CYBER DEFENSE MAGAZINE

# eMAGAZINE

## IN THIS EDITION


*Security by Design: How to Protect the Future of Business*

*How To Grow Your Cyber Expertise During A Pandemic*

*Is What's Lurking in Your Network About to Come Out?*

*Cyber Security Market to Reach USD 400 Billion by 2026*

*...and much more...*


# AUGUST 2020

*MORE INSIDE!*

# CONTENTS


Welcome to CDM's August 2020 Issue ---------- 6

*Security by Design: How to Protect the Future of Business* ---------- *23*

By Jim Zuffoletti, CEO & co-founder of SafeGuard Cyber

*How To Grow Your Cyber Expertise During A Pandemic* ---------- *27*

By Bradley Hayes, Chief Technology Officer at Circadence

*Is What's Lurking in Your Network About to Come Out?* ---------- *30*

By Carolyn Crandall, Chief Deception Officer, Attivo Networks

*Cyber Security Market to Reach USD 400 Billion by 2026* ---------- *34*

By Saloni Walimbe, Content Writer at Global Market Insights, Inc.

*COVID-19 And Security Team Cuts Are Costing Businesses in Cyber and Financial Risks* ---------- *37*

By Samantha Humphries, security strategist, Exabeam

*Cybersecurity Challenges When Working from Home* ---------- *50*

By Renuka Sahane, Sr. Content Writer, Scalefusion

*Network Security Is Not Data Security* ---------- *54*

By Matt Cable, VP Solutions Architects & MD Europe, Certes Networks

*WireGuard - Separating Fact from Fiction* ---------- *57*

By Tomislav Čohar, co-founder, hide.me VPN

*Conducting Risk Prioritization and Remediation to Combat Challenges in The Distributed Workforce* ---------- *60*

By Egon Rinderer, Global Vice President of Technology and Federal CTO, Tanium

*Can We Better Leverage Our – Already Scarce – Cyber Security Human Resources?* ---------- *64*

By Douglas Ferguson, Founder & CTO, Pharos Security

*CERT Warns Bad Actors Are Targeting Remote Access – How Security Operations Find and Route These "Below the Radar" Attacks* ---------- *67*

By Saryu Nayyar, CEO, Gurucul

*4 Simple Ways to Repel Ransomware as The Rise in Remote Work Continues* ---------- *70*

**By Kris Lahiri, Co-founder and Chief Security Officer of Egnyte**

*Ransomware, Risk, And Recovery* ---------- *73*

**By Mickey Bresman, CEO, Semperis**

*Getting Employees Back to the New Normal* ---------- *77*

**By Brendan O'Connor, CEO and Co-founder, AppOmni**

*Security in The New Normal Requires an Agile Approach* ---------- *80*

**By Danny Presten, Chief Methodologist at Digital.ai**

*Why Are Fully Staffed Cybersecurity Teams Unable to Keep Up with Hacks?* ---------- *84*

**By Steve Salinas, Head of Product Marketing, Deep Instinct**

*Looks Like Russian Hackers Are on An Email Scam Spree* ---------- *88*

**By Tim Sadler, CEO, Tessian**

*TLS/ SSL Decryption – One of the Main Pillars of Zero Trust Model* ---------- *91*

**By Adil Baghir, Technology Consultant Lead, Middle East & Africa at A10 Networks**

*Build Your AI Incident Response Plan… Before It's Too Late* ---------- *94*

**By Patrick Hall* and Andrew Burt****

*Why Academic Openness and A Rise in Online Classes Should Invoke A Renewed Focus on Security* - *99*

**By Anthony Bettini, CTO, WhiteHat Security**

*Is API Usage Putting Your Organization Out of Compliance?* ---------- *102*

**By Matt Keil, Director of Product Marketing, Cequence Security**

*HIPAA Compliance and The Protection of Cyber Security* ---------- *105*

**By Andrew Mikhailov, CTO at Zfort Group**

*Smart Gadgets in Proving Workplace Violence* ---------- *109*

**By Milica D. Djekic**

*Cyber Against Granny* ---------- *116*

**By Yotam Gutman, SentinelOne**

*Are the Worst Cryptocurrency Security Breaches Behind Us?* ---------- *119*

**By Tim Fries, Co-Founder, The Tokenist**

@MILIEFSKY

## From the

# Publisher...

**New CyberDefenseMagazine.com website, plus updates at CyberDefenseTV.com & CyberDefenseRadio.com**

**Dear Friends,**

In the August issue of Cyber Defense Magazine, you will find both relevant and actionable intelligence from a broad spectrum of cyber experts. We at Cyber Defense Media Group are pleased to provide our readers and clients with up-to-date and cogent articles on which you can rely in fulfilling your own duties.


In my role as Publisher, I make it my daily responsibility to observe, digest, and select those topics of greatest value and interest to practitioners in the world of cybersecurity.

Today, we face a continuation and deepening of the effects of COVID-19 on nearly all enterprises which depend on cyberspace for their operations. The challenges of maintaining security continue to grow with our dependence on cyber-related systems of all kinds.

In the midst of increasing attacks on cyber systems across the board, we must keep an eye on the effects of "social distancing" and the prospect of re-opening in-person activities. Since these restrictions do not appear to be going away in the near future, it's imperative to concentrate on strengthening protections against cyber exploits. Sharing actionable intelligence is the first and best means of doing so.

In this spirit, we are pleased to continue providing the powerful combination of monthly eMagazines, daily updates and features on the Cyber Defense Magazine home page, and webinars featuring national and international experts on topics of immediate interest.

We've also launched our Black Unicorn Report for 2020 which you can download by visiting www.cyberdefenseawards.com. Please share in our enthusiasm and congratulations for all of the winners, as they help us get one step ahead of the next breach.

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*

**InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.**

# From the International Editor-in-Chief…

The word “quarantine” has been in use in one form or another for many centuries. In any search for its root, the Italian term *quarantena*, meaning "forty days" will appear. In its original concept, the period of 40 days was considered to be an adequate period for a disease to run its course and general health to return. Today, we are experiencing physical quarantine requirements for both national and other jurisdictional borders.

In contrast, there is no assurance that any such set period can provide a way to avoid cyber disruptions brought about by “viruses” or other criminal exploits. Both the private and government sectors must undertake immediate and ongoing actions to overcome these incursions.

As we observed last month, the international effects of COVID-19 include restrictions on physical travel, resulting in greater dependence on cyber “travel” to accomplish necessary business and government functions. As might be expected, this expanded reliance on cyber resources also provides greater opportunities for criminal activity. Only by concerted and cooperative efforts can we succeed in implementing an effective defense.

Accordingly, let me take this occasion to renew my suggestion that in the days ahead we agree to put our differences aside in favor of responding to our common enemies: the COVID-19 virus itself and those who would take advantage of this crisis to perpetrate criminal schemes.

**To our faithful readers, we thank you,**

Pierluigi Paganini

International Editor-in-Chief

**@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.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

US EDITOR-IN-CHIEF
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

http://www.cyberdefensemagazine.com



PUBLISHER

**Gary S. Miliefsky, CISSP®**

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

## 8 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**

**WEBINARS**

# Welcome to CDM's August 2020 Issue

## From the U.S. Editor-in-Chief

**There is no "new normal" – and there isn't going to be.**

Regardless of what you may read elsewhere about the "new normal," it's no more than wishful thinking or sales puffery. The very term **"normal"** implies stability, but the entire cyber system is in flux. As a *dynamic* rather than *static* phenomenon, the concept of "normal" is no longer appropriate in our world, and the sooner we all prepare to live with that fact, the better prepared we will all be to exercise effective cyber defenses.

The closest battle analogy to what we now face is "asymmetrical warfare." In short, that refers to the situation where the attackers and defenders play by two different sets of rules. In the cyber world, the attackers honor no rules at all. Moreover, the defenders have to repel 100% of the attacks to prevail, but the attackers only have to score occasionally.

In the case of malware and ransomware, the target organizations are proscribed from engaging in criminal activity, such as hunting down and destroying the criminals. We must rely on government action to find and punish them. But that doesn't mean we can't provide helpful information to law enforcement. At least they have remedies like seizing assets, confiscating accounts, and imprisonment.

In that perspective, we are pleased to present the August 2020 issue of Cyber Defense Magazine, with over two dozen articles on cyber and security topics of immediate interest. We continue to provide thoughtful articles from a broad spectrum of contributors who share their expertise and insights with our community.

Wishing you all success in your cyber security endeavors,

Yan Ross

US Editor-in-Chief
Cyber Defense Magazine

**About the US Editor-in-Chief**

Yan Ross, J.D., is a Cybersecurity Journalist & US Editor-in-Chief for 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 via his e-mail address at yan.ross@cyberdefensemediagroup.com


SPONSORS

cythereal

# Predictive Cyber Defense

**Lucio Frega, Threat Researcher**
Deutsche Telekom - Cyber Threat Intelligence

MALWARE

YARA

HUNT

PREDICT

cythereal.com

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

## About the Author/Disclosure

Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.

RSAConference | Where the world talks security

# CYBERSECURITY KNOWLEDGE. WHEN YOU NEED IT.

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

**rsaconference.com/cyberdefense-2020**

# Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

# SEAN DRAKE

U.S.ARMY

***"At Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "***


***Sean Drake***
***Managing Partner***
***Stony Lonesome Group LLC***
***203-247-2479***
***www.stonylonesomegroupllc.com***

# By the time an attacker tastes the difference, their presence is known.


"Attacker mistakes are made when they cannot distinguish real from fake."
Tony Cole, CTO Attivo Networks

## DECEPTION-BASED THREAT DETECTION

Detecting threats needs to be comprehensive, however it doesn't have to be complicated. Designed for simplicity, Attivo Networks brings uncertainty to the mind of the attacker, redirecting them away from the target assets and providing defenders with high-fidelity alerting that is backed with actionable attack and forensic data on malicious activity and insider policy violations.

Attivo NETWORKS®

Deceive. Detect. Defend.

Learn more at attivonetworks.com/ebook

# Setting the Standard

## in Cyber Defense Training & Education

Transform your cyber defense capabilities with customized training. Regent's Institute for Cybersecurity will help you develop your workforce credentials, manage your cyber risks and defend your assets.

**CORPORATE | GOVERNMENT | MILITARY | EDUCATION**

- Powerful Hyper-Realistic Range Simulation
- Industry Certifications
- Executive & Senior Leadership Cyber Workshops
- Associate, Bachelor's & Master's Programs


Regent's B.S. in Cybersecurity has received NSA and DHS designation.

**Learn More**

**regent.edu/cyber | 757.352.4590**

REGENT UNIVERSITY | Institute for Cybersecurity

# OneTrust

Privacy Management Software

# World's #1 Most Widely Used Privacy Management Software

## *For Privacy, Security & Third-Party Compliance*

Solutions to Comply with the CCPA, GDPR & Global Privacy Laws & Security Frameworks

### Privacy Program Management:

- **Maturity & Planning:** Compliance Reporting Scorecard
- **Program Benchmarking:** Comparison Against Peers
- **DataGuidance Research:** Regulatory Tracking Portal
- **Assessment Automation:** PIAs, DPIAs & Info Security

### Marketing & Privacy UX

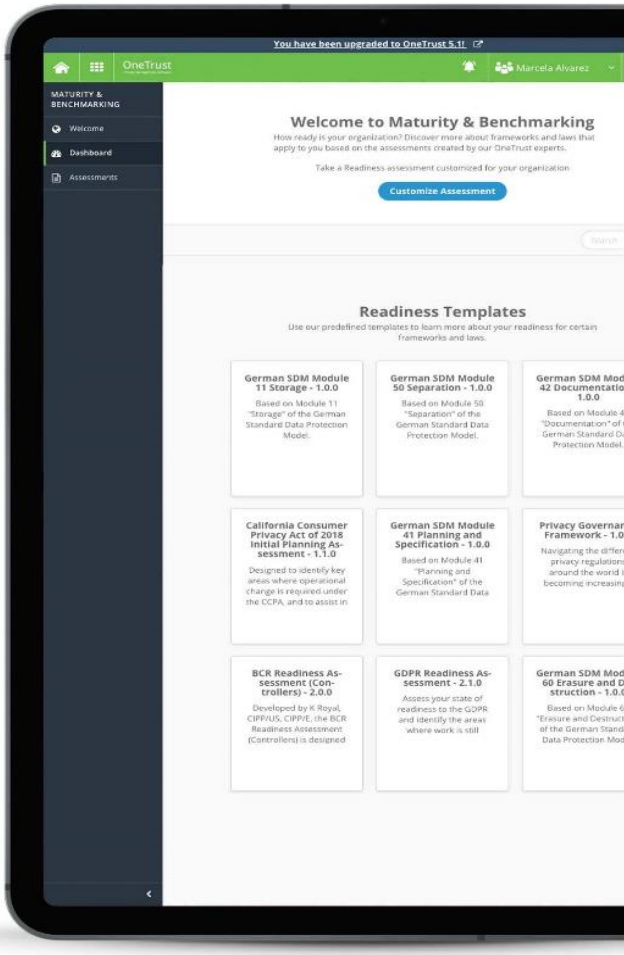
- **Cookie Compliance:** Website Scanning & Consent
- **Mobile App Compliance:** App Scanning & Consent
- **Universal Consent:** Consent Receipts & Analytics
- **Preference Management:** End User Preference Center
- **Consumer & Subject Requests:** Intake to Fulfillment
- **Policy & Notice:** Centrally Host, Track & Update

### Third-Party Risk Management

- **Vendorpedia Management:** Assessment & Lifecycle
- **Vendorpedia Risk Exchange:** Security & Privacy Risks
- **Vendorpedia Contracts:** Contract Scanning & Analytics
- **Vendorpedia Monitoring:** Privacy & Security Threats
- **Vendor Chasing Services:** Managed Chasing Services

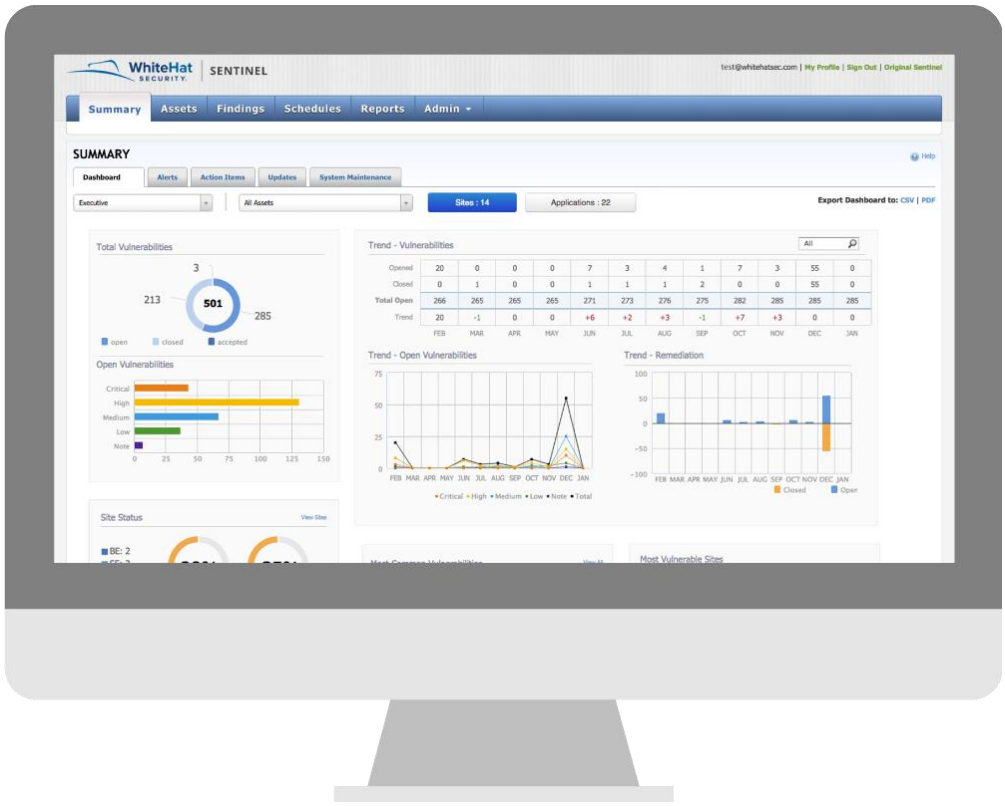
### Incident & Breach Response

- **Incident & Breach Response:** Intake & Lifecycle Management
- **DatabreachPedia Guidance:** Built-in guidance from 300 laws




**GET STARTED TODAY | ONETRUST.COM/FREE-EDITION**

LEARN MORE ABOUT ONETRUST | REQUEST A DEMO | ONETRUST.COM




***Your website could be vulnerable to outside attacks.*** Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With this trial you will get:

An evaluation of the security of one of your organization's websites

Application security guidance from security engineers in WhiteHat's Threat Research Center

Full access to Sentinel's web-based interface, offering the ability to review and generate reports as well as share findings with internal developers and security management

A customized review and complimentary final executive and technical report

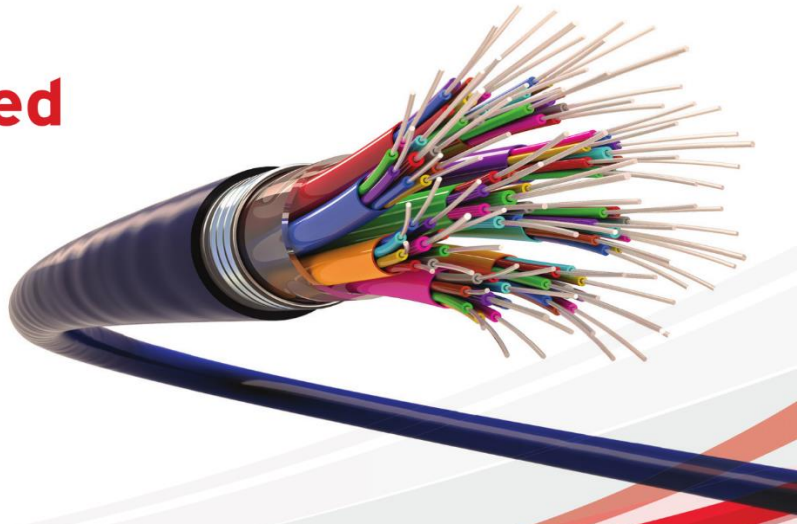
Click here to sign up at this URL: https://www.whitehatsec.com/info/security-check/

***PLEASE NOTE: Trial participation is subject to qualification.***

TREND MICRO™

POWERED BY XGen™ SECURITY

# Detect and prevent breaches at wire speed



Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.

NSS LABS RECOMMENDED

## Proven capability

Trend Micro TippingPoint:
"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:
"Recommended" Breach Detection System 4 years in a row and 100% detection rate

## Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

Please get in touch:
Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber


# Now More Than Ever, You Need To Be Connecting With

Customers

Influencers

Media

**At Vrge Strategies,** we've been making connections that businesses build around for more than a decade.

Cybersecurity companies (from VC-funded startups to the Fortune 500) and global nonprofits count on us every day to deliver results that lead, influence, as well as spark conversations and new business.

Isn't it time you maximized the value of your **strategic communications?**

## Come talk to us, we'd love to connect.

Email Adam Benson
adam@vrge.us
or visit us at
www.vrge.us/cybersecurity

vrge

Navigate the Politics of Disruption

# Database Cyber Security Guard

**Don't be the next data breach. Equifax paid $575 million, British Airways $230 million and Marriott $124 million in fines.**

**Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.**

## Product Features

- **Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.**
- **Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.**
- **View all suspicious database activity and attempted data theft.**
- **Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.**

## Get a FREE COPY now.

www.DontBeBreached.com/Free

NIGHTDRAGON

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

*-David DeWalt*

*Managing Director and Founder NightDragon Security*

## ADVISE

*WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS*

## INVEST

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

## ACCELERATE

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

**www.nightdragon.com**

IronNet

# Two Years Later

## NotPetya's Game-Changing Lessons for Cybersecurity and Collective Defense

In early Summer 2017, the highly destructive NotPetya malware appeared and spread with devastating efficiency across data systems and architectures worldwide. The attack not only shattered records for speed and destruction, but also served as a wake up call for security professionals to up their game on cyberdefense. Here are key lessons learned from NotPetya, and how those lessons continue to shape today's leading practices in cybersecurity.

**LESSON 1**

### Malware is increasingly designed to disrupt business operations in the physical world.

NOTPETYA CREATED AN UNPRECEDENTED

**$10 billion**

IN DAMAGE WORLDWIDE[1]

**How NotPetya changed the game** — Unlike ransomware and other profit-driven attacks, NotPetya was built simply to destroy.

**How the cybersecurity industry is adapting** — NotPetya has taught today's security teams to assume destruction is a potential goal, appreciate the elevated risk and then act accordingly.

**LESSON 2**

### NotPetya raised the speed limit for modern cyber attacks.

NOTPETYA SPREAD TO MORE THAN

**64 countries**

IN JUST THE FIRST

**24 hours**[2]

**How NotPetya changed the game** — NotPetya was built for speed, with code designed to proliferate automatically, rapidly and indiscriminately.

**How the cybersecurity industry is adapting** — Cyberdefenses today should ideally use near-real time network traffic analysis and behavioral analytics to rapidly catch new forms of attacks that perpetually outdated signature-based systems would miss.

LESSON 3

## The worst attacks take lateral movement to the extreme — across all organizational and industry barriers.

THE FAR-FLUNG INDUSTRIES AFFECTED BY NOTPETYA INCLUDE

shipping, pharmaceuticals, banking, advertising, energy

AND OTHER MAJOR SECTORS [3]

**How NotPetya changed the game** — NotPetya's spread was not only fast, but also far and wide — with cross-sector damage at major organizations like Maersk, FedEx and others. NotPetya was also patch-resistant, vacuuming up credentials on infected targets for use later as workarounds on protected servers.

**How the cybersecurity industry is adapting** — Companies must assume the when, not if, mindset to penetration and lateral movement, and embrace collective defense and threat information sharing — across entire industries and even between many different sectors.

LESSON 4

## NotPetya shows the limits of attribution.

CYBERATTACK ATTRIBUTION IS GETTING MORE COMPLEX, WITH AT LEAST

10 variations

OF NATION-STATE RESPONSIBILITY [6]

**How NotPetya changed the game** — While Russia is generally blamed for NotPetya,[4] the attribution is less critical, given the indiscriminate nature of the attack and increased "collective offense" between criminal groups and nation-states sharing tactics and targets.[5]

**How the cybersecurity industry is adapting** — Security teams must meet threat actor's collective offense approach with collective defense — working with peers to share threat information and identified attack techniques.

1 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
2 https://www.securityweek.com/petyanotpetya-what-we-know-first-24-hours
3 https://www.securityweek.com/notpetya-attack-costs-big-companies-millions
4 https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/
5 https://ironnet.com/white-paper-survey-download/
6 https://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF


ARTICLES

# Security by Design: How to Protect the Future of Business

By Jim Zuffoletti, CEO & co-founder of SafeGuard Cyber

Estimates suggest that by 2021, cybercrime will cost the world $6 trillion every year. This will constitute "the greatest transfer of economic wealth in history," making cybercrime "more profitable than the global trade of all major illegal drugs combined."

Too many enterprises fail to protect themselves adequately because most of them are approaching cybersecurity in the wrong way. They are recapitulating Web 1.0 models of information security, in which security is applied as an afterthought, bolted on to a process or technology solution.

This approach is inadequate. Modern forms of digital risk are too sophisticated and too dangerous. Instead, to simultaneously drive business growth and properly protect themselves, forward-looking enterprises need to implement a Security by Design approach. This approach enables companies to build comprehensive security into the foundations of all enterprise teams, processes, and behavior – empowering organizations to embrace new digital tools with peace of mind.

## Security by Design: Trading the Reactive for the Proactive

The security perimeter is gone. Today, every aspect of the business is tied to cloud SaaS applications and mobile chat apps that live outside the traditional perimeter. Marketing makes constant use of social media apps; customer data is stored in a cloud-based CRM; internal communications are conducted over collaboration platforms like Microsoft Teams; sales teams might even leverage WhatsApp and WeChat to talk to prospects. An enterprise's daily operations are conducted in the cloud, and more importantly, that's where data resides, too. Business communications contain customer data, IP, and more.

With a Security by Design approach, you react to this reality by constructing a flexible network perimeter around every end user. You depart from the 64% of businesses who don't include the security team in discussions of technology-enabled business initiatives. Instead, you start with understanding what tools are needed by all the people within the enterprise, and then you apply security to all of those tools – at the end user level. You create a tech stack and a set of practices that mean security is woven through every part of the business.

Traditional security tools are not built to deal with a post-perimeter, multi-channel security landscape. Because of this, they can only offer a reactive security stance. Events like these become commonplace:

- **Information security** finds out that an employee opened a malicious link sent over LinkedIn, and malware has transited from their home computer over the VPN. They rush to try and repair the damage.
- **HR** finds out that a group of employees is bullying another employee over Slack, and has to go and investigate – weeks after the issue started.
- **Marketing** suddenly finds themselves locked out of the company Instagram, and only then do they try to roll out an account takeover response plan.
- A **sales** rep discovers a fake website that has been up and running for months, and belatedly begins the long process of trying to get the website taken down.
- A **compliance** office discovers that a rep has been having a noncompliant conversation with a prospect, and can only try and correct the behavior after the fact.

Everything is reactivity. However, if you are only trying to deal with incidents once they have already occurred, you are setting yourself up for controlled failure. Eventually, one of these incidents will be serious: a ransomware attack, IP theft, or something else that can seriously hamper growth.

By contrast, a Security by Design framework establishes protection from digital risks *prior* to their emergence as a threat.

## Security by Design = Growth by Design

The real beauty of Security by Design is that the approach can have a material business impact. A bad ransomware attack, or IP theft, can be devastating, and seriously hamper ambitions of growth. To be productive, reach customers, and stay competitive, businesses need to embrace social media, collaboration apps, and messaging apps. But without the right protections, in embracing these cloud channels, they are rolling the dice on the integrity of their enterprise. Their digital transformation is risky, and contains blind spots.

However, once security is built into an enterprise's approach, new tools and platforms are secure from the start. This immediately creates secondary business benefits. When you are proactively monitoring your cloud channels, entire new datasets are generated. These can then be piped via an API into a business insights engine. Compliance issues can be monitored in real time, at scale, across various languages.

Security by Design is an approach that powers business goals. Security teams have become accustomed to being seen as the department that wants to put the brakes on sales and marketing's embrace of new tools – but with this approach, they can do the opposite. They can greenlight new tools, and work with growth teams to optimize the output of those tools so that they become a part of the revenue engine.

One layer down, the business benefits of Security by Design compound again. Alongside staff members, consumers also value security. Individuals are tired of data breaches, and solemn promises by enterprises to do better next time. As Ernst & Young put it, "when data confidentiality, integrity or availability are compromised, or products and services cease to perform as expected, trust built over years can be lost in a day."

Being able to present yourself as a company that is prioritizing security in active and innovative ways is a major competitive advantage. By moving toward a proactive security model, you both better protect your company and your employees from attacks – *and* better satisfy customers.

Let's revisit how a Security by Design approach changes the business examples cited above. When you trade a security as bolt-on approach for a Security by Design approach, you move from a reactive stance to a proactive stance:

- **Information security** procures technology to enable employees to use LinkedIn. The technology immediately detects any malicious links, flags the posts and intercepts the content – before anything malicious can be clicked on.

- **HR** procures technology to protect the company's expanded Slack environment. Inappropriate conduct is immediately flagged, and HR can intervene early and stop the problem from worsening.

- **Marketing** and security defined the roles and responsibilities for social media and fake accounts. Using a cross-function approach, **Marketing** detects an account takeover, and immediately retakes control. They alert security to the incident.

- **Sales** can work with marketing and security to initiate a takedown of any fake account. Such accounts are detected by technology that actively crawls the internet (both surface and dark) around the clock.

- A **compliance** officer is notified that a message sent by a rep might contain an issue, because compliance and sales have agreed on what channels need monitoring. The message has been quarantined so it can be checked before it is allowed to be sent.

## The Future of Security is by Design

A Security by Design framework enables enterprises to properly protect themselves, and move from a reactive stance, where a crisis is always around the corner, to a proactive stance. Security by Design is the only sensible approach in an era where so many business-critical tools live outside the traditional perimeter, and modern digital risks are so numerous, complex, and sophisticated.

Security by Design is also the only sensible approach for enterprises that want to do everything they can do to drive growth. When a Security by Design framework is properly implemented, security becomes a driver of business success. Executives and board members can view digital security as achieving a positive goal that helps drive business growth. Security becomes synonymous with revenue. When properly safeguarding the organization is understood as simple financial prudence, including security at the inception of a product or service becomes an obvious best practice. This view of security is the future.

### About the Author

Jim Zuffoletti has been a founder of start-up organizations as both an entrepreneur and an intrapreneur for the past twenty-five years. Jim is CEO and co-founder of SafeGuard Cyber, a digital risk protection company securing brands, VIPs, and team members in the new world of social media and digital communications. Jim was previously CEO and President of OpenQ which enabled pharmaceutical, biotech, and medical device companies to discover, regulate, and leverage the social networks forged with outside influencers and researchers. Jim Zuffoletti can be reached at our company website at www.safeguardcyber.com.

# How To Grow Your Cyber Expertise During A Pandemic

By Bradley Hayes, Chief Technology Officer at Circadence

IT pros can still learn new skills despite perceived barriers to progressing professionally during the pandemic. While work circumstances and environmental factors have changed in our world and most people are working and learning remote, a professional's ability to learn is the one thing we can be certain about right now. And, let's face it, now it's more important than ever for cyber pros to be up-to-date on cybersecurity skills since so many people are encountering increasing amounts of cyber risks *while* working remote. Even with the shift to remote work, IT pros can stay connected to the industry and continue advancing their skills with professional IT/cyber groups, online trainings, cyber games and more. Here are a few ways cyber professionals and cyber newcomers can continue to grow their career and expertise during this pandemic.

