply critical security patches promptly and monitor systems for deviations from expected norms.

Establish ways and means to detect and respond to incidents and develop sound business continuity and disaster recovery plans. Make certain third-party providers are also secure by conducting an audit of their security measures or building standards into their contracts with you.

Q #5: Did we conduct a penetration test against our application?

Most security vulnerabilities are not identified until an external party conducts a penetration test. A penetration test is one of the best ways to identify any significant security issues with an application. Penetration tests go a step further than a risk assessment by attempting to exploit the weaknesses identified.

For example, a vulnerability assessment might discover patches are not being updated regularly, leaving a company vulnerable to attacks. A penetration test would attempt to access the company systems through unpatched vulnerabilities, enabling the cybersecurity team to shore up any potential risk areas in advance.

Being Prepared

Any company building a cloud security strategy must comply with the requirements of their industry but it is just as important to go beyond required compliance by being prepared ahead of time for any possible cybersecurity incidents. Put processes in place to detect anomalies and attempted breaches. Exercise reasonable security measures to anticipate problems. Make sure you have adequate backup and restoration procedures. If you are unsure about moving forward, get expert help to secure your systems and protect your customers and staff.

About the Author

Metin Kortak the Chief Information Security Officer at Rhymetec. Metin Kortak has been working as the Chief Information Security Officer at Rhymetec since 2017. He started out his career working in IT Security and gained extensive knowledge on compliance and data privacy frameworks such as: SOC; ISO 27001; PCI; FEDRAMP; NIST 800-53; GDPR; CCPA; HITRUST and HIPAA.

Metin joined Rhymetec to build the Data Privacy and Compliance as a service offering and under his leadership, the service offerings have grown to more than 200 customers and is now a leading SaaS security service provider in the industry. Metin splits his time between his homes in California and New York City and in his free time, he enjoys traveling, exercising, and spending quality time with his friends.

Metin can be reached online at https://www.linkedin.com/in/mkortak/ and at his company website https://rhymetec.com/

Vulnerability Prioritization is Not a One-Size Fits All Approach

By Victor Gamra, CISSP, Founder and CEO of FortifyData

System vulnerabilities are ever increasing as adoption of new and emerging technologies are implemented. Security professionals struggle to keep up with remediation efforts presented by a variety of new technologies and the lack of vulnerability prioritization. In 2022, we have already surpassed 22,000 recorded Common Vulnerabilities and Exposures (CVEs), which exceeds the previous record set in 2021 with 20,170, according to the National Vulnerability Database. Security teams are already stretched and are drowning in a sea of vulnerabilities. With new ones popping up each day, plus a shortage of IT security staff, mitigating them all would be impossible. So, security teams must do their due diligence to prioritize them.

Historically, a de facto prioritization method relied on Common Vulnerability Scoring System (CVSS) scores, combined with regulatory guidance on which level of vulnerability should be remediated in a certain time frame. CVSS ratings do a good job at looking for opportunistic vulnerabilities (i.e. can they be exploited remotely?), but they were never meant to be used to prioritize because they lacked the association to asset criticality to an organization.

According to a 2021 publication by CISA, "CISA has observed that risk scores, based on the Forum of Incident Response and Security Teams' Common Vulnerability Scoring System (CVSS), do not always accurately depict the danger or actual hazard that a CVE presents. Attackers do not rely on "critical" vulnerabilities to achieve their goals; some of the most widespread and devastating attacks have included multiple vulnerabilities rated "high," "medium," or even "low."

"Since CVSS was never intended to provide risk prioritization within each enterprise's unique environment, this has led to goal misalignment. SLAs such as 'Patch all critical CVSS scores within 30 days' do not weigh the business context of asset criticality, whether exploits are published and active for that vulnerability, and if there are compensating controls that can protect against that exploit," wrote Erik Nost, Senior Analyst at Forrester, in the Forrester blog, "Vulnerability Programs Must Regain Trust to Inspire Action."

It's time to be smarter about how we prioritize vulnerabilities because there is no one-size fits all approach. To do this, we need to bring more meaning to the vulnerability data with contextualized risk intelligence that incorporates threat intelligence and impact to the business. You need data to tell you what the vulnerabilities mean for your specific organization.

- Do you know your assets?
- Is the vulnerability present on mission critical asset?
- Are there threat actors currently exploiting this vulnerability within my industry?
- Do we have compensating controls in place?
- What is the likelihood of a threat being realized?

This is how vulnerability management is evolving – into Risk-Based Vulnerability Management – and it will solve a major problem for a lot of organizations. But to get there, you need to take a few steps.

Step 1: Discover Your Assets

We see a lot of organizations experience issues with asset detection, and that's no surprise given the increasing number of assets and entry points that each organization has. Not to mention shadow IT – where organizations are spinning up resources or signing onto technologies that the IT teams don't know about.

Keep in mind that attackers are scanning your environment to try and discover your assets.
So being able to map your entire attack surface is very important. Start with your on-prem assets, as well as assets with external facing IPs. Then make sure to discover mobile devices, and dynamic assets, like cloud infrastructure, web applications and containers. Automating the continuous identification of assets is fundamental to developing a risk base vulnerability management program. CISA recently published a Binding Operational Directive on Improving Asset Visibility and Vulnerability Detection on Federal Networks calling attention to the importance of knowing the assets and managing them accordingly.

Step 2: Classify Your Assets

Once you're able to gain that initial view, you need to be able to classify those assets because they will all have varying degrees of criticality to your business. Correct asset classification enables vulnerability prioritization.

To understand which are the most valuable resources, you need to understand what type of data is stored, processed or transmitted on them, that tells you how important specific asseets are to the business. We suggest doing a business impact analysis and making sure that you have agreement from the C-suite.

Make sure to also do an analysis of compensating controls, which can help you de-prioritize certain vulnerabilities. And finally, you must automatically discover new assets on a continuous basis and ensure those new assets are classified according to business impact.

