



**CYBER DEFENSE**  
MAGAZINE

**eMAGAZINE**

## IN THIS EDITION

*Covid-19 Unveiled a New Security Gap*

*There's a Hole in Your Threat Detection Strategy—It's Called East/West Traffic*

*Industrial Control System - Security Focus of Federal Effort*

*What Is Being Done, And How Can They Improve this Critical Infrastructure...?*

*...and much more...*

**SEPTEMBER 2020**

**MORE INSIDE!**

---

# CONTENTS

<b>Welcome to CDM's September 2020 Issue-----</b>	<b>7</b>
<b><i>Covid-19 Unveiled a New Security Gap-----</i></b>	<b>25</b>
By Eddy Bobritsky, CEO & Co-Founder, Minerva Labs	
<b><i>There's a Hole in Your Threat Detection Strategy—It's Called East/West Traffic -----</i></b>	<b>28</b>
By Carolyn Crandall, Chief Deception Officer, Attivo Networks	
<b><i>Industrial Control System - Security Focus of Federal Effort-----</i></b>	<b>33</b>
By Trip Hillman, Director of Cybersecurity Services at Weaver	
<b><i>What Is Being Done, And How Can They Improve this Critical Infrastructure?-----</i></b>	<b>35</b>
By Martin Banks	
<b><i>Low Latency Encryption Will Secure the U.S. Electrical Grid -----</i></b>	<b>39</b>
By John Downing, President, Encrypted Grid, LLC	
<b><i>Cyber Warfare and Its Impact on Businesses -----</i></b>	<b>45</b>
By Kumar Ritesh, Founder and CEO, CYFIRMA	
<b><i>Cyber Literacy in Post-Digital Era as Part of National Security-----</i></b>	<b>49</b>
By Aliaksei Hapeyeu, master's degree student from Shandong University	
<b><i>New Research Highlights Importance of HTTPS Inspection to Detect Encrypted Malware -----</i></b>	<b>55</b>
By Marc Laliberte, Senior Security Analyst at WatchGuard Technologies	
<b><i>Protecting a Mobile Workforce with Hybrid DNS Security-----</i></b>	<b>58</b>
By Ashraf Sheet, Regional Director, Middle East & Africa at Infoblox	
<b><i>Unstructured Data, Unsecured Data -----</i></b>	<b>61</b>
By Deborah Kish, EVP, Marketing & Research, Fasoo, Inc.	

---

<b><i>Securing the Weakest Links in Today's Public Cloud Environments</i></b> .....	<b>65</b>
By Avi Shua, CEO, Orca Security	
<b><i>Compliance in A Connected World</i></b> .....	<b>70</b>
By Kirsty Fisher, CFO, Titania	
<b><i>Defending Ever Expanding Networks and IT Systems</i></b> .....	<b>74</b>
By Trevor Pott, Product Marketing Director, Juniper Networks	
<b><i>The "New Normal" – Navigating Remote Work and Security in the COVID-19 Era</i></b> .....	<b>78</b>
By Bill Delisi, CEO of GOFBA	
<b><i>Do Not Forget to Securely Lock Your Data in Microsoft Teams</i></b> .....	<b>81</b>
By Johanna Reisacher, Marketing Manager, Secomba GmbH	
<b><i>Building Secure Software Right from the Start: Four Steps for an Effective AppSec Strategy</i></b> .....	<b>88</b>
By Joanne Godfrey, Security Evangelist, ZeroNorth	
<b><i>How to Close the Door on Ripple20 Vulnerabilities by Combining Local Security with Software Defined Perimeters</i></b> .....	<b>92</b>
By Don Boxley, Co-founder and CEO, DH2i [ <a href="https://dh2i.com">https://dh2i.com</a> ]	
<b><i>Funding Schemes and Cyber Security</i></b> .....	<b>95</b>
By Milica D. Djekic	
<b><i>Media Content Captured on Mobile Is Driving Compliance Problems</i></b> .....	<b>97</b>
By Josh Bohls, CEO, Inkscreen	
<b><i>Weaknesses of Biometric Authentication</i></b> .....	<b>100</b>
By Mark Perkins, MS, CISSP, IT Manager	



---

<b><i>5 Ways to Avoid Security Automation Pitfalls -----</i></b>	<b><i>104</i></b>
By Joe Partlow, CTO at ReliaQuest	
<b><i>Manual vs. Automatic Cybersecurity Testing: What's the Difference? -----</i></b>	<b><i>107</i></b>
By Tamir Shriki, Customer Operations Manager, XM Cyber	
<b><i>Privacy Shield Revoked -----</i></b>	<b><i>110</i></b>
By Dan Piazza, Technical Product Manager, Stealthbits Technologies	
<b><i>Automotive Cybersecurity Is Not One-Size-Fits-All. Here's How Oems And Tier 1s Can Tailor Their Approach to Meet the Needs of The Market -----</i></b>	<b><i>114</i></b>
By Nathaniel Meron, Chief Product and Marketing Officer, C2A Security	
<b><i>Mapping Automation to the MITRE ATT&amp;CK Framework -----</i></b>	<b><i>118</i></b>
By Chris Calvert, vice president, product strategy, and co-founder, Respond Software	
<b><i>Cyber Liability Insurance – Safe Bet or Sales Gimmick? -----</i></b>	<b><i>121</i></b>
By Darren T. Kimura, Spin Technology	





@MILIEFSKY

From the  
Publisher...



New [CyberDefenseMagazine.com](https://www.cyberdefensemagazine.com) website, plus updates at [CyberDefenseTV.com](https://www.cyberdefensetv.com) & [CyberDefenseRadio.com](https://www.cyberdefensetv.com)

Dear Friends,

In the September issue of Cyber Defense Magazine, we bring our readers a varied and diverse group of articles concentrating on the continued and pervasive cyber security challenges we face together. There is no time in recent, or at least digital, history when such a state of flux has existed, both among the “home team” defenders and among the threat actors.



The cyber practices of social distancing have become more and more widespread, and appear to be entering a transitional phase from temporary stopgap “work from home” remedies to a more permanent structural change in how work gets done outside the HQ environment. Many workers will never return to the traditional office, and may even be deemed surplus to requirements by their employers.

The exploitation of vulnerabilities grows apace, with a potential broadening of the realms of financial criminal activity, state-sponsored interference, and the ever-present thrill-seekers whose payoff is seeing the disruption they can cause. We are also in the critical campaign period leading up to the presidential election in the U.S., which is by any measure fraught with vulnerabilities and threats from within and without. The effects of COVID-19 on nearly all enterprises which depend on cyberspace for their operations are growing. The actionable intelligence Cyber Defense Magazine provides is the first and best means of meeting these challenges.

Starting with the cogent articles in this new issue, 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 compelling interest.