## Build cyber skills with hands-on, online training

It's more vital than ever for cyber professionals to get the training they need to learn about new threats and protect company assets. From safeguarding a remote workforce to protecting sensitive online data, cyber professionals have a lot to do, but need to be highly trained to know ***how*** to do it. Distance learning

has been a massive shift for many students, and even for those who are 'students of the business' learning and training virtually certainly requires a different mindset. Luckily, new emerging training platforms are making it easy and fun for cyber professionals to learn new skills from anywhere at a pace that works for them. Circadence's Project Ares gamified training platform allows learners to build skills via engaging and personalized hands-on methods. Using gamification and intelligent tutoring AI, learners participate in a realistic, interactive curriculum of foundational and specialized scenarios in the form of *battle rooms* and *missions*, addressing real, current cyber threats across multiple industries, providing a comprehensive level of knowledge and practical experience. In a gamified cyber learning environment, cyber professionals are:

- ✓ **rewarded** for completing tasks and objectives
- ✓ **incentivized** to learn new skills persistently
- ✓ **encouraged** to dialogue and learn together with peers
- ✓ **reminded** of what they don't yet know and held accountable
- ✓ **engaged** in their progress through scores and leaderboards

Gamified training is not only a viable solution that will impact today's defenders, but it will truly change how cyber professionals learn and intellectualize a new skill.

## Network with cyber experts online

Cyber professionals are in high demand right now. According to a report from cybersecurity nonprofit $(ISC)^2$ there are currently about 2.8 million cybersecurity professionals around the world, but that workforce would need to grow by roughly 145% to meet the global demand for digital security expertise. Since cyber careers are in high demand, it's important for cyber professionals to network and put themselves out there…*online*. A few ways professionals can use digital connection to learn are:

- ✓ Follow and engage with cyber companies on social media (i.e.; Twitter, Linkedin, Facebook)
- ✓ Track topical hashtags like #cybertraining #cybersecurity #blackhat
- ✓ Join cyber professional groups on LinkedIn
- ✓ Participate in virtual conferences or online meet-ups such as the DC Cybersecurity Professionals or Bay Area Cybersecurity Meet-up

Another way to show off skills and knowledge is with a platform like Project Ares, which maintains leaderboards and badges of accomplishments. This is a great way to attract a potential employer by demonstrating skills and expertise.

## Connect with formal cyber organizations

There are also organizations that offer online networking events and educational webinars. For example, NICE/NIST and ISSA are highly reputable outlets to get connected on additional resources and cyber education. Many companies also offer live and on-demand webinars on current trending cyber topics. Here are a few as an example: Kickstarting a Cyber Career and Learning Happens Better with Games.

Cyber competitions and hackathons are also great ways to connect. Cyber competitions expose contestants to a real-life cyber-attack or threat, making them think quick under tight deadlines to defend against it and protect their team's assets. This is a great way for a cyber professional or newcomer to practice one's skillset, engage with others in the community, and engage in some friendly competition! Cyber competitions positively impact a cyber professional or cyber newcomer's experience to the industry by supporting new emerging technologies, engaging in environments for learners to demonstrate their abilities, and providing an opportunity for recruitment.

## Gain real-world experience during the pandemic

Since there is such a strong need for cyber professionals right now, another way to advance your career or get noticed would be to offer up your expertise via a service to inspect a company's remote workforce to ensure they are taking basic safety precautions during the pandemic. Since many companies do not have adequate cybersecurity support, your cyber intelligence and service might be simultaneously beneficial to a company in need and lead to a potential job or continued contract work with that company. More than likely, if you have a skill set in cyber, there is someone out there that needs your help.

In times like these it can be easy to forget the importance of growing and advancing a career. Dramatic changes to how we work make it even more important to continue to train and learn to be that much more prepared for potential cyber threats. It's important for all of us to continue to take part in being cyber-safe personally and professionally, but also to do our part in keeping the companies we work for and the broader economy safe from the increasing prevalence of costly cyber-attacks.

### About the Author

**Bradley Hayes, Chief Technology Officer at Circadence**

With decades of professional experience, Dr. Hayes' expertise in Artificial Intelligence and Machine Learning supports continual innovation for Circadence's cyber readiness solutions Hayes teachers as a professor at the University of Colorado's Department of Computer Science and serves as the Director of the Collaborative AI and Robotics (CAIRO) Lab. He has in-depth experience developing techniques to build autonomous AI that can learn from and collaborate with humans, making people more efficient and capable during task execution.

# Is What's Lurking in Your Network About to Come Out?

*The COVID-19 crisis was an unprecedented opportunity for attackers. Now, many may be ready to strike.*

By Carolyn Crandall, Chief Deception Officer, Attivo Networks

The COVID-19 pandemic has forced countless millions of people to work remotely, and the rush to enable that remote work created opportunities for attackers to infiltrate corporate networks due to new devices, unmanaged endpoints, security gaps, and other issues. Now that the initial adjustment period is over, some businesses believe that the imminent danger has passed because they have yet to experience an attack. Unfortunately, this may not be the case. There is reason to believe that attackers may be hiding under the surface, lurking in corporate networks, and preparing to emerge and do damage. We will likely soon see new attacks as attackers begin to make their demands known.

## Why Now?

Recent studies show that dwell time—the period that attackers spend inside the network before detection—is now just under 60 days for incidents discovered externally, though this can expand into months or even years for more advanced attacks. As the COVID-19 lockdown pushes past its third month,

that 60-day threshold has begun to pass. Attackers who have been biding their time may soon be ready to strike.

Today's ransomware attackers don't operate like they used to. While older ransomware attacks tended to be "smash and grab" operations stealing and encrypting any data they could, human-operated Ransomware 2.0 involves attackers spreading throughout the network to identify and target the most valuable information for the highest financial gain. For the largest possible payout, attackers want to take down a whole organization, not just one machine. Quickly spreading throughout the network to establish a stronger foothold is the smartest move, and given that the average ransomware payout was over $111,000 in Q1 2020 (up 33% from the previous quarter), the strategy appears to be working.

## The COVID-19 Lockdown Has Created New Opportunities

The extensive remote work necessitated by COVID-19 has, unfortunately, exacerbated the issue. Most businesses simply were not prepared for this volume of employees working from home, and the sudden onset of the crisis meant that they had to make security compromises in the spirit of achieving service availability. Naturally, both technology-based and human-based security issues have arisen as a result.

Network endpoints are more exposed, as employees access the network from the outside rather than from within. Employees are pulling data out of the company that may never have been off-premises before, creating opportunities for attackers to target less secure machines. Similarly, attackers are entering the network via split-tunneling VPNs, which separates personal employee traffic from company networks but doesn't have all the traditional security controls needed to protect the remote systems from attacks. Multi-factor authentication can help verify identity as employees work remotely, but some organizations still do not mandate its use, and it is not always effective against targeted attacks.

Phishing and other scams have also noticeably increased during the lockdown, preying on employees that are distracted or flustered by the sudden shift in routine, underscoring the fact that organizations have less control over employees working remotely. The number of BYOD devices (laptops, routers, access points, etc.) on the network has increased, and it is harder to verify that employees are doing things like installing security updates promptly, creating potential vulnerabilities. Even employee turnover can create openings for attackers, as it can be harder to verify the full removal of stored credentials and other attack paths from all applications and systems. Given that misused or stolen credentials continue to be at the center of countless breaches, this poses a significant threat.

There are tools designed to help protect against these new threats, but they require effective security controls at multiple levels of the network. Traditional Endpoint Protection Platforms (EPPs) and Endpoint Detection and Response (EDR) tools try to stop attacks at the initial compromise of the system. Still, given the potential new vulnerabilities created by extensive remote work, attackers may have an easier time bypassing those tools during the current crisis, highlighting the importance of overlapping security controls and building in a safety net to boost detection capabilities.

## Assessing and Addressing These New Risks

A balance of security controls is necessary for initial compromise, lateral movement, privilege escalation, and data loss prevention. If the attackers have already evaded EPP and EDR tools and compromised an internal system, technology like cyber deception plays a valuable role in detecting lateral movement and protecting applications from unauthorized access. Additionally, data loss prevention capabilities can stop employees (or attackers) from saving sensitive information to personal devices.

Improving lateral movement detection is vital. After the initial compromise of a network, there is a dark period of lateral movement and privilege escalation before the data protection tools detect anything. This lack of visibility means that there is no detection mechanism present until the tail end of the attack, which may be too late. Most security controls will also have challenges pinpointing attack path vulnerabilities, and tactics, techniques, and procedures (TTPs). Unless the organization has a mechanism to record an attacker's activity during a live attack (like a decoy or engagement environment), it can be difficult for security teams to understand the attack methods, their objectives, and how broad of a footprint the attacker has established.

To this end, it is vital to have visibility into attack paths to essential assets and network activity that includes seeing devices coming on or off the network, and can they find shadow admin accounts? This sort of credential tracking is more important than ever and having the correct tools in place can stop the execution of a successful breach. Decoys can also record and replay attacks for a better correlation of attack activities and gathering company-specific threat intelligence.

The spike in remote employees underscores the need to boost VPN security, as new traffic patterns amid remote work have shattered traditional activity baselines and made suspicious behavior harder to identify. This need also applies to cloud security as well, since much of the remote work uses PaaS, SaaS, and IaaS accounts to collaborate between sites. Decoys systems and accounts can also identify unauthorized attempts to gain credential or administrative access to the VPN network segment or cloud service, giving organizations visibility into suspicious activity in those areas.

Active Directory is also a prime target, and the ability to track unauthorized AD queries from endpoints is critical. Attackers target AD because it contains all the information, objects, and accounts they need to compromise an enterprise network, and such activity is difficult to detect. Detection capabilities that alert on unauthorized queries and misinform attackers can be instrumental in derailing this form of attack.

## Layered Defenses Secure the Present and the Future

To invoke a sports analogy, you can't spike the football before you get to the end zone. There remains a legitimate likelihood that attackers are actively lurking in networks. The situation underscores the importance of layered defenses that forces attackers to jump as many hurdles as possible to conduct their attacks. Attackers have taken advantage of the unfamiliar remote working situation to enter corporate networks, so it is vital to have protections in place to detect their lateral movement within those networks and stop them before harm can be done.

**About the Author**

Carolyn holds the roles of Chief Deception Officer and CMO at Attivo Networks. She is a high-impact technology executive with over 30 years of experience in building new markets and successful enterprise infrastructure companies. She has a demonstrated track record of effectively taking companies from pre-IPO through to multi-billion-dollar sales and has held leadership positions at Cisco, Juniper Networks, Nimble Storage, Riverbed, and Seagate. Carolyn is recognized as a global thought leader in technology trends and for building strategies that connect technology with customers to solve difficult operations, digitalization, and security challenges. Her current focus is on breach risk mitigation by teaching organizations how to shift from a prevention-based cybersecurity infrastructure to one of an active security defense based on the adoption of deception technology.


# Cyber Security Market to Reach USD 400 Billion by 2026

*Cyber security market will be driven by rising demand for cyber protection as well as advanced network infrastructure security across enterprises.*

By Saloni Walimbe, Content Writer at Global Market Insights, Inc.

According to Global Market Insights, Cyber Security Market is expected to exceed USD 400 billion by 2026. The rising demand for cyber protection as well as advanced network infrastructure security across enterprises is set to drive cyber security market in the forthcoming timeframe.

Furthermore, rising internet penetration and technological advancement are leading the enterprises to move to cloud-based business models. The established enterprises are investing majorly in cyber security solutions since widespread digitization throughout enterprises is prone to information breach and cyber threats.

The organizations are also establishing infrastructure and network security solutions which includes internet protocols and firewalls. This further allows them to prevent possible monetary as well as non-monetary losses like data storage devices and interconnected servers.

The demand for products related to infrastructure protection is anticipated to grow substantially through 2020-2026. Several organizations are adopting the BYOD work practice at a larger level in order to boost the business productivity and to provide flexibility to the employees. They are also adopting endpoint protection in order to stop any unauthenticated access and vulnerabilities to enterprise data resources by mobile devices. Subsequently, owing to huge penetration of cloud services, enterprises are further adopting cloud security solutions.

Since the cloud business infrastructure is vulnerable to cyber risks, cloud security solutions allows the company to maintain efficient network operations by following set rules. They tend to manage the total network security and also prevents unauthenticated alterations over network.

The adoption of cybersecurity solutions across SMEs is likely to grow over 15% CAGR through 2020-2026. The increasing number of cyber-attacks over small & medium enterprises along with rising monetary losses have further led to increasing adoption of cutting-edge security solutions.

Furthermore, these enterprises have also embraced the BYOD guidelines to lessen the capital expenditure as well as enhance the productivities of employees. They are also making substantial investments in advanced security solution in order to secure their data, majorly because they are prone to data breaches and cyber threats.

Cybersecurity products & services demand is increasing in the IT and Telecommunication organizations owing to the demand for protecting of personal sensitive data. The companies are adopting security solutions in efforts to protect their virtual information systems, servers, and data centers. This further helps them to alleviate cyber risks and also sense vulnerabilities at an early stage, thereby protecting from live attacks. In addition to this, the introduction of strict regulations from government authorities is impelling the cyber security market growth.

The Europe cyber security market is likely to grow at a CAGR of over 15% by the end of the forecast timespan. Several enterprises functioning in banking sectors are increasingly adopting technologically advanced cybersecurity solutions. The private corporates and government enterprises have registered increasing number of cyberattacks. Additionally, private corporates and government authorities are also making collective efforts to stop such vulnerabilities.

Citing an instance, European Central Bank collaborated with the members of Euro Cyber Resilience Board. The two together introduced the Cyber Information and Intelligence Sharing initiative, which focuses on detecting and preventing cyberattacks as well as enhancing the cybersecurity throughout financial institutions.

The competitive landscape of the global cyber security market is inclusive of players such as Google LLC, Nokia Networks, Oracle Corporation, IBM Corporation, Microsoft Corporation, Amazon Web Services, and others.

Source: - https://www.gminsights.com/pressrelease/cyber-security-market

**About the Author**

**Saloni Walimbe,**An avid reader since childhood, Saloni is currently following her passion for content creation by penning down insightful articles relating to global industry trends, business, and trade & finance. With an MBA-Marketing qualification under her belt, she has spent two years as a content writer in the advertising field. Aside from her professional work, she is an ardent animal lover and enjoys movies, music and books in her spare time.

Company Website: - https://www.gminsights.com/

**Author Social Media URLs-** 1) LinkedIn - https://www.linkedin.com/in/saloni-walimbe-5929b99b/

2) Twitter - https://twitter.com/WalimbeSaloni

# COVID-19 And Security Team Cuts Are Costing Businesses in Cyber and Financial Risks

By Samantha Humphries, security strategist, Exabeam

With 71% of cyber professionals reporting increased threats since the COVID-19 pandemic started, are SOCs prepared to mitigate these threats? The Exabeam 2020 State of the SOC report revealed 40% of companies reported being understaffed, which puts additional strain on security teams and makes their jobs much more challenging.

And our latest survey reveals that this problem is being exacerbated by the challenges of working from home, budget cuts and security team reductions. We received responses from 1,005 U.S. and U.K. cybersecurity professionals who manage and operate SOCs. Our study included CIOs (50%) and security analysts and practitioners from companies across 12 different industries. Employee size ran the gamut, although the majority (53%) had between 100-249 security professionals.

The results paint a striking picture of SOC organizations trying to manage more significant security threats with fewer resources.

## Furloughs Are Commonplace Despite Increasing Threats

Unfortunately, despite the increase in cyberthreats, our survey found three-quarters of organizations had to furlough members from the SOC team. About 50% had to furlough between 1-2 employees. The U.S. furloughed fewer SOC employees compared to their U.K. counterparts.

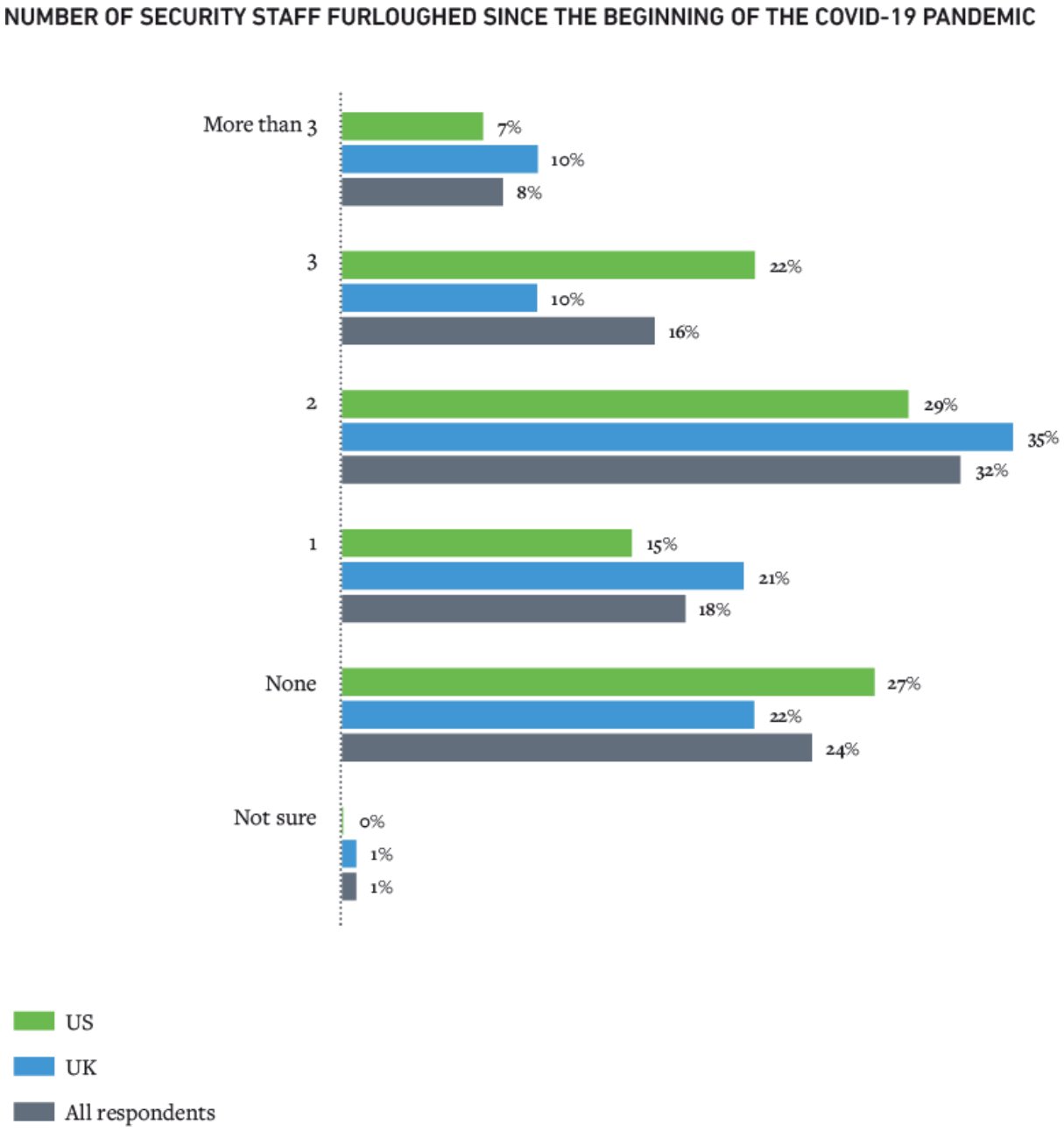



*Figure 1: Seventy-five percent of organizations had to furlough SOC staff.*

## Soc Teams Impacted by Redundancies

Overall, 68% of companies report having laid off staff members. The majority had between 1-3 employees laid off. U.S. SOCs had fewer layoffs  compared to the U.K. SOCs.

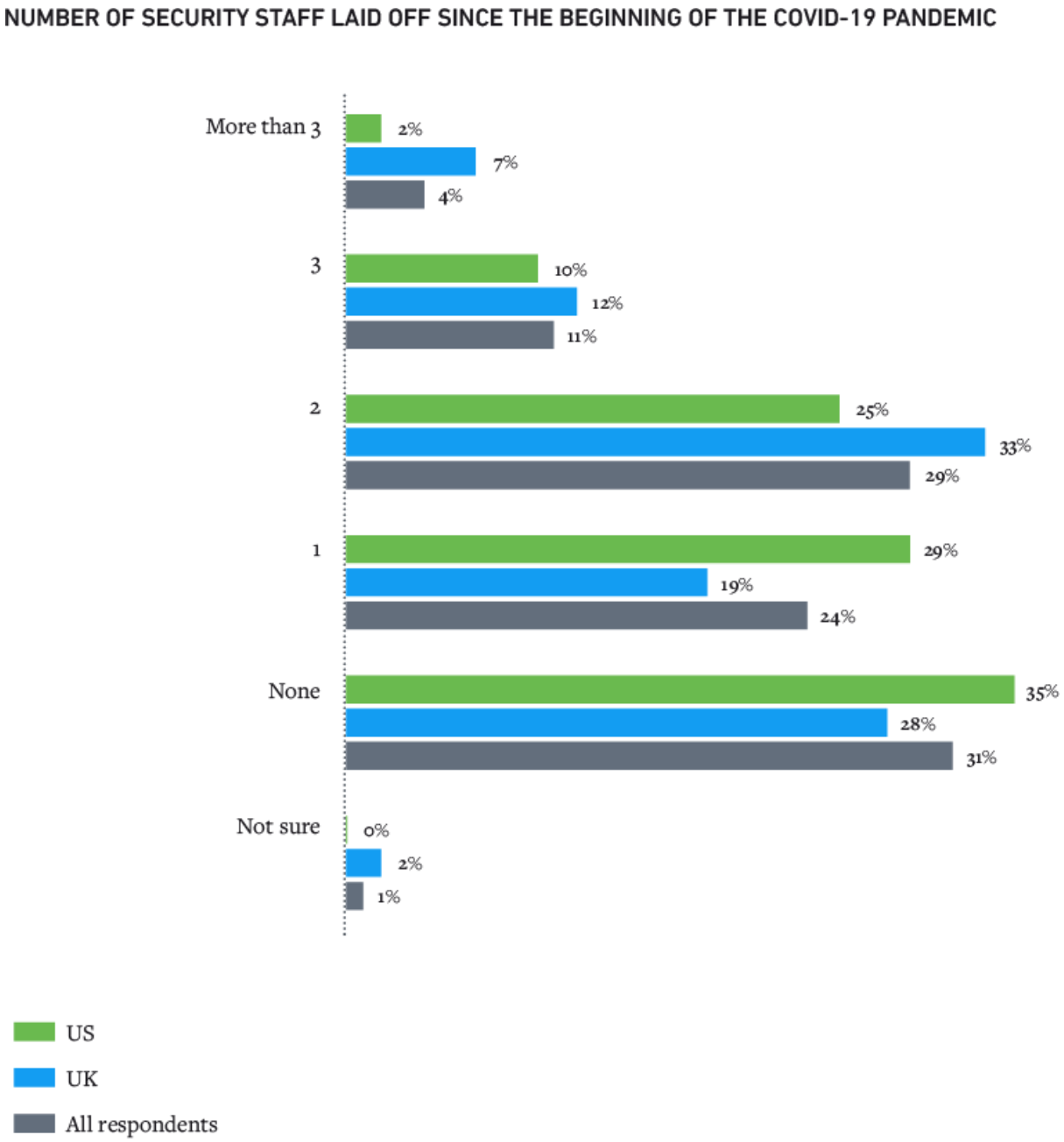



*Figure 2: Almost 30% of companies laid off two staff members from their security teams.*

## Many Companies Are Deferring New Hires

Given the furlough and redundancy findings, it's no surprise that 57% of the companies had to defer hiring since the start of the COVID-19 pandemic. A higher percentage of U.S. companies (71%) delayed hiring compared to the U.K. with 42% deferring.

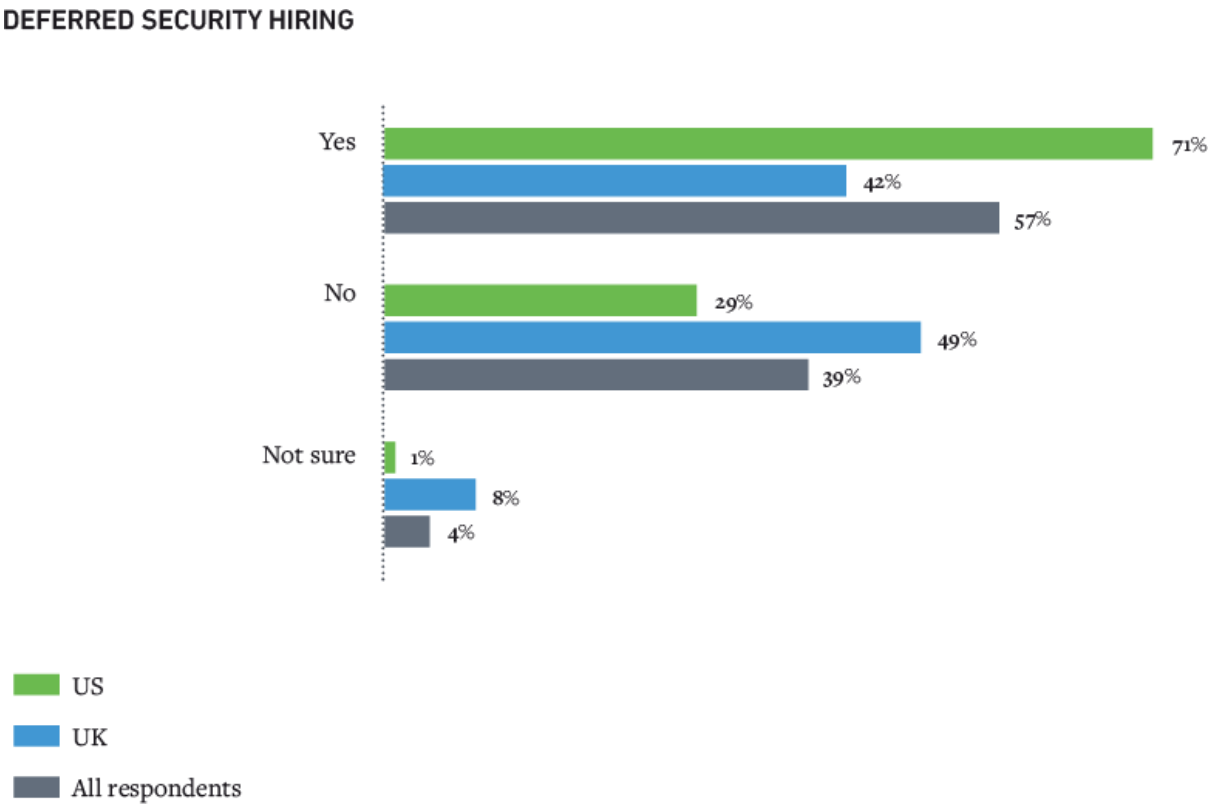



*Figure 3: Fifty-seven percent of organizations had to defer hiring.*

## Security Tech Investments Also on Hold

The COVID-19 pandemic has not only harmed people, but it also forced 60% of companies to defer investments in security technology, which were previously planned. The U.S. had a higher deferment rate of 68% compared to the U.K. rate of 51%.

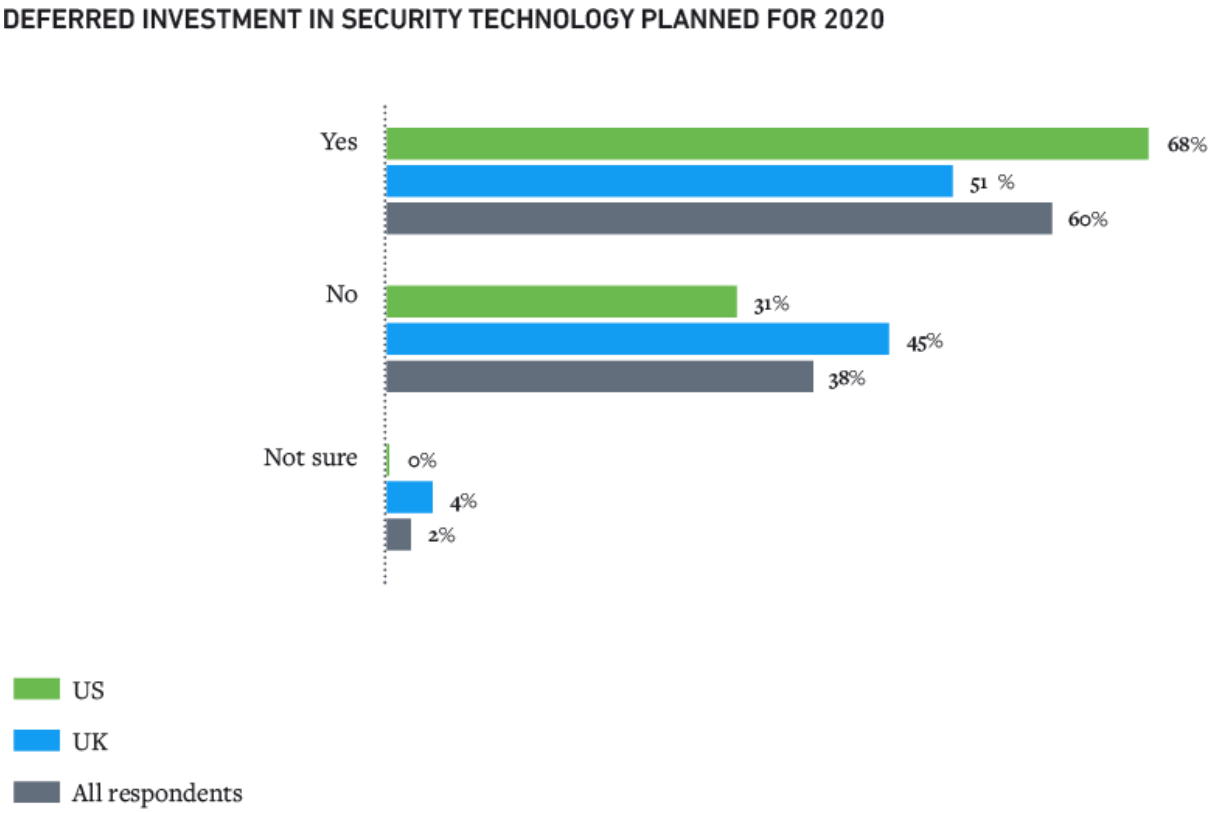



*Figure 4: Nearly sixty percent of organizations had to defer investments in security technology previously planned.*

## Cyberattacks Are Skyrocketing

Unfortunately, only 18% of companies overall had not seen an increase in the number of cyberattacks since the beginning of the COVID-19 pandemic. Eighty-eight percent of U.S. companies reported seeing slightly more and considerably more attacks compared to 74% of U.K. organizations.