Step 3: Automate Your Process

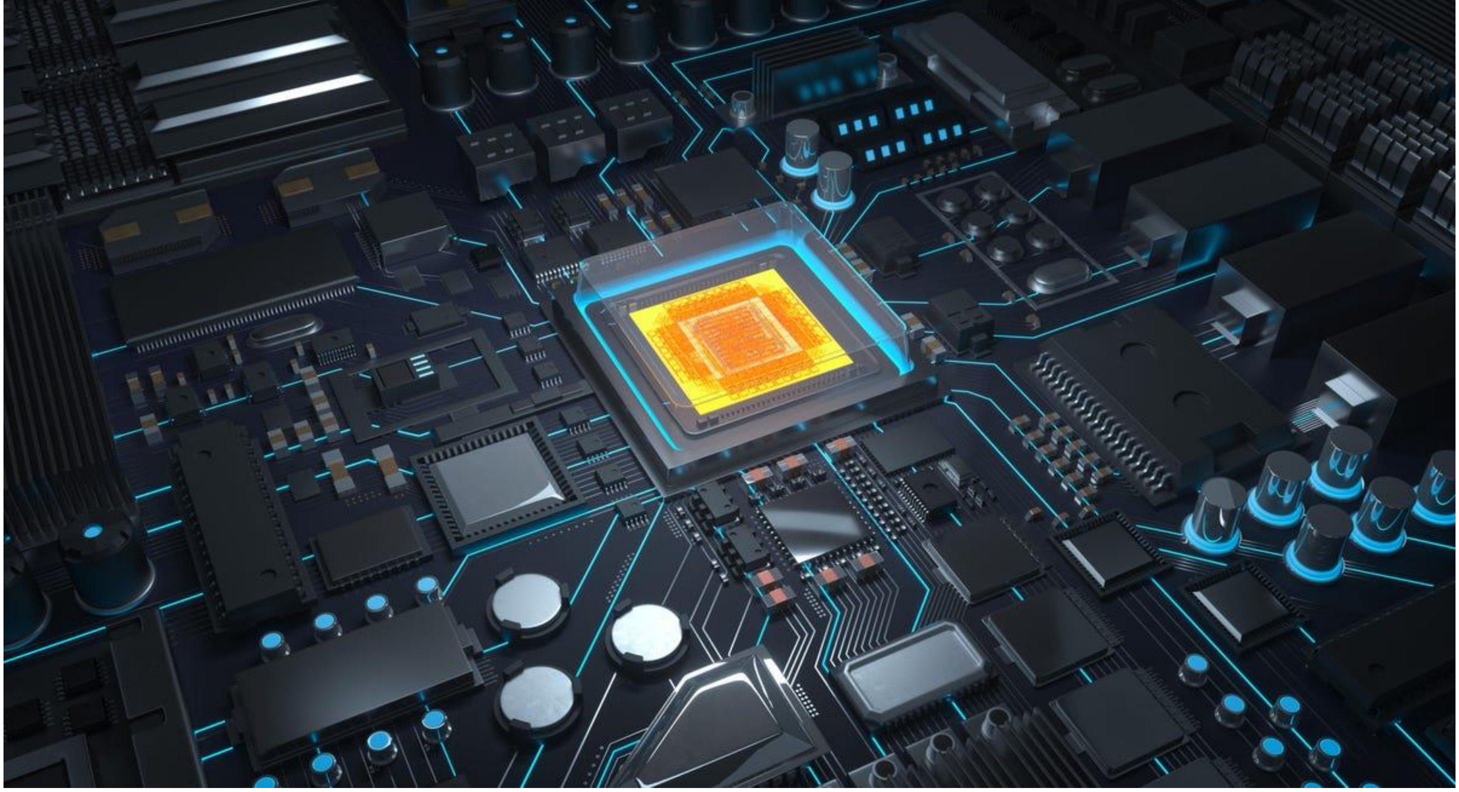
Automation is the key to making vulnerability prioritization work effectively. The volume of vulnerabilities is way too high and security teams are way to lean to go through each vulnerability one-by-one. Automation is done with risk-based vulnerability management married with threat intelligence and controls analysis. Whatever platform you choose should be able to:

- Continuously monitor with live assessment data
- Auto-discover assets and classify them
- Auto-sync updates from the National Vulnerability Database
- Prioritize findings that include currently exploited vulnerabilities from sources like CISA
- Present remediation guidance on how to remediate critical risks

Risk-based vulnerability management powered with automation enables your team to prioritize remediation of the most impactful vulnerabilities. You will become more effective by knowing what to remediate and how to remediate the identified vulnerabilities to reduce the critical risks to your organization.

About the Author

Victor Gamra, CISSP, is a former CISO and the Founder and CEO of FortifyData. FortifyData is an automated cyber risk management platform that provides risk-based vulnerability management, third-party risk management, security ratings and cyber risk quantification. Visit www.fortifydata.com for more information.



Why Businesses Need to Leverage the NIST Post Quantum Cryptographic Standards to Fortify Their Cybersecurity Future

By Dr Ali El Kaafarani, Founder and CEO of PQShield

July 5th, 2022, marked an important milestone in the fight to secure sensitive data against future cyber-attacks from quantum computers.

The U.S. National Institute of Standards and Technology (NIST) selected the first group of quantum-ready cryptographic standards known as post-quantum cryptography. These cryptography schemes are purpose built to withstand attacks from a quantum computer, which will eventually have the power to break the current security encryption used to protect virtually all of the world's sensitive information.

The announcement, which was the culmination of the first stage of a six-year effort managed by NIST, showcased the fruits of global cooperation from the cryptographic community. For the second stage additional algorithms are under consideration for inclusion in the standard, with this multi-stage process allowing for the robust and thorough testing of all algorithms. This process has already allowed the cryptographic community to scrutinise and rule out weak candidates.