Please take time to visit and signup for a webinar at <https://www.cyberdefensewebinars.com> – free, highly educational, fun, memorable, interactive and you’ll get a certificate emailed to you after each webinar.

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...

In contrast to a well-known phrase from the French “Plus ça change...,” we find ourselves in a rapidly changing cyber world, one in which the changes will present more and more difficulty in maintaining stability.

As this instability continues, it will be more and more difficult to adopt and implement cross-border standards for the protection of digital assets and maintenance of cybersecurity integrity.

The better aspect of this challenge is that it’s not impossible. But it’s not going to be easy to establish consistency across jurisdictions. It will be a time-consuming process, and require the will to confront the attackers together rather than with a vast set of inconsistent, overlapping, and even contrary laws and regulations.

All of this takes place in the context of a physical as well as digital state of affairs in which trust issues and political expediencies constantly hamper the authorities.

Once again, 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](mailto:stevinv@cyberdefensemagazine.com)

### INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER

Pierluigi Paganini, CEH

[Pierluigi.paganini@cyberdefensemagazine.com](mailto:Pierluigi.paganini@cyberdefensemagazine.com)

### US EDITOR-IN-CHIEF

Yan Ross, JD

[Yan.Ross@cyberdefensemediagroup.com](mailto:Yan.Ross@cyberdefensemediagroup.com)

### ADVERTISING

Marketing Team

[marketing@cyberdefensemagazine.com](mailto: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>

Copyright © 2020, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (a Steven G. Samuels LLC d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001  
EIN: 454-18-8465, DUNS# 078358935.  
All rights reserved worldwide.

### 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](http://CYBERDEFENSEMEDIAGROUP.COM)**  
**[MAGAZINE](#)   [TV](#)   [RADIO](#)   [AWARDS](#)**  
**[WEBINARS](#) & new [VENTURES](#) platform**

---

## Welcome to CDM's September 2020 Issue

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

As the summer winds down (in the Northern Hemisphere), along with the change in seasons comes a broadening of the concerns facing the practitioners of cybersecurity.

In this issue, we are pleased to present articles recognizing a new set of challenges and potential solutions offered by over two dozen contributors. The range of articles covers everything from high-altitude perspectives of the effects of the COVID-19 pandemic down to granular views of industry-specific concerns.

While there are many points of view, even disagreements, about what will constitute the dynamics of a "new normal" playing field, there is little doubt that we are facing fundamental and persistent changes in the size and shape of cybersecurity practices.

We encourage our readers to take a brief walk through the Table of Contents, and then drill down into the articles which most affect your individual activities. You will find thoughtful and instructive descriptions of challenges and suggested answers, and we encourage you to reach out to our authors for more detail and advice.

With that perspective, we are pleased to present the September 2020 issue of Cyber Defense Magazine. We would like once again to express our appreciation to our 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](mailto:yan.ross@cyberdefensemediagroup.com)







# SPONSORS





# **CYBER DEFENSE MEDIA GROUP**

**WHERE INFOSEC KNOWLEDGE IS POWER**

**Rise above the noise,  
take your Infosec story to the moon and back!  
Only with Cyber Defense Media Group**



[www.cyberdefensetv.com](http://www.cyberdefensetv.com)  
[www.cyberdefenseradio.com](http://www.cyberdefenseradio.com)  
[www.cyberdefenseawards.com](http://www.cyberdefenseawards.com)  
[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)





# Predictive Cyber Defense

**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.


  
MALWARE  
YARA

PREDICT

  
HUNT

cythereal.com





# 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](https://rsaconference.com/cyberdefense-2020)

# Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011



Founder & Managing Partner

# SEAN DRAKE



***“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](http://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](https://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](https://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