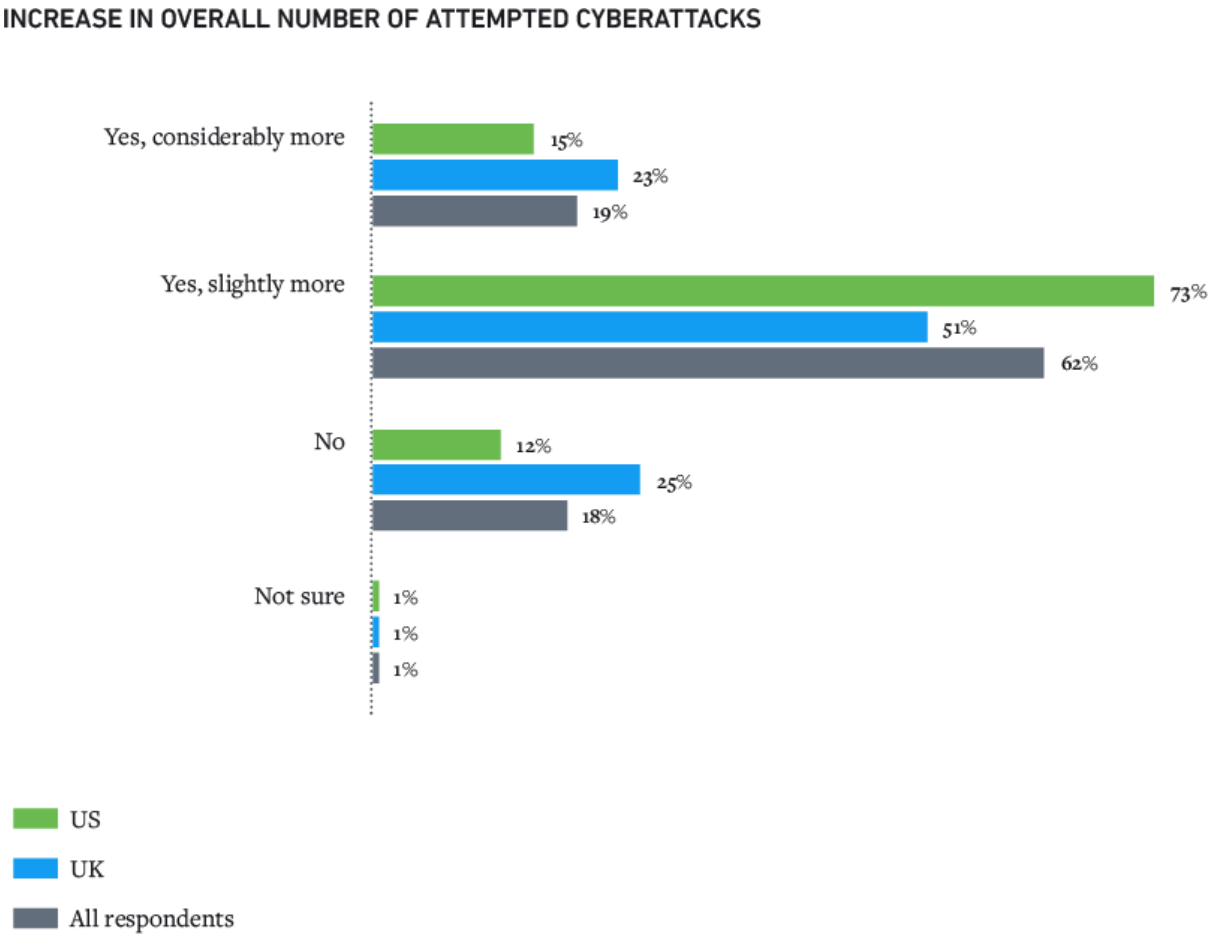



*Figure 5: Eighteen percent of organizations reported not having an increase in the number of cyberattacks since the beginning of COVID-19.*

## Work from Home = New Challenges for Security Teams

Remote work has presented challenges for many SOC staff members. No doubt reduced staff numbers made their jobs even more difficult. Respondents cited communications within their security team as the most significant challenge mitigating threats while working remotely, followed by communications with other IT departments. Twenty-nine percent reported difficulty investigating attacks. There was little significant variance in problems between U.S. and U.K. companies, although a higher percentage of U.S. companies 40% had more difficulty communicating with other IT teams compared to 22% in the U.K.

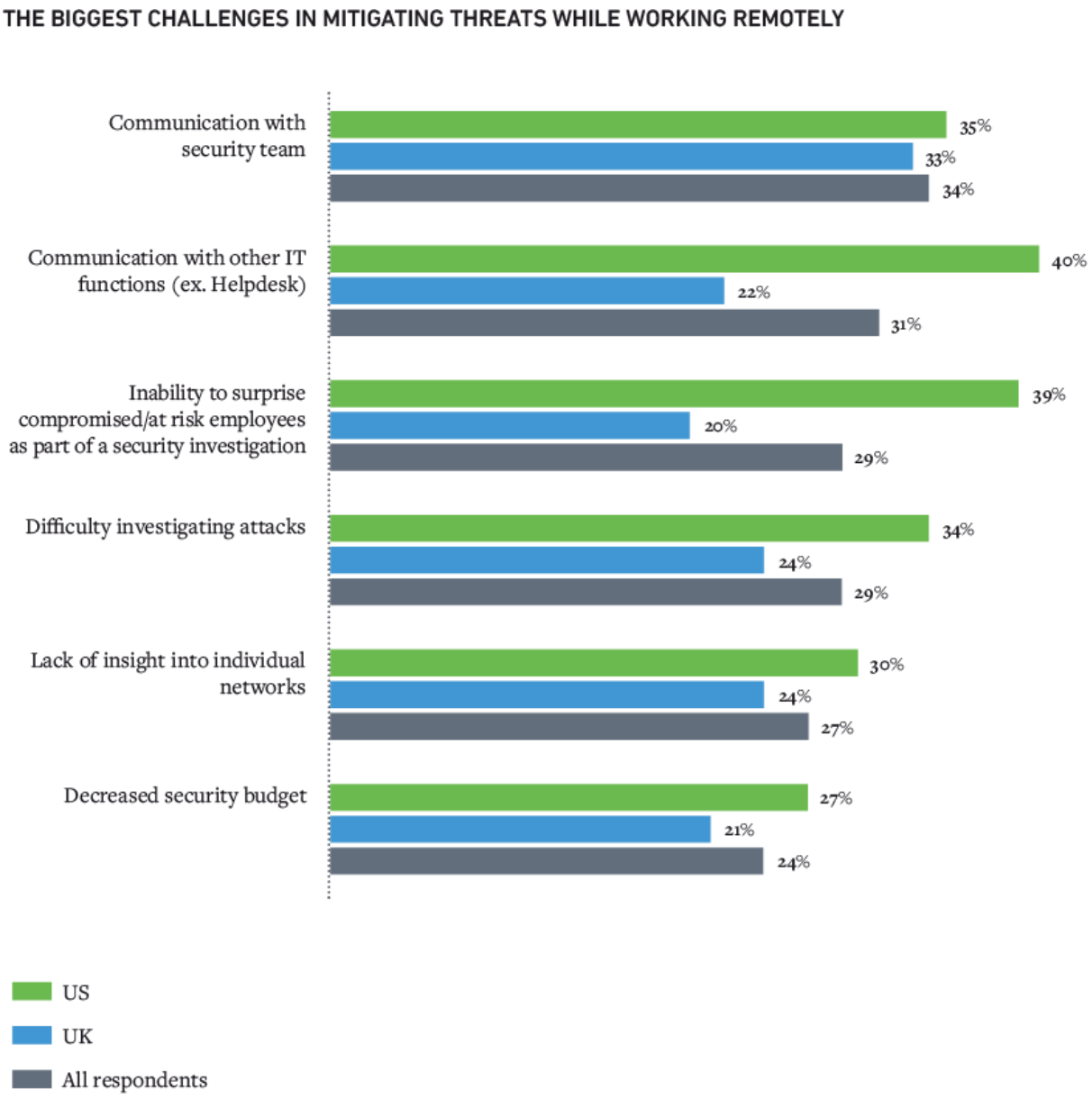



*Figure 6: Twenty-nine percent of organizations reported difficulty investigating attacks.*

## Home Workers More Prone to Error

The shift to WFH has harmed many employees' mental states and their ability to do their jobs. Some of the biggest challenges working remotely included being more prone to making mistakes due to distractions in the house — 49%, increased blurring of the line between personal and operated computers and data — 42% and learning new tools — 39%.

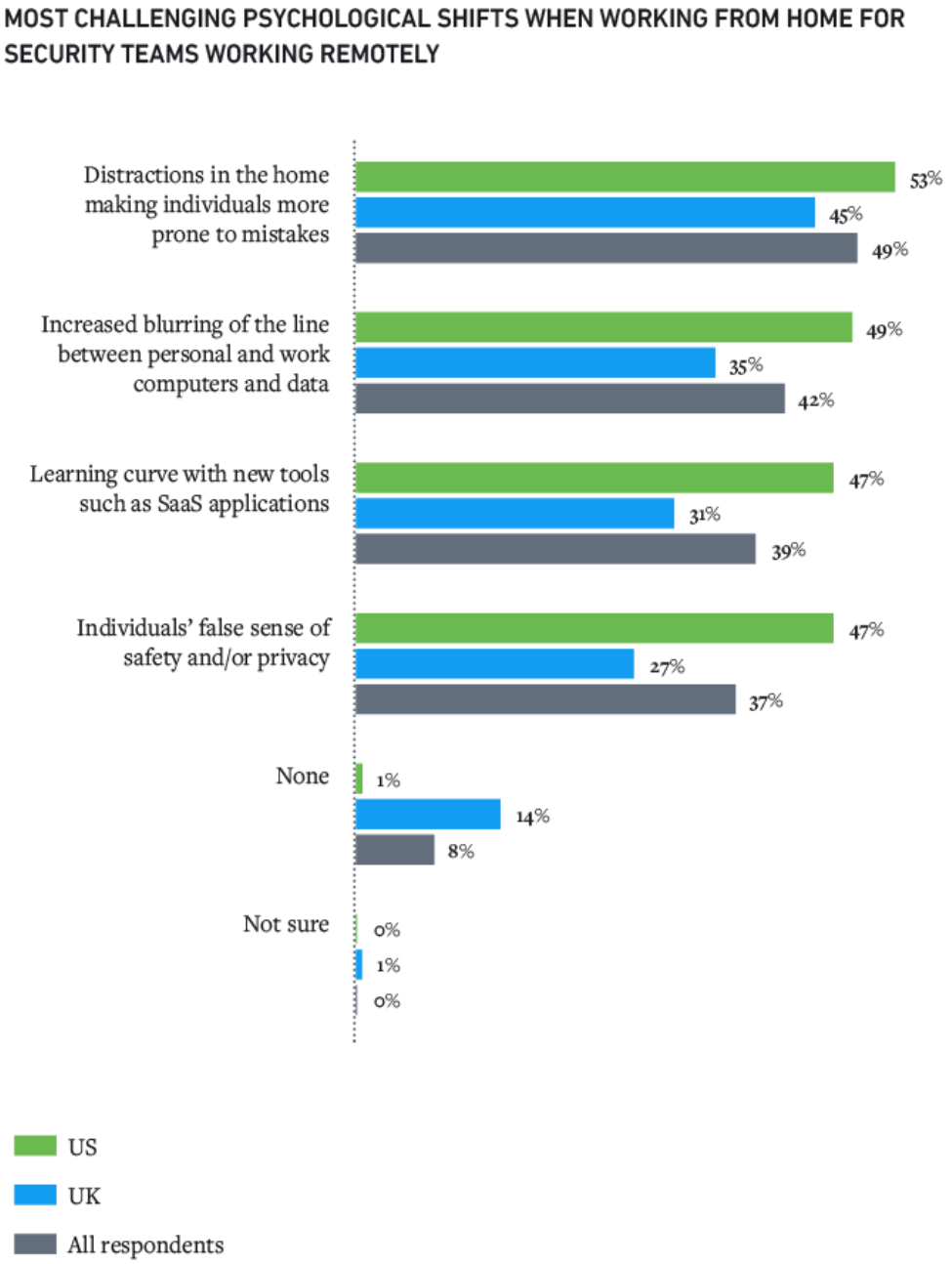



*Figure 7: Forty-nine percent of security professionals were prone to making mistakes due to distractions in the home.*

## Most Companies Continue to Use/Invest in Automation Tools

With fewer SOC staff, automation tools are essential in mitigating security threats. Only 17% of companies decreased their use/investment in automation tools. Fifty-two percent reported neither increased/decreased use or investment. Only 8% of the U.S. reduced their use/investment in comparison to 26% of U.K. organizations.

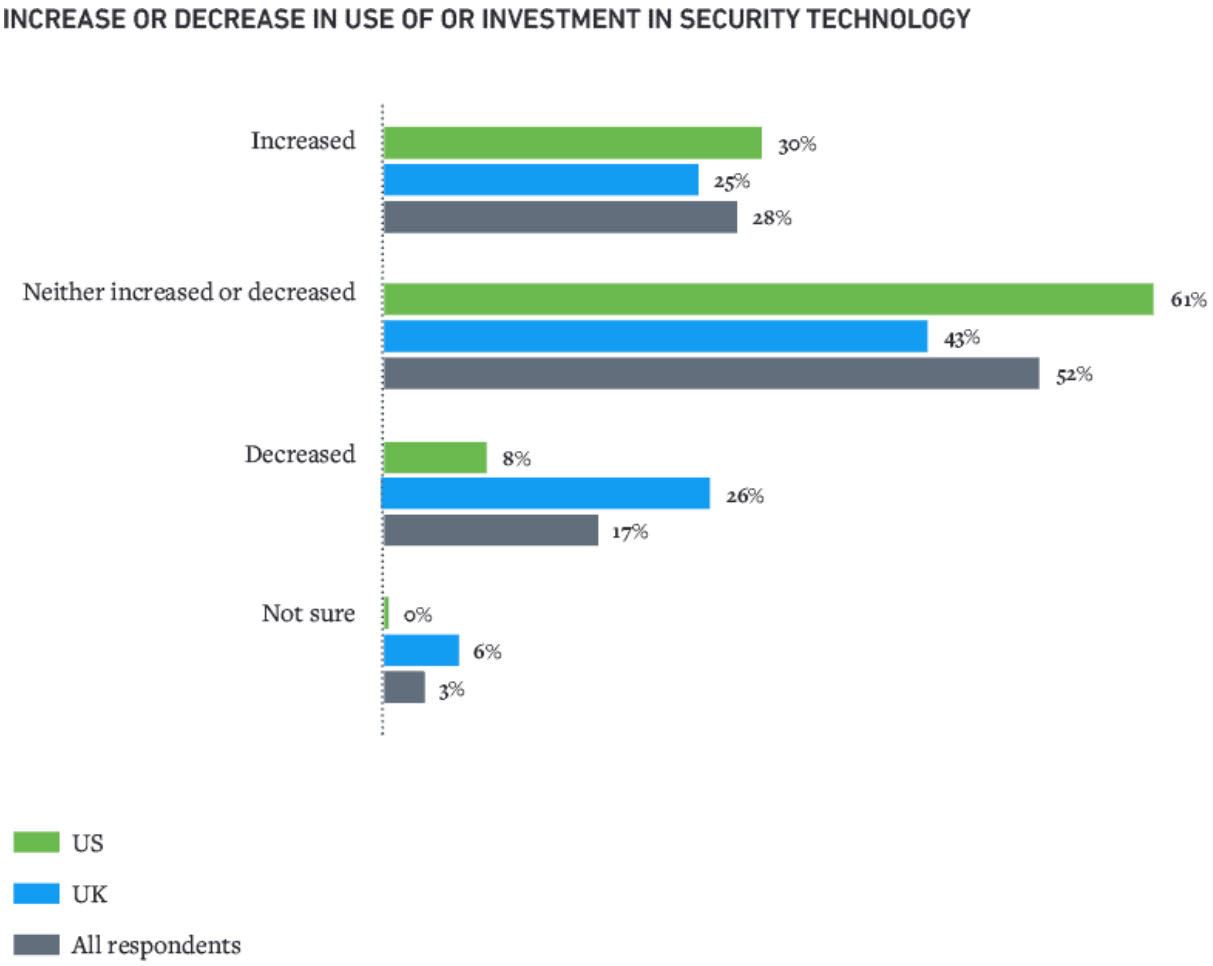



*Figure 8: Seventeen percent of companies decreased their use/investment in automation tools.*

## ⅓ Of Companies Have Been Hit with A Successful Cyberattack During the Pandemic

Thirty-three percent of overall companies reported encountering a successful cyberattack since the beginning of the pandemic. There were no significant variances between U.S. and U.K. companies

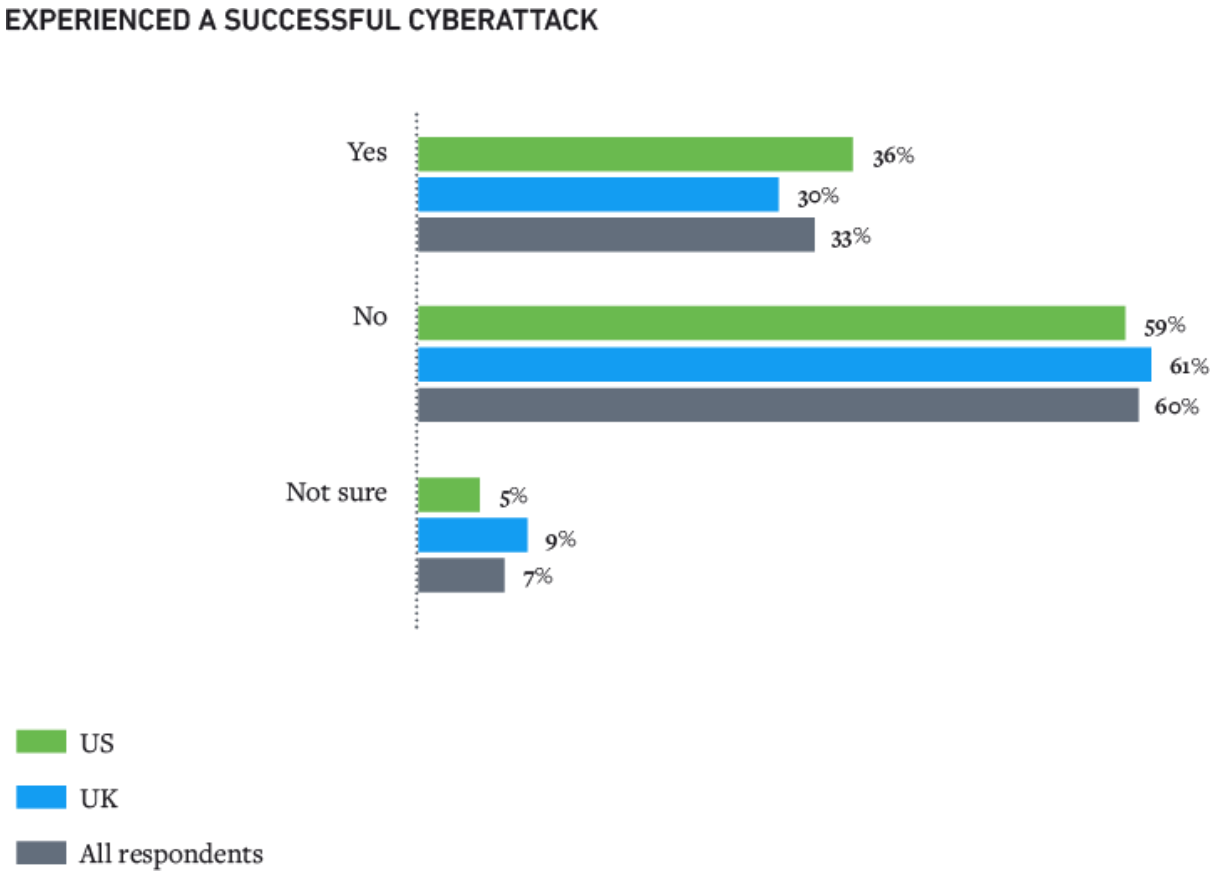



*Figure 9: Thirty-three percent of companies reported experiencing a successful cyberattack since the beginning of the COVID-19 pandemic.*

## Mitigation and Legal Costs Are the Top Consequence of Cyberattacks

Companies reported several consequences of successful cyberattacks. The most common effect was mitigation and legal costs — 44%, followed by loss of business revenue — 41% and a negative impact on brand reputation — 41%.

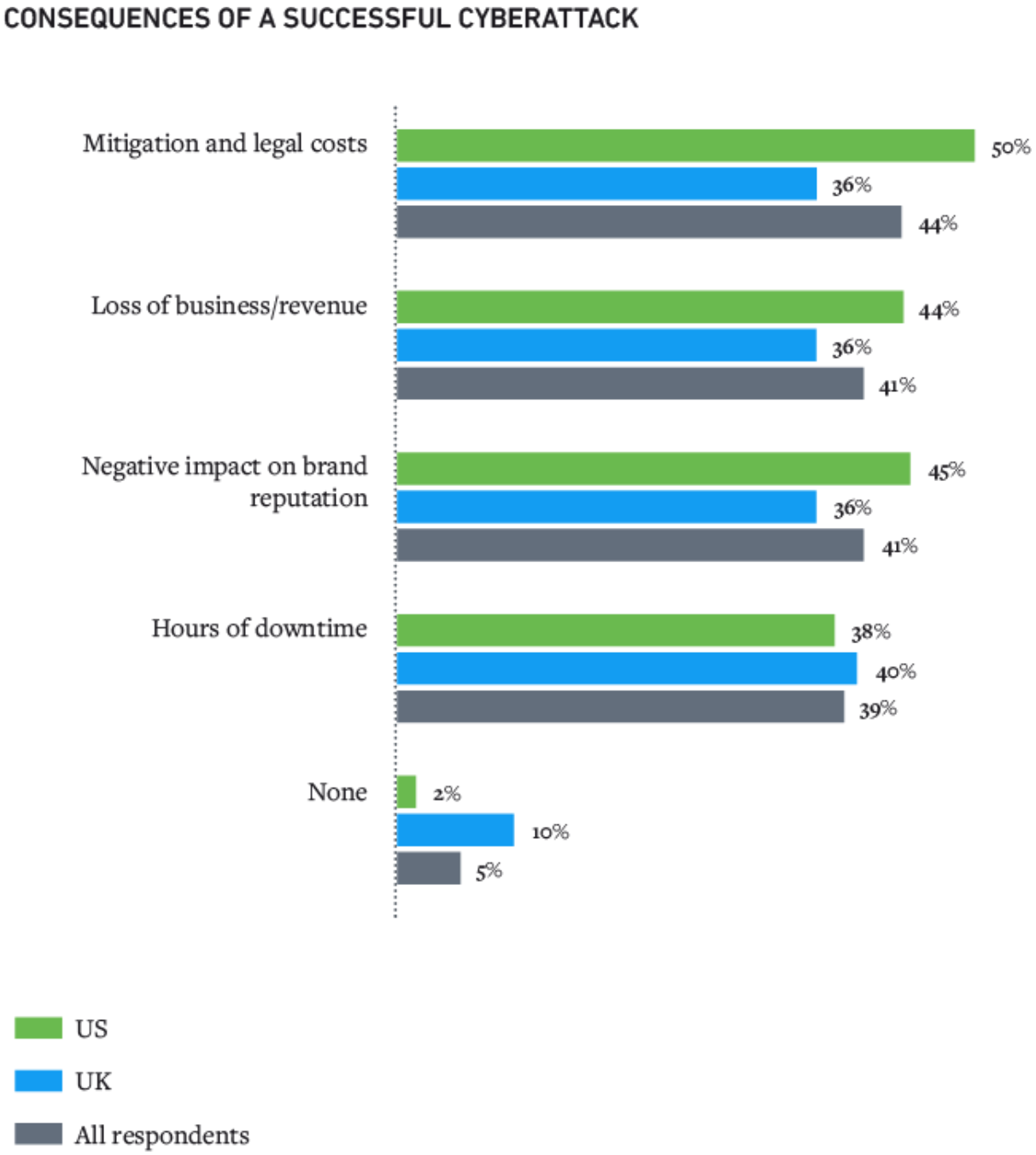



*Figure 10: Forty-four percent of companies reported mitigation and legal costs were a consequence of successful cyberattacks.*

## Cyberattacks Hitting Organizations in The Wallet

Considering many organizations are seeing a financial impact due to the pandemic, the additional cost of a cyberattack could not come at a worse time. Regarding lost business revenue, our survey found in the U.S., 35% lost between $38K-63K, and 14% reached losses of $63K-95K; in the U.K., 40% lost between £30K-50K. In terms of the financial impact on a brand, in the U.K., 43% saw between £30K-50K in losses; in the U.S., 38% reported between $38K-63K in losses. Also, 7.5% in each region lost between £50K-75K or $63K-95K.

Concerning the financial impact of legal and mitigation costs, in the U.K., 33% spent between £20K-40K; in the U.S., approximately 30% spent between $38K-63K, and for 11 % the costs hit the $63K-95K range.

## DOWNTIME IS PROMINENT TOO

Since the beginning of the COVID-19 pandemic, 97% of companies experienced downtime between 1-4 hours. Fortunately, only 3% reported downtime higher than four hours.

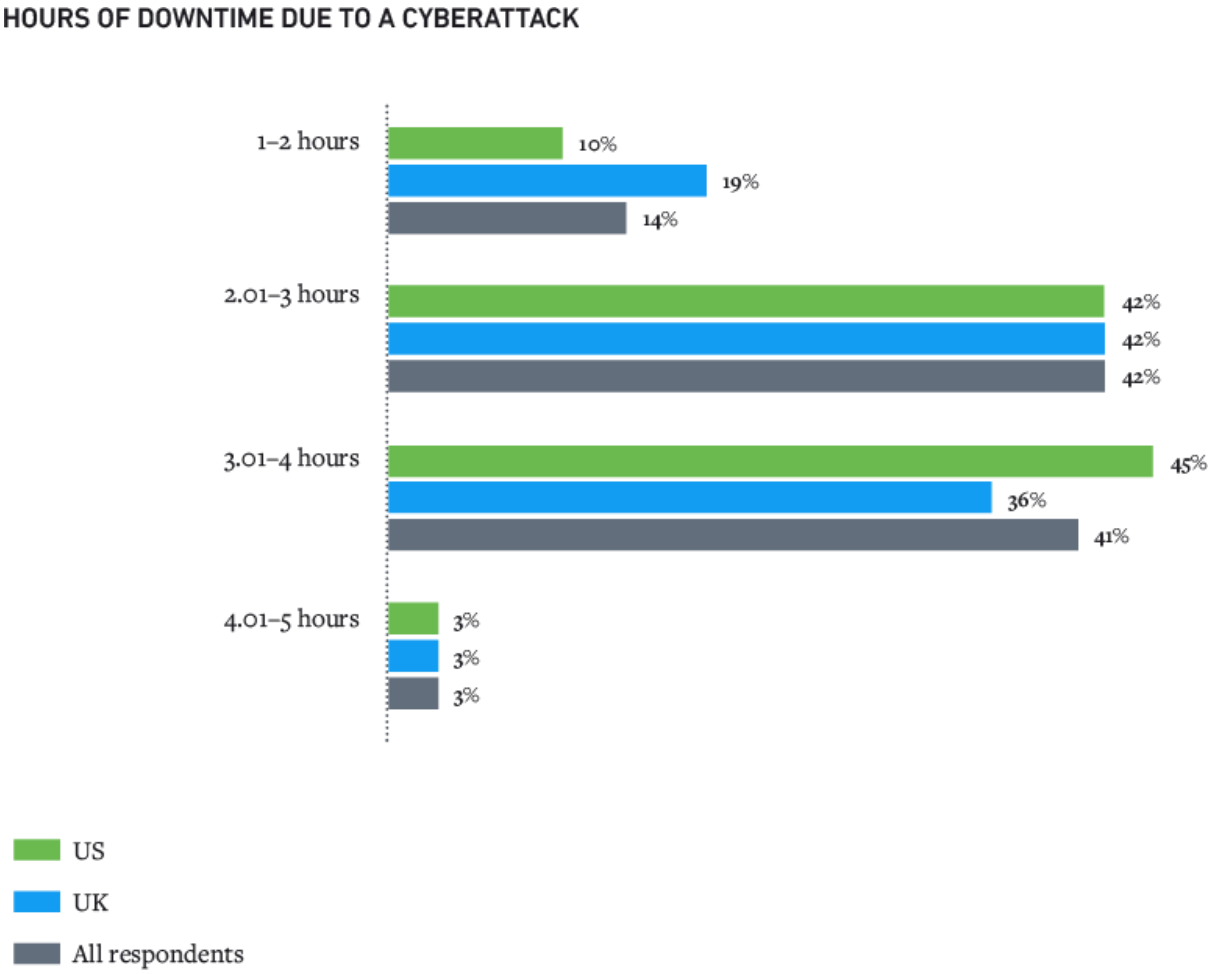



*Figure 11: Only 3% percent of companies experienced downtime greater than four hours.*

The findings from our survey clearly show many SOCs have to manage a much more significant number of cyberthreats with a leaner staff. Exabeam is committed to helping you and your SOC get through the COVID pandemic. Here are a few resources to help:

- Webinar: SOC-from-home. Actionable Insights for Security Practitioners
- Blog Series: Securing Your Remote Workforce
- Webinar: Adapting Security Programs for an Unprecedented Future

**About the Author**

Samantha has 20 years of experience in cyber security. She has defined strategy for multiple security products and technologies, helped hundreds of organisations of all shapes, sizes, and geographies recover and learn from cyberattacks, and trained anyone who'll listen on security concepts and solutions. She authors articles for various security publications, and is a regular speaker and volunteer at industry events, including BSides, IPExpo, CyberSecurityX, The Diana Initiative, and Blue Team Village (DEFCON)."