Why the quantum threat isn't overhyped

For many, the prospect of a quantum computer at a scale needed to threaten our encryption is in the long and distant future. However, with $3.2 billion investment in 2021 for quantum technologies and

China already committing $10 billion investment towards its development, the threat they pose to encryption is no longer a question of if, but when.

Quantum computers are a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers. Through this new computational model, quantum computers will be able to break all current public key encryption used ubiquitously today.

The risk is rapidly becoming a major concern for policy makers: the G7, led by the White House, recently included the quantum threat in their key 21st Century challenges.

From a risk perspective however, independent of how quickly this emerging technology is developing, what makes the threat even more dangerous is that quantum attacks, namely the "*Harvest Now. Decrypt Later (HNDL)*, can be carried out retrospectively. This means that an institution can be targeted today with a 'harvest now and decrypt later' attack. Threat actors have the capability of harvesting encrypted sensitive data from across sectors and levels including financial information, national security intelligence and business and consumer data and then storing this data for decryption at a later date.

It is this fact that demands an urgent response from the cybersecurity community. Security is about identifying and mitigating risk: the longer businesses delay replacing exposed encryption with post-quantum cryptography, the greater the quantity of data will be exposed.

What do the NIST standards mean for businesses?

There is growing recognition of the need for businesses to prepare for this new and sophisticated threat, especially to the cyber systems that our critical infrastructure and democratic institutions rely on. The primary purpose of the NIST process was to identify a robust suite of encryption that businesses could trust and utilise in defending themselves against this threat.

Under the guidelines and protection of these new standards, businesses can chart a path to long term cybersecurity with the certainty that the encryption they are using is quantum secure.

The process to achieve quantum security is simple in concept but the challenge will be in the execution.

Businesses first need to identify their exposure through a comprehensive audit of the encryption they use and its locations. With this clear picture and armed with these new standards we can chart a roadmap and timeline to move forward in replacing the vulnerable encryption and adopt PQC.

What's next for post quantum cryptography

Now is not the time for complacency. The global post quantum cryptography community has worked tirelessly to establish these new schemes and standards, but the focus now must turn on adopting them within its cybersecurity infrastructure imminently.

These new standards also represent the beginning of the journey towards actualising a quantum secure future. Just as businesses and governments need to stay alert to adapt to the growing and changing threats, so does the cryptography industry which needs to continuously innovate to stay ahead of looming risks.

NIST is already leveraging the momentum gathered with the announcement of the new standards with additional algorithms under consideration for inclusion in a fourth round. Since the beginning of NIST's effort there has been a recognition that various systems and processes use different approaches to encryption. In order to develop and cater for all the variations, further security scrutiny by cryptographers and mathematicians is crucial to protect us. Cryptography is a never-ending field and requires constant innovation to keep ahead of current and future threats.

Still, as the process to find more tools goes on, CISOs and cybersecurity leaders need to be adding the adoption of these standards to their objectives for the coming years. We must include quantum security in new products being developed, PQC guarantees in vendor contracts and upgrades to legacy infrastructure must include installing PQC components. Current encryption has permeated every aspect of business and life making the adoption of post-quantum cryptography the biggest cybersecurity challenge in decades.

About the Author

Bio: Dr Ali El Kaafarani is the Founder and CEO of PQShield, a British cybersecurity startup specialising in quantum-secure solutions. A University of Oxford spin-out, PQShield is pioneering the commercial roll-out of a new generation of cryptography that's fit for the quantum challenge, yet integrates with companies' legacy technology systems to protect them from the biggest threats of today and tomorrow. Dr El Kaafarani is a research fellow at Oxford's Mathematical Institute and a former engineer at Hewlett-Packard Labs, with over a decade of academic and industrial experience. He is also a leading authority in the cryptography community.

Why Tackling Financial Crime Calls for A Privacy-First Approach

By Dr. Alon Kaufman, CEO and Co-Founder of Duality Technologies

To gain the upper hand in the fight against financial crime, banks and other financial institutions need to share data, but concerns around privacy, confidentiality and regulatory compliance often prevent them from doing so. Alon Kaufman, chief executive officer and co-founder at Duality Technologies, looks at how firms are adopting a privacy-first approach to overcome these barriers and enable greater collaboration.

Cybercrime, fraud and money laundering continue to pose major threats to financial institutions and their customers. As attacks become more sophisticated, detecting, investigating and preventing risks grows more challenging and firms often find that existing approaches have notable limitations.

Success hinges on having access to the right data, but the problem is that data is dispersed across multiple lines of business within an institution, geographic locations and third-party institutions. This fragmentation can make it near impossible to access and analyze all the relevant data quickly in order to gain insights.

A typical customer will have multiple accounts with different providers as well as relationships with separate divisions within the same provider. As a result, the customer's financial life is broken up to the point that no single institution has a complete view of the customer. In fact, a typical financial institution only sees 15%-25% of its own customers' activity, which means it cannot effectively protect itself nor its customers from financial crime.

An evolving data collaboration regulatory framework

Collaboration between firms is crucial and regulation has gone some way to encouraging this. The USA Patriot Act, specifically Section 314(b), allows financial institutions to share information with one another so they can identify and report to the federal government activities that may involve money laundering or terrorist financing activity, including predicate offenses.

Other governments and regulators around the world have joined the cause. The Financial Action Task Force (FATF), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Financial Conduct Authority (FCA), Monetary Authority of Singapore (MAS), and of course Financial Crimes Enforcement Network (FinCEN), have continued calling for more information sharing and collaboration among regulated entities to better fight financial crimes and terrorism. However, while Section 314(b) has been well-received, it remains underutilized and, therefore, still far from reaching its full potential.

Existing approaches

The problem is that firms can only share appropriate data if they can preserve privacy, confidentiality, and regulatory compliance. Too much transparency would fuel competitive concerns, as revealing details of a key account, for example, could expose valuable information to the market. Firms must also respect their country's privacy laws, which in some cases outside the US prohibits them from declaring they have a business relationship with a specific party.