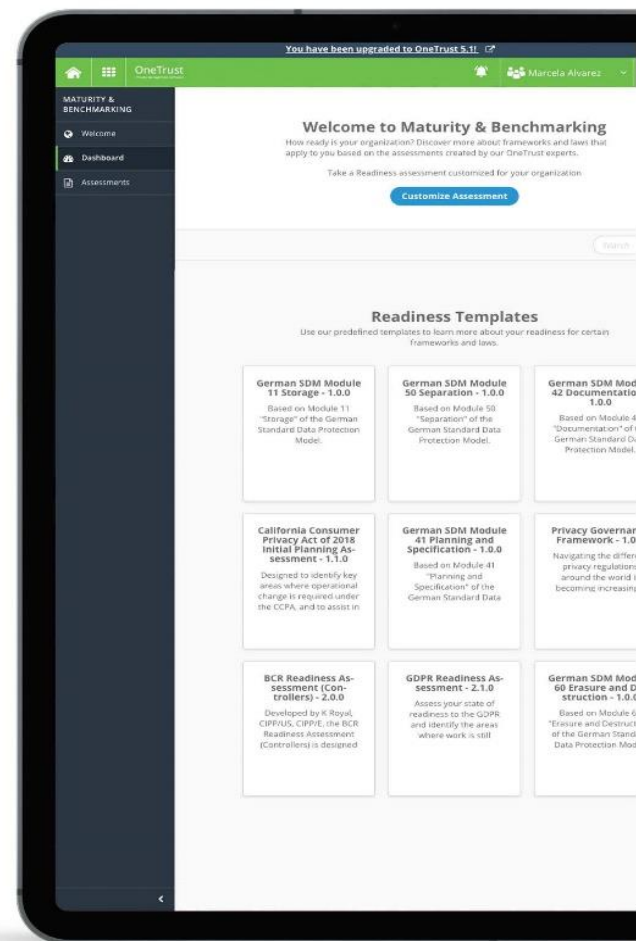
#### Third-Party Risk Management

- **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

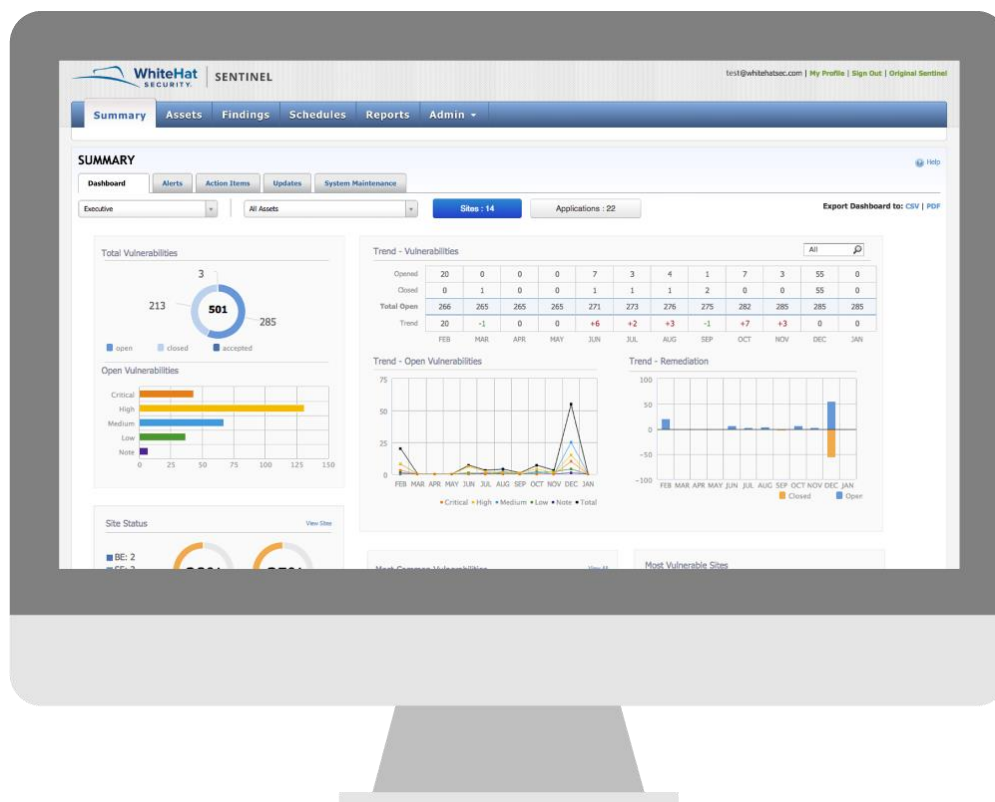
- **Incident & Breach Response:** Intake & Lifecycle Management
- **DatabreachPedia Guidance:** Built-in guidance from 300 laws



**GET STARTED TODAY | [ONETRUST.COM/FREE-EDITION](https://onetrust.com/free-edition)**

**LEARN MORE ABOUT ONETRUST | [REQUEST A DEMO | ONETRUST.COM](https://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](https://www.whitehatsec.com/info/security-check/) to sign up at this URL: <https://www.whitehatsec.com/info/security-check/>

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

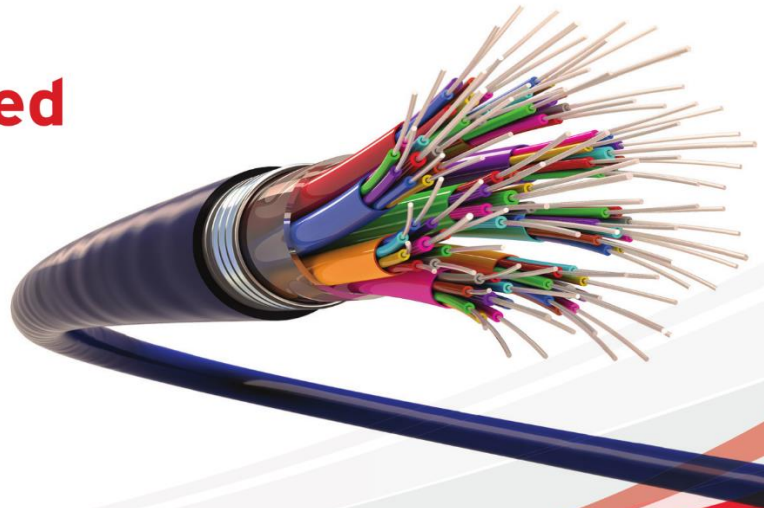


# Detect and prevent breaches at wire speed

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.



## 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



### Please get in touch:

Bharat Mistry, Principal Security Strategist  
Bharat\_mistry@trendmicro.co.uk

[www.trendmicro.co.uk/xgen-cyber](http://www.trendmicro.co.uk/xgen-cyber)

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.



# STRATEGIC COMMUNICATIONS

## 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](http://www.vrge.us/cybersecurity)

**vrge**

Navigate the Politics  
of Disruption



# WORK ON THE FRONT LINES PROTECTING AMERICAN INTERESTS

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working to safeguard Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll find a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.



**AFCivilianCareers.com/CYBER | #ItsACivilianThing**

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.





# 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](http://www.DontBeBreached.com/Free)





**"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](http://www.nightdragon.com)

# 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<sup>1</sup>



**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<sup>2</sup>**



**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<sup>3</sup>



**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<sup>6</sup>



**How NotPetya changed the game** — While Russia is generally blamed for NotPetya,<sup>4</sup> 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.<sup>5</sup>



**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.

<sup>1</sup> <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

<sup>2</sup> <https://www.securityweek.com/petyanotpetya-what-we-know-first-24-hours>

<sup>3</sup> <https://www.securityweek.com/notpetya-attack-costs-big-companies-millions>

<sup>4</sup> <https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/>

<sup>5</sup> <https://ironnet.com/white-paper-survey-download/>

<sup>6</sup> [https://www.atlanticcouncil.org/images/files/publication\\_pdfs/403/022212\\_ACUS\\_NatlResponsibilityCyber.PDF](https://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF)

# ARTICLES

A hand holding a black pen is positioned over a spiral-bound notebook on a wooden desk. To the left of the notebook is a white computer keyboard. The background is a blurred office setting with bookshelves. A semi-transparent network diagram with blue lines and nodes is overlaid on the right side of the image. The word "ARTICLES" is written in large, bold, black capital letters across the center of the image.





## Covid-19 Unveiled a New Security Gap

By Eddy Bobritsky, CEO & Co-Founder, Minerva Labs

As COVID-19 spreads, more organisations are enforcing remote work from home, making employees home computers more vulnerable than ever to cyberattacks.

The attackers don't need to attack the perimeter any more, they can go for much easier targets such as home PCs and Users.

The solutions organisations use to day are limited at the same time, there is a desire to increase the home-user's productivity as much as possible during these times.

The desire, force organisations to take extra risks without solid defense (endpoint security) as the CISO used to within the organisation or the corporate PCs and laptops.

The two main reasons for limited endpoint security are:

- operational challenge:
  - the variety of OS and Applications flavour on Home-PCs are huge, and it's simply impossible to deploy and manage endpoint security at scale.
- privacy
  - privacy regulations do NOT allow corporates deploy corporate endpoint security controls on non-corporate endpoints, simply because, if after working hours the Home-PCs been used to surf funny sites, it's non of the corporate business. deploying endpoint security on such home-PCs will enable the corporate to access such data, which is private therefore it's illegal.

In the work-from-home reality, CISO is limited with the security controls it can deploy, and usually will use VPNs, Virtual Working Environment, 2FA, etc. these are great, but do not provide the security controls that are needed on the endpoint.

Minerva is the only vendor that eliminates this risk by providing a unique, install-free Remote User Protection for any endpoint throughout the entire VPN session with full user privacy

---

Modern enterprises increasingly rely on a distributed workforce, with contractors, employees and other users connecting remotely over VPN. In many cases, these individuals access sensitive resources from unmanaged devices (BYOD). This might be because they are user- owned devices or because another organization owns them.