Samantha can be reached online at shumphries@exabeam.com and at https://exabeam.com

# Cybersecurity Challenges When Working from Home

By Renuka Sahane, Sr. Content Writer, Scalefusion

Maintaining the security of corporate data when employees work remotely in the new normal.

IT governance and cybersecurity have gained much-needed attention in the enterprise environment, thanks to the exponentially growing number of digital devices used in the workplace. The need to access the internet and intuitive apps that sit on mobile devices used across all industries is rapidly growing. From conventionally operating businesses such as retail to technology-driven businesses that are into manufacturing or supply chain, technology has touched based and revamped operations from the top to bottom.

## The era of remote working

And just when the businesses globally were finding and implementing solid strategies to secure corporate devices and data from unknown threats and cybersecurity challenges, the pandemic hit. COVID-19 pushed all businesses- even the ones without a mobility strategy into a new

normal that not everyone was prepared to endure. Remote working caught up, first out of hesitation, then out of need and now looks like it's here to stay.

For companies that had strong strategies in place before moving to remote working, the transition was easy but for those that did not have policies and security protocols in place, the change has been a real challenge. Employees have no choice but to work from home and companies have no option but to facilitate the same. Ensuring work-friendly devices are available to the employees to upkeep the business performance and employee productivity has been the primary concern of business leaders.

Equally daunting are the security concerns and cybersecurity challenges that might arise when employees work from home, for an indefinite period. When the employees and the devices they use to exit the physical boundaries of the office, they are essentially out of the security posture of the company.

## Cybersecurity challenges during remote working

### Unmanaged devices, routers, printers, and other devices

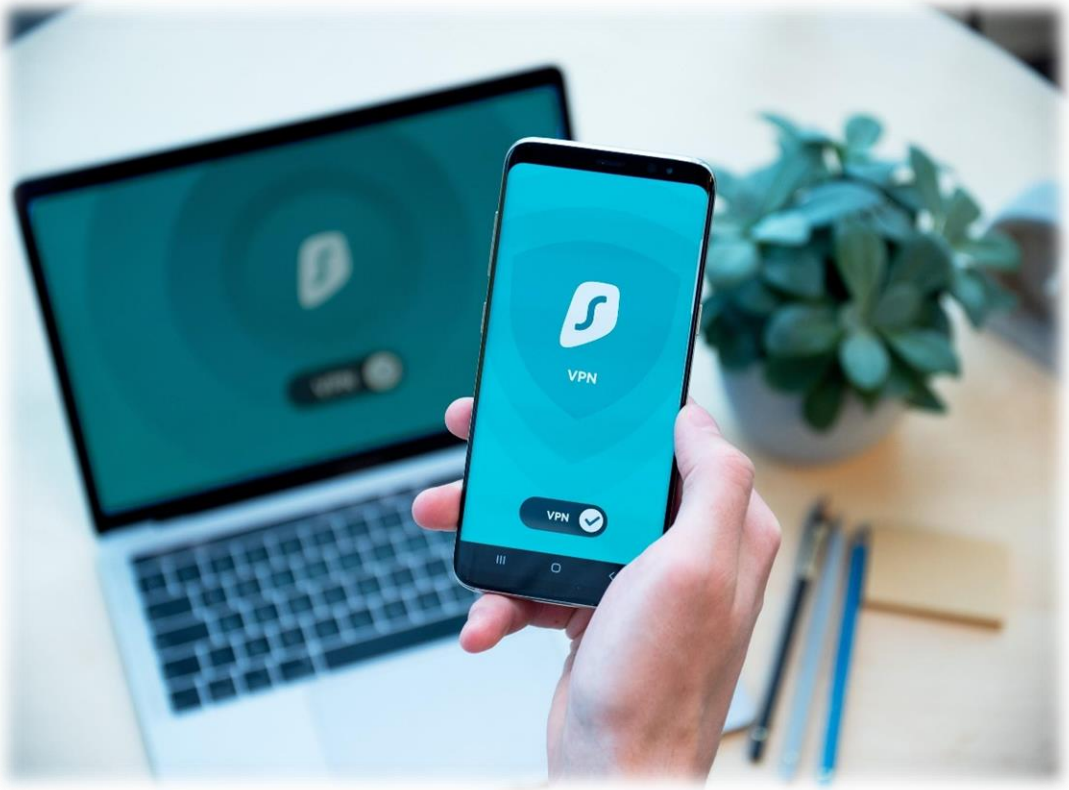
If the employees working from home have not been provided with provisioned and managed devices including laptops, desktops, and tablets, they choose to opt for personal devices for work. Unless the company has a BYOD management policy in place and can enable security restrictions on the work container or profile of these devices, the device usage is safe and can in fact help add to the employee productivity, since they use their favorite devices for work. But if the devices are unmanaged and yet the employee is accessing work resources, corporate and user data on these devices, the data is practically exposed to every possible cybersecurity threat there is- from apps, websites, and unmonitored personal communication and collaboration tools.

Moreso, the devices are invariably connected to an internet router, peripherals such as printers. Work calls happen in the presence of family/roommates and there are home automation systems and bots eavesdropping on every work-related conversation. Clearly, the security protocols are dull, if not faded during remote working.

### How secure is home WiFi and/or VPN?

This has been a serious concern for organizations that haven't extended secure internet hotspot devices for employees to connect to while working remotely. The security of personal WiFi is highly questionable, especially when it is accessed by multiple users for personal use. Home networks commonly have the WEP protocols, which are known to be weaker, paving the way for cybercriminals to walk into your data and devices.

Also, while VPN might look like the best option for providing network security via encryption, if the VPN connects to any of the compromised devices, for example, the personal tablet of the employee, the hackers can crawl in the gaps created. It is important to ensure endpoint authentication to VPN access via certificate management, for instance, to ensure that only managed/work devices are connected to such networks. Needless to say, monitoring the VPN security at all times, recognizing potential failures, and extending support via patch management is crucial.




It is also important to note that if the employees are using legacy PCs, managing them outside of the corporate network or via VPN is practically impossible. In such cases, quickly procuring the latest tech by leasing or leveraging 'desktop as a service' can be a good option.

## Phishers taking advantage of emotional vulnerabilities

Reports of increased phishing scams since the COVID-19 pandemic are surfacing. People are vulnerable, anxious and it is a tough time for all. The employees are susceptible to click on malicious emails that appear to be from government agencies, healthcare bodies, or WHO or might give away critical personal data to healthcare-related apps that are not authorized.

## What companies can do...

Start with a robust policy to maintain security for remote working. Manage employee-owned as well as corporate-owned devices with an EMM solution and exercise access control, manage website access, and add security to corporate content with extensive policy configurations. Be on the top of the device security and rectify potential threats quickly.

And most importantly, build a culture of security among your employees and train them on the best practices. Your corporate data is only as safe as your employees want it to be. Go beyond device policies to educate your employees on the importance of data and cybersecurity

### About the Author

Renuka Shahane is a Sr. Content Writer at Scalefusion -a leading Mobile Device Management solution. Renuka is keen in learning new trends surrounding cybersecurity, repercussions of remote working and the evolution of enterprise mobility. You can read more of her work at https://blog.scalefusion.com/.


# Network Security Is Not Data Security

*Data is an organization's most valuable asset, yet data loss is one of the biggest repercussions of a cyber-attack.*

By Matt Cable, VP Solutions Architects & MD Europe, Certes Networks

Data is an organization's most valuable asset, yet data loss is one of the biggest repercussions of a cyber attack. In 2019, more than 15 billion records were exposed in data breaches, amounting to more than $3.5 billion lost to cyber crime.

Moreover, the unprecedented events of recent months in 2020 have seen the number of attempted data breaches continue to rise, with cyber hackers taking advantage of remote working and individuals' fears over COVID-19. In fact, a survey showed that 50% of organizations were unable to guarantee that their data was adequately secured when being used by remote workers.

There is clearly a lot at stake. Organizations need to protect their data, but they also need a robust data assurance solution. Data assurance, or information assurance, is a challenge due to the many networking technologies deployed in today's environments, making policies disjointed due to differing technology and network infrastructures, as well as data regulations driving data security.

Regulatory compliance is becoming more complex, and each regulatory policy widens the scope for required data security controls, often resulting in point solutions, added complexity and the loss of network visibility.

Therefore, strict separation of duties is a core compliance requirement to ensure there is no risk of network policy interfering with data security policy; but this is often difficult to enforce when security is tied to infrastructure.

So, how can organizations secure their data, even when the network isn't secure to begin with? And how can they ensure the security posture is always visible in order to ensure their data is always secure? Simon Hill, Director Sales Operations at Certes Networks explains why a five-step approach is essential to keep a customer's data secure.

## The Five Step Approach to Data Assurance as a Business Strategy

Due to increasing pressures to keep data secure, securing data as it travels across the network has never been more important. Encryption is certainly one way to keep data secure as it travels across the network, but it is not as simple as just deploying an encryption solution. Organizations must follow these five steps.

1. Convert data assurance requirements into an intent-based policy. This is then used to configure and enforce the required security parameters for sensitive data.

2. Creating multiple polices, one for each data classification or regulation, not only ensures that data is protected at all times, but with each policy using its own keys, customers are creating micro-segments using strong cryptography or crypto-segments. These crypto-segments keep data flows protected using separate keys and also provide critical protection against the lateral movement of threats.

3. Organizations must look at the requirements of their environment. Whether it is low latency applications, high throughput data requirements or rapidly changing network environments, organizations must have the flexibility and scalability to secure any environment to meet the depth and breadth of their organization's needs.

4. Organizations also need full network visibility without compromising data security. With traditional encryption blinding the network and security operations tools, monitoring, troubleshooting, adds, moves, or changes are made difficult without first turning encryption off. An encryption technology solution should enable the network to look and work in the same way after deployment as it did before, enabling all networking and security functions even while data is being protected.

5. Lastly, with a data assurance strategy, organizations can benefit from a real-time view of their data security posture, graphically showing data security performance at all times. An observability tool or a third-party security dashboard can ensure rapid detection, response and remediation of non-conformance and provide evidence as part of any required audit. Organizations using Artificial

Intelligence can also take advantage of the programmable interfaces when using a dynamic program with a security overlay, which reduces the time to remediation and removes the need for manual intervention when threats are detected within the security stack.

## Confidence in Data Assurance

The goal of a data assurance solution should be high confidence with low impact, and the ability to scale to the needs of an organization with, for example, a zero-impact software-defined overlay and real-time reporting of policy conformance to achieve this.

Taking a software-defined approach truly delivers on true separation of duties, enabling security teams to retain control of the data security posture at all times without compromising network performance or the agility needed so that applications teams can be effective.

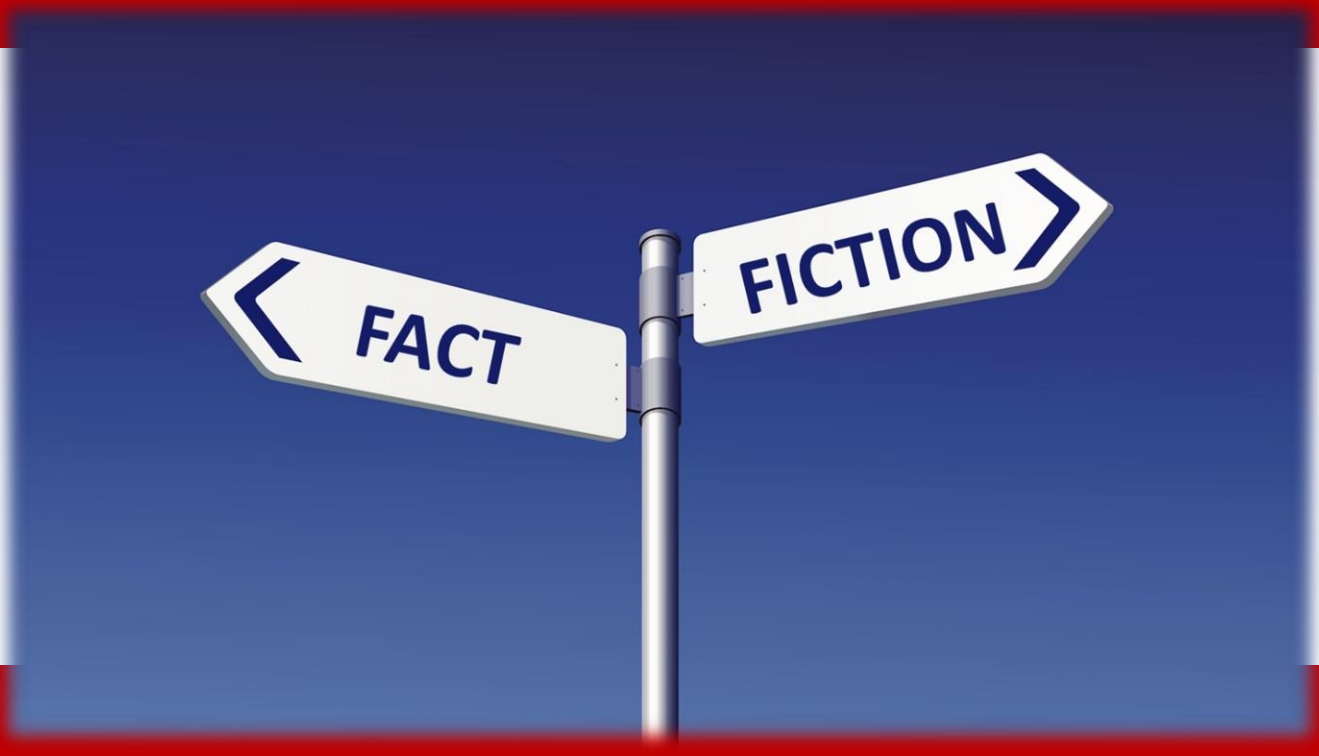
Furthermore, with a robust data security strategy, organizations can quickly turn their data cyber assurance requirements into intent-based policy which can be monitored in real time to ensure round-the-clock visibility of their data assurance posture. Whether one data classification or multiple, securing data using crypto-segmentation to micro-segment data flows, protects against the lateral movement of threats whilst also ensuring all data is secure in motion.

Armed with this five-step approach, organizations can take actionable steps not only gain a deep understanding of how to enhance their security posture and to manage and enforce policies but to measure the effectiveness of their security strategy. When securing data vs. securing the network is the priority, data loss can be prevented and data security can truly be seen as a strategic contributor to the organization's success.


**About the Author**

Matt Cable is VP Solutions Architect and MD Europe, Certes Networks. Matt is a Cyber-Security and Cryptography expert with more than 20 years of consultancy experience that covers IT Strategy and Enterprise.

Matt can be reached on LinkedIn here - https://www.linkedin.com/in/mattcable72/ - and at our company website www.certesnetworks.com




# WireGuard - Separating Fact from Fiction

By Tomislav Čohar, co-founder, hide.me VPN

Offering high speeds, excellent levels of security and a low footprint, WireGuard has rightly caused ripples within the VPN industry. WireGuard is an open-source protocol that employs cutting-edge cryptography and provides fierce competition for the likes of IPsec and OpenVPN. As a user then, what advances can you expect from WireGuard? Has this protocol been over-hyped and are we just seeing a flurry of smoke and mirrors from a biased media?

WireGuard certainly offers a lower footprint - it was made to be as lightweight as possible and can be implemented with just a few thousand lines of code. The resulting reduced attack surface is certainly a benefit and also makes auditing the code a much more straightforward process. Users enjoy the benefits of being able to switch seamlessly from something like Wi-FI to 4G LTE due to WireGuard's built-in roaming capabilities. Also, WireGuard uses your network more adroitly than other VPN protocols. With a mere 32 bytes overhead, it trumps other protocols that use much more space for their signaling. As a user, you get more space for your data with higher throughput.

WireGuard is a remarkably fast protocol that doesn't skimp on security. This is thanks to the use of modern and efficient cryptography constructs. WireGuard works from within the Linux kernel meaning that it can process data faster, eliminating much of the latency associated with other protocols. Keeping

on the security track, with WireGuard being a more recent addition compared to the likes of OpenVPN, it has benefitted from being built from the ground up to support more modern encryption methods and hash functions.

## Telling it straight

Taking all of these benefits into account, recent media coverage and some claims have certainly been a cause to raise eyebrows. Let's take a look at just a few of the myths that have been circulating in recent weeks and months so that you can better understand exactly what WireGuard can deliver.

## Fixed IP address

So does WireGuard insist that each device on the network get a fixed IP address? No, not really. In fact, it doesn't really demand anything and largely performs in a similar fashion to any other protocol; operating as a versatile cryptographic piece of a larger puzzle called a VPN tunnel. It's more useful to think about how you manage it. If you use a simple or rigid setup, this requires static IPs on the servers. However, it can be managed in a more dynamic fashion. WireGuard is able to perform just like any other VPN protocol by adding IPs when they're needed and getting rid of them as soon as the VPN session is concluded.

## Server Communication and data exchange

Can WireGuard offer a considerable change to the way servers communicate with each other?

Again, not really, it operates in a similar fashion to all the other protocols. What about the exchange and verification of data? Is it the case that WireGuard sticks to strong but simple ways of exchanging and verifying data? In fact, WireGuard only supports one method of key exchange. There is only support for one AEAD. Other protocols support a profusion of cryptosystems but tend to settle on AES. AES is not flawed, no exploit has been found yet. Also, AES256 cipher is cryptographically stronger than ChaCha20 which is used by WireGuard. However, It is computationally expensive when compared to ChaCha20. ChaCha20 offers the best bang for the buck. One could argue that Poly1305 MAC is stronger than GHASH, but then again we come to the point of the whole AES-GCM construct being supported in Intel's hardware.

## Internet Speed

When we talk about who is quick and who is slow, are other protocols more sluggish than WireGuard? Would you see a dramatic increase in speed by adopting WireGuard? Essentially, some VPN protocols are slower, but this is almost entirely down to circumstances and not really related to crypto. If you are connecting through a dialup modem, for example, then speedy crypto becomes a moot point. Additionally, if you are a provider that supports much faster protocols then WireGuard isn't going to be able to deliver on impressive speed promises.

Our measurements show that OpenVPN usually outperforms WireGuard by at least 10 percent (on the Windows platform when WinTUN driver is used and when the OS is running on an Intel CPU. On Linux, again on an Intel CPU, WireGuard outperforms OpenVPN significantly (by more than 40%), but it is still significantly slower than IPSec (by more than 10 percent). These measurements were performed on an 1 Gigabit LAN since such a speed is commercially available for our customers. On 10 Gigabit Ethernet, OpenVPN pales in comparison with WireGuard as it is about 10 times slower. IPSec, on the other hand, outperforms WireGuard by more than 30 percent when AES is used as a symmetric algorithm.

## Running in-kernel

Can you achieve the highest possible performance just by running in-kernel? Not really - actually, IPSec is way faster on all platforms. IPSec runs much faster because it runs in the kernel too, but is significantly more optimised for Intel CPUs. The point is, running within the kernel offers a major speed increase but WireGuard is not the only protocol to run in such a way. PPTP/L2TP do too. OpenVPN developers plan to release a kernel module for Linux soon. SoftEther (which runs completely in the userspace) outperforms WireGuard when throughput is the primary concern.

WireGuard definitely warrants all of the interest it has garnered - it remains to be seen whether it becomes a revolution for the VPN industry. As things stand it certainly offers faster speeds and better reliability compared to some of the existing VPN protocols - and there is the added promise of new and improved encryption standards. It is surely only a matter of time before we see more and more VPN services incorporating WireGuard into their structure.


**About the Author**

Tomislav Čohar is the co-founder of hide.me VPN.

https://hide.me/en/


# Conducting Risk Prioritization and Remediation to Combat Challenges in The Distributed Workforce

By Egon Rinderer, Global Vice President of Technology and Federal CTO, Tanium

Most agencies have successfully met initial telework surge requirements – putting the basics in place to continue essential operations. Recent research found approximately 90 percent of federal employees now telework and 76 percent feel they will be able to telework at least part-time in the future. With the basics now in place, the next priority for every IT team is a careful assessment of cyber risks, current protections, and what is needed to keep systems and data safe in an environment with exponentially more endpoints in more places.

Data residing on endpoint devices operating beyond the agency network perimeter isn't all that's at risk– if compromised, those devices can also be used by malicious actors to tamper with or steal sensitive data on the agency's enterprise network. As the number of devices outside of the protected network grows, the attack surface expands and risk increases.

The reality is that many organizations were already struggling with basic cyber hygiene before the telework surge – and most of the security tools implemented were designed for local enterprises. With a distributed workforce, this means increased cyber risk, as the security tools in place become even *less* effective.

In this new environment, federal IT teams should focus on risk prioritization and remediation – identifying and addressing the vulnerabilities that pose the highest risk and could have the biggest negative impact on the agency and its mission.

## Performing Risk Prioritization and Remediation

Almost half of federal agencies say the new distributed workforce has affected the execution of projects and over one-quarter feel planning for the next fiscal year has been delayed. April and May were months of change, and June is predicted to be a catch up month. Demand and expectations for real-time information and IT support from customers are up, so agencies must be prepared.

Risk prioritization can help IT teams evaluate the infrastructure beyond data vulnerabilities to help determine which vulnerabilities to patch and assess an endpoint's security level – which can dramatically change the risk level. By prioritizing risks, security teams can more effectively allocate their already limited resources to focus on mission critical tasks.

However, IT teams now have to consider the degrees of separation between each endpoint in context. In addition to the connectivity to the enterprise network, there's often connectivity to other endpoints, the applications and users authenticated to each, and the rights and privileges conveyed through such mechanisms as AD group membership. Even if one endpoint is completely secure, a user profile on another more vulnerable endpoint could provide an access point for lateral movement into the entire network. Given that these factors and variables can change by the second in a large enterprise, a quarterly, monthly or even weekly risk assessment is insufficient.

Often, the security problems that agencies are facing are oversimplified, and vendors can only provide partial solutions to help; they run a vulnerability assessment and receive a risk score from systems such as the industry standard Common Vulnerability Scoring System (CVSS), helping them assess and rank their vulnerability management processes. However, while risk scoring systems such as these combine several types of data in order to provide the vulnerability risk score, they aren't always based on real time data and the results are only as good as the data that's input.

Vendors have completed a piece of the puzzle by diagnosing vulnerabilities and identifying threats, but have to now take into consideration the millions of risk scores across millions of endpoints – some of which are unknown – trying to access the network and the context of the relationship between these endpoints over time.

The lack of complete visibility into the network leaves many vulnerabilities unknown and makes risk assessments little more than guesswork for IT teams – increasing the likelihood of a breach. Risk scores are living, breathing things and, especially in the new teleworking environment, must be based on real time data to protect the agency's environment and overall mission.

## Connectivity Hurdles

Now that agencies have established basic connectivity, the focus has shifted to optimizing connections and improving security. There are a variety of approaches – some agencies have deemed split tunnel virtual private networks (VPNs) too risky, opting for full tunnel VPNs where both user and management traffic flow through the same channel. While this approach can achieve the short-term goal of establishing and maintaining secure connectivity, it also has unintended consequences.

Using full tunnel VPNs can lead to slow response times, causing employees to disconnect from the VPN altogether. When this happens, IT teams are blind to those devices and they don't get routine patches, making them increasingly vulnerable to cyberattacks. While these endpoints used to enjoy the added protection of an existence behind the protective boundary of the enterprise network perimeter, they are now isolated in an uncontrolled environment with only their point tools protecting them and active management and visibility only afforded while connected to the VPN.

BYOD has added another layer of risk and complexity, with many employees turning to personal devices to continue working. However, there's often a discrepancy between not just the out of the box tools that reside on an individual's personal device and their work computer, but also the security tools loaded and managed on each. And, when these BYOD devices only have periodic connectivity to the agency network, cyber criminals no longer have to penetrate a multi-layered protected perimeter to get into the main server. They can use the unprotected device as an entry point into the network.

A holistic approach helps enable improved visibility and control over the network, regardless of where an asset is located. The challenge is that decisions about connectivity, endpoint security, and perimeter security are often made in a vacuum by those independent teams responsible for each versus a combined solution. With a holistic approach in mind, teams can understand what is impacting the agency's risk, mitigate each risk for the time being, and remediate it for the long-term.

## The Next Phase

As agencies look to the future, operations will not resume as in times past and budgets will be impacted. Agencies must consider the sustainability of solutions long-term, specifically in terms of mitigation of the inherent risk a distributed workforce carries. They should be pragmatic in their future plans, having ideological discussions around assessing and measuring risk, dealing with steps to mitigate risks, and finding cost-effective ways to address risk and secure the network. IT teams need to be data driven and look at the validity of the data agencies are working with.

Agencies must build a foundation for assessing and addressing risk based on real time data to maintain business and mission continuity amid a risk landscape that's changed dramatically and irrevocably.

It may seem impossible to get a hold of the amount of data needed quickly enough to make good risk decisions. But, it's not impossible – it's being done today. With the new levels and types of risk that arise from this remote environment, it is critical to set aside traditional risk assessments and protections and start looking at risk pragmatically. Agencies must take a hard look at existing tools and how they are hamstrung when dealing with remote endpoints - and consider replacing those legacy tools/platforms that fall short.

## About the Author

Egon Rinderer is the Global Vice President of Technology and Federal CTO at Tanium. With 30 years of Federal and private sector industry experience, Egon currently leads the global Enterprise Services Organization as well as leading Tanium Federal as Chief Technology Officer. Joining Tanium at a time when the company was made up of less than 20 employees, he has held roles ranging from Technical Account Manager to Federal Pod Lead to global Vice President of the TAM organization. Prior to joining Tanium, Egon was with Intel Corporation and served throughout the US military and intelligence community in the United States and abroad in an operational capacity. Egon can be reached at egon.rinderer@tanium.com, online at https://www.linkedin.com/in/egon-rinderer/, or at our company website at https://www.tanium.com/solutions/federal-government/


# Can We Better Leverage Our – Already Scarce – Cyber Security Human Resources?

By Douglas Ferguson, Founder & CTO, Pharos Security

It is accepted that there is a significant cyber security skills deficit. The result, it is argued, is that cyber security teams do not have access to the human resources they need to be successful. Therefore, CISOs and security teams cannot effectively protect their organization from cyber breach and impact. Often left unsaid is that cyber security teams often undermine themselves by poorly calibrating and pitching resource requirements and inadequately leveraging available expertise.

Security can be described, in simple terms, like a wall. Where the height corresponds to the level of threat sophistication security can counter, the width corresponds to coverage, and the depth corresponds to types of control (predict, protect, detect, respond, recover). Each of these dimensions strongly influence the costs of a security program – and the ability to control breach outcomes vs. different types and sophistications of attack.

## Not enough expertise

These are two key issues surrounding perceived expertise shortages:

1. The over reliance on high-end expertise
2. The suboptimal leverage of adequate expertise

Countless times I have seen an organization lament the ability to find high-end security experts to anchor and properly design and implement high – believed – priority security controls. Often, when high-profile experts are brought in, these controls become an ivory tower and a significant resource hog usurping resources for less flashy, more commodity, but critical foundational controls. Unfortunately, much more common and commodity skills are deemphasized, and sub optimally leveraged to build out the more mundane, but foundational, security controls.

What has happened in the above case is an over reliance on high-end expertise (as saviours) to compensate for lack of an effective threat and cost calibrated cyber security strategy and unbalanced SecOps. This results in unexpectedly weak overall protection performance, which is why we see, again and again, security breaches at high profile organizations that have lots of security budget, technology, and experts.

It is analogous to many professional sports teams that overspend on a few superstars, to the detriment of having enough budget to pay for supporting players. Because you win as a team, the superstar's value is frittered away when their skill is relied on to carry the team, rather than a cohesive team strategy. The 1980 Olympic hockey Miracle on Ice is a classic example of US teamwork triumphing over the collection of Soviet superstars for the gold medal.

Effective security strategy follows a process like learning to crawl, then walk, then run. You must first be able to control low sophistication threats (like accidents and mischief) before you try to protect against hackers before you then should even consider trying to control espionage and nation states.

The reality is, high-end cyber security expertise is rarely required for the bulk of foundational SecOps implementation and operation; rather, strong planning, threat, resource and cost calibration, project management, and measurement of SecOps KPIs aligned to pragmatic protection goals is what is needed. There is a time for high-end expertise – in initial strategic planning and then advanced tactics – but never to cover up for lack of these.

## Not enough budget

We often experience budget requests denied or reduced because of headcount unit costs, or quantity requested – and sometimes location. How do we justify these costs in a pragmatic way?

The fundamental question to answer is: "What are we trying to achieve?" Because to answer that is to control cost variables. And human resource costs vary by skills sophistication, with more advanced skills being rarer and more expensive. You only need to pay for these when the time is right.

In the eyes of executive leadership – those that ultimately approve budgets - security teams today do an inadequate job calibrating and articulating necessary levels, quantity, and location of specific skills. Because the cost of these skills varies depending on the security wall dimensions introduced above, security budgets are often uncalibrated with overspend and underspend. The conclusion drawn by many

executives is that security is a necessary evil because it is very difficult to measure budget performance and protection outcomes.

## Lack of cyber security 'common sense'

We often hear that 'humans are the weak link in cyber security' – usually meaning that they do 'stupid things' that unintentionally help hackers. Security controls (e.g. people, process, technology) exist to control security outcomes. They are largely intended to control humans from doing something or having access to something. When we blame humans as the weakest link, we are simply pointing out that controls do not effectively control desired security outcomes. Largely, the people to blame here are not the 'general workforce and public' but the security practitioners whose job it is to produce controlled and expected outcomes. And for the challenges of effectively calibrating, gaining access to, and leveraging required skills, they are often the victims of their own vicious cycle.

Programmatic and control cyber security performance is challenged because humans are the weakest link, just not in the way that cyber security experts are pointing their fingers.