Many existing approaches cannot offer privacy guarantees. In financial crime, previous efforts have included the creation of utilities and consortia but, typically, these have leant on manual approaches and the sharing of strategies rather than actual data, which only goes so far.

Other efforts have lacked automation and proven to be inefficient. Often, participants don't share all the available data due to privacy issues and protections around that information, and the manual nature of these efforts are difficult to scale. The processes required to share data on a one-to-one basis don't work when it comes to sharing data with an entire network.

A third approach, which is used across the industry, is implementing transaction monitoring systems. These go a long way to helping understand risk and suspicion, but the challenge with these systems is that they rely on data that the firm or jurisdiction already has, so they don't actually address the data sharing and collaboration problem.

More recent approaches to tackle financial crime are based on blockchain or hashing. With blockchain, however, the problem is that its key benefit is also its downfall – transparency. Even in a closed network, any participant can see the data being shared, which compromises privacy and security, and reveals information about competitors' customers and transactions.

As a result, firms are often reluctant to join blockchain initiatives or avoid contributing their most valuable data, making the solution incomplete and ineffective. Essentially, blockchain does not adequately address these regulatory and competitive concerns, which hampers how effective these solutions can be.

Alternatively, hashing has enabled simple comparisons, but the problem is it is easy for criminals to circumnavigate these checks. In trade finance fraud, for example, a fraudster trying to hide duplicate financing can easily use different purchase order numbers or change data across documents to make them seem different and evade searches for matches or similarities. Firms need technology that is fit for purpose and able to detect the more complex tactics that criminals deploy.

Customer financial data is highly sensitive and must be kept private and secure. Unfortunately, locking data away in silos creates blind spots for malicious actors to evade detection by freely maneuvering between institutions and across borders. Banks and financial institutions use Duality to shine a bright light on the dark shadows of data silos by allowing them to collaborate on customer data while preserving privacy.

A privacy-first approach

If financial institutions could have the privacy and security guarantees that ensure the protection of their data and customers, as well as regulatory compliance, they would be more open to sharing information.

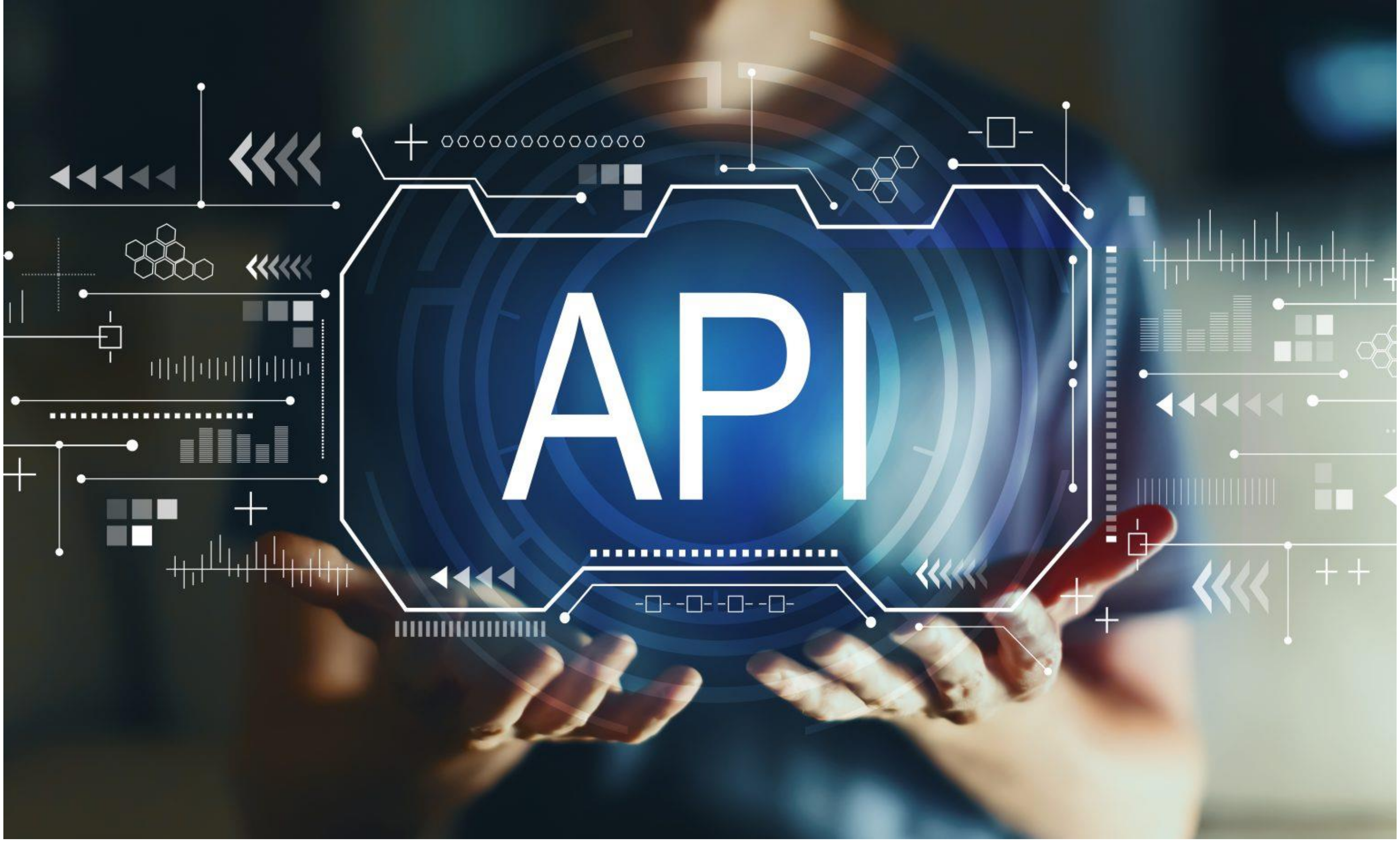
A new approach has emerged – leveraging privacy enhancing technologies (PETs). The term covers an array of technologies, including homomorphic encryption, which allows financial institutions to perform computations on encrypted data without ever decrypting. This means they can share and analyze sensitive data without revealing the underlying information.