In such scenarios, the enterprise still needs to take reasonable precautions regarding the security posture of the connecting system.

Minerva Labs offers a unique, effective and endpoint protection solution for unmanaged devices in such scenarios.

Minerva's Install-free Remote User Protection (RUP) software protects unmanaged endpoint devices (BYOD) that are connecting to enterprises throughout the entire remote (VPN) session from malware and non-<sup>[SEP]</sup>malware-based attacks. Minerva accomplishes this by integrating with the organization's VPN via the security policy, known as the Host Checker software, and provide a solution that delivers Minerva's protection benefits in a click of a button. This approach reinforces other security mechanisms that might exist on the remote system without interfering with the user's day-to-day activities and without compromising its privacy. Minerva's Remote User Protection is configured as part of the VPN's security policy that is activated when the user attempts to initiate the VPN connection without requiring the user to reboot and without interfering with other security tools or software on the system. Once activated, Minerva provides all of Minerva's prevention abilities to the end-user with no installation required.<sup>[SEP]</sup>Minerva's Remote User Protection doesn't require any type of installation or any special permissions thus, the install-free agent will run with the user session permissions that are executing the remote (VPN) session and will prevent any attacks during that session.

When allowing users to connect to their network over a VPN, enterprises often struggle to balance the need to protect their resources from infected remote systems by imposing strict security requirements on those endpoints. In many cases, the connection is initiated from an unmanaged device—an endpoint that the enterprise doesn't own (BYOD), for instance when employees use their personal home PC or when contractors establish a VPN connection from a computer not owned by the enterprise. Sometimes the VPN creates a false assumption that the connected system is secure, while only the connection (tunnel) is secured, the endpoint is NOT.

Though the organization could impose some security requirements on the connecting system, it often lacks the ability to enforce them or to mandate that the full corporate endpoint security stack be present on the remote host. Minerva's Remote User Protection offers the following benefits for such circumstances:

- It provides safeguards against vast numbers of malware that otherwise would put the enterprise at risk.
- It integrates with the organization's VPN software to launch malware scans and to refuse or terminate the connection when necessary.
- It is seamless, able to operate without slowing down the remote user's system.
- It doesn't conflict with security or other non-malicious software on the remote system.



---

## About the Author

Eddy Bobritsky, CEO & Co-Founder, Minerva Labs

Eddy is a cyber and information security domain expert. Before founding Minerva Labs, Eddy was a senior cyber security consultant for the defense and financial sectors. During his military career in the Israel Defense Forces (IDF) as an officer in different cyber units, Eddy was in charge of the largest Endpoint Protection project in Israel, from design, through implementation, to maintenance of hundreds of thousands of endpoints. Eddy's rule of thumb is to 'keep things simple' in order to help businesses operate seamlessly, which is why he started Minerva. Eddy holds a Master's degree in Business Management and Information Technology.





# threat

## There's a Hole in Your Threat Detection Strategy—It's Called East/West Traffic

By Carolyn Crandall, Chief Deception Officer, Attivo Networks

One of the most popular targets for attackers, cybercriminals, and other bad actors is east/west network traffic. This is network traffic that originates from one internal host or network segment, and whose destination is another internal host or network segment.

North/south traffic, on the other hand, moves from an internal network out to the Internet. North/south is where organizations have historically invested, and includes security controls such as firewalls, intrusion detection/prevention systems, and proxies.

Ensuring good threat detection for east/west—or lateral—traffic has never been more important for organizations. The ability to move undetected through the network is key for successful ransomware attacks, and detecting that movement is increasingly critical as damaging and sophisticated ransomware becomes more pervasive.



---

Companies can choose from several methods to address the challenge of protecting lateral traffic, but each of these has limitations that ultimately make them ineffective at detecting lateral movement. One emerging method—threat deception—uses new technology and a different approach that delivers the comprehensive protection organizations need to efficiently monitor east/west network traffic.

Before exploring this new approach that centers on concealment, fakes, and misdirections, let's take a look at the other options.

### Logging at the endpoint

With this approach, organizations use technology such as security information and event management (SIEM) logging to aggregate and monitor endpoint logs to look for suspicious behavior that might indicate a security incident.

Upside: This is a native capability in all modern operating systems, making it readily available.

Downside: The storage and analysis of log data is a big challenge. Security teams need to pull audit logs from a large number of systems used throughout the organization and then bring that into a SIEM platform. The volume of data can be enormous, especially for large enterprises. Because of the strain, companies can't rely on SIEM only. They need to leverage a big data analytics platform, which does not work well as an alerting system.

### Monitoring agents at every endpoint

This involves deploying agents such as endpoint detection and response (EDR) tools that can log network connections.

Upside: Many EDR products have this function, and using behavioral detection provides insights that include forensics and supporting information for root cause analysis and threat hunting.

Downside: As with logging at the endpoint, storage and analytics at scale is a challenge. Companies need to install agents at every endpoint, and while EDR agents work well for real-time detection, managing the large and growing volume of alerts generated can be overwhelming for cybersecurity teams. The filtering process needed is labor-intensive and time-consuming. Often, manual analysis is required to identify issues, and there can be long delays in addressing genuine threats.

### Deploying NetFlow collection at core routers and switches

NetFlow, a network protocol developed by Cisco to collect and monitor network traffic flow data generated by NetFlow-enabled routers and switches, analyzes network traffic flow and volume to determine where the traffic is originating, where it's going, and how much traffic is being generated.

---

Upside: NetFlow, now a de facto industry standard, is supported by platforms from several leading network equipment providers, so it is built into most core routers and switches.

Downside: NetFlow is known to affect the performance of the devices where it is enabled, such as routers and switches. This can have a detrimental impact on network performance, which can be a problem for companies trying to keep up with growing volumes of data and demand for higher network speeds.

### Implementing a dedicated monitoring network

With this method, organizations aggregate network traffic to one location via tap and span ports or inline proxies and monitor the traffic.

Upside: This provides a dedicated function for continuous visibility to the overall performance of the network and allows organizations to observe all traffic traveling, as well as monitor every connected device and their performance metrics. It is typically simple to manage and operate.

Downside: Scaling of this method is problematic. Increasing internal bandwidth can quickly overwhelm the aggregator, causing loss of monitoring or dropped packets, and there can be network performance issues.

### Deploying an internal firewall

Using this tactic, companies leverage their legacy firewalls to segment and monitor the network and then look at the connection logs.

Upside: Many organizations can use older firewalls that they had decommissioned when they updated their infrastructure with Web application firewalls. They've already made the investment in these products, so there's no new purchase cost. They can redeploy the equipment internally to meet their needs.