### About the Author

Douglas Ferguson, a security professional of over 20 years, is the Founder and CTO of Pharos Security. Pharos specializes in aligning security goals and strategy to the business and a calibrated risk appetite, ensuring an integrated business plan and optimized operations build that to plan and on budget.
Prior to Pharos, Ferguson was with Barclays Bank in London, where he was responsible for numerous security programs and initiatives across more than 40 countries. Previously, Ferguson was a Managing Consultant and researcher on the acclaimed X-Force at Internet Security Systems. He delivered security services to more than 200 clients globally and was a co-creator of the breakthrough System Scanner technology. Douglas can be reached online at dferguson@pharossecurity.com and the Pharos website: https://pharossecurity.com/

# CERT Warns Bad Actors Are Targeting Remote Access – How Security Operations Find and Route These "Below the Radar" Attacks

*New Ransomware/Exfiltration Campaign Targeting Remote Access Resists Resolution Through Data Restoration*

By Saryu Nayyar, CEO, Gurucul

Remote access tools, such as VPN's, RDP, VNC, Citrix, and others, have always been an inviting target for attackers. Even 2003's Matrix Reloaded used an exploit against an old version of Secure Shell (SSH) as a plot device in a rare cinematic example of a real-world cyber-security threat. The recent shift to a remote workforce in response to a global pandemic has made remote access an even more inviting target for threat actors of all stripes.

As a recent report from New Zealand's CERT pointed out, malicious actors are actively focusing on remote access vectors, using a range of attack techniques. While unpatched systems are an ongoing issue, attackers are also targeting weak authentication schemes, including a notable lack of two-factor authentication. The users themselves are also a primary target. Targeted email such as spear phishing, which goes for a specific target, or cast-netting, that targets people within a single organization, have a history of success and have seen a noticeable rise.

Fortunately, information security professionals still have a range of tools and techniques they can use to help prevent breaches and to mitigate them when they do happen.

Many attack scenarios, especially ones involving remote access attacks, start with targeting the users themselves. Many penetration testers will tell you the users are the easiest target and the first thing they'll go after. But this also gives an organization the opportunity to convert their user base from part of the attack surface into their first line of defense. Making sure you have trained them on best practices and have enabled a strong multi-factor authentication scheme can go a long way to preventing unauthorized access.

For many organizations, the Security Operations team, rather than their users, is the main line of defense. Even when the services are provided whole, or in part, by a third party, they are the ones who have the ultimate responsibility for the organization's security well-being. Which means assuring they have the correct tools and the right training is as important as making sure the users are trained and equipped. The question becomes whether they have the right tools and training to identify and mitigate attack profiles that have now shifted to target the remote workforce.

The threats they have been historically focused on have not disappeared, but they may no longer be the primary attack surface. Likewise, the tools they use to identify and mitigate attacks may not be the best ones now that the attacker's focus has shifted.

Threat actors have become increasingly skilled at compromising systems and then hiding their activity "below the radar" to avoid detection, which makes their activity harder to detect. More so now that they have a remote workforce to both target for attack and use for concealment. That means the SecOps team will need to look at the situation holistically rather than relying on single indicators of compromise.

To that end, an advanced security analytics platform that can consolidate all the organization's security data into a single place and then perform AI-based analytics the entirety of the data may be in order. By looking at all the information, it is possible to identify anomalous behavior that differs subtly from what's expected, or accepted, for a normal user. That can be the first indication of a compromise. Using machine learning techniques, the system can adapt to the changing threat surface and present a risk-based assessment to the SecOps team.

Combined with their existing tools and efficient automation, security operations personnel can get ahead of an attack to keep a single compromised account or remote access system from escalating to a serious data breach.

**About the Author**

Saryu Nayyar is the CEO of Gurucul. She is an internationally recognized cybersecurity expert, author and speaker with more than 15 years of experience in the information security, identity and access management, IT risk and compliance, and security risk management sectors. She was named EY Entrepreneurial Winning Women in 2017. She has held leadership roles in security products and services strategy at Oracle, Simeio, Sun Microsystems, Vaau (acquired by Sun) and Disney, and held senior positions in the technology security and risk management practice of Ernst & Young. She is passionate about building disruptive technologies and has several patents pending for behavior analytics, anomaly detection and dynamic risk scoring inventions.

Saryu can be reached on Twitter at @Gurucul


# 4 Simple Ways to Repel Ransomware as The Rise in Remote Work Continues

By Kris Lahiri, Co-founder and Chief Security Officer of Egnyte

Ransomware attacks are now the most common security incident taking place today. According to a recent report from TrustWave, ransomware rates quadrupled in 2019, accounting for one out of every five security incidents and unseating payment card theft as the most prevalent threat category. This spike in ransomware couldn't come at a worse time, as companies all over the world are grappling with many operational and security challenges associated with the coronavirus-induced shift to remote work.

Why is this such a problem? IT and security leaders are generally all too aware of this threat and well-equipped to defend against it in conventional business environments. But with the vast majority of employees working from home, the traditional network perimeter has evaporated and so have many foundational security protections. For a 1,000 person company that's become 100% remote, administrators now have 1,000 mini networks to protect against this onslaught of ransomware attacks instead of one or several – but without the same level of control or defenses. And unfortunately the tried and true method of simply implementing backup and recovery policies to safeguard against successful ransomware infections isn't as practical or realistic with a massively distributed, off-network workforce.

Luckily there are several best practices beyond general endpoint protections and malware defenses that every security administrator can and should implement today to protect remote workers from this threat. Here are four keys to securing your off-network employees and fending off ransomware attacks as the COVID-19 pandemic continues:

1. **Implement ransomware education and training** – According to Verizon, 80% of reported security incidents involve phishing, and according to one report, phishing attacks are to blame for two-thirds of successful ransomware infections in 2019. Although remote employees are not "on their own" as they work from home, they are further away from your skilled IT and security staff and must be trained to independently identify and avoid potential ransomware attacks. Regardless of the size of your organization, invest in educational programs and regular training that teach employees about common ransomware delivery techniques and red flags to watch out for. Better yet, incorporate regular practical tests that entice users into clicking on would-be malicious links or downloads, and provide additional training as needed. Investing in ransomware education and training is well worth it when you consider the potential financial and reputational damage caused by a breach.

2. **Strengthen data access policies** – Now that the majority of your workforce is operating outside the office network perimeter, it's never been more critical to tightly control permissions. Create strict identity and access policies and buttress your access control lists so you can limit employee access to areas of your infrastructure in which you're storing valuable company data and content. Shoring up these policies will allow you to enable or deny permissions by account, user, or based on specific elements such as date, time, IP address, or whether requests are sent with SSL/TLS. Use the principle of least privilege, only giving users access to the accounts, systems and data that's absolutely necessary for them to be productive. This is a crucial step when it comes to ensuring attackers or unauthorized parties can't get access to, delete or expose your business-critical data.

3. **Require multi-factor authentication** – It goes without saying that you should put in place policies that require users to set complex passwords that are 16 characters at a minimum. That said, even strong passwords are no longer enough when it comes to secure authentication. Given enough time, a simple brute force attack can crack highly complex credentials. Deploying a multi-factor authentication solution should be a no-brainer for every organization today, especially with so many employees accessing company data from outside the enterprise perimeter. A second or third authentication factor delivers another critical layer of protection, so that even if an attacker gets their hands on a weak or stolen employee password, they'll be unable to log in and compromise your systems without a physical token, personal smartphone or unique biometric signature.

4. **Reexamine and harden the compute layer** – If you haven't already, now is the time to assess and secure your compute layer to ensure your systems and data remain available and to keep any threat actors that could potentially find a way in through one of many remote entry points from using your resources to spread malware. One easy way to do this is to remove outdated or unnecessary programs from user devices, which just offer additional attack surfaces for bad

actors to target. Ensure that all user devices are updated and patched automatically, or as frequently as possible. While these measures can't provide 100% protection against zero-days, they can significantly reduce your risk. Additionally, take time to adjust your hypervisor firewall rules. This is important because you can manage both ingress and egress traffic to set granular rules for which users can send, receive and access both inbound and outbound data, as well as how much and which types. Setting strict outbound rules is incredibly important here due to the fact that ransomware attacks often threaten to leak confidential company data.

Our research shows that exposure of just a single terabyte of data could cost you $129,324; now think about how many terabytes of data your organization stores today. Most companies end up storing hundreds of thousands to hundreds of millions of files, many of which are highly valuable and critical to business operations. Ransomware attacks continue to wreak havoc on companies of all types and sizes by locking those assets away as leverage for cyber extortion. Even though there are advanced solutions out there that can allow you to simply roll back your environment to a pre-attack state and restore all files to the last unaffected version, a widely distributed workforce can make this much more challenging (and increase the odds of reinfection without the proper preventative measures in place).

As the coronavirus pandemic continues to play out over the coming months, attackers will focus their attention on the many new targets supplied by the burgeoning population of remote workers – just hoping that they're unprepared and unprotected enough to make for easy footholds into your organization. The most effective approach is to prevent ransomware infections before they can inflict damage. Implementing the above best practices today will help you better secure off-network employees if and when ransomware comes calling.

**About the Author**

Kris Lahiri is a co-founder and the Chief Security Officer of Egnyte. He is responsible for creating and implementing Egnyte's global information security and compliance management strategies, policies and controls that protect all of Egnyte's customers' content and users. Prior to Egnyte, Kris spent many years in the design and deployment of large-scale infrastructures for Fortune 100 customers of Valdero and KPMG Consulting. Kris has a B.Tech in Engineering from the Indian Institute of Technology, Banaras, and an MS from the University of Cincinnati. For more information, visit: https://www.egnyte.com.


# Ransomware, Risk, And Recovery

*Why You Need to Take A Hard Look At Your Corporate Recovery Plan*

By Mickey Bresman, CEO, Semperis

What we as IT and security professionals worry about when planning for disaster recovery has evolved over time.

At first, the major concerns were natural (e.g. hurricanes) or man-made (power failure) physical disasters. After 9/11, we included other physical disasters such as airplanes or explosives to the risk list. Today we have COVID-19, which has emptied not datacenters but offices as entire economies have struggled to suddenly work remotely. Along the way, insider-triggered logical disasters – whether deliberately through an angry employee or an "oops" admin mistake – were also added to the list.

In the last couple of years, however, one cyber threat has eclipsed all the others: denial of availability (DoA) malware, including wiperware and ransomware. If you don't update your business continuity / disaster recovery (BC/DR) strategy to be "cyber first" to account for this threat, you're needlessly exposing your organization to potentially catastrophic risk.

Let's look at how the ransomware threat, enterprise vulnerability to this threat, and the threat's impact combine to move it to the top of your BC/DR risk matrix. Finally, we'll recommend action you must take to minimize ransomware's impact to your organization.

## The shape of historic disaster recovery plans

Most historic disaster threats share one characteristic: they can be mitigated with physical or logical distribution or redundancy. East coast data center threatened with a hurricane? Ensure you have a redundant data center in the central US. Worried about power loss? Install a backup UPS for fault tolerance.

Insider logical disasters can be more difficult to recover from than physical disasters, as corruption can spread via the same mechanisms that provide your systems their fault tolerance. But the history of such incidents has shown that these occurrences are relatively rare, companies have mitigating controls in place, and the incident's damage is usually limited.

## The DoA threat

In contrast, the threat of cyber disaster has come to dominate all other threats due to its frequency and massive impact. Wipers like NotPetya, Shamoon, Destover and ransomware such as Petya, WannaCry, and LockerGoga have crippled organizations large and small around the world, encrypting some or all of their IT infrastructure within minutes or hours of a single computer's infection and sending them back to manual operations until (or if) they can recover their systems.

Originating as broadly distributed campaigns, ransomware attacks have evolved into highly targeted and extremely damaging network-wide infections[i]. Cybersecurity Ventures predicts that ransomware damages will cost the world $20 billion by 2021[ii]. In addition to large enterprises, state and local governments have also become targets: 53 were reported in 2018, and at least 70 in 2019 including Baltimore and Atlanta[iii].

## The enterprise vulnerability

Organizations of all sizes are highly vulnerable to ransomware attacks. Phishing, especially targeted (spear) phishing, remains an extremely effective infection vector because it plays on human nature. Microsoft has stated[iv] that phishing maintains an approximately 15% success rate regardless of education programs – even among its own employees.

There's also critical vulnerability well understood by IT professionals that has less awareness up the management chain. Microsoft's Active Directory - the distributed security system that controls user authentication and systems authorization in well over 90% of the world's medium and large organizations – is devilishly hard to restore. Because of this, only a small percentage of companies have a comprehensive, *regularly tested* AD recovery plan. (Look your AD admin in the eye and ask.)

Why, after a product lifetime of almost 20 years, do IT departments not have the same level of recovery plan for AD as they would for a critical file server? Mainly because AD is very robust to both physical domain controller failures and logical failures. But it was designed in the late 90's when no one could conceive of malware that encrypts every single domain controller within minutes.

Under the very best circumstances, it takes days to restore AD in medium to large organizations. All applications that depend upon AD – most of the enterprise, from file servers to physical security systems - cannot be returned to availability until it's restored. And a ransomware attack that has encrypted most of your network is not the best of circumstances.

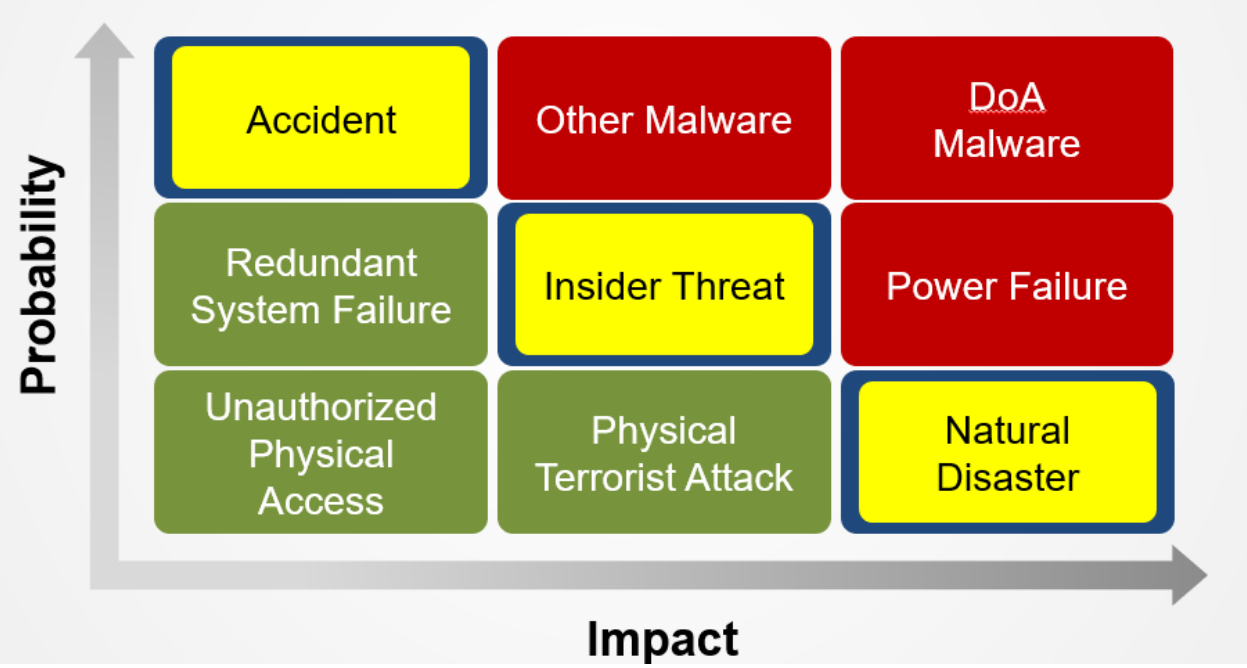
## The devastating impact

Unlike a natural disaster, every computer system within network reach of a malware attack is at risk regardless of its location in the world. But for one African server, Maersk's AD would have been entirely destroyed by NotPetya. That server just happened to be offline due to power failure. Its hard drives were hand-flown from Ghana to IT headquarters in England to begin the AD recovery process, which ultimately took nine days. And most applications couldn't be restored until AD was restored. NotPetya is conservatively estimated to have cost the company $300M and its suppliers much more. In total, NotPetya was estimated to have caused $10 billion damage to organizations worldwide.

A month after they were hit with LockerGoga, 100-year-old Norsk Hydro was still operating most of its 160 manufacturing facilities manually using pre-printed order lists. When all of the computers of Houston County, Alabama were encrypted, the high school principal said, "People are going to learn what it was like 50 years ago, 30 years ago."

## Updated Risk Matrix

Given this new reality, BC/DR professionals must adopt a cyber first mindset for their inherent risk analysis:




*Cyber First BC/DR Risk Matrix*

This updated matrix considers the threat frequency, enterprise vulnerability, and impact of ransomware and other malware.

## Remediating the ransomware risk

How do you lower the risk associated with a ransomware attack? Historically, prevention and detection have been the main defenses against malware, but for ransomware we've already shown these approaches are only moderately effective. Recreating lost data is usually impossible or impractical. Some victims have paid to recover their data, but this is a chancy (and morally ambiguous) approach. Further, data encrypted by worms like NotPetya are unrecoverable.

This leaves recovery as a keystone strategy to minimize the impact of ransomware to your organization. An automated, tested recovery plan for all your critical systems is the best way to minimize the damage inflicted by a ransomware attack. Infrastructure such as Active Directory, DNS, and DHCP must be your top priority because they are foundational to recovering everything else on your network.

Ransomware attacks are the leading cause of organizational IT disruption today. Business continuity and disaster recovery planning need to take this new reality into account and update their risk analysis accordingly. Recovery has traditionally taken a back seat to prevention and detection for malware protection, but today rapid, automated restoration of your systems and data may be the only shield your organization has against corporate Armageddon.

[i] Multiple sources – Microsoft SIR, Verizon, etc.

[ii] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[iii] https://www.recordedfuture.com/state-local-government-ransomware-attacks/

[iv] "Shut the door to cybercrime…" Ignite 2017, BRK3016, 35:45

### About the Author

Mickey Bresman, CEO, Semperis

Mickey is a co-founder of Semperis and leads the company's overall strategic vision and implementation. A long-time enterprise software expert, Mickey began his technical career in the Navy computing technical unit over a decade ago. Prior to co-founding Semperis, Mickey was the CTO of a Microsoft gold partner integration company, YouCC Technologies, successfully growing the company's overall performance year over year. Mickey holds a BA in Technical Management and a Minor in Electronic Engineering.

Mickey can be reached on Twitter at @ber_mic and at our company website http://www.semperis.com/

# Getting Employees Back to the New Normal

*Work will never be quite the same once the pandemic has passed*

By Brendan O'Connor, CEO and Co-founder, AppOmni

There are encouraging signs that the Covid-19 pandemic – arguably the greatest disaster of our generation – is beginning to recede, at least in some parts of the world. While the disarray it provoked throughout the economy is still very much with us, there is reason to believe that a tolerable new normal will emerge – an innovative set of practices representing a tectonic shift away from what normal used to be – in the workplace, in leisure pursuits, and in commerce.

Although the contours of that new normal are still in flux, the experience of the past few months has driven home some durable lessons – lessons we expect will help shape post-pandemic life as recovery gets underway. One of the most apparent is that working from home is almost certain to become an enduring element of employment for millions of workers. That's good, both for the workers and their employers. But it comes with certain caveats.

For starters, I've heard from leaders of several organizations that employees working from home have been asking their companies to slow down the release of new and updated versions of their enterprise software. Learning new software and mastering feature changes, particularly without hands-on personal

guidance, is disruptive, often leading to a surge of help desk calls that can be hard for IT staff, working remotely, to keep up with.

The practical consequences of slowing the rollouts might include accepting longer lives for software versions that would previously have been considered obsolete. It would also argue for greater use of automated instructional software layered atop the enterprise application – software that enables employees to master changes more quickly and with greater confidence.

Another result of the coronavirus outbreak has been an acceleration of information movement from on-site data centers into the cloud – a transition that had already been underway. Cloud-based applications and related data can be readily accessed by people working remotely using just about any kind of digital device, which makes it attractive for homebound workers. And today, public clouds are widely regarded as secure. It is in cloud providers' best interest to ensure the highest security of the application and data to attract more adopters. Increasing adoption of public cloud and transition away from traditional datacenter solutions will be additional added changes in the digital landscape.

Then there's the Big One: security. Data security has always been a focus of IT professionals and frequently a concern to senior management as well. But the explosion of off-site computing resulting from employees working at home, frequently using their own consumer-level digital devices, has made security an imperative. Of course, there was serious concern from the onset of Covid-19 that large-scale work-from-home patterns would present a temptation to hackers. Less effective security in home environments – including network sharing with children and other family members – would make it much easier for criminals to perpetrate fraud or attack unsuspecting users.

As it turns out, those suspicions were right. According to the Wall Street Journal, cyberattacks against banks and other financial firms rose by 238 percent between February and April[1], just as the bulk of their employees began working remotely. At the same time, aggressive furloughing for cost reduction led to a decrease in the number of employees whose regular assignments involved responding to cyberattacks. The problem has been amplified by the government's mass distribution of stimulus funds for individuals and businesses through financial institutions, which play a central role in the pandemic response. Capitalizing on chaos is a familiar pattern for every sort of criminality, and the confusion resulting from the coronavirus response provided a perfect recipe for abuse.

What does that mean going forward into a post-pandemic world? There are, as a report pointed out, various technical steps that would be prudent to take including multi-factor authentication, special controls for certain facility-based applications, and device virtualization. But the primary focus needs to be on people – the system's users.

An indefinitely and perhaps permanently distributed workforce needs to stay aware of how the things they do can either create or abate risks. That means constantly communicating the basics of digital hygiene, possibly engaging a service that focuses on raising user awareness of cyber mischief, along with vigilant monitoring for telltale signs of a security breach. Among the best practices for users:

- Keep business and personal email and other work accounts separate.
- Require the use of multi-factor authentication and ensure such policies are continuously enforced.
- Make sure users know what to do if a device is lost, stolen or compromised.
- Keep processes as simple as possible; when they get complicated, they get ignored.

- Equip IT and security teams with tools for continuous monitoring across multiple SaaS environments.

Of course, there are likely to be other features about the emerging 'new normal' that touch in one way or another on the digital lives of organizations, their employees, and the people they serve. For example, one commentator in Forbes argued that adopting and then complying with a new international cybersecurity regulatory framework – a regimen similar to GDPR or HIPPA – would be timely. Whether the political and economic support for such a regimen will materialize in the U.S. is an open question. But with or without one, the pandemic has given the need to create a secure and resilient digital ecosphere of technology, processes, and people, greater urgency than ever before.


**About the Author**

**Brendan O'Connor – CEO and Co-founder**

Brendan is a 20 year veteran of the security industry. Prior to founding AppOmni, he was Security CTO at ServiceNow. Before joining ServiceNow, Brendan spent 10 years at Salesforce where he led Salesforce's global information security organization as CSO. Prior to his role as CSO, Brendan was VP Product Security at Salesforce. Brendan has also worked in the Financial Services and Communications sectors. His past experience includes work as a vulnerability researcher, security engineer, and privacy advocate. He is passionate about securing the technology that connects the world.

Brendan can be reached on Twitter at @AppOmniSecurity and at our company website https://appomni.com/.


# Security in The New Normal Requires an Agile Approach

By Danny Presten, Chief Methodologist at Digital.ai

Phishing attacks are up 600%, ransomware attacks have increased 148%, and the FBI has reported a 300% increase in cybercrimes. Cyber criminals are stepping up their game during the COVID-19 pandemic and, to ensure safety and security, businesses must do the same.

To keep pace with the ever-increasing threat level and achieve results in the new normal of remote-based working, many organisations are taking an Agile approach. Once thought of as the domain of DevOps, Agile is making its way into DevSecOps, cybersecurity and beyond, and for good reason.

Agile is an iterative way of working that encourages rapidly releasing smaller slices of value as opposed to the long lead in times of larger, traditional projects. In this way, results can be continuously improved as quickly as circumstances change to meet ever evolving business needs. Many companies have benefited from an Agile approach to delivering software and now organisations are expanding those ways of working to include more and more security teams.

Agile offers huge benefits in cybersecurity where security teams are faced with threats that are continually evolving, and bad actors who will look to adjust their methods almost instantaneously to find the best attack vector.

The 14th Annual State of Agile Report explores this uptake and the reasons for it, along with wider issues concerning Agile.

## The importance of Agile

The 14th Annual State of Agile report, based on a survey of more than 1,000 global IT and business professionals, highlights how Agile adoption improves key capabilities needed to respond to current business challenges. Around six in ten respondents said Agile has both helped increase speed to market and improved team productivity.

A follow up survey conducted in mid-May 2020 to learn more about how the COVID-19 pandemic has affected Agile adoption revealed that 55 percent of respondents said their company plans to increase the use of Agile in the next 12-24 months. This is a rise of 13 percent over the original survey completed just five months previously. Additionally, 43 percent of organisations said their momentum for Agile adoption has increased over the past 90 days, with 15 percent saying the increase is significant.

The main catalyst for organisations to adopt Agile comes from wanting to accelerate delivery of value to customers as well as being able to quickly respond to changing circumstances. Indeed, our survey found that the second largest reason for adopting Agile is to enhance the ability to manage changing priorities, with two-thirds (63 percent) of respondents citing this as a key motivator.

This key advantage has led to Agile being adopted in many areas of the business. Software development and IT are understandably the most popular at 37 percent and 26 percent. However, increasingly it is being utilised in operations, marketing, HR and sales. Cybersecurity is no exception as Agile can help security teams combat continually evolving threats.

## The diffusion of Agile principles

The concept of Agile has been around for many years now. It began in the late 2000s with the Scrum framework, which focuses on teamwork, accountability and iterative releases for the development of hardware and software. This was expanded throughout the early 2000s through a variety of scaling frameworks allowing multiple small teams to collaborate effectively on various parts of the product. Today teams collaborate in a variety of ways beyond the traditional face to face interactions with 71 percent of companies reporting teams collaborating across multiple geographies.

As companies began to benefit from increased development productivity, they realised their next bottleneck was actually getting the new product to production. This led to the rise in prominence of DevOps in the middle of the 2010s ushering in an expansion in Agile practices and culture. To that end more than 90 percent of respondents are now placing a high value on DevOps and 75 percent of organisations are actively planning and/or implementing transformation in this area. Organisations going through their DevOps transformation look to achieve accelerated delivery speed (70 percent), improved quality (62 percent) and reduced risk (48 percent). In an increasingly digital world, it's critical to get high quality, valuable software to consumers as rapidly as possible. It's clear that organisations are realising focus in this area is critical for their survival.

As DevOps began to address operational bottlenecks, organisations started to see issues in other areas and have realised they need to look at the entire end-to-end value stream. Value Stream Management

(VSM) helps to decrease time to value by providing a systematic approach for measuring and improving workflow across the organisation through a combination of people, processes, and technologies.

Currently, eight out of 10 respondents said they have an interest in, are planning to implement, or are implementing VSM. Having an end-to-end view of how value flows in an organisation will enable firms to tie actual outcomes to deliveries enabling a much-improved view of value planned and delivered.

The rise of VSM has led to the incorporation of security into the DevOps process, rather than as an afterthought, to create DevSecOps. This approach enables organisations to address security issues during development, reducing cycle time and rework while improving quality and streamlining the workflow. Additionally, this also means the security team now has a seat at the DevOps table and can make sure that the appropriate security is in place as an app is being built, reducing vulnerabilities.

## Challenges implementing Agile

With all the advantages an Agile framework offers, why aren't more businesses fully adopting it? Organisational obstacles can often be considerable. More than 40 percent of respondents report an overall organisational resistance to change, not enough leadership participation, inconsistent practices across teams and an organisational culture that is at odds with Agile values. Even more challenging to note is that these have been top barriers for Agile adoption consistently for more than five years.

It's critical that leadership understands the principles that make an Agile ecosystem work and take effort to bring about the necessary organisation change to harness their benefit.

Making Agile a success relies on implementing proven practices and principles that are executed through a culture immersed in this way of working. Increasingly we're seeing management learn and own those core Agile values. While it's obvious there is more work to do it's encouraging to see movement as an organisation's success depends on it.

Coping with increasingly sophisticated bad actors while simultaneously working through the new realities brought on by the pandemic require an organisation that can pivot at a moment's notice. Those organisations leveraging an Agile approach are better able to respond to changing conditions, maintain quality and security, and provide solutions that bring value to their customers.

**About the Author**

Danny is Chief Methodologist at Digital.ai. He has several transformation tours of duty behind him in which he's worked in agile organisations, consulted with senior leaders and led training initiatives. He is an entrepreneurial self-starter with over 20 years' experience successfully addressing complex delivery challenges in a variety of industries including web development, e-commerce, healthcare, nonprofit, supply chain, and legal.

Danny can be reached online at can be reached online at https://www.linkedin.com/in/danny-presten-3b5b413/ and at our company website https://digital.ai/


# Why Are Fully Staffed Cybersecurity Teams Unable to Keep Up with Hacks?

By Steve Salinas, Head of Product Marketing, Deep Instinct

Faced with mounting cyber threats, large enterprises are devoting more resources than ever to improving their cybersecurity posture. According to a Cisco survey released last fall, 93% of enterprises with 10,000 or more employees spend more than $250,000 annually on cybersecurity, with half spending over $1 million each year.

The return on those investments leaves much to be desired. A 2019 report from Accenture and the Ponemon Institute found that security breaches had increased 11% since 2018 and had spiked 67% since 2014. Some experts ascribe the problem to woefully understaffed cybersecurity teams – but even fully staffed, highly experienced cyber teams are encountering hacks they can't fully prevent or contain.

The real culprit isn't necessarily the size of the typical organization's cybersecurity staff, but the outdated tools and operational methodologies many of these teams use. As hacks grow more frequent and more complex, organizations should rethink the tools and technologies they're using to meet the threat.

## The Rising Cost of Failure

How much is cybersecurity costing companies? In a recent Ponemon-Deep Instinct survey of IT and IT security practitioners, only 40% of respondents believed their budgets were sufficient for achieving a robust cybersecurity posture.

These budgets are predominantly funneled into containing and remediating threats rather than preventing them – in large part because cyber staff are overwhelmed with the amount of data that they need to monitor. Yet this "assume a breach and then contain" approach comes at a big cost, with the time and money spend remediating attacks costing well into the hundreds of thousands of dollars. The value of preventing a cyber-attack ranges from $400,000 to $1.4 million, depending on the nature of the attack. If an attack is the first of its kind, it's virtually guaranteed to succeed with absent strong preventative capabilities, and organizations stand to lose upwards of $1 million per successful attack.