The data itself remains decentralized so it does not move across parties. Homomorphic encryption also means the firm's customer relationship is never revealed and any answers cannot be attributed back to a specific financial institution, thereby preserving competition.

Mitigating risk will remain a top priority for financial institutions and PETs have emerged as valuable tools in organizations'' armories. Ultimately, these technologies are paving the way for firms to collaborate in new ways and finally unlock the value in their data – and this could prove to be a major game-changer in the fight against financial crime.

About the Author

Dr. Alon Kaufman, CEO and Co-Founder of Duality Technologies. has 20 years of experience in the hi-tech arena, commercializing data-science technologies, leading industrial research and corporate innovation teams. Prior to founding Duality, he served as RSA's global director of Data Science, Research and Innovation. In addition to his leadership experience, he is accomplished in the fields of artificial intelligence, machine learning and how they interplay with security and privacy, with over 30 approved US patents in these fields. He holds a PhD. in Computational Neuroscience and machine learning from the Hebrew University and an MBA from Tel Aviv University.Alon can be reached online at https://dualitytech.com



Why You Can't Have True Zero Trust Without API Security

By Richard Bird, Chief Security Officer, Traceable

Global adoption of Zero Trust security models is soaring and with good reason. Due to organizations' embrace of digital business models and enablement of hybrid workforces, more users and devices are accessing organizations' networks than ever before. A Cloud Security Alliance survey finds that 94 percent of organizations are implementing Zero Trust strategies, and 77 percent will increase their spending on Zero Trust over the next 12 months. President Biden's Executive Order on Cyber Security, issued in May 2021, has also given this security model a public boost. The order requires federal agencies to develop and implement Zero Trust architectures at pace.

The concept of Zero Trust was popularized by Forrester analyst John Kindervag in 2010. Organizations that embrace Zero Trust "never trust, always verify." That means continuously validating every user and device accept attempt and enforcing the principle of least privilege granted to right-size user privileges to the job at hand. As a result, Zero Trust has historically been focused on improving network access and identity access management security.

So far, so good. Yet, the reality is that distributed networks are growing exponentially. In addition, organizations are tilting from running monolithic business applications to using myriad microservices to create and deploy new applications. Organizations then use application programming interfaces (APIs) to connect clients to servers; send and receive sensitive data; and execute increasingly complex interdependent business processes.

While APIs are the foundation of modern business, they also are creating new risks. The fast rate of API adoption is outpacing organizations' ability to create strong governance and security tools around this layer. In addition, organizations are using APIs to connect to legacy applications that perform as expected but lack the security of cloud-native services and architectures.

Recognizing these trends, OWASP has published a top-10 API security risk list, that includes issues such as broken object-level authorization, broken user authorization, excessive data exposure, and more.

Gartner predicted that APIs will be the number-one attack vector in 2022. Breaches due to API security risks have already snared Coinbase, Optus, Uber, and others.

Zero Trust Must Secure the API Layer

So, it's clear that Zero Trust security models need to extend beyond the user and the device layer to include the application, data, and integration layers. Organizations can do so by tackling the problem of API security, and considering partners, vendors, customers, and other third parties in their Zero Trust frameworks.

To manage, control, and secure APIs, IT and security teams need to be able to:

1. **Discover and test APIs:** Teams want to automatically discover APIs and sensitive data flows. API security platforms that enable continuous discovery empower teams to track APIs as their environments change and create an always-up-to-date inventory of all of their APIs. As a result, it's easy for teams to identify shadow and orphaned APIs, as well as any changes.

2. **Evaluate API risk posture:** Risk scoring has transformed security and also applies to APIs. API security platforms provide a security risk score for every APIs. These risk scores consider runtime details, such as sensitive data flows, API call maps, usage behavior, threat details and activity levels, and other factors, to help teams focus on the areas of greatest risk. Teams are then able to identify which APIs are most vulnerable to abuse, so that they can prioritize remediation and take fast action to reduce threats.

3. **Stop API attacks:** API security platforms equip teams to detect and stop known and unknown API, business logic abuse, and zero-day attacks, as well as API abuse, fraud, and sensitive data exfiltration. Being able to identify where hackers have gained access to sensitive data enables IT and security teams to rapidly shut down these attempts, limiting their harm.

4. **Analyze APIs for threat hunting and research:** Organizations can improve threat hunting by using API security platforms to create an end-to-end path trace of all of their API calls and service behavior. This information can be aggregated in an API data lake that security operations teams, threat hunters, and forensic researchers can use to identify root causes, speed incident detection and resolution, and improve processes. With these insights, organizations can reduce their API attack surface over time.

There are myriad API security vendors that purport to offer these four capabilities, yet many struggle to deliver across one or more of these areas. These platforms may be unable to prevent bot or DDoS attacks, fail to detect changes in API behavior, lack the ability to analyze sensitive data flows, or have other limitations. As a result, IT and security teams seeking an API security partner should ask companies to benchmark their capabilities against others in the space.

It’s Time to Strengthen API Security

Zero Trust models have done much to shore up organizational security. But the time has come to extend Zero Trust to the API layer. APIs represent a significant – and growing vulnerability – for organizations that need to be immediately triaged.

Security platforms that provide API discovery and risk mitigation, attack blocking, and threat analytics enable organizations to monitor, track, and remediate APIs. While APIs create open endpoints, there’s no reason bad actors should be able to walk in through this front door.