Downside: This deployment does result in extra infrastructure to maintain and new rules sets to manage. There are scaling issues with logging and analysis. Companies must also deal with the same issues as they do when pulling data from a lot of locations on the network.

### Using an internal intrusion detection and prevention system (IDPS)

IDPS is a network security tool that monitors network and system activities and detects possible intrusions. Organizations can deploy IDPS inside their networks and monitor east-west traffic.



---

Upside: Many organizations are already doing this and can use decommissioned systems or Linux systems for simple IDPS functions.

Downside: Signature-based detection can miss threats. In addition, organizations can have deployment issues, such as failing to have sufficient sensors to provide the required visibility.

### Implementing network traffic analysis

This is where organizations collect network traffic and analyze it to look for potential threats.

Upside: Network traffic analysis is a dedicated function that has useful capabilities for internal threat detection and analysis.

Downside: This tends to be an inefficient method for organizations. Data storage and analysis at scale is problematic. For many companies, it's a challenge to tune systems, and there are visibility issues.

### Leveraging the deception approach

Deception and data concealment technology is an emerging category of cybersecurity, with products that can prevent, detect, analyze, and defend against advanced attacks by hiding and denying access to data. Deception uses misdirections to lead attackers away from production assets, and a variety of decoys placed at the network and endpoint level to identify threats. The technology takes a proactive approach to security by aiming to deceive attackers, control their path, and then defeat them.

Upside: These tools do not rely on signatures, network traffic capture, or behavioral analysis. There is no need to collect logs or for traffic storage, log aggregation, analysis, or creating rules. Alerts are based upon engagement or detection of unauthorized activity, which removes false-positives and includes threat intelligence for actionable incident response.

These solutions can identify threats starting at the endpoint, targeting Active Directory, and through the network, as they attempt to move laterally and escalate privileges. From the network side, decoys can detect suspicious or malicious connection attempts from another internal host. From the endpoint, local deception functions can identify inbound or outbound connection attempts to non-existent ports and services as suspicious or malicious. This is important because it prevents an attacker from fingerprinting a system and targeting vulnerable services.

Downside: Misperception may be the biggest challenge for this technology. There remains a limiting association with legacy honeypots, and some believe it is only for organizations with mature security operations. Not all deception technology providers offer products that can achieve all of the capabilities, and as such, cybersecurity teams will need to be careful in their solution selection.

---

## Conclusion—Aiming for Efficiency and Effectiveness

Many of the options for east/west threat detection clearly provide efficiencies for organizations. They can choose to implement one or more tools they already have in place and know how to use them, so there's no extra cost. Why invest in something new when you can get by with the old?

Unfortunately, organizations that rely on less-than-ideal solutions will come to the realization that convenience does not always equate to effectiveness. Many of these methods are not inherently designed to detect all the various types of attacks.

With security technology based on both prevention and detection, organizations have an opportunity to get the best of both worlds—efficiency with effectiveness—and protect themselves and their business partners from the latest threats.

### About the Author

Carolyn Crandall is the Chief Deception Officer and CMO at [Attivo Networks](#), the leader in deception for cybersecurity threat detection. 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 taking companies from pre-IPO through to multi-billion-dollar sales and 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 operational, 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.

Carolyn is an active evangelist, blogger, byline contributor, and speaker on industry trends and security innovation. She's received many industry recognitions including a Top 100 Women in Cybersecurity 2020 and Top 25 Women in Cybersecurity 2019 by Cyber Defense Magazine, Cyber Security Marketer of the Year 2020 by CyberDojo (RSA), Reboot Leadership Honoree (CIO/C-Suite) 2018 by SC Media, Marketing Hall of Femme Honoree 2018 by DMN, Business Woman of the Year 2018 by CEO Today Magazine, a Women of the Channel (11 consecutive years) and a Power 100 member (10 consecutive years) by CRN.

Carolyn serves as an Advisory Board Member for the Santa Clara University Executive MBA program and co-authored the e-book Deception-based Threat Detection, Shifting Power to the Defenders.







# Industrial Control System - Security Focus of Federal Effort

By Trip Hillman, Director of Cybersecurity Services at Weaver

More and more, industrial control systems have been the targets of malware, ransomware and other kinds of cyberattacks. These attacks jeopardize operations that control essential service and critical functions, and may result in loss of life, property damage and disruption of essential services, such as electricity, water and telecommunications.

Industrial enterprises that operate SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control System) devices are even more likely to be vulnerable to these cybersecurity threats. With SCADA system life cycles reaching 15 years or longer, older devices may be more sensitive or may not be compatible with newer computers and protection measures. This makes them more vulnerable to cyberattack, which can lead to breaches of connected networks, of physical plant operations, environmental controls, or even life- threatening safety failures.

The Cybersecurity and Infrastructure Security Agency (CISA) recently announced [an initiative to strengthen and secure industrial control systems](#) in response to such growing cybersecurity threats and risk management issues.

CISA was created in 2018. Part of the federal Department of Homeland Security, it is responsible for functions previously performed by the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

This new initiative signals the federal agency's intention to bring resources and focus to ICS security to drive meaningful, measurable and sustainable change.

---

Typically, the SCADA system functions as an active operation's nervous system, notifying operators of failed activities, errors and equipment that is functioning out of tolerance. Data from a comprehensive SCADA system permeates an organization's business processes by:

- driving maintenance and safety programs
- informing operational efficiency assessments
- providing details for capital investment decisions
- incorporating the data into the Enterprise Risk Management function

Because SCADA systems provide such foundational and pervasive data, if it is inaccurate or compromised, the impact on a business can be dramatic.

CISA's vision is to achieve a collective approach with industry and government that will:

- Empower the ICS community to defend itself
- Inform ICS investments and proactive risk management of NCFs
- Unify capabilities and resources of the Federal Government
- Move to proactive ICS security
- Drive positive, sustainable, and measurable change to the ICS risk environment

While taking responsibility for leading the initiative, CISA calls on the private sector to participate. In the first of four pillars that will guide its efforts, CISA aims to "Ask more of the ICS community, and deliver more to them."

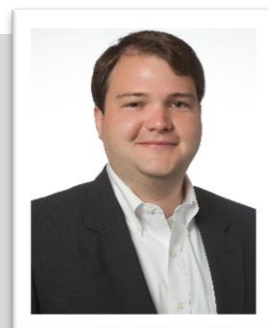
The initiative places significant emphasis on developing and implementing joint ICS security capabilities, mapping and identifying the degree to which specific national critical functions (NCFs) depend on ICS, and elevating and prioritizing ICS security around a unified "One CISA" strategy.

Over the next several years, CISA will work with other government agencies at the federal, state and local level as well as private partners in the ICS community. Working together, the goal is to achieve sustainable ICS security and to drive wise ICS security investments in the future.