## Subpar Solutions, Subpar Results

Why are current approaches to cybersecurity proving so inadequate? Because they over-rely on the human intervention.

Specifically, most AI-based cybersecurity solutions are powered by traditional machine learning (ML), which is inhibited by a number of limitations that have become substantial problems in the recent past. Chief among these limitations is data: ML models are trained on only a fraction of the available raw data, and are trained on features identified by experts.

Human error, of course, also comes into play, even when highly specialized computer scientists with expertise in cybersecurity carry out ML feature engineering. These professionals excel at training ML models on known threats – but even seasoned cybersecurity professionals are unable to anticipate emerging, first-seen attacks, that are designed to be evasive. Hackers of course, understand this, which is why they now building malware that is capable of fooling ML models into classifying it as benign.

Finally, there's a limit to the size of the dataset for training ML systems before reaching learning curve saturation – the point past which the system no longer improves its accuracy.

Given these limitations, ML systems struggle to detect new, previously unseen malware, while generating high rates of false positives. Just as the cost of an unprevented attack can deliver a real blow to the bottom line, the time and resources required to investigate false positives also strains security teams' resources. This, in turn, breeds a sense of "alert fatigue," making teams more prone to error when genuine threats emerge.

Simply put, AI trade-offs – not understaffed cybersecurity teams – may be one of the biggest inhibitors to achieving a resilient cybersecurity posture.

## AI-Powered Hackers and the Increased Pace of Attacks

Compounding the challenges posed by flawed cybersecurity solutions, hackers are increasingly leveraging automation to diversify their attacks and execute them at an accelerated pace. The AV-Test Institute found that over 350,000 new malware are generated every day and networks regularly experience thousands of security events daily– making it all the more difficult for human security professionals to sift through all potential threats. Even the largest, most skilled cybersecurity teams can't be expected to handle this load. And when cybersecurity teams successfully detect a threat, they often run out of time to respond before hackers have already caused substantial damage.

Take the 2019 Equifax data breach. In the wake of the breach, Equifax's security team worked 36-hour shifts, which the company's CISO acknowledged had come at a great cost to the team's mental health.

On average, it takes 191 days – half a year – to identify an attack. Without the luxury of months to spare, how should organizations adjust their cybersecurity approach?

## A Cyber Paradigm Shift

In the short term, adding more cyber professionals to IT teams can help – but even a large and experienced team won't be able to compensate for subpar security tools.

Because today's hackers are operating autonomously, cyber solutions need to do so, as well. Such solutions require minimal staff intervention, enabling teams to triage potential security events and prevent time wasted on false positives. Deep learning-based autonomous solutions also offer powerful capabilities for detecting and preventing attacks *before* they are executed – potentially helping organizations save millions.

It's little wonder, then, that two-thirds of IT and IT security leaders believe that using automation and advanced AI like deep learning, will improve their ability to prevent attacks and that they plan to implement these solutions within the next two years.

While beefing up staffing isn't a panacea, implementing autonomous solutions isn't about putting cyber professionals out of work. Instead, it's about putting their essential skillset towards more efficient and strategic use while simultaneously tightening and improving existing cybersecurity measures.

The dizzying pace at which today's cyber threats are evolving underscores the need for a cyber paradigm shift that emphasizes autonomous protection and attack prevention. Humans alone can't combat the hyper-efficient machines hackers are employing. Only when malicious actors' sophisticated technology is met by even *more* sophisticated technology, will organizations achieve resilient protection.

## About the Author

Steve Salinas is the Head of Product Marketing at Deep Instinct.

**Steve Salinas is Head of Product Marketing for Deep Instinct, a leading provider of deep learning-based cybersecurity solutions.** His experience includes holding product management, product marketing, and solution engineering positions with leading security vendors, including Guidance Software (now OpenText), Alert Logic, Siemplify, and Cylance. He is a frequent presenter at industry conferences, podcasts, and regularly publishes blogs aimed at providing both business and technical insights to the security community. Steve went to Texas A&M University for undergrad and earned an MBA from Pepperdine University. Steve lives in Huntington Beach, California. Steve can be reached online at @so_cal_aggie and at the company website https://www.deepinstinct.com/.

# Looks Like Russian Hackers Are on An Email Scam Spree

By Tim Sadler, CEO, Tessian

In 2019, businesses lost a staggering $1.8bn because of Business Email Compromise (BEC). These types of attacks, whereby a trusted relationship is compromised through email impersonation or email account hacking, are becoming more common and also more successful. The reason? First, they are easier and cost-effective to carry out, making such attack methods attractive and lucrative for cybercriminals. Second, to improve the success rate of their scams, hackers are making it much more difficult for their victims to detect that they are being targeted.

In fact, just recently, researchers identified a cybercriminal gang called Cosmic Lynx that has carried out more than 200 BEC campaigns since July last year, in attempts to steal as much as $2.7m from Fortune 500 or Global 2000 companies. Believed to be the first reported case of a BEC gang operating from Russia, the group delivers sophisticated and creative email campaigns that target senior executives, tailoring their messages to discuss legitimate mergers and acquisitions.

## Why Cosmic Lynx is cause for concern

BEC scams are not, traditionally, this group's method of attack. However, as BEC offers a lucrative opportunity to steal millions of dollars in just a few emails, it appears that this Russian cyber gang is changing its tact.

One of the defining characteristics of Cosmic Lynx's campaigns is that they are far more sophisticated than generic phishing scams. This is a well-researched operation, run by experienced hackers who have clearly done their homework. The hackers investigated companies that were completing an acquisition, identified a senior executive target, and impersonated the CEO of the target company in order to deceive their victim into wiring money to a fraudulent account.

To add another layer of perceived legitimacy, the hackers also impersonated an external lawyer at a well-regarded law firm to "facilitate the payment", making it very difficult for the target to think that they are being scammed. Finally, the hackers ensured a high level of quality and diligence in their campaigns, paying particular attention to brands' details, and making sure grammar and spelling were without error.

Social engineering campaigns like this can be devastating to businesses, and anyone in an organisation can fall for the scams. As hackers up their game, businesses need to ensure all employees are aware of the threats in their inboxes and consider whether they have the security measures in place to detect the deception before it's too late.

My company has DMARC so I should be protected against email impersonation, right?

Implementing Domain-based Message Authentication, Reporting & Conformance (DMARC) is a necessary first step for businesses to prevent hackers spoofing your company's domain in its email attacks. Without it, an attacker can directly impersonate your company's domain and users will think they are receiving an email from a legitimate (and trusted) source.

In the particular case of Cosmic Lynx, researchers found that the group has a strong understanding of DMARC and analyses the public DMARC records to select its targets and methods of attack. The problem is that, as DMARC records are publicly available, it's very easy for hackers to identify companies that do not have email authentication protocols in place, allowing them to directly impersonate a company's domain and pose as the CEO.

But even if your company does have a DMARC policy in place, attackers can also assess how strictly you've configured it. If your company has a strict email policy in place, the attacker can still carry out an advanced spear phishing attack by registering a look-a-like domain, banking on the fact that a busy employee may miss the slight deviation from the original domain. This highlights why companies cannot rely on the email authentication protocol as a silver bullet to prevent email impersonation scams.

The other problem is that while your organisation might have DMARC in place, your external contacts may not. This means that while your organisation's domain is protected against direct impersonation, your employees may be vulnerable to impersonation of external contacts like partners, customers or lawyers. Again, this knowledge has worked to Cosmic Lynx's advantage; they impersonated external lawyers from real UK law firms to add another layer of legitimacy to their scams.

## How do I protect my company from BEC?

Of course, security teams put rules and policies in place to stop malicious messages landing in inboxes but, as we've seen, hackers find ways around these rules. Another solution is to train employees on the threats. And security training helps to raise awareness, but solely relying on training means relying on your employees to spot every scam and every threat. This is unrealistic; businesses cannot expect busy and stressed employees to get it right 100% of the time, especially when hackers make their deceptions so difficult to detect.

To prevent BEC attacks, you need to detect the impersonation but it's a difficult problem to solve. To accurately detect it, you need to understand what is being impersonated. You need to be able to answer the question, "for this user, at this point in time, given this context, is the sender really who they say they are?".

Machine learning can help, though. By using machine learning algorithms to analyse historical email communications and understand each and every employees' relationships over email, you can start to build a picture of normal (and abnormal) behaviour. When an employee receives an email that looks out of the ordinary, they can be alerted in real-time to the threat and given advice on what to do next.

The example of Cosmic Lynx has shown that more and more cyber-criminal gangs are turning to BEC to achieve their objective of scamming businesses out of hundreds of thousands of dollars. Companies need an advanced, multi-layered solution to this increasingly sophisticated problem. By using machine learning to protect people on email, and by solving the problem at the human layer, businesses can start to tackle the rising threat of BEC.


**About the Author**

Tim Sadler, CEO, Tessian

Tessian is building the world's first Human Layer Security platform to automatically secure all human-digital interactions within the enterprise. Today, our products use stateful machine learning to protect people using email and to prevent threats like spear phishing, accidental data loss due to misdirected emails, data exfiltration and other non-compliant email activity. We've raised $60m from legendary security investors like Sequoia and Accel and have over 150 employees located in New York and London.

https://www.tessian.com/

# TLS/ SSL Decryption – One of the Main Pillars of Zero Trust Model

By Adil Baghir, Technology Consultant Lead, Middle East & Africa at A10 Networks

In a world where everything and everyone is connected to the internet, in one way or another, it's hard to imagine a network that is truly secure. Data, large amounts of it, are at the centre of it all. With industries from healthcare to the education sector to the government using the internet to provide easy access to data, it is no wonder that cybersecurity teams are always working around the clock to try and come up with better ways of defending these networks and the data they store.

## Insider Threats – Need for Security to Evolve from "Castle and Moat" Approach

Modern cyberattacks are not limited to just network intrusion from the outside. Internal threat actors can often be found at the centre of sophisticated attacks.

Initially, we had the concept of zones, perimeters and network segments – placing all the protected assets "inside" the secured network perimeter. However, attackers are always evolving the methods they use; always on the lookout for weak points in your network defences; and coming up with newer ways of infiltrating the perimeter. Keeping up with them is a challenging and ongoing struggle. We also need to realize that the "castle and moat" approach to our network defences was mostly effective against threats that resided outside the network. But what about the threats on the inside? What about modern attacks that work on multiple levels to try to bring your networks down? How do we protect our networks from people who have legitimate access to all its resources? How do we battle the ever-growing and ever-evolving modern cyberattacks? Add to these questions, regulations like GDPR, and the rising fines, and you will see that having your networks attacked and data breached is one of the worst things that can happen to your company. With these issues as the backdrop, we are forced to re-assess and re-think the way we defend our networks, users and data.

## Zero Trust Model – a Modern Cybersecurity Approach

Zero Trust attempts to fix the problems, and patch the holes, in our cybersecurity strategies. At the core of it, the Zero Trust model is based on the principal of "trust nobody." The Zero Trust model dictates that no one in your network should be trusted completely, that access should be restricted as much as possible, and that trust should be seen as yet another vulnerability that can put your network at risk.

Some of the precepts of the Zero Trust model are:

- Networks need to be redesigned in a way that east-west traffic and access can be restricted.
- Incident detection and response should be facilitated and improved using comprehensive analytics and automation solutions, as well as centralized management and visibility into the network, data, workloads, users and devices used.
- Access should be restricted as much as possible, limiting excessive privileges for all users.
- In multi-vendor networks, all solutions should integrate and work together seamlessly, enabling compliance and unified security. The solutions should also be easy to use so that additional complexity can be removed.

## Danger of Security Blind Spots

In recent times, we have witnessed a phenomenal rise in the use of encryption across the internet. Google reports that over 90 percent of the traffic passing through its services is encrypted. The same is true for all the other vendors. This rise has been driven by many factors, including privacy concerns.

However, with encryption comes the creation of a "blind spot" in our network defences as most of the security devices we use are not designed to decrypt and inspect traffic. The Zero Trust model is not immune to this problem as visibility is considered as one of the key elements to its successful implementation. Without complete encrypted traffic visibility, the model will fail, introducing vulnerabilities that can be exploited by both insiders and hackers.

## TLS/SSL Decryption – One of the Main Pillars of Zero Trust

A centralized and dedicated decryption solution must be placed at the centre of the Zero Trust model and should be included as one of the essential components your security strategy.

Many security vendors will make claims of the ability to decrypt their own traffic, working independently of a centralized decryption solution. However, this "distributed decryption" approach can introduce problems of its own, including inferior performance and network bottlenecks, and fixing these would require costly upgrades. In a multi-vendor, multidevice security infrastructure, the distributed decryption also forces you to deploy your private keys in multiple locations, creating an unnecessarily large threat surface in your network, which could be subject to exploitation.

## Key features of a good TLS/ SSL Decryption Solution

It is important that a dedicated, centralized decryption solution provides full visibility to the enterprise security infrastructure for TLS/SSL traffic. Not only that, but the solution also needs to provide a multi-layered security approach, which then makes it the perfect candidate to be deployed at the centre of a Zero Trust network.

Below are some of the features to look out for when looking to implement a TLS/ SSL Decryption Solution:

- **Full Traffic Visibility** – It needs to enable the entire security infrastructure to inspect all traffic in clear-text, at fast speeds, ensuring that no encrypted attacks or data breaches can slip through
- **Ease of Integration** – It should be vendor agnostic and easily integrate with security devices already deployed within the network. This drives down additional costs and upgrades.
- **Multi-Layered Security Services** – These are additional security services, including URL filtering, application visibility and control, threat intelligence and threat investigation, that help strengthen the security efficacy of the entire enterprise network
- **User Access Control** – The product should be able to enforce authentication and authorization policies to restrict unneeded access, log access information and provide the ability to apply different security policies based on user and group IDs.
- **Micro Segmentation** – It should facilitate micro-segmentation through its ability to provide granular traffic control, user and group ID-based traffic control, and support for multi-tenancy
- **Securing Cloud Access** – SaaS security is an important feature which can be provided by enforcing tenant access control and visibility into user activities.

In conclusion, without a centralized and dedicated TLS/SSL decryption solution, the Zero Trust model is unable to do what it was designed to do – protect our networks, users and data from threats residing inside and outside the network.


### About the Author

Adil Baghir is Technology Consultant Lead for Middle East & Africa at A10 Networks. He is a security and networking specialist having worked for tech powerhouses like STC, Mobily and Applied Technologies Company.

Adil can be reached online at (abaghir@a10networks.com) and at our company website https://www.a10networks.com/


# Build Your AI Incident Response Plan… Before It's Too Late

By Patrick Hall* and Andrew Burt**


** Patrick Hall is principal scientist at bnh.ai, a boutique law firm focused on AI and analytics, and an adjunct professor in the Department of Decision Sciences at GWU.*

*** Andrew Burt is managing partner at bnh.ai and chief legal officer at Immuta.*


Artificial intelligence can fail. It can also be attacked. When a failure or attack spins out of control, this is a major AI incident. There have been over 1,000 public reports of AI incidents in recent years. Yet many organizations are operating nascent AI efforts without incident response plans - using AI, in other words, without any clear understanding of what to do when it fails.

Why? Organizations simply aren't thinking about AI failures, they're focused on AI successes instead. Indeed, there's a great deal of hype on the positive side of this technology, and deservedly so. It can make and save money, and it can even be transformational. However, AI is probably more likely to fail than traditional enterprise software, at least as of today. It's for this reason that some have called the technology the "high-interest credit card of technical debt." Governments around the world are

increasingly interested in enforcing best practices for AI. And numerous damaging attacks against AI systems have already been published in machine learning and security research journals.

Our bet is you'll be hearing more about AI incidents in the coming years. Below, we'll go over why AI is (and is not) different from more traditional software systems, some of the primary lessons we've learned writing AI incident response plans, and we'll introduce the free and open bnh.ai Sample AI Incident Response Plan to help you make your organization better prepared for AI incidents.

How AI Is (and Is Not) Different

What's so different about AI? Basically, it's much more complex than traditional software, it has a nasty tendency to drift toward failure, and it's often based on statistical modeling. What does that really mean?

**More complexity:** For starters, AI systems can have millions or billions of rules or parameters that consider combinations of thousands of inputs to make a decision. That's a lot to debug and it's hard to tell if an AI system has been manipulated by an adversary.

**Drift toward failure:** Most AI systems are trained on static snapshots of the world encapsulated in training datasets. And just in case you haven't noticed, the world is not a particularly static place. As the world changes, the AI system's understanding of reality becomes less and less valid, leading to degrading quality of decisions or predictions over time. This is known as "model decay" or "concept drift," and it applies to nearly all current AI systems.

**Probabilistic outcomes:** Most AI systems today are inherently probabilistic, which means that their decisions and predictions are guaranteed to be wrong at least some of the time. In standard software, wrong outcomes are bugs. In AI, they are features. This makes testing and establishing tolerances for failure more difficult.

The combination of these three characteristics present a number of testing difficulties, potential attack surfaces and failure modes for AI-based systems that often are not present in more traditional software applications.

## If that's what's different, then what's the same?

In the end, AI is still just software. It's not magically exempt from the bugs and attacks that plague other software, and it should be documented, tested, managed, and monitored just like any other valuable enterprise software asset. This means that AI incident response plans, and AI security plans more generally, needn't reinvent the wheel. Frequently they can piggyback on existing plans and processes.

## What We Learned About AI Incident Response

Drafting AI incident response plans has been eye-opening, even for us. In putting to paper for our customers all the various ways AI can fail and its many attack surfaces, we've learned several big lessons.

## Neither MRM Nor Conventional IR is Enough

The basics of our AI incident response plans come from combining model risk management (MRM) practices, which have become fairly mature within the financial industry, with pre-existing computer incident response guidance and other information security best practices. MRM helps protect against AI failures. Conventional incident response provides a framework to prepare for AI attacks. These are both great starts, but as we detail below, a simple combination of both is still not quite right for AI incident response. This is why our Sample AI Incident Response plan includes guidance on both MRM and traditional computer incident response, plus plans to handle novel AI risks in the context of the burgeoning AI regulation landscape in the US.

MRM practices, illustrated in, among other places, the Federal Reserve's Supervisory Guidance on Model Risk Management, known as SR 11-7, are an excellent start for decreasing risk in AI. (In fact, if your organization is using AI and is not familiar with the SR 11-7 guidance, stop reading this article and start reading the guidance.) Broadly, MRM calls for testing of AI systems, management of AI systems with inventories and documentation, and careful monitoring of AI systems once they are deployed. MRM also relies on the concept of "effective challenge" - which consists of models and processes being questioned and reviewed by humans in multiple lines of technology, compliance, and audit functions. However, MRM practices do not specifically address AI security or incident response, and they often require resources not available to smaller organizations.

We'll address incident response for smaller organizations in the next section, but from an information security perspective, traditional incident response guidance is helpful - though not a perfect fit. For instance, AI attacks can occur without traditional routes of infiltration and exfiltration. They can manifest as high usage of prediction APIs, insider manipulation of AI training data or models, or as specialized trojans buried in complex third-party AI software or artifacts. Standard incident response guidance, say from SANS or NIST, will get you started in preparing for AI incidents, but they also weren't specifically designed for newer attacks against AI and could leave your organization with AI security blindspots.

## When Going Fast and Breaking Things Goes Wrong

MRM practices require serious resources: lots of people, time, and technology. Standard MRM may not be feasible for early-stage or small organizations under commercial pressure to "go fast and break things." Common sense indicates that when going fast and breaking things, and without conventional MRM, AI incidents are even more likely. With AI incident response, smaller organizations without the capability for heavy-handed supervision on the build side of AI can spend limited resources in a manner that allows them to stay agile while also confronting the reality of AI incidents.

## Attitude Adjustments

There is a lot of hype surrounding AI and the profession of data science. This hype, coupled with lax regulatory oversight has led to a wild west of AI implementations that can favor the kitchen sink over the scientific method.

A hype-driven sense of entitlement can sometimes lead to friction and resistance from front line AI practitioners. We've found that some practitioners are unwilling or unable to understand that, despite their best intentions, their AI systems can fail, discriminate, get hacked, or even worse. There's not much to say about this except that it's time for the commercial practice of AI to mature and accept that with increasing privilege comes increased responsibility. AI can, and is already starting to, causes serious harm. As of today, compliance, legal, security and risk functions in large organizations may have to make manual attitude adjustments, and insist that AI groups are subject to the same level of oversight as other IT groups, including incident response planning for AI attacks and failures.

## Don't Deploy AI Without an Incident Response Plan

The final takeaway? AI is not magic -- meaning organizations can and should govern it. If AI is the transformative technology it is hyped to be (and we do believe it is), then deploying AI with no incident response plans is a recipe for disaster. After all, we don't fly commercial jetliners without detailed plans for systems failures; we don't run nuclear reactors without emergency plans; if the activity is important to us, we think and plan in advance about its risks.

And that means we also need to be prepared for AI to fail. Having an AI incident response plan in place can be the difference between an easily manageable deviation in AI system behavior and serious AI-driven harm and liabilities.

## About the Authors

**Andrew Burt** is managing partner at bnh.ai, a boutique law firm focused on AI and analytics, and chief legal officer at Immuta. He is also a visiting fellow at Yale Law School's Information Society Project.

Previously, Andrew was Special Advisor for Policy to the head of the FBI Cyber Division, where he served as lead author on the FBI's after action report on the 2014 Sony data breach, in addition to serving as chief compliance and chief privacy officer for the division.

A frequent speaker and writer, Andrew has published articles on law and technology for the New York Times, the Financial Times and Harvard Business Review, where he is a regular contributor. He holds a JD from Yale Law School.

**Patrick Hall** is principal scientist at bnh.ai, a boutique law firm focused on AI and analytics. Patrick also serves as an advisor to H2O.ai and as an adjunct professor in the Department of Decision Sciences at The George Washington University.

Before co-founding bnh.ai, Patrick led H2O.ai's efforts in responsible AI, resulting in one of the world's first widely deployed commercial solutions for explainable and fair machine learning. He also held global customer-facing roles and R&D research roles at SAS Institute. Patrick studied computational chemistry at the University of Illinois before graduating from the Institute for Advanced Analytics at North Carolina State University.

# Why Academic Openness and A Rise in Online Classes Should Invoke A Renewed Focus on Security

By Anthony Bettini, CTO, WhiteHat Security

For decades, researchers and students from around the world have come to study and collaborate, research and innovate at American universities and colleges under the auspices of academic openness at our schools. Unfortunately, that academic openness has resulted in universities and colleges becoming attractive targets for nation-state hackers, cybercriminals, and reportedly, espionage operations. Part of the reason for this could be because these institutions possess massive amounts of valuable data, as well as vital information pertaining to government projects and research, personal data of students and professors, financial and health information and much more.

While higher education has been gradually increasing the number of online classes, the recent global pandemic has accelerated the process dramatically. Now, universities and colleges have had to quickly procure or build additional applications to accommodate distance learning and deliver to their students the same quality educational experiences they would have previously had on campus and in person. The emergency transition to online classes for students this past spring and the uncertainty for the upcoming fall adds to risks for security vulnerabilities and compounds the stress for IT administrators, who are responsible for safeguarding staff and student privacy.

In fact, New York City-based security analytics firm Security Scorecard ranked education last among 17 major industries for cybersecurity preparedness. This lack of vigilance is further illustrated by the increasing number of cybersecurity-related incidents at higher education schools in recent years. For example, Harvard University, Stanford University, University of Connecticut, Oregon State University and many others are reported to have all experienced security breaches of varying degrees.

## Make Application Security a Priority

One of the first and easiest steps to ensuring that security remains a priority, either on or off campus, is to focus on application security.

For some time now, universities and colleges have used software applications in the classroom and throughout the campus experience to aid students, professors, researchers and visitors in their work. However, the current global health concerns have forced many schools to re-examine remote education tools and implement new applications, to augment distance learning capabilities amid uncertainty. This is especially true for schools that plan for classes to remain online-only in the fall. Under the high-pressure circumstances of managing expectations for professors, students and even parents, it might be easy to overlook proper security protocols in the technology, when preparing for a non-typical college experience. There are several causes of this security oversight, and not all of the responsibility falls on the universities. Sometimes, software vendors cut corners in the software development process, and that can result in vulnerabilities that are easy for hackers to exploit within applications.

## Applications Need Rigorous Testing Before Deployment

Most higher education institutions rely on a mix of in-house and third-party applications for instruction including Blackboard, Canvas and others. Regardless of where or from whom the applications are sourced, they must be rigorously tested for vulnerabilities and exploits before they are deployed for use at the university.

To know if an application has been properly tested and secured, university IT teams should thoroughly research the products the universities are considering for use and understand the apps as much as possible. If they are confident in the development process used and are assured that appropriate testing and scanning was completed with dynamic application security testing (DAST), static application security testing (SAST), and software composition analysis (SCA), that is a step in a positive direction. Any failure to properly test and secure applications will undoubtedly leave students, professors, administration and university property vulnerable to exploits and hackers.

## Security Training for Students

Another priority to securing a university or college is educating the students and faculty about common practices used to launch cyberattacks on applications and campus networks. These include phishing attacks, human error, and techniques like formjacking. Most, if not all schools, offer an orientation for new students, and an orientation session just might be a perfect opportunity to highlight cybersecurity risks and help students to understand how to safeguard themselves and their personal data from any attempts by malicious actors to gain unauthorized access to campus applications.

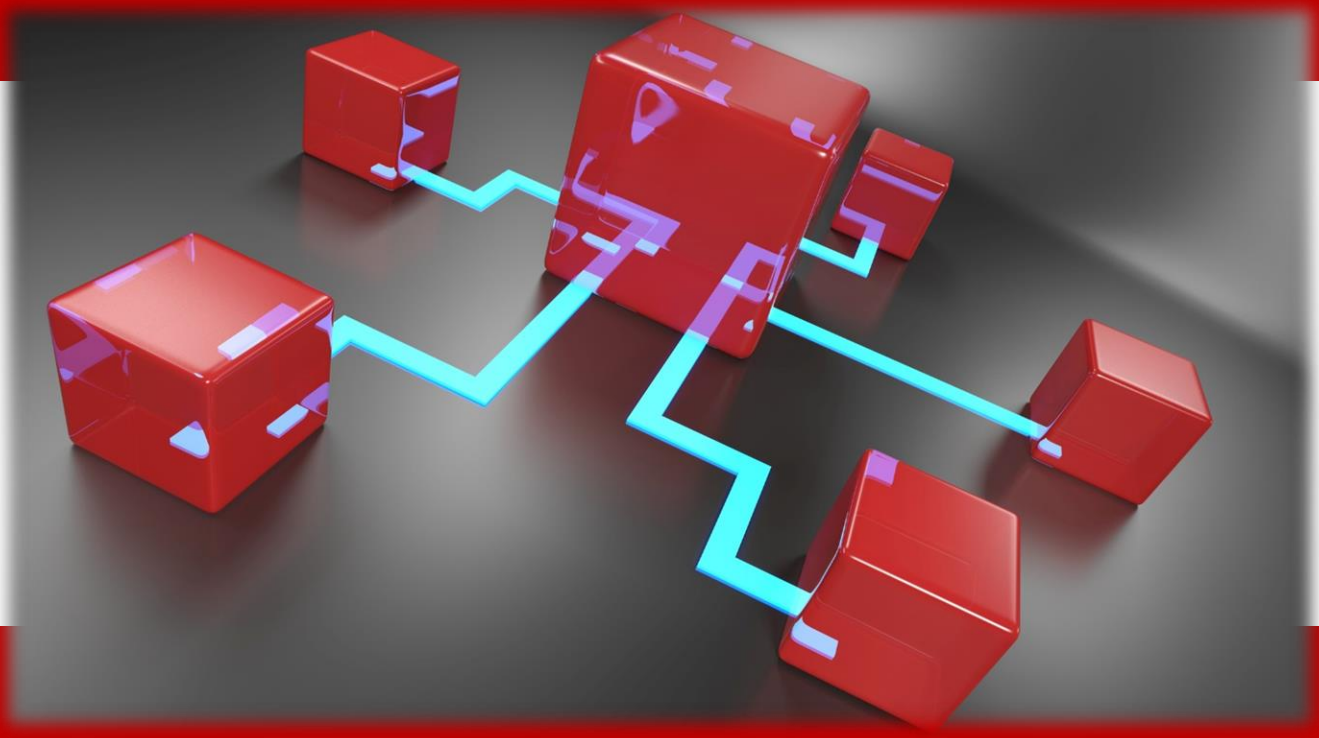
Of course, it is always a good idea to remind returning students of the practical security measures to protect themselves. To be sure all students are helping to prevent data exposure or cyberattacks, these reminders can be given via an informative video shown during class, or perhaps as a required gate for the class registration process.

## Share the Responsibility of Security

No matter the circumstance, application security must not take a backseat when developing applications for use in higher education systems. Similar to the concerns for K-12, higher education institutions must share the responsibility for security in the applications they use. This means investing time and resources into ensuring that the tools, software programs and applications are safe and secure, and free of known vulnerabilities and exploits.


**About the Author**

Anthony Bettini is the CTO for WhiteHat Security, the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. Previously, Anthony ran Tenable Research where he joined via Tenable's acquisition of FlawCheck – a leading container security startup where he served as the CEO & founder. Before its acquisition by Symantec, Anthony was CEO & founder of Appthority, a leading mobile security startup and winner of the "Most Innovative Company of the Year" award at the RSA Conference.

# Is API Usage Putting Your Organization Out of Compliance?

By Matt Keil, Director of Product Marketing, Cequence Security

APIs ("Application Programming Interfaces") are increasingly being used as the conduit for data exchange between applications, infrastructure, and IoT devices. The recent explosion in cloud usage and the urgency around digital transformation and creation of mobile apps has caused a steep increase in the dependence of APIs as a way to speed and simplify development efforts. Today, most organizations expose multiple APIs to customers and partners, published from different product teams, different application stacks, and following various DevOps and security procedures, oftentimes, without consistent security or compliance oversight. According to Gartner, by 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 2019.