About the Author

Richard Bird is the Chief Security Officer for Traceable.ai. A multi-time C-level executive in both the corporate and start-up worlds, Richard is internationally recognized for his expert insights, work and views on cybersecurity, data privacy, digital consumer rights and next generation security topics. Richard delivers keynote presentations around the world and is a highly sought-after speaker, particularly when he is translating cybersecurity and risk realities into business language and imperatives. He is a Senior Fellow with the CyberTheory Zero Trust Institute, a Forbes Tech council member and has been interviewed frequently by media outlets including the Wall Street Journal, CNBC, Bloomberg, The Financial Times, Business Insider, CNN, NBC Nightly News and TechRepublic. https://www.traceable.ai/

EVENTS

Organized by

CRAFTING DIALOGUE

2ND ME EDITION

DIGITAL TALENT ECOSYSTEM DIALOGUE

#DTECOSYSTEM

Organization of Future | Digital Talent & Skill Gap
Digital Experience | Future Workplace

2 - 3 FEBRUARY, 2023 | DUBAI, UAE

KEY FEATURED DISCUSSIONS

- Evolving role of CIO & CHRO in digital talent ecosystem
- Facilitating digital transformation with the right technology, talent & culture
- Aligning CX & EX for Organizational Success
- Data driven workplace & employee experience in the digital era
- Evaluating future of work for tech teams & long-term implications of a distributed work environment

KNOW MORE

Contact Info:

MILAN ROY

info@crafting-dialogue.com

ESTEEMED SPEAKERS

YAHYAH PANDOR
Chief Information & Digital Officer
Fine Hygienic Holding, UAE

SHUMON A ZAMAN
Chief Information and Digital Officer
Ali & Sons Holding LLC, UAE

HEIKE VERMOND
Chief People Officer
Kitopi, UAE

FRANCIS ARUL
Chief Information Officer
Alshaya Group, UAE

KELLY LUKER
Chief People Officer
Tabby, UAE

2ND ME EDITION

DIGITAL TALENT ECOSYSTEM DIALOGUE

#DTECOSYSTEM

Organized by

CRAFTING DIALOGUE

Organization of Future | Digital Talent & Skill Gap | Digital Experience | Future Workplace

2 - 3 FEBRUARY, 2023 | ADDRESS DUBAI MARINA, UAE

FRANCIS ARUL
Director Digital Technology
Alshaya Group, UAE

HEIKE VIRMOND
Chief People Officer
Kitopi, UAE

DR. GHALIB AL HOSNI
Chief People Officer
Omantel, Oman

YAHYAH PANDOR
Chief Information & Digital Officer
Fine Hygienic Holding, UAE

DR. EBRAHIM HASAN AL KHAJEH
Division Director- Human Capital, Program Manager, Member of the Strategic Transformation Committee
Abu Dhabi Customs, UAE

FATIMA ALLOGHANI
Emiratisation Director
Majid Al Futtaim, UAE

SHUMON A ZAMAN
Chief Information and Digital Officer
Ali & Sons Holding LLC, UAE

MOHAMED H. AMEEN
Head Talent Management
Roads and Transport Authority, Dubai, UAE

KELLY LUKER
Chief People Officer
Tabby, UAE

SAAIM ASLAM
Head of IT planning & Enterprise Architecture
Seera Group, UAE

HAZEM EL ZAYAT
Chief Experience Officer
Ogilvy, UAE

JAYAKUMAR MOHANACHANDRAN
Group Chief Information Officer
Easa Saleh Al Gurg Group, UAE

DEBRA TELES
Group Vice President People & Culture
Al Ghurair Investments, UAE

UMESH MOOLCHANDANI
Chief Information Officer
Bin Dasmal Group, UAE

FASYUDDIN ALI MOHAMMED
Group Chief Information Officer
Suhail Bahwan Group (Holding) LLC, Oman

IMAD GHAZZAWI
AVP People Experience
noon, KSA

CHITRANSHA MATHUR
Director of Strategic Planning and Transformation
Emirates Post, UAE

ASHIRVAD LOBO
Learning Expert & Co-Author
Full of Life
UAE

SHARON KOTUT
HR Head- UAE, Oman, Qatar
A.P. Moller - Maersk, UAE

WASSIM GHADBAN
Vice President, Global Innovation & Digital Engineering
Kent, UAE

ROHIT BHAGAT
Future of Work Facilitator
ADQ, UAE

RAISA GHAZI
Award-winning international Inclusive & Women's Leadership Coach

MANAL ALLAM
IT Head & Business Partner - Middle East
Merck Group, UAE

REGISTER

CONTACT INFO:

MILAN ROY | info@crafting-dialogue.com

CDI OPENING REMARKS
KEY TRENDS IN DEFENCE INTELLIGENCE
Lt General Sir Jim Hockenhull
Chief of Defence Intelligence UK MoD

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Collaborating and Cooperating for Greater Security

For Securing Critical Infrastructure and Safer Cities

Register Today

SPECIAL DEAL FOR INFRAGARD LA MEMBERS, GOVERNMENT AND OWNER/OPERATORS

For further details and to register visit www.ciprna-expo.com/registration

The latest Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from operator/owners, agencies, governments and industry to debate and collaborate on securing America's critical infrastructure.

As we come out of one of the most challenging times in recent history, it has stressed how important collaboration in protrection of critical infrastructure is for a country's national security.

Agenda includes Industry Sector Mini Symposiums to focus on your specific CI sector, with the enhanced opportunity to discover and share experiences across these sectors:

- Power & Energy Sector Symposium
- Transport Sector Symposium
- Communications Sector Symposium
- CBRNE Sector Symposium
- Critical Manufacturing & Logistics Sector Symposium
- Government, Defence & Space Sector Symposium

Join us in Baton Rouge, LA, USA for the premier event for operator/owners and government establishments tasked with the region's Critical Infrastructure Protection and Resilience.