Organizations should view this as an opportunity to take a fresh look at the overall security strategy for ICS and SCADA devices and networks and ensure plans have been updated to meet current expectations.

#### About the Author

[Trip Hillman](#) is Director of Cybersecurity Services at [Weaver](#), a national accounting firm. He has nearly a decade of hands-on experience evaluating IT security in a broad range of environments. He has performed and led over 200 substantial audits across hundreds of unique IT environments and is called on regularly to help organizations evaluate their overall security posture and to develop prioritized, balanced roadmaps for increasing security maturity. Trip can be reached at [trip.hillman@weaver.com](mailto:trip.hillman@weaver.com) and at our company website: [www.weaver.com](http://www.weaver.com).







## What Is Being Done, And How Can They Improve This Critical Infrastructure's Cyber Risk?

By Martin Banks

People have worried about the safety of nuclear energy since it first came around in the mid-twentieth century. Nuclear energy has a lot of potential for powering our world, but it has just as much potential for destruction. As a result, the facilities that deal with this kind of power have to pay extra attention to their security.

The nuclear industry is no stranger to high security, but today's threat landscape is changing. It's not just physical hazards and attacks that organizations and governments have to worry about anymore. Cyberattacks are the fastest-growing crime in America, and the nuclear industry may be unprepared to handle them.

The Nuclear Threat Initiative (NTI) recently released their biennial Nuclear Security Index, and the results are troubling. Since cybercrime has started to become a more prominent threat, the Index has taken cybersecurity measures into account. According to this year's report, the world's nuclear facilities have some work to do.

### Cyberthreats to the Nuclear Industry

The digitization of the industry makes preventing physical threats a more complicated process. As helpful as IoT security measures can be, they also present the danger of hackers. When criminals can hack their way past things like cameras and locks, it's more challenging to stop them.

---

Cybercrime's most significant danger is that criminals don't have to step foot in a facility to infiltrate it. Hackers could steal sensitive data about material transports, allowing them to get their hands on dangerous resources. Cyberterrorists could overload a reactor's system, causing a catastrophic meltdown.

The threats that cybercrime poses to nuclear facilities run from monetary theft at best to radioactive fallout at worst. If a facility suffered a cybersecurity breach, it could put countless people in danger. If the world hopes to avoid another Chernobyl, nuclear facilities need to adopt thorough cybersecurity practices.

### Nuclear Cybersecurity Needs Improvement

According to the NTI's report, nuclear security as a whole saw significant improvements between 2012 and 2018. The NTI started looking at cybersecurity in 2016, so that means even previous cyber efforts seemed good. Unfortunately, between 2018 and 2020, the nuclear industry's cybersecurity efforts fell short.

As cyberthreats have evolved, the industry's security should have evolved alongside them. The 2020 Nuclear Security Index says that while regulations are adapting, many countries haven't adopted them. Cybersecurity remains one of the three most significant areas of weakness, and these threats are growing.

Only 24% of indexed countries scored high for cybersecurity, and just 4% got a perfect score. Perhaps more troubling, another 24% of nations didn't get any points for their nuclear cybersecurity. The Index also introduced a security culture score this year, and 65% of countries scored low or got a zero there.

### How the Industry Can Improve

The NTI's report also contains suggestions for how nations can improve their nuclear security. Their first recommendation for low cybersecurity is to avoid becoming complacent about cyberthreats. Nuclear facilities have to take a proactive approach to cybersecurity, updating and upgrading it as threats evolve.

The NTI also recommends that nations establish regulations about cybersecurity in nuclear facilities. While having these rules in place is critical, it's not the only part of the equation. After setting up these regulations, authorities need to enforce them, as many countries with guidelines in place don't necessarily adhere to them.

Another point that the NTI has made repeatedly through the years is to reduce complexity. In an earlier cybersecurity release, they explained how being digitally sophisticated can be a threat in risky areas like nuclear power. The more complicated the system, the more staff may not know how to secure it properly.

### How Current U.S. Cybersecurity Requirements Measure Up



---

According to the NTI's rankings, the U.S. achieved ninth place in securing materials and seventh in protecting facilities. Those results indicate that the country's relatively safe when it comes to nuclear facilities, but there's still some work to do. For both categories, the NTI recommends that the U.S. pay more attention to its cybersecurity.

The U.S. has specific regulations for access security in high-risk sites like these facilities, and cybersecurity is no different. Atomic power plants have to meet requirements from the U.S. Nuclear Regulatory Commission (USNRC). While the NTI praises this step, it notes how the nation needs to mandate regular cybersecurity assessments.

For all their regulations, the U.S. doesn't require frequent testing of cybersecurity systems. Given the evolving nature of cybercrime and the sensitivity of nuclear facilities, that's quite the risk. The NTI also recommends that the U.S. mandate regular assessments of sites' security cultures.

### About the NTI

The NTI came about in 2001, founded by former senator Sam Nunn and CNN founder Ted Turner. Working with experts and governments around the world, the NTI works to assess global nuclear threats and establish a framework to address these dangers. While cybersecurity isn't their only point of focus, it's become a more prominent one as cyberthreats have grown.

Security, business, science and international diplomacy experts make up the NTI's board of trustees. They also feature a panel of world leaders from governments and academic institutions to assess these issues accurately. The Nuclear Security Index, their primary publication, has come out since 2012.

The Index covers three different areas: countries with nuclear materials, those with nuclear facilities and those that could be safe havens for illegal nuclear activity. Those categories include 22, 47 and 154 nations, respectively, with some overlap. Some countries provide data directly to the NTI, while publicly accessible data fills in the gaps.

### Cybersecurity Is Essential in a Digital World

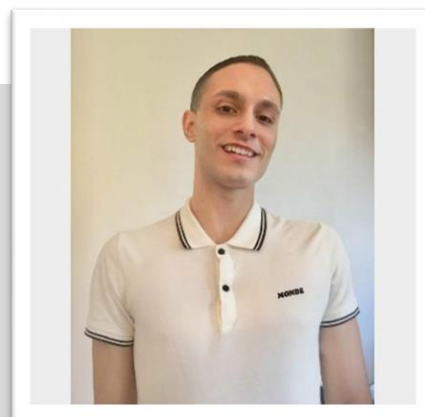
Fear of nuclear fallout may not be as high as it once was, but it's still a relevant concern. With the rise of cybercrime, these fears may grow again, especially as some nations struggle to meet security standards. In any industry, cybersecurity is now essential, and atomic materials are no different.

Without strong cybersecurity standards, any kind of facility could be at risk of an attack. With assets as risky as nuclear materials, these standards are even more crucial. If the world wants to avoid a catastrophic nuclear event, these facilities will need better cybersecurity.