When secured, APIs are a smart way to interconnect endpoints and systems to transmit data and deliver critical features and functionality. But, when published outside of your normal process (if you have one), and left unprotected or misconfigured, they give hackers easy access to large volumes of data, and make it easier to commit fraud and expose private data by automating actions normally done by humans through web forms. In the end, the API provides the same benefits – ease of use, efficiency and flexibility – to both developers and bad actors.

It's important that compliance, privacy, and risk professionals dig deeper to understand the usage of APIs across the organization, and gain insight into the vulnerabilities that exist so that risk can be measured

and mitigated. Unfortunately, the fragmented API management space, along with an increase in decentralized development, has created a situation where most enterprises lack even the most basic understanding of their API landscape. According to Aite Group, the organizations have an average of 620 APIs – do you know where they all are, who owns them and what they do?

Gaining visibility into your API footprint in the form of inventory, usage, potential vulnerabilities and specification conformance is vitally important to understand the overall exposure and compliance impact created by APIs in use. Some questions that every organization should be able to answer (but rarely can) include the following:

- How many APIs do we have? What applications are these APIs used by or associated with?
- How many were sanctioned by security and how many are “shadow” or unknown APIs?
- Are they all necessary for operations or were deployed inadvertently or forgotten about after they were no longer necessary?
- Which ones are not actively managed or monitored? Do they have traffic? Is the traffic expected, or do patterns suggest misuse?
- How many APIs have vulnerabilities or don’t conform to approved API specifications? Do we have any hidden API headers, parameters or response codes?
- Is there PII or sensitive data being transmitted through APIs unencrypted? Is access regulated data limited in a way that will keep us in compliance?

Unfortunately, too many organizations get answers to these questions the hard way – when they are breached. For example, an API might expose too much information when a request is made providing attackers with insights, they can use to further breach a system. Or, an API might completely lack proper access authentication or inadvertently grant users with elevated privileges (like giving them Admin rights) which could be used to exfiltrate or change the data.

"The hallmark of cyber attackers is they are always searching for a path of least resistance. The expanding use of public facing APIs, especially those that are unknown, coupled with the lack of security associated with those APIs make them a prime target," says Charles Kolodgy, Principal at Security Mindsets LLC. "It is important for organizations to know what APIs are used by the website, especially shadow APIs, in order to secure them thus making it more difficult for cyber criminals to achieve their end goal."

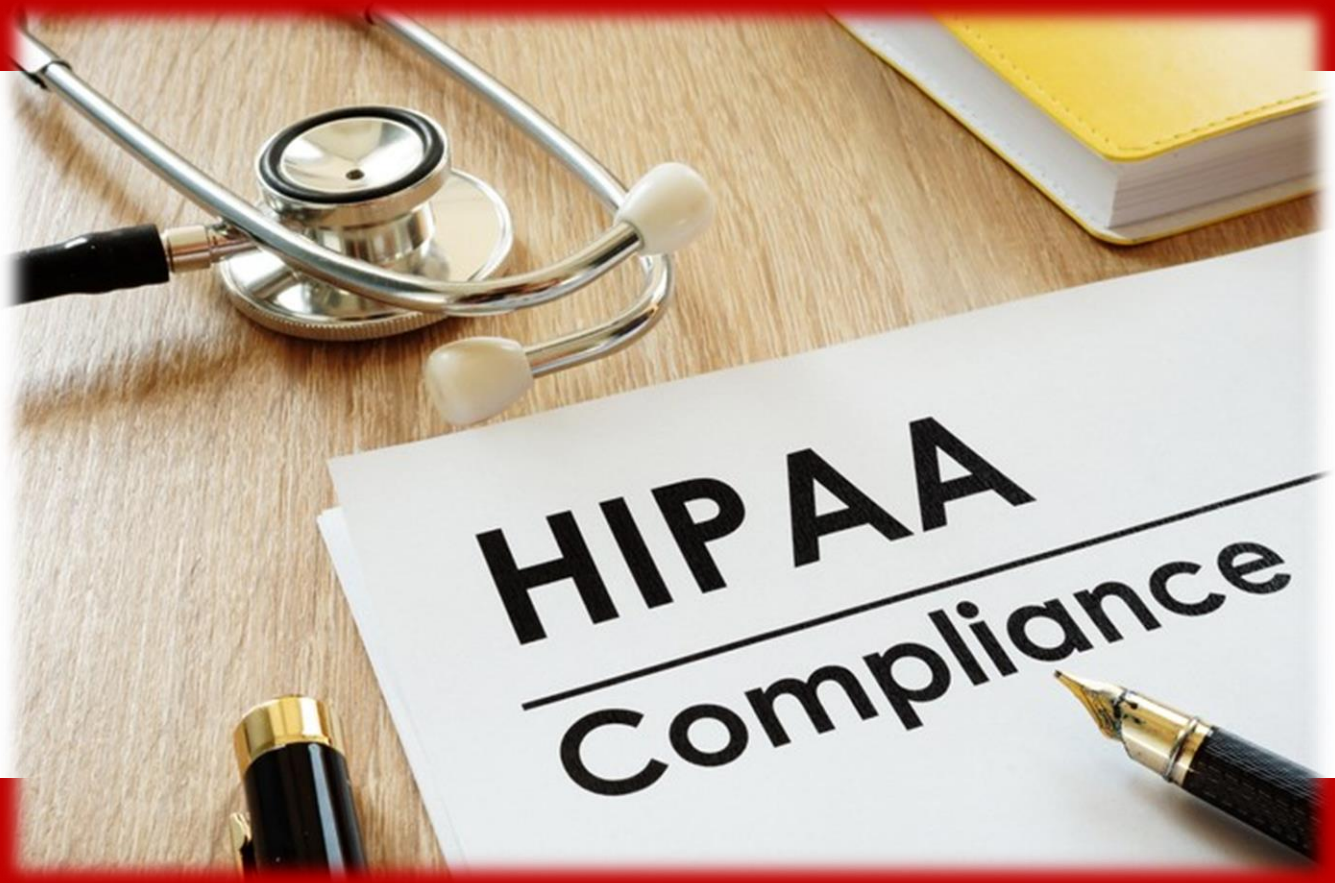
While there are security tools that address some aspects of API security, this problem of visibility needs to be solved.

“If your organization delivers APIs to external parties, such as your customers or partners, you need a centralized place to help monitor the security posture and compliance of all your published APIs, detect any risks immediately, and respond proactively to mitigate risks of data exfiltration,” says Subbu Iyer, VP of product for Cequence Security. “The first step in developing a mature API security and compliance program is to discover all the APIs your organization delivers to external parties and analyze their risk postures.”

## About the Author

Matt Keil, Director of Product Marketing, Cequence Security

Matt Keil joined Cequence Security in April of 2019 as a member of the product marketing team, driving product related messaging and outbound content creation. Prior to joining Cequence Security, Mr. Keil worked at Palo Alto Networks for 12 years, where he was part of the team that launched the company and his most current role was Director of Product Marketing for Public Cloud. Cumulatively, Mr. Keil has 18 years of experience in the enterprise network security market, working for Check Point Software, NetScreen/Juniper Networks, then Palo Alto Networks and Now Cequence Security.




# HIPAA Compliance and The Protection of Cyber Security

By Andrew Mikhailov, CTO at Zfort Group

Businesses face the risk of severe cyber-attacks - the present-day **cyberspace criminals are well-organized, thoughtful, and marketable**. And one of the most sensitive sectors **exposed to privacy risk is the healthcare system**. If hackers manage to get in, they would have access to patient health data, which they could sell to global entities with evil intentions.

About 15% of all data breaches in 2019 involved the healthcare system. As a result, the estimated losses for this industry in 2019 reached $25 billion. "***Over the last three years, the number of breaches, lost medical records, and settlements of fines is staggering. During this span, nearly 140 million medical records were involved in a privacy breach***", - writes Eric Thompson, a cyber security leader in his book.

In 2019, an Israeli cyber security center found a computer virus that added tumors into MRI and CT scans. This malware could also remove actual malignant growths from image files to prevent patients from getting the care they need. The researchers showed the **safety holes to sow doubt about the health of government** figures, commit insurance fraud, or be part of a terrorist attack.

In this situation, basic security tools such as **antivirus or firewalls are no longer making the cut**. Healthcare information security obeys data protection laws, particularly the Health Insurance Portability and Accountability Act (HIPAA) applies in the US.

If a data breach occurs, **HIPAA regulation presupposes financial and criminal penalties**. HIPAA outlines requirements to keep the personal health information of clients and patients safe.

## What Does HIPAA Protect?

An average incident costs a company about $6.45 million. Thus, organizations should consider both whether they are compliant and whether all the risks are considered. Generally speaking, HIPAA restricts uses and disclosures to healthcare operations, the provision of treatment, or payment for healthcare unless the patient agreed to provide information to a third party, and HIPAA gave authorization.

HIPAA Security Rule ensures the confidentiality, integrity, and availability of health information. Its Privacy Rule directs the uses and disclosures of health information (the HIPAA Privacy Rule). Thus, these elements help Covered Entities and their Business Associates to protect Electronic Protected Health Information (ePHI). The US Department of Health and Human Services (HHS) outlines who HIPAA refers to in its definition of a Covered Entity.

The HHS Office For Civil Rights (OCR) manages HIPAA. They conduct audits to ensure compliance with the Covered Entities and businesses that control medical data. HIPAA audits are conducted to track progress on compliance and to identify areas to improve.

These protected records include diagnoses, treatment information, test results, medications, health insurance ID numbers, and other identifiers. HIPAA also covers contact information, including phone numbers, addresses, email addresses, birthdates, and demographic information. So, while the OCR prepares for the next HIPAA audits, businesses ought to make sure they are ready.

## Why HIPAA Needs Cyber Security?

HIPAA Security Rule specifies that Covered Entities need to establish and maintain protections for ePHI. Moreover, protection must defend the organization against breach through any physical, administrative, and technical means. The rule mandates that HIPAA-compliant organizations:

- All the health data sent, stores, received, or produced has strong **confidentiality**. It means that it can be available **only** to authorized people to access, change, or remove it. The data should also be **always** available for authorized individuals.

- **Threats** to data integrity or security should be predicted whenever possible. Organizations should defend against any information disclosure or use not allowed by HIPAA.

- **Verifying that the workforce complies** with this law is also a business's responsibility.

Under this regulation, companies will need to implement technical and procedural checks to protect this information and perform risk analysis on risk and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Technical controls include such things as **encryption, authentication, password complexity, access auditing, and segmentation**. Procedural controls normally include password policies, incident response plans, contingency plans, and audit procedures.

Nowadays, healthcare information is part of the Big Data revolution and exists in a range of different digital ecosystems. In the healthcare industry, patients use wearables and implantable **IoT medical devices** such as heart monitors and pacemakers. With all these items now connected to the Internet, the **data gets exposed to cyberattacks**.

With the number of IoT devices increasing every year, most of them do not have endpoint security. That being said, it is vital to have a plan to protect your company's HIPAA data. One of the major security issues is how the device collects the information and then transmits it to the hospital. From an ePHI and HIPAA compliance viewpoint, this is a risk your business must **understand and develop a protection strategy**.

As we can see, cyber security and HIPAA compliance are strongly connected. Unfortunately, **being HIPAA compliant does not make your organization safe from cybercriminals**. At the same time, having a robust cyber security program does not make you HIPAA compliant as well. Your business needs a comprehensive HIPAA compliance and security provider to guarantee your patients' data's genuine security.

The industry should develop a holistic strategy for healthcare security, including administrative, physical, and technical safeguards.

## Strategies for Improving Cyber Security

HIPAA rules are not enough to resist cybercrime. Looking at precisely what this law requires, it doesn't necessarily align with cyber security best practices. Besides, healthcare organizations shouldn't see cyber security and HIPAA compliance as separate components, but rather as two concepts working parallel to one another. In fact, a robust cyber security program supports compliance.

To ensure cyber security in healthcare and prevent sophisticated attacks, healthcare organizations can implement the following practices:

1. Review your current **security risk analyses** and identify gaps and areas for improvement. Check that risk analysis is documented to guarantee regulatory compliance, enhancing the risk analysis's attorney-client privilege.

2. Assess **risk management plans** to make sure that measures to reduce vulnerabilities identified. Adopt the best practices used in healthcare. It's a must to use unique IDs, strong passwords, role-based permissions, auto time-out and screen lock.

3. Compare **HIPAA and other cyber-related policies** and procedures against legal and regulatory obligations, and ensure they are updated based on the results of your most recent risk analysis.

4. Expect the unexpected. Prepare **safety incident response plans** that meet HIPAA requirements and other applicable laws for your business to be ready to respond to a possible data breach. Besides, leave some room in your strategy for the unexpected. This could include everything from hacker attacks to natural disasters, threatening your healthcare records, and other vital assets.

5. Create **backups and develop a recovery plan**. While creating backups seems like a common-sense thing, it can be missed in a small practice environment. Ensure that the medium used to store your backup data is safe and cannot be wiped out by an attack that would take down your office systems.

6. Make **additional investments** in people, processes, technology, and management. Defending digital assets can no longer be delegated solely to the IT staff. Instead, security planning needs to be blended into new product and service, security, development plans, and business initiatives.

You can't afford to neglect cyber security or compliance. That is why it is critical to match them together in a secure network that protects your patients and your reputation.


**About the Author**

From 2017 as a CTO at Zfort Group, Andrew Mikhailov concentrates on growing the company into the areas of modern technologies like Artificial Intelligence, BigData, and IoT. Being a CTO, Andrew doesn't give up programming himself because it is critical for some of the projects Andrew curates as a CTO.

Andrew LinkedIn: https://www.linkedin.com/in/andrew-mikhailov-66571912/

Contact Andrew: andrei.michaiolov@gmail.com

# Smart Gadgets in Proving Workplace Violence

By Milica D. Djekic

The violence at the workplace could start as the common insult, continue as the verbal abuse and end up as the mobbing attack that could get correlated with any way of the psychological assault. In other words, it's quite obvious why any kind of the workplace violence should go under the Criminal Code and why the cases of any sort of the mobbing are treated as the crime. The point is anyone breaching the behavioral codex at the work should get reported to the authorities as they could use such information to run the investigation. In the business surrounding, there is no place for the personal level as there are the recommended methods of dealing with the co-workers. Also, any kind of abusive and rude behavior should get stated to the manager as he would find the way to resolve such an incidental situation. The well-developed organizations should get adopted the best practice how to tackle such a concern and in so many cases the abusive employees could get suspended from the work or even fired with the complaint to the Police as they would deeply break the law and put anyone under the stressful condition. The stress is the huge disadvantage to anyone and the person coping with such a state could suffer the real traumatic syndromes. In addition, there are a plenty of sensitive working groups including the persons with disability or any kind of disorder that should get handled carefully as they could get deeply affected with any kind of the violent behavior. According to the United Nations conventions these people need the extra care and any employer getting those guys in its team is the equal opportunity employment provider

and it would go under the entire procedure of benefits and appreciations giving the chance to such hard working individuals to contribute.

On the other hand, it could be quite difficult managing the person with the inappropriate vocabulary, poor manners and any lack of the good family education and does not matter how those persons being effective at the work or not – they should learn their behavior is adequate for the street, not the office. The office is not the place for the unkind persons as everyone in the business is overloaded enough with his tasks and schedules, so what the people need the most is the support and fair treatment. Anyone being exposed to the workplace violence is the victim of the crime and no intelligent employer would tolerate such a behavior. Why? If you support someone being so aggressive about the other people mostly for his intent to obtain some of his commonly unrealistic ambitions and prove some sort of the professionalism – you are doing so wrong. There are the ways to investigate and prove the violence at the work and anyone encouraging such an atmosphere at the workplace is committing the crime as well. Sometimes the employee being the victim of the mobbing would complain to the manager seeking from him to resolve such an incident and the manager would show the insufficient skill to deal with such a situation, so probably being driven with some irrationalities he would just fire the person who reported the abusive behavior at the workplace. In other words, it's not professional at all getting no business manners and being so subjective about everyone. The victim of the mobbing needs support as everyone deserves the respect and even if there are no well-developed procedures and policies in the organization how to tackle such a concern – the employer should know that it must discourage such a tendency.

The business arena is like the other sport courts – it's not enough to deal with the skill only, you need to cope with the fair play and meet so strict requirements and rules. If you are abusive in any sport and that can happen especially if you lose your tamper – you would definitely suffer some restrictions suggesting you that the sport's battlefield is not the place to heal your deep frustrations on anyone and anything. The similar situation is with the business! It's not sufficient to get competitive only – you need to operate according to the law; otherwise, you are not legally acceptable at all. No legal business would need the troubling staffs at most and if anyone tolerates such a condition in his office that person is equally guilty as anyone committing the crime over his co-workers. Simply, it's not about the unhealthy relations at the work – it's about the criminal justice case. The rules are rules and no one could avoid them, so it's clear that any kind of the violent behavior at the work could pull with itself some legal sanctions. It's quite difficult working in the office with so disturbed working correlations and anyone belonging to the sensitive group of the people could develop some sort of the shock or the real trauma that could get confirmed through the medical examinations. So, if you do not want to pay a lot for your lack of ethics about your staffs – you should develop the good behavioral codex that would cope with all possible legal frameworks and regulations, so far.

The fact is we live at the quite fast pace and the people could get anxious for so many reasons. Apparently, that's not the reason to take all your private frustrations with yourself and embarrass the other people with all of those. If you feel the stress about anything in your life – just attend your doctor and he would prescribe you the adequate remedies on. For instance, in the developed countries – the autism is so treatable condition and any kid suffering from so would never get left without any social care and attention. In other words, there are a plenty of programs supporting such a sensitive group of the people. In our opinion, the reason why so many people would break the law in the working environment is that they would suffer some kind of the psychological concern. Maybe they would get stressed, worried or scared about something, so they would not choose to look for the healthcare support – but they would rather express themselves as troubling and deal in the quite uncivilized and impatient manners putting their everything on the risk. It's the 21st century and it's not the shame seeking the medical advice or attending your healthcare professional for any reason. Anyone with the modern beliefs should understand so!

Through this effort, we would try to discuss the need of smart gadgets in proving the violence in the workplace. At this stage, it's quite clear that there are the methodologies and steps to evident that sort of the crime, but the point is if the recordings of the smart gadgets regarding some incidental situations could get approved as the valid clues in the criminal justice case – that could open up nearly limitless options to those gadgets manufacturers to get the bigger marketplace for their solutions that could get in need for many people. In other words, if you get the permission to record some condition and if such a recording is the valid proof, the number of your customers would increase as those products could be trusted by the authorities. At this moment, there are so many companies worldwide that can make the wide spectrum of the smart gadgets for practically any usage and the majority of those products are attested which guarantees they would work accurately, but if someone makes the legal regulations suggesting their footage could serve in the criminal justice case under the defined conditions – it's clear that so many people could buy those gadgets in order to prevent or prove something getting deeply illegal.

In other words, this effort is all about the proposed business ideas and some explanations how the good business plan could cope with the marketplace demands. Also, it's the suggestion to many governments across the globe how to leverage their economies putting into their laws and frameworks the outputs of the emerging technologies as stuffs that could find their applications even under the Criminal Code, so far.

**Assumption #1.** The workplace violence could be a consequence of the stress.

**Explanation #1.** Getting at the work day by day and coping with no break could be quite annoying. Apparently, there are some lunch pauses, but sooner or later you would get aware that you are beginning preoccupied with your daily schedule. For such a reason, it's recommended by the medical experts to make at least a half of hour break per a working day. Would this support you remaining fresh through the entire working week? Probably yes, but many people would need some holiday time to recover from the heavy tasks and renew their energy resources. The fact is so many professions cannot offer to their staffs to take that long leave and those employees could count on the several days off per a year. The fact is in so many cases those hard working persons would not get even the weekend off. Many would say they would be in the shape to work that hard, but sooner or later they would deal with the deeply accumulated stress. For such a reason, it's recommended to keep your professional manners and try to avoid any sort of bullying at the work. Why? You do not need anyone to provoke you as you do not need to provoke anyone as that person can get back to you. In the both cases, the conflicting situation is unavoidable and even if you are trying to appear as perfect someone could try to challenge your perfection targeting your psyche being oversaturated with the stress and if you make an incident you would need to provide so many explanations before you return things into balance. So, if anyone chooses the workplace violence as the response to the stress in the workplace it's clear that's the result of overtiredness, shocking events and a lot of struggling with the schedules and deadlines. The good manager should take all these into consideration as he would be responsible for his employees' wellbeing. The fact is so many outsourcing businesses would choose the less developed parts of the world to run the business as the workforce would be cheap, but suitable – so the profits getting available from there would be so high. Any business is about the risk and if the government of some developing economy attracts the investors to make a factory in their country they should know there would be a plenty of challenges to get managed for a reason those communities could be the sources of some kind of instability. The smart investors would take everything into account and as they would cope with the paid intelligence on a daily basis they would figure out if it is worth that to take such a risk on. Any profit maker would want to get the highest possible incomes from his activities counting on the lowest feasible expanses, so far. For such a reason, those clever guys would offer the minimal salary to their staffs in order to reduce that sort of the cost. The people must feed their families from those wedges and on the other hand, their employers would seek

the maximal level of the professionalism, productivity and effectiveness in return. In the case of the outsourcing business, it would appear someone would exploit someone. Also, the situation in the developed countries is not far more different as any capitalist would want to take advantage on the marketplace and his key players would get satisfied with their incomes, but they would need to push hard and hard as well as offer the new and innovative solutions and approaches pulling the entire company ahead. In other words, those guys are not the part of the assembly business as the case is with the developing societies. They are someone who would be with the brain and who would need to create the ingenious ideas on. Does not matter if you would work for the normative or the new business strategy sooner or later you would figure out that the stress is something that can distract you from being well-productive and well-creative. In other words, if you are overloaded day by day even the good intended suggestion from your co-worker could make you attempt the workplace violence and once that happens you would be in the trouble. Basically, it's up to your manger how hard you would need to work. Anyone making the profit would want your maximal effort for the minimal time and if you can provide the encouraging results within so short deadlines you would get the compliments that you are competitive. If not, the people would just say thank you for everything! That's quite stressful, right?

**Assumption #2.** Employees with the medical condition could be more sensitive to stress.

**Explanation #2.** If you hire a person with disability or another medical condition, you should be extremely careful how you would mange that staff. Those persons could be partially dysfunctional about some sorts of the tasks, but if managed skillfully they can give their maximum with something. The disability could be mental, physical, sensing or the other and even if you want to hire the totally blind person you should know that individual can contribute as well and get some kind of personal satisfaction for getting the chance to work. There are a lot of blind people who would deliver the online classes in the foreign language. Maybe they would not see well enough, but they would hear exceptionally and adopt some skills using their bright minds. It's not always pushing the poor people aside and making them get marginalized. It's about giving them opportunity to work and feed their kids. So, if you want to hire the person with the special condition, you need to provide him the special circumstances. Many people would believe that cyber defense area is only for the highly skillful persons. We would disagree with so! Even someone with the mental or physical disadvantage could become the IT security professional, but that person should not get discriminated at the beginning. There are so many talented people who cannot hear or walk, but they can sit in front of the screen and create so amazing software solutions being competitive even for the highest standard IT industries. The fact is those guys are so sensitive to the stress and it needs the skill to manage them. Remember the Rain Man and the guy with the autism who got the genius mind. That's what we talk about! Just try to figure out what could happen if anyone wanted to discriminate that person. The situation in the developing world in such a sense is hard. There are still a lot of unresolved concerns about the support and opportunities those folks get from their communities. Practically, there are some legal regulations, but they are not strictly followed and someone who could contribute in some manner would stay without the chance to even attempt to do so. On the other hand, the developed societies would show some care about those guys and they would create them the conditions to work and progress in their occupation. So surprisingly, some companies from the developed economies that would run the outsourcing business would choose to remain blind in front of those people's needs probably for the reason their local sources would suggest them it's better to pay some penalties to the government than to hire the person with disability. Would there be the difference between the guy with disability in the developed and developing economy? Basically, no! So, the only reasons why some respectful companies would not treat those people equally as they would do in their counties are so irrational stories from their outsourcing managers who would not cope with the skill to handle those hard working individuals. Luckily, the rational part of the human kind would not discriminate anyone and that's why we have the Paralympics Games every single season across the globe. If the business is only

who would take advantage over whom a lot of brilliant people would miss the chance to make something out of their lives. No one can succeed on his own and indeed, there is the need for support and encouragement from the entire community. The nations that would help their people make a progress would be the nations of successful people, while the small nations would look for the chance to revenge leading themselves to suffering and nothing else. In other words, go beyond your limits and think big no matter how poor your conditions are.

**Assumption #3.** The stress management techniques could reduce the violence at work.

**Explanation #3.** The people under the stressful condition could develop some kind of anxiety, tension or fear about what is going on around them. That sort of negative emotion could sabotage their efforts to be productive and effective at the workplace. Also, they can react so aggressively if anyone says anything because they are overloaded with their obligations. In addition, the people can express the violence for working hard and making some kind of the flaw that could go under the self-criticism or the criticism of their surroundings. Simply, they are a lot of reasons why someone can feel the pressure and give so assaultive response to that condition. The experience in criminology would suggest that so many violent offenders have been the victims of mobbing in some period of their lives. So, if someone is under the pressure chronically that person can develop resilience or respond with the dose of despite and probably some kind of the violence. The good manager should understand the limits as well as the strong and weak sides of his team and so skillfully manage all of them on. If the conflict occurs, the team leader should know how to put it under the control and following the procedures so carefully investigate what have happened for real. It's not only about collecting the claims through the catch up interview; it's more about coping with the best practice how the inconvenient situation could get resolved peacefully. Any competitive organization should deal with such a level of the development and also, it's necessary to organize some sort of the stress management workshops for your employees as they could get the free advice and instruction how to reduce their amount of the stress. It's also about the level of trust and confidence the employees have about each other as sometimes there is the need to openly talk about your concerns without any fear that you would get put under the wrong and misunderstanding interpretation. In other words, the co-workers should see each other as support, not the competitors as they work united like a team in order to beat the competition on the marketplace for their employer. Every good manager should know that and if anyone complains to him that person should receive the support to overcome such a situation. The point is being assertive, not revenging! If you maintain that "I win – You win" attitude you would easily figure out it's all about solidarity and team effort that can make everyone succeeds. The main trick is anyone with the bad manners would take the criticism so personally and that person could try to do some kind of bullying once she got reported to her principles. The employees could warn about someone's inappropriate behavior and it's not always about the reward and punishment – it's about teaching the staffs how to work as the one. The fact is the stress management training could be so expansive and the employer that wants to reduce his costs would not pay even a cent for that, in his opinion, unnecessary stuff. That's the quite wrong decision for a reason those sorts of things could serve as the good preventive measure in avoiding the violence at the workplace. Apparently, the good employer should get developed the adequate procedures, policies and best practices for tackling that spectrum of situations. Any kind of the mobbing is something that goes under the Criminal Code and anyone who wants to remain within the legal constrains would try to prevent that sort of behavior amongst his organization. So, the stress management techniques could reduce the workplace violence and it's not wasting of anything protecting your own interests investing into that sort of prevention, so far.

**Assumption #4.** Smart gadgets could serve in monitoring a condition of the organism.

**Explanation #4.** The stress is the natural follower of any organism's activity and according to some studies there is the certain amount of the stress the body can handle. Anything above that could be disadvantaging to the health and cause some acute or chronical medical conditions. So, if it's defined by some medical research studies which level of the stress can impact our health and how long it's necessary to get under that condition in order to develop some symptoms – it's quite clear that anyone or anything throwing us through such a drawback could deal with some kind of guiltiness or crime's responsibility. In other words, if your boss is doing the mobbing about you every single day and if you can notice through your smart hand-wear that your heart rate is increasing then and especially if that is happening day by day – you can say that such a guy is directly responsible for your cardiovascular disorder. So, if your smart watch is telling you your body is in the concerning condition and if such a product has passed through the laboratory testing and validation, so it got the approval it works accurately – it's obvious that the recordings of that gadget can serve as something for proving something else being under the criminal justice. The point is if the law makers would create the law suggesting that those footages could get used as the valid evidence in the case for proving someone guiltiness in causing the stressful condition and directly affecting someone's wellbeing that could mean anyone getting the capacity to manufacture those devices could sell them on the marketplace for a reason the people would buy them in order to assure the liability of their claims in front of the authorities. So, if your blood pressure is going up and your heart rate is getting arrhythmic because of someone's violence in the workplace there are the ways to prove that condition and leave the minimal space to the suspect to bend the truth on the court. On the other hand, the law makers could make a decision to put something like so into the legal framework because of the interests of their economies that could progress taking advantage over that sort of the business. It's all about the business and in so many times it's not enough to tell your story to your doctor in order to prove something. Apparently, there are so many approved methods in colleting the evidence, but once you get in position to deal with something such a rigid and touchable no one could try to avoid the responsibility. The stress is so unhealthy and only very few people would welcome so and, in other words, it would harm anyone's organism and anyone causing the harm is committing the crime, right? For such a reason the mobbing is seen as the crime in so many countries across the world. In addition, if you cope with your passively aggressive co-worker who would give you some sort of the psychological pressure and violence, you can easily suggest him that your smart gadget can record how you feel about him and once that recording gets the valid evidence on the court that aggressive person get count on the punishment only. At this stage, the medical forensic investigators could count on the approved procedures on statements gathering as well as expert's estimation of the made disadvantages. On the other hand, if you have reported the incident to the authorities and if even them can catch the internet signal from your smart gadget – it's obvious how the case could get its strength in front the public. The good thing about the smart devices is that they got assigned their IP address and apparently, that's the security concern, but also so convenient channel to the investigation to trace what such a gadget can sense or measure. What's needed is to approve that methodology in the legal fashion as well as provide the devices' manufacturers to obtain the right to produce the solutions that could serve as the evidence collectors.

## Comments

In this effort, we would provide a deep insight into the certain topic in order to explain some of its perspectives in more details. In our opinion, such a review could get used as the starting point to the development of some security and safety procedures and policies. Also, it could help to the law enforcement and intelligence agencies to navigate some investigative process as well as create the law enforcement and intelligence knowledge bases. Next, this effort could support the forensic detectives and investigators in their need to clarify some aspects of their work. In addition, those could be the helpful updates to the law makers to cover on and respond to all the security challenges through the appropriate

legal frameworks and regulations. In our belief, some suggestions to the best practice in the criminal justice environment have been made as well. Finally, this review would cope with some business ideas and it could serve as the encouragement to an emerging marketplace economy, so far.