Leading the debate for securing America's critical infrastructure

Opening Keynotes:

- Dr David Mussington, Assistant Director, CISA
- Clay Rives, MPA, LEM-P, Director, East Baton Rouge Mayor's Office of Homeland Security & Emergency Preparedness

Confirmed speakers include:

- Richard Tenney, Senior Advisor, Cyber, CISA Emergency Communications Division, CISA
- Vanessa Tibbits, Special Officer In Charge, FBI
- Jill Farria, Supervisory Transportation Security Inspector, TSA
- Dr Ashley Pennington, Chemical Engineer CISA
- Douglas DeLancey, Chief, Strategy Branch, Office for Bombing Prevention
- Lester Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Colleen Wright, Priority Telecommunications Area Representatives, CISA
- Leigh J. Blackburn, Ph.D., Senior IT Specialist, Program Manager for Secure Tomorrow Series, CISA
- Charles Burton, Technology Director, Calcasieu Parish Government
- Sunny Wescott, Lead Meteorologist - Extreme Weather Outreach, CISA
- Dawn Manga, Associate Director Priority Communications, CISA
- Ron Martin, Professor Of Practice, Critical Infrastructure, Capitol Technology University

For speaker line-up visit www.ciprna-expo.com

REGISTER ONLINE AT www.ciprna-expo.com/registration

DIGITAL REVOLUTION SUMMIT

8th - 9th MARCH 2023

THE EMPIRE BRUNEI

Leaders In *Powering A Digital - Age,* Interconnected World

30+ SPONSORS & **EXHIBITORS**

30+ **SPEAKERS** & PANELISTS

TECHNICAL **WORKSHOPS**

REAL-TIME **DATA CENTER**

INTERNATIONAL **CONFERENCE**

UNLIMITED ACCESS TO MEET THE **DECISION MAKERS**

UNLIMITED NETWORKING

PRIOR NOTIFICATION OF **ATTENDEES**

EVENT OVERVIEW

Brunei is currently undergoing a **major transformation** in the **Information** and Communications Technology (ICT) sector. The **Digital Economy Masterplan 2025 vision** is to become a **smart nation through digital transformation.** Hence in an **effort to support** the **government's vision** of a **smart nation Brunei,** we at TraiCon will be hosting The **"Digital Revolution Series"** scheduled on **March 2023** in Bandar Seri **Begawan, Brunei. Digital Revolution Series** is connecting the global **digital transformation** experts and **technology providers** with the CIO, CTO, CDO, CISO and Head of **IT under** one roof. This event is an international platform where **government authority,** policy makers, industry leaders & **solution providers** to gather and discuss the challenges, **technologies and initiatives** that are driving **digital transformation** in the **region.**

For More Opportunities

Eng. Prasanna | Tel: +91 77085 23918 | **Email:** prasanna@traiconevents.com

EXPERIENCE INNOVATIVE SOLUTIONS & GAME-CHANGING TECHNOLOGIES AT **#ITSLISBON2023**

its EUROPEAN CONGRESS

LISBON, PORTUGAL
22-24 MAY 2023

ITS: The Game Changer.

EXTENDED DEADLINE FOR CALL FOR CONTRIBUTIONS!

20 January 2023

Submit your proposals for the Technical Programme:

Download the Call for Contributions Brochure here.

www.itseuropeancongress.com/call-for-contributions/

ORGANISED BY ERTICO ITS EUROPE

HOSTED BY LISBOA ITS PORTUGAL

SUPPORTED BY Turismo de Lisboa TURISMO DE PORTUGAL

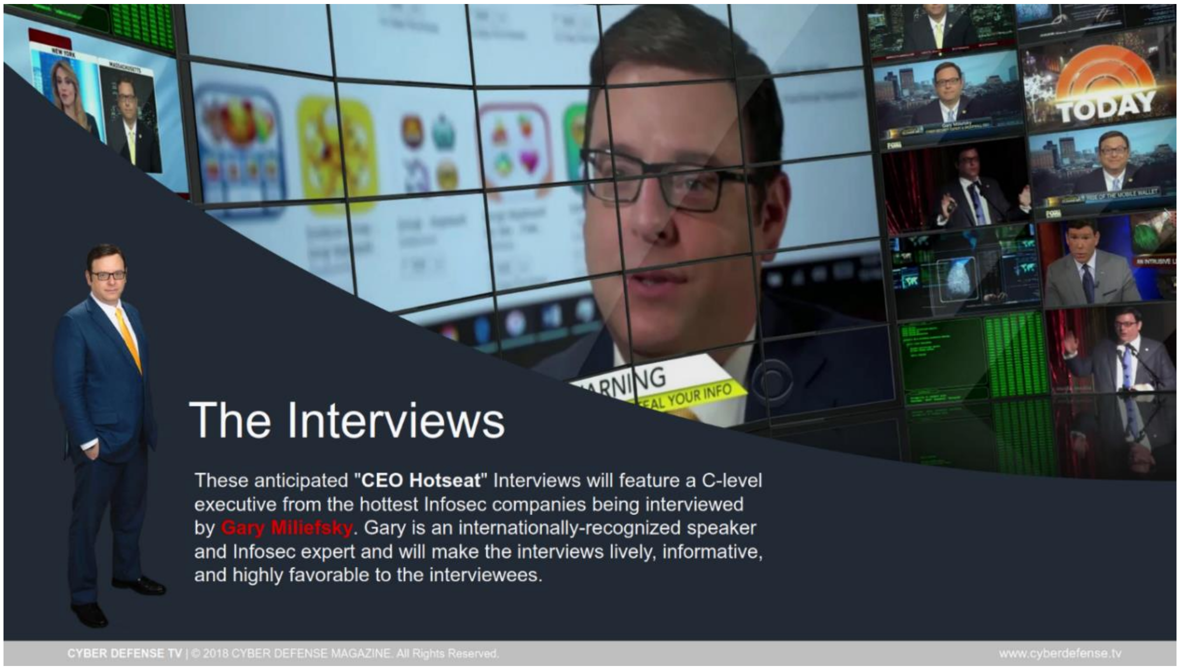
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



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

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

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

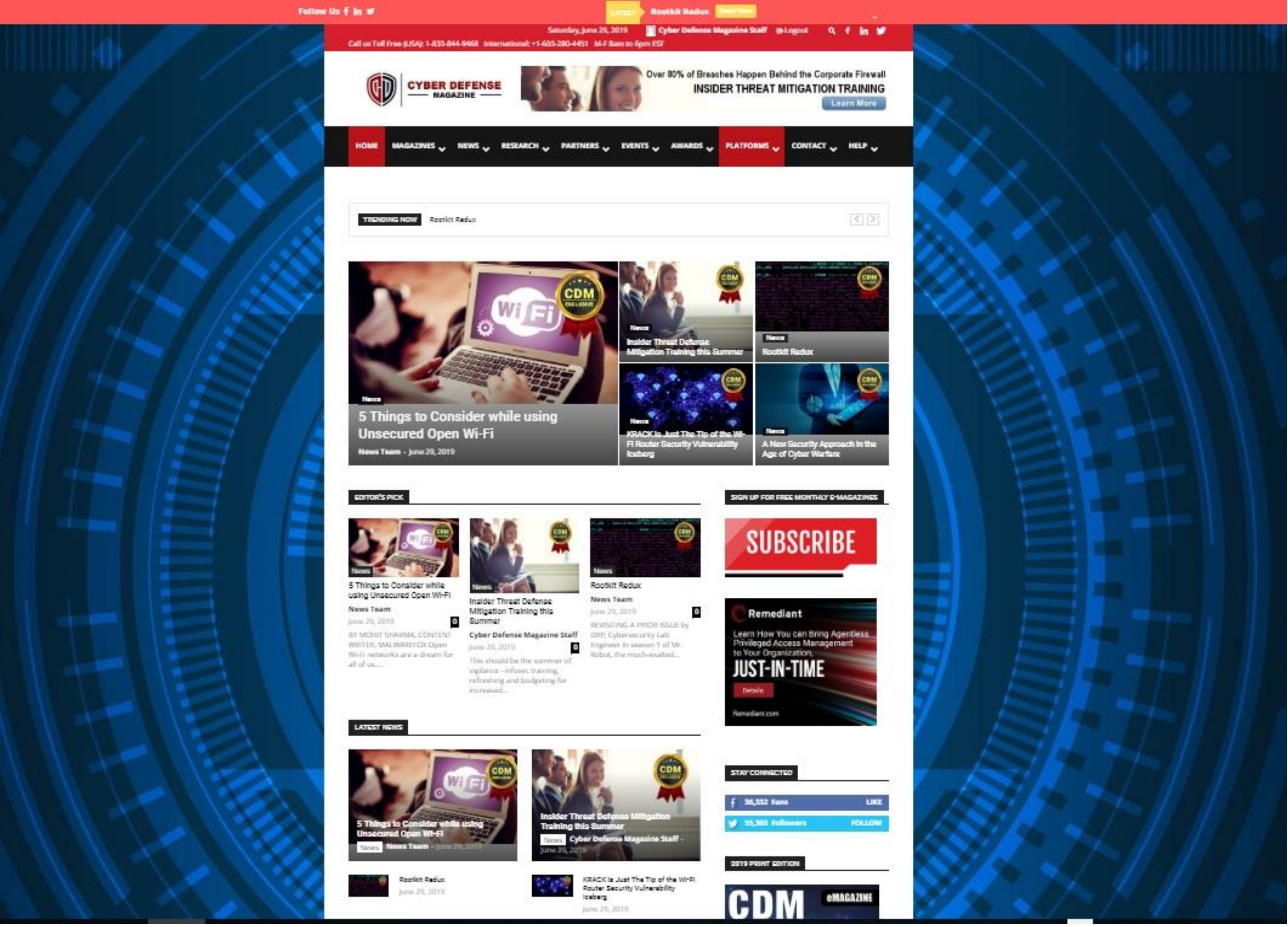
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 01/03/2023



Follow Us | LATEST | Rootkit Redux

Saturday, June 29, 2019 | Cyber Defense Magazine Staff | Logout

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

CYBER DEFENSE MAGAZINE

Over 80% of Breaches Happen Behind the Corporate Firewall
INSIDER THREAT MITIGATION TRAINING
Learn More

HOME | MAGAZINES | NEWS | RESEARCH | PARTNERS | EVENTS | AWARDS | PLATFORMS | CONTACT | HELP

TRENDING NOW Rootkit Redux

News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team – June 29, 2019

News
Insider Threat Defense Mitigation Training this Summer

News
Rootkit Redux

News
KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

News
A New Security Approach in the Age of Cyber Warfare

EDITOR'S PICK

News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team
June 29, 2019
0
BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

News
Insider Threat Defense Mitigation Training this Summer
Cyber Defense Magazine Staff
June 29, 2019
0
This should be the summer of vigilance – infosec training, refreshing and budgeting for increased...

News
Rootkit Redux
News Team
June 29, 2019
0
REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

SIGN UP FOR FREE MONTHLY E-MAGAZINES

SUBSCRIBE

Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization.
JUST-IN-TIME
Details
Remediant.com

LATEST NEWS

5 Things to Consider while using Unsecured Open Wi-Fi
News | News Team – June 29, 2019

Insider Threat Defense Mitigation Training this Summer
News | Cyber Defense Magazine Staff – June 29, 2019

Rootkit Redux
June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
June 29, 2019

STAY CONNECTED

f	36,332 Fans	LIKE
🐦	55,383 Followers	FOLLOW

2019 PRINT EDITION

Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

10 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com. ***Millions of monthly readers and new platforms coming…starting with www.cyberdefenseconferences.com this month…***

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

* with help from writers
and friends all over the Globe.