---

### About the Author

Martin Banks is the founder and Editor-in-Chief of Modded. You can find his writing all over the internet. He covers tech, gear, cars, and more.







# Low Latency Encryption Will Secure the U.S. Electrical Grid

By John Downing, President, Encrypted Grid, LLC

The electric power grid is the backbone of America, generating and transmitting the energy to empower all sectors of our economy. Reliance on the electric grid is our fundamental need. Because of this, it has long been considered a logical target for a catastrophic cyberattack.

Power grid outages are inevitable, and the economic impacts can be significant. One of the most notable in the United States was the 2003 Northeast Blackout which left 50 million people without power for four days and caused economic losses between \$4 billion and \$10 billion. In 2015, a cyber attack took down parts of a power grid in Ukraine. In March 2019, a solar generation utility in the United States experienced communications outages when an attacker exploited known firewall vulnerabilities to cause unexpected device reboots. Most recent was the June 2020 cyberattack that disrupted Honda's internal computer networks, forcing it to shut factories across the globe and leaving employees cut off from email or internal servers. The attack appears to have been carried out by software designed to attack the control systems for a wide variety of industrial facilities, including power plants.

America has been heeding warnings of a widespread cyberattack on the power grid. In the last two years, reports from DHS, the Federal Bureau of Investigation and the U.S. Intelligence Community have revealed that Russian cyber attackers have covertly gained access to U.S. and European critical infrastructure. In June 2019, U.S. officials revealed ongoing efforts to deploy hacking tools against Russian grid systems as a deterrent and a warning to Russia. Around the same time, U.S. grid regulator, the North American Electric Reliability Corporation (NERC), warned of a major hacking group with suspected Russian ties was conducting reconnaissance into the networks of electrical utilities. If successful, these foreign adversaries -- most notably from Russia, China, North Korea and even Al Qaeda -- can shut off power to millions.

---

These threats from cybercriminal groups, including Dragonfly, a.k.a. TEMP.Isotope or Energetic Bear, and Industroyer, are escalating and have prompted an executive order signed by President Trump in May 2020 declaring these types of threats to be a national emergency.

In adhering to NERC's mandated Critical Infrastructure Protection (CIP) protocols, power companies have continued to fortify their defenses for protecting electricity generation and transmission systems against cyberattacks. But because of a technical issue, the power grid remains vulnerable.

### **The Power Grid's Command and Control Operations Require Lightning-Fast Communication.**

The U.S. power grid today comprises roughly 3,300 utilities that work together to deliver power through 200,000 miles of high-voltage transmission lines; 55,000 substations; and 5.5 million miles of distribution lines that bring power to hundreds of millions of homes and businesses.

The ability to protect the grid is not possible with the existing encryption systems of today. The grid's command and control systems in a lot of cases must communicate as close to real time as possible. Unfortunately, encryption systems currently on the market take over 50 milliseconds to encrypt and transmit this data. The current use of overlaying firewalls, routers, and network switches can be defeated by hackers. Even physical separation of systems falls prey to human error.

The grid's command and control systems include:

- Supervisory control and data acquisition (SCADA), for monitoring, gathering, and processing real-time data through human-machine interface (HMI) software often at remote locations;
- Distributed control systems (DCS) that improve reliability of control, process quality and power plant efficiency;
- Turbine generator control systems;
- Substation and generator protection systems.

The ability to protect and guard these systems requires never before seen speeds of data encryption and networking.

### **Vulnerabilities Leave the Power Grid Wide Open to Cyberattacks.**

If the COVID-19 pandemic has taught us anything, the unthinkable can happen. In the United States, there currently are around 10,000 power plants producing greater than 1 megawatt. In addition, there are thousands of extra power plants. If a hacker gets into the operational technology (OT) system and effectively controls system voltage or frequency, this could damage not only one plant, but dozens -- upwards of 20 to 40 power plants in a region -- thus possibly resulting in extended periods of loss of electricity.



---

In such a situation, the needed components that make up the power grid, such as transformers and substation equipment, are not readily available. The largest transformers that make up the biggest substations in every state are built on demand; these take 12 months or more to build. Power companies can redirect electricity around a single substation, but if hackers gain access into command and control stations, they can adjust voltage and frequency of the power grid causing multiple failures in a region.

For years, industry leaders have known about the power grid's vulnerabilities, especially an aging infrastructure that's extremely expensive to replace. Most leaders are praying that the unthinkable will never happen, or that these hackers will just magically "go away."

U.S. Senator Angus King (I-Maine), co-chair of the bipartisan Cyberspace Solarium Commission (CSC), has been advocating for the inclusion of vital cybersecurity amendments in the 2021 National Defense Authorization Act (NDAA). In a speech on the U.S. Senate floor on June 30, 2020, Sen. King stated: "Just as the pandemic was unthinkable, nobody could think of an attack that could bring down the electric system, or the transport system, or the internet, but it can happen. The technology is there... I believe, Mr. President, the next Pearl Harbor will be cyber. That's going to be the attack that attempts to bring this country to its knees, and as we've learned in the pandemic, we have vulnerability, and we have to prepare for it."

Progress has been made in detecting hacks and threats when they are occurring. However, we need encryption systems that will prevent hacks from ever occurring in the first place.

### **Power Providers' Out-of-Date Software Systems are Difficult to Protect.**

Among its many directives, the North American Electric Reliability Corporation (NERC) issues critical infrastructure protocols (CIPs) that mandate all owners, operators and users of the U.S. bulk power system comply with Federal regulations (FERC) from the U.S. Department of Energy.

Among NERC's CIP requirements are monthly or quarterly virus updates on HMIs. Despite Windows 10 being the latest upgrade, many power control systems are still operating on legacy technology platforms, such as Windows XP, Windows NT and Windows 2000 platforms, which were not designed with advanced security in mind. They are extremely vulnerable and expensive to upgrade. An internal employee tasked with running NERC's CIP updates on a legacy platform could inject a virus simply by using a thumb drive or USB stick.

NERC requires energy providers to perform daily tests and report their levels of protection; fines for violating these regulations can be up to \$1 million per day, per offense. These entities spend hundreds of thousands or millions to stay up to date on NERC guidelines. The average power plant producing greater than 10 megawatts spends typically \$250,000 per year minimum to maintain NERC and FERC regulations.

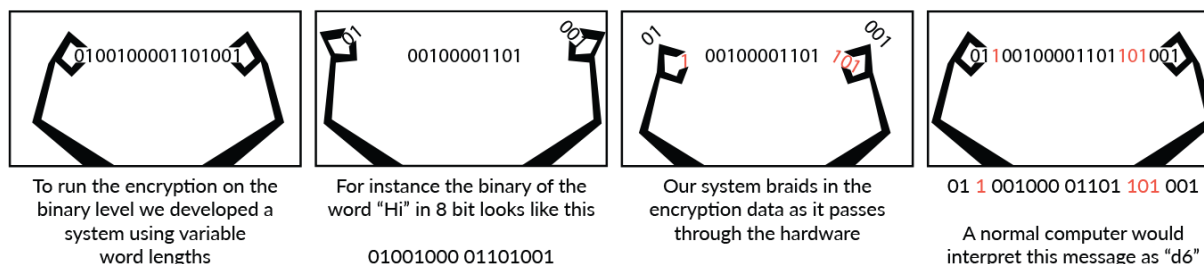
Most large utilities and independent power producers (IPP's) use a remote central location to monitor and collect data from their plants. These remote connections are only being guarded by fancy firewalls and routers. Because of the high speed of the data required by command and control systems, none of

them are encrypted. Many encryption companies are attempting to offer the next best solution, including services to scrub systems of malware, ransomware and viruses. But this is not enough.

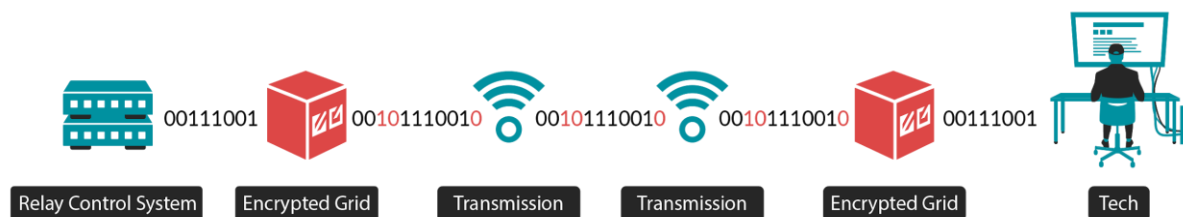
### The Solution: 0.06 Milliseconds.

Until now, the need for an extremely high encryption speed (less than 4 milliseconds) to protect the power grid's command and control systems has not come close to being solved.

In July 2020, Encrypted Grid, LLC, successfully tested a patented encryption solution to protect the power grid at an extremely low latency of 0.06 milliseconds. The encryption is non-algebraic and happens at the binary level. Everything is secured; the binary encryption scheme creates its own ever-changing computer language using variable word lengths. Placed in stand-alone hardware units, the technology braids the encryption data as it passes through, eliminating backdoors and user errors that can occur on user-driven software programs.



Because the system has zero software controls or operating systems, it's called an Actual Private Network (APN, versus the software-reliant VPN). The encryption can effectively protect and overlay even the oldest legacy systems, at a fraction of the cost of upgrading or replacing existing networks. It is proven to keep non-corporate traffic outside of its walls. Here's how this will work:



- The APN forms a solid cyber wall around the entire corporation, protecting everything from the IT to the OT. This impenetrable wall allows both sides to continue full communications within their organization without disruptions and without fear of someone in an admin role giving access via their computer being hooked up to a combination network.

- 
- Substations, switchyards and generator protection relays can remotely communicate with one another through the Generic Object Oriented Substation Event (GOOSE) network enabling super high-speed data collection, command and control. The IEC 16850 protocol mandates that all OEMs use GOOSE. Because the protocol requires a high encryption speed of less than 4 milliseconds for protective relaying, GOOSE is vulnerable to cyberattacks.
  - Encrypted Grid's technology is able to seamlessly convert and encrypt hundreds of access points in every power plant, including multiple protocols from GOOSE, turbine generator control systems, SCADA and DCS all on the same network.

In November 2019, Encrypted Grid began testing its encryption in lab environments. In July 2020, this testing was extended throughout the United States. The algorithms have been tested by highly advanced mathematicians at the Ph.D. and doctoral levels, who have validated them for strength and legitimacy. In multiple tests performed, Encrypted Grid successfully demonstrated the ability to encrypt data fast enough to not interfere with command and control systems. This is using our prototype system that currently has a latency of less than 0.06 milliseconds.

In June 2020, Encrypted Grid demonstrated its hardware to Casco Systems in Cumberland, Maine.

"I was skeptical when first introduced to the Encrypted Grid hardware," said Casco Systems president, Kevin Mahoney, PE. "I didn't believe that you could encrypt high speed communications in under 2 milliseconds from end to end, without adversely impacting system performance. This speed is necessary for protective relays and control systems used in power generation and transmission. When Encrypted Grid demonstrated reliable encryption and transmission of IEC 61850 GOOSE messages in under 1 millisecond, I became convinced that a solution is here."

"I've been in controls and protection for over 30 years and am amazed how efficiently this encryption technology works," added Mahoney. "I finally have hope that we can secure the grid from cyberattacks."

Securing America's power grid from foreign adversaries and cybercriminal groups cannot depend on vulnerable software programs and operating systems. The solution lies in a hardware-based device with extremely high encryption speeds, which until now has not been commercially available. The solution is encryption in 0.06 milliseconds, and I believe it's here.



---

## About the Author



John Downing is president of Encrypted Grid, LLC, a patented data encryption technology that will revolutionize cyber security of the Bulk Electric System. He is a power generation thought leader with over 30 years of experience in the design, manufacture, operation, troubleshooting and repair of complex power generation control systems. He is the CEO and Principal of multiple power generation companies.

John Downing can be reached online at [john.downing@encryptedgrid.com](mailto:john.downing@encryptedgrid.com). For more information, visit <https://encryptedgrid.com/>.



## Cyber Warfare and Its Impact on Businesses

By Kumar Ritesh, Founder and CEO, CYFIRMA

Over the past two decades, businesses, governments and the public have all witnessed unprecedented growth in the digital economy. From the design of critical infrastructure to the sale and purchase of a simple pen, all this can be done on a digital platform. But every evolution has a parallel, and this is true for digitization. Threat actors and their attack surfaces have evolved, expanded, and are now replacing the traditional combat war with a new approach – the Cyber Warfare.

Since the turn of the 21st century, the world has seen a shift from traditional combat to cyber warfare. One of the main factors for this shift is the fact that digitization has now become part of the very fabric of growth for organizations, and with it, the increased attack vectors.

According to IDG 's 2018 Digital Business Survey, 89% of organizations have already adopted or are pursuing a digital-first strategy. Of the 7 per cent respondents who fully implemented this strategy, almost one-third (32%) said that digital transformation has already helped their organization achieve an average increase of 23 per cent in revenue growth.

Governments have become increasingly aware that digitization and its advanced networks are now the driving force of a country's economy. From the financial sector, including banking services, to sectors such as transport, power and utilities, everything is digitally controlled and monitored by computers. Intelligence agencies are particularly focused on cyberattacks on businesses that control key and critical infrastructures such as nuclear installations, defence services, hospitals and air traffic.

---

State-sponsored hackers have found a preference for