**About the Author**

**Milica D. Djekic** is an Independent Researcher from Subotica, 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 book “The Internet of Things: Concept, Applications and Security” being published in 2017 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 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.

# Cyber Against Granny

By Yotam Gutman, SentinelOne

Every year, cybercriminals steal approximately $40 billion from older adults (senior citizens aged 60 and over) in the United States. Cybercrime can be defined as “any criminal activity in which a computer (or networked device) is targeted and/or used.” Cybercriminals with access to an older adult person’s information via a computer, smartphone, or other networked device, can easily exploit it for nefarious intent, defined as “*an act of forcing, compelling, or exerting undue influence over a vulnerable adult causing the vulnerable adult to act in a way that is inconsistent with relevant past behavior or causing the vulnerable adult to perform services for the benefit of another”.*

The scope of bad actors targeting senior citizens can be explained by the lack of experience and skills in using computers/technology among the elderly, against the growing popularity of computer systems held by people of the same age, and the fact that most of them have credit cards.

In the past, people in their 70s and 80s hardly ever used computers. Nowadays, people of the same age have social media accounts, surf the Internet, and of course use smartphones.

Unlike their younger counterparts, seniors are less aware of cyber threats and, in many cases, lack the tools and experience to identify attacks and fraudulent attempts. Even elderly people with no access to computers or smartphones can fall victim to cyber-related crime such as in the case where their personal details have been leaked from a database and sold to criminals who can then exploit. Seniors also give

bad actors the highest hit rates from phone phishing scams with frequent attempts being compromise of personal information and news of harm/captivity of the elderly's children.

Most of the crimes against the adult population use a similar pattern as fraud against the elderly with no connection to computers (such as telemarketing of unnecessary services by highly aggressive sales reps).

The criminals will reach out to those people in a non-suspicious manner - sending a legitimate-looking email, offering to connect on Facebook or by using a legitimate website that offers them some vacation or other prize. The criminals will then try to obtain the details of those people. In particular, they will seek credit card and identification details that allow them to use these cards. Another tactic is impersonating a person in need and requesting a transfer of funds.

Recently, the FBI arrested a network of criminals impersonating other people ("Captain Garcia" of the US military stationed in Syria, for example) who then persuaded their victims - many of whom were elderly - to transfer money to various causes, all of which were fictitious.

Another favorite method of criminals is impersonating "official" entities - government officials, municipalities and various authorities, while exploiting the trust (or innocence) of those veteran citizens and fraudulently obtaining their details.

In addition, this population is exposed to "normal" cybercrime - phishing, infection by malware and theft of personal information. The only difference is that the likelihood of this population recognizing such an attack is extremely slim, as the ability of people in this age group to understand that they have been compromised and to seek assistance is minimal. It should be noted that such attacks can also be carried out against people through their smartphones, which are very popular with this age group. These devices are usually not installed with protection software that could alert the user to malicious websites or warn them of attempts to exfiltrate personal details from the device.

## What can be done?

It all starts and ends with education, but this time it is the younger generation which needs to educate their parents. We should remember the warnings they repeatedly told us when we were younger, and echo similar messages back to them, though in a slightly different way:

- Know your friends and enemies: research shows that the elderly are oblivious to cyber risks, so it's worthwhile explaining to them some basic concepts and providing them with some examples of criminal or fraudulent online activities for them to learn from and avoid.

- Do not open the door to strangers, and do not receive anything from strangers: Any communication from a party that they do not know personally should be treated with caution. It's wise to assume all profiles on social networks are fake until proven otherwise.

-Don't tell anyone any personal information - even if you are convinced that you are in contact with an official, or a real person - do not provide credit card details, residential address or social security number - certainly not by email or messenger.

- If there is any suspicion, call "a responsible adult" - if requests are made to provide contact information, it is advisable to consult a person who is well-versed in security to see that the site is genuine. Yes, that person could be your 13-year-old grandson!

- If something looks too good to be true, it's probably not true - this old adage is just as true in the online world as it is in the physical world. Resist those tempting offers that pop up while browsing for weird apps that install themselves on the mobile device, and avoid those people who offer big, congested "if only" details or who to send you money.

## Conclusion

Unfortunately, today's elderly will continue to be the victims of cybercrime. This phenomenon will likely become worse before getting better as more elderly dabble in technology their generation adopts digital means of payment and banking through smartphones. It will probably take years until the generation who "grew up using computers" come of age, and are immune to such scams with their decades of built-in experience and suspicion of every poor girl from Nigeria who needs a hundred dollars a month to buy dresses for school. Until then, watch out for your parents, and help guard them against those they cannot guard against themselves.

Aspen initiative for protecting older users online-

https://www.aspentechpolicyhub.org/project/protecting-older-users-online/


**About the Author**

Lt. Commander (Ret.) Israel Navy, Yotam Gutman, has filled several operational, technical, and business positions at defense, HLS, Intelligence, and cybersecurity companies, and provided consulting services for numerous others. Yotam joined SentinelOne 6 months ago to oversee local marketing activities in Israel and contribute to the global content marketing team. Yotam founded and managed the Cybersecurity Marketing Professionals Community, which includes over 300 marketing professionals from more than 170 cyber companies. Yotam was chosen as one of the 5 Security Influencers to Follow on LinkedIn.



# Are the Worst Cryptocurrency Security Breaches Behind Us?

By Tim Fries, Co-Founder, The Tokenist

You would be right in assuming that blockchain itself was never hacked, but that doesn't mean people don't like to give up security features for the sake of convenience. Crypto exchanges are especially notorious for mass hacks that besmirch the entire cryptocurrency ecosystem.

Moreover, no matter what kind of crypto wallet you have, due to the decentralized nature of cryptocurrencies, it's akin to having a bank account in your pocket. In the end, we may as well rely upon the insured deposits of web-based wallets – crypto exchanges – more than anything else.

## People Demand Digital Money

It may surprise you to learn that the concept of internet money did not start with the first cryptocurrency in the form of Bitcoin (BTC). In fact, the most ancient and pervasive form of money – gold – was the first basis for digital currency in 1996. Called e-gold, it was effectively a stablecoin before there was such a thing. Anyone with an e-gold account was able to transfer money equivalent in value to grams of gold to other e-gold accounts. Unfortunately, it grew too much in popularity before the government shut it down in 2008.

E-gold may have ultimately failed as a digital currency, which is what people called it at the time, but it demonstrated a high demand for money that is not externally tempered with and controlled by governments. Just one year later, Bitcoin emerged on the scene as a digital currency entirely confined to the digital realm and outside government control. As Bitcoin gained more traction and value, the legacy media became fever-pitched in tying Bitcoin to the criminal underground.

Fortunately, all their efforts failed along with their trustworthiness. On the other hand, the most current data on Bitcoin adoption rate provided by The Tokenist, tells a story of increased trust in Bitcoin over traditional institutions, by 29%. The upward shift in Bitcoin trust and familiarity is primarily led by male millennials, while people older than 65 are least likely to own and use Bitcoin.

The latter part is important to note because older people represent a demographic that views money as something that is strictly:

1. Physical
2. Government-controlled

Regardless of age, we can safely say that these two money attributes are more or less present in the minds of all demographic groups. Therefore, they represent substantial psychological barriers to overcome for further cryptocurrency adoption. Thankfully, the government's reaction to the coronavirus greatly eroded the embedded notion that money, as physical and government-controlled, is inherently superior to digital money.

When the Federal Reserve decided to summon trillions of dollars on multiple occasions to save the market from totally crashing, no one with a straight face could say ever again that government money is derived from real wealth. On the other hand, Bitcoin draws from a predetermined, finite pool of coins, with each Bitcoin ever-growing in value.

However, there is another aspect to digital money that makes people instinctively distrust it – cybersecurity. In particular, the prevailing sentiment that anything digital is hackable.

## Shortcuts Lead to Cryptocurrency Vulnerability

Although fiat money can be counterfeited, it's almost unheard of with the modern protections applied in the money printing presses. This is not the case with Bitcoin and other cryptocurrencies. There are many cases of mass Bitcoin thefts/hacks from crypto exchanges, such as Japan's Mt. Gox, Bitcoin7, Bitomat, Linode, BTC-e, Bitcoinica, Bitfloor, Vicurex, and Hong Kong's Bitfinex as the largest case of hacking with 120,000 BTC stolen.

Moreover, an alternative marketplace powered by cryptocurrencies, Silk Road, greatly harmed the public image of new digital money. Operating in the underbelly of the internet, the Tor network, Silk Road facilitated many hacker attacks, money laundering, and blackmail operations. Criminal activity in this sector not only harms the directly-affected crypto-holders, but it suppresses further adoption of blockchain-powered digital money.

In the best of times, outside of stablecoins, cryptocurrencies suffer from volatility compared to fiat money. Big crypto exchange hacks cause the price of Bitcoin to plummet, which then drags down all lesser cryptocurrencies with it. Inevitably, this further increases cryptocurrency volatility and decreases its usage as money.

With all this in mind, it bears emphasizing that blockchain still remains effectively unhackable. People lost money from crypto exchange hacks because users gave their private keys to these companies. By doing that, a user forgoes a vital security feature of cryptocurrencies – private and public keys – and places all the trust into crypto exchanges for the sake of convenience.

## Unhackable Blockchain is Only the Beginning of Cybersecurity

Let's face it. If digital currencies operated under any other system other than blockchain, only hardcore enthusiasts and first-time adopters would flirt with that kind of digital money. As it stands, blockchain, as a distributed ledger across nodes, can withstand any malicious attempts at record alteration. This is why numerous governmental and corporate organizations, from military to healthcare and art galleries, have started to view blockchain as a low-cost, high-end implementation of cybersecurity.

As we have seen with the latest hacking of Twitter accounts, the human factor is the weakest link in the cybersecurity chain. In this instance, they befriended the Twitter employee on Discord and then convinced the employee with some extra incentives to share the administrator account.

**Likewise, Bitcoin thefts and breaches occur outside the impervious blockchain:**

- Opting to give crypto-exchanges your private key instead of using private wallets – hard, mobile, or desktop. Then, you must rely on the company in charge of the crypto exchange to have trustworthy employees and security measures.
- Opting to have a private wallet with both private and public keys, but not securing it enough. Usually, by leaving passwords and word phrases in other unprotected locations and files.

- Falling for scams by email, imposter websites, and apps (or Twitter…)
- Acquiring malware by visiting scam websites and opening files in your email from untrustworthy sources. Then, this malware gains access to your web-based wallet and is extremely difficult to remove. Some malware programs even scan your clipboard and text files to replace your cryptocurrency address with the address of the scammer. Other malware installs a miner to use your computer as a free mining resource.

More skillful scammers have developed a roundabout way of taking your money, mainly by exploiting human nature.

- As Bitcoin entered the mainstream news cycle and soared in value, people were starting to feel left out of the game. Trying to catch up with lesser, cheaper altcoins, they fell into the embrace of ICO scammers. In 2017, fake Initial Coin Offering (ICOs) was a huge problem, with at least 80% of ICOs uncovered as scams.
- Pumping and dumping. Relying on the same sentiment as with ICO scams, pump and dump scammers have adopted a strategy of picking an altcoin low in market cap, buying it in bulk to spike its price, then selling it after other people bought it for an even higher price.
- Closely related to the aforementioned Twitter hacking, you will also find celebrity impersonation scams. All of those hacked accounts of famous people were used as cryptocurrency giveaway scams. Usually, they promise to send you more than what you sent them, as a part of some kind of charity drive.

As you can see, you can have fool-proof security in the form of blockchain and still be duped if you lack knowledge and discipline to resist baits.

## User-Education Must Come First

Blockchain may be the revolutionary bulwark against hard hacks we were all waiting for, but soft hacks will continue to plague cryptocurrency users. Even outside of hacks and scams, cryptocurrency, with Bitcoin leading the charge, has become the perfect means of laundering money. Moreover, money-laundering goes hand-in-hand with blackmail and ransom.

Such is the flexibility of digital technology that cybercriminals don't even have to hack anything at all. They can simply threaten to hack or insinuate to have some dirt on someone by using vague language, and the victim would then just have to send a certain cryptocurrency sum to their address. No physical contact, and no risk.

At least, some careless cybercriminals would assume so.

Only initially could you claim that Bitcoin is anonymous money. In 2011, that all changed with the first release of the block explorer. Because blockchain keeps an immutable ledger of all transactions, it only takes such a tool to track down every transaction. However, even this can be countered by creating multiple wallets and addresses with privacy-focused browsers such as Tor. Some cryptocurrencies, like Monero (XMR), are designed with untraceability as the core feature.

## Takeaway

We can say that digital technology was inevitable. We can even say that blockchain was inevitable. We are lucky to live in the timeline where we have both. However, what we cannot say is that unbreachable cybersecurity is inevitable. No matter what kind of cybersecurity system we design, it will have to cater to the lowest common denominator – human markets.

### About the Author

Tim Fries is co-founder of Protective Technologies Capital, an investment firm focused on helping owners of industrial technology businesses manage succession planning and ownership transitions. He is also co-founder of the financial education site The Tokenist. **Previously**, Tim was a member of the Global Industrial Solutions investment team at Baird Capital, a Chicago-based lower-middle market private equity firm.


EVENTS

# GSX
GLOBAL SECURITY EXCHANGE

POWERED BY ASIS INTERNATIONAL

**21–23 SEPTEMBER 2020**
**ATLANTA, GA | GSX.ORG | #GSX20**

## Education XCELLENCE

**Global Security Exchange (GSX) is the security industry's premier global education event.**

The GSX education program is full of quality content in an immersive and interactive learning environment. The program offers insights and valuable takeaways like how physical security and cybersecurity are integral partners for solutions, ranging from analytics to visitor management.

View a complete list of sessions and start planning your GSX experience today at **GSX.org.**

**REGISTER WITH CONFIDENCE » GSX.org/CDM**

If you register for GSX and cannot attend due to COVID-19, rest assured, we have you covered.


ISAF CyberSecurity
9th International Cyber Security, Information & Network Security Exhibition
OCTOBER 08th-11th, 2020
Istanbul Expo Center (İFM) - Turkiye
ISAF
"smart exhibitions"
www.isaffuari.com
T. +90 212 503 32 32 - marmara@marmarafuar.com.tr
MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr
/marmarafuar
/isafexhibition
/company/marmara-fuar


1,100+
ATTENDEES
85+
SPONSORS
50+
CONFERENCE
SESSIONS
90+
SPEAKERS
THE INDUSTRY'S LARGEST
INDEPENDENT AI
GOVERNMENT EVENT
2nd Annual
aiworld
GOVERNMENT
NEW DATES:
OCTOBER 28-30, 2020 | WASHINGTON, DC
RENAISSANCE DOWNTOWN HOTEL
Save $200
with discount
code CDM2020
Accelerating Innovation in the Public Sector
AI World Government provides a comprehensive three-day forum to educate and inform
public sector agencies on proven strategies and tactics to successfully deploy
AI and cognitive technologies.
AIWorldGov.com

# QUBIT CONFERENCE SOFIA 2020

3rd Cybersecurity Community Event

**29OCTOBER/ SOFIA, BULGARIA**

# CALL FOR SPEAKERS IS OPEN!

## We are looking for:

- new speakers with original, innovative and creative topic and session outline
- real-life stories, strategies and mind opening ideas, case studies that Conference Attendees can apply to their jobs

## Speakers should focus on the main Conference Streams:

Threat intelligence | Cloud security | Disaster recovery
Secure team cooperation

**SUBMIT YOUR PROPOSAL**

Excellent speakers | Educational session | News & networking | Practical workshops

# EURONAVAL

THE WORLD NAVAL DEFENCE EXHIBITION

**OCTOBER 2020**

EXHIBITION
20/23
LE BOURGET

CONFERENCE
19
PARIS

www.euronaval.fr

# 5th BRAND PROTECTION CONGRESS

BPC

## 09 - 10 November 2020

## Kuala Lumpur, Malaysia

### *Experience:*

- *Our unique and inspiring program*
- *Countless networking opportunities.*
- *Remarkable one-to-one meeting sessions.*
- *The congenial gathering of distinguished industry leaders*
- *The Magnificient petronas twin towers & shoppers paradise that is Kuala Lumpur , Malaysia.*

00 44 (0) 20 3129 8222 | 00 44 (0) 20 7691 7383 | info@worldbigroup.com

WORLDBI CONFERENCES | SUMMITS | WEBINARS

# 6th BRAND PROTECTION CONGRESS

BPC

## 02 - 03 December 2020
## Nice, France

### *Experience:*

- *Our unique and inspiring program*
- *Countless networking opportunities.*
- *Remarkable one-to-one meeting sessions.*
- *The congenial gathering of distinguished industry leaders*
- *The fabulous beaches, beautiful coastline and fantastic architecture of Nice, France.*

00 44 (0) 20 3129 8222 | 00 44 (0) 20 7691 7383 | info@worldbigroup.com

HELD UNDER THE PATRONAGE OF HIS EXCELLENCY, PRESIDENT ABDEL FATTAH EL-SISI
THE PRESIDENT OF THE ARAB REPUBLIC OF EGYPT, THE SUPREME COMMANDER OF THE EGYPTIAN ARMED FORCES

# EGYPT DEFENCE EXPO

7-10 DECEMBER 2020
EGYPT INTERNATIONAL EXHIBITION CENTRE

www.egyptdefenceexpo.com
@egyptdefenceexpo
/egyptdefenceexpo
@visitedex
#edex2020

## THE 2ND EDITION OF EGYPT'S ONLY INTERNATIONAL DEFENCE EXHIBITION

EGYPT INTERNATIONAL EXHIBITION CENTRE
7-10 DECEMBER 2020

**400 +** EXHIBITORS

**30,000 +** VISITORS

**FULLY-HOSTED VIP** DELEGATION PROGRAMME

Media Partner

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Supported by

Ministry of Defence

Egyptian Armed Forces

Ministry of Military Production

جهاز مشروعات الخدمة الوطنية

Organised by

CLARION EVENTS


Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

**rsaconference.com/cyberdefense-2020**

# You don't need to be next in line for a data breach.

## Put on your thinking hat and step into the shoes of a hacker.

Cyber incidents are on the rise. While most organizations play defense--creating plans that tell them what to secure and how to react if their security settings fail--it's not enough to respond to a data breach.

What if you looked at cybersecurity from a different point of view?

In our guide, "How to Think Like a Hacker and Secure Your Data," you'll discover how to go on offense with your data by:

- Diving into modern data breach statistics
- Exploring hacking terminology and techniques
- Walking through seven strategies for data protection

***Are you ready to put yourself in the shoes of a hacker?***

Visit **https://www.goanywhere.com/think-like-a-hacker**

to get a free copy of our cybersecurity guide.

GO ANYWHERE®
Managed File Transfer

## Meet Our Publisher:  Gary S. Miliefsky, CISSP, fmDHS

## “Amazing Keynote”

## “Best Speaker on the Hacking Stage”

## “Most Entertaining and Engaging”

Gary has been keynoting cyber security events throughout the year.  He’s also been a moderator, a panelist and has numerous upcoming events throughout the year.

If you are looking for a cybersecurity expert who can make the difference from a nice event to a stellar conference, look no further email marketing@cyberdefensemagazine.com

# CYBER DEFENSE TV

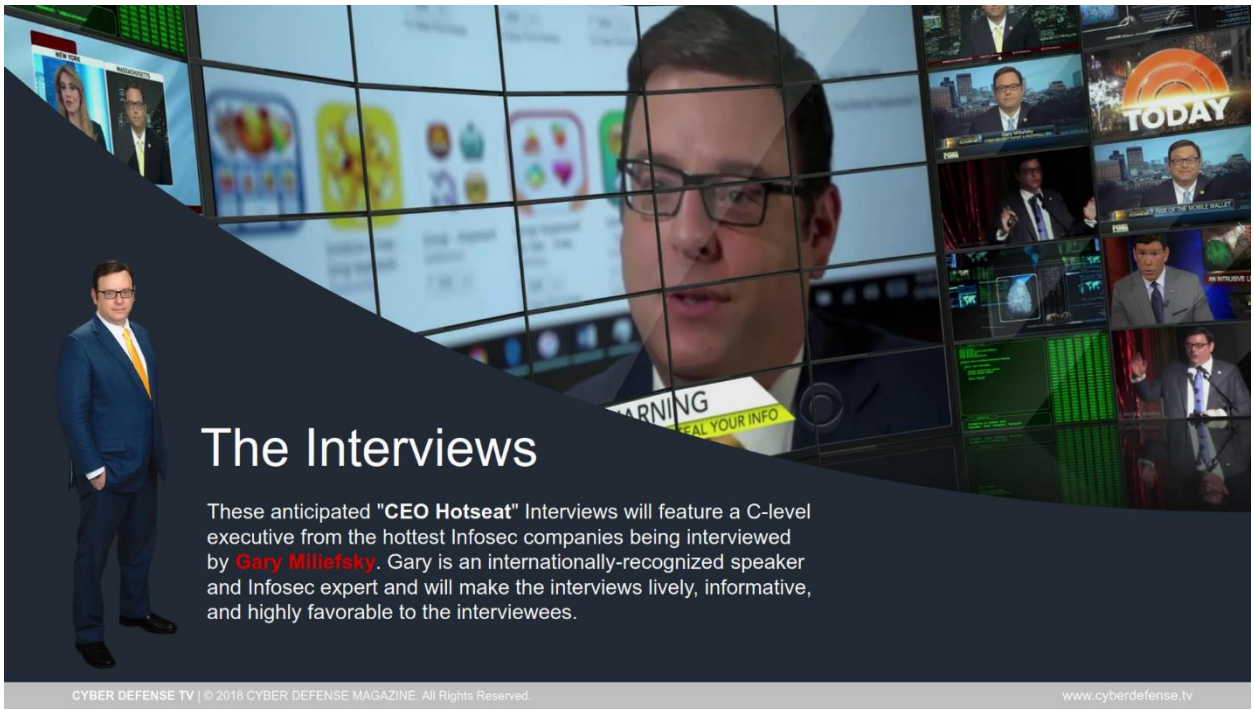
## INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here…we've launched CyberDefense.TV

At least a dozen exceptional interviews rolling out each month starting this summer…

Market leaders, innovators, CEO hot seat interviews and much more.

A new division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



## Free Monthly Cyber Defense eMagazine Via Email

## Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

---



**Cyber Defense Magazine**

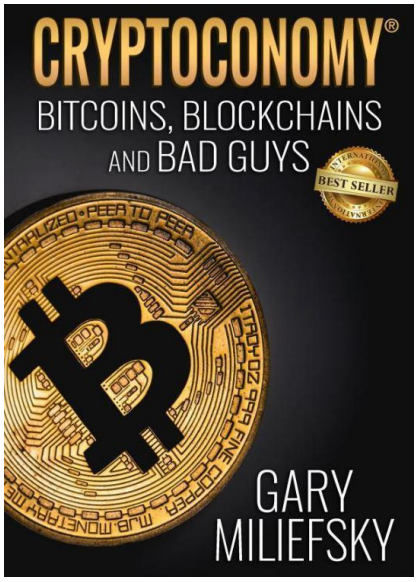
276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

**NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)**
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 08/03/2020

# TRILLIONS ARE AT STAKE

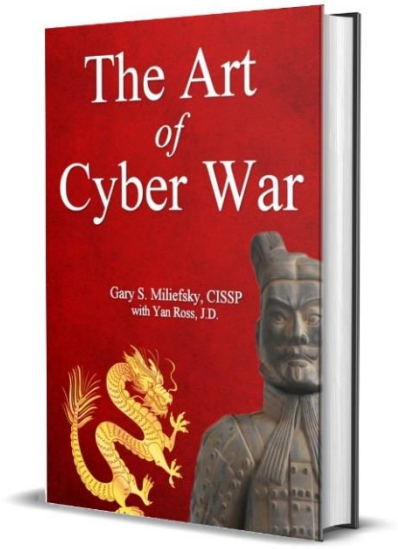
## No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES

Released:




https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH

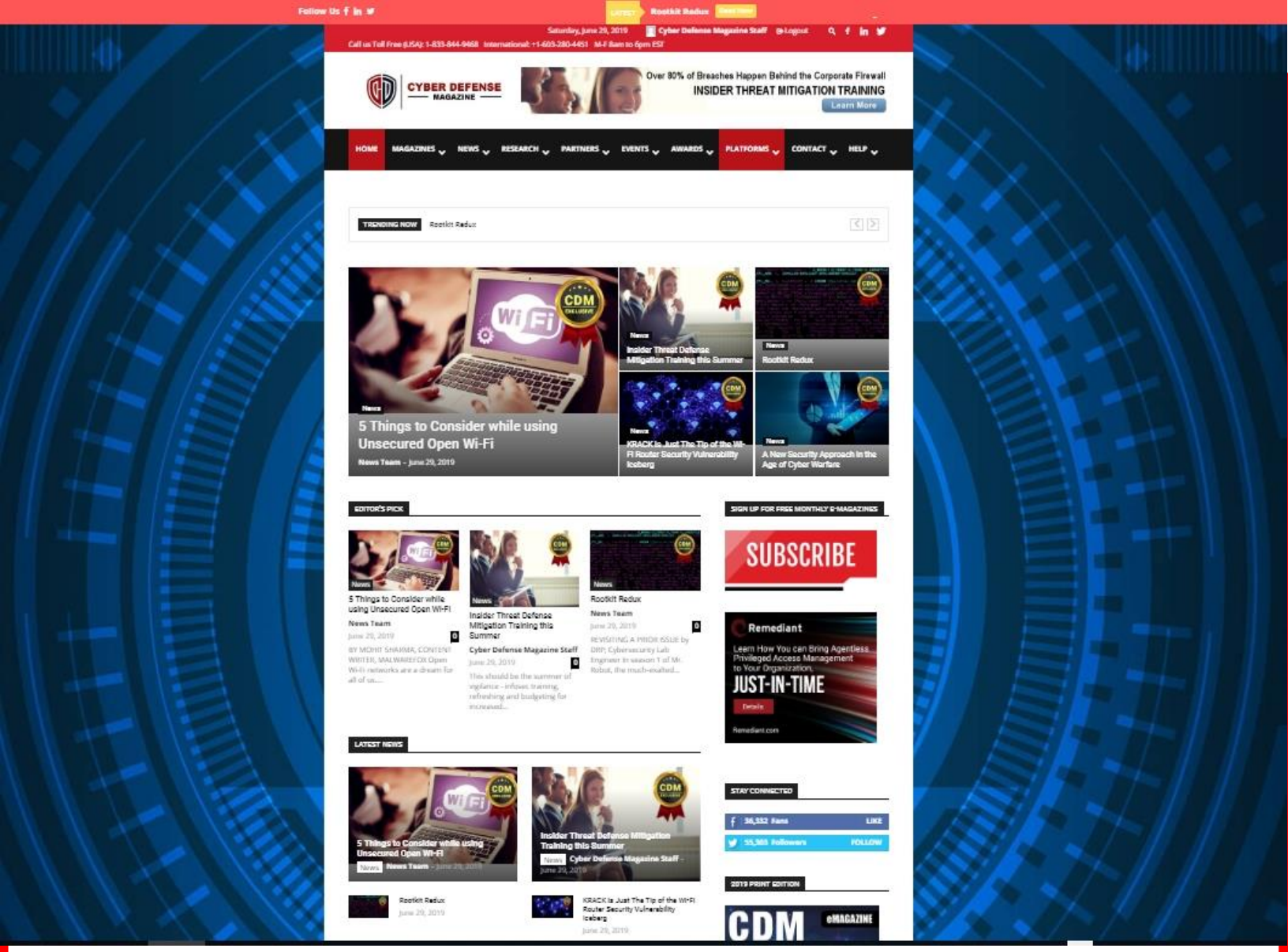
In Development:






To learn more:
Call +1.512.372.1004, Visit www.brinqa.com

brinqa




# *8 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 shooting for 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.**

***Millions of monthly readers and new platforms coming…***

**JUNE 2–4, 2020**
David L. Lawrence Convention Center | Pittsburgh, PA

# SMART MANUFACTURING EXPERIENCE

# the path to the connected world of manufacturing

## Greater Connectivity = Greater Need for Cybersecurity Solutions

- **Thousands of buyers.** Engage with qualified attendees searching for the best ways to secure their data and their business
- **Exclusive opportunity.** Only open to companies that can demonstrate a connection/application to smart manufacturing
- **Active participants.** Demonstrate your solutions and educate manufacturers on the most effective methods to safeguard their valuable data

## The Event is Focused on These Transformative Technologies:

- Cybersecurity
- Additive Manufacturing (AM) & 3D Printing
- Artificial Intelligence/Machine Learning
- Augmented Reality (AR) and Virtual Reality (VR)
- Automation & Robotics
- Data Analytics
- Industrial IoT (Internet of Things)
- Workforce Transformation

## Be Part of the Experience!

Call **800.733.3976** or visit **smartmanufacturingexperience.com**

sme AMT

# HERJAVEC GROUP

## Celebrating Over 15 Years of
## Cybersecurity Operations Excellence

**At Herjavec Group, information security is what we do.**

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection…the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

**Robert Herjavec**
Black Unicorn Awards Judge
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

## Recognized Industry-Wide

- MOST INNOVATIVE IAM PROVIDER — Cyber Defense Global Awards 2018 Winner
- SECURITY SERVICES LEADER — IDC Analyze the Future
- LEADER IN MANAGED SECURITY SERVICES — Cyber Defense Global Awards 2018 Winner
- SECURITY COMPANY OF THE YEAR — CDM Cyber Defense Magazine
- #1 ON THE Cyber Security 500 — World's Hottest Security Companies
- TOP 10 ON THE 2018 Top 100 MSSPs — MSSPAlert.com/Top100

# 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**


Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

**rsaconference.com/cyberdefense-2020**


**Lucio Frega, Threat Researcher**
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

## About the Author/Disclosure

Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.


*** with help from writers and friends all over the Globe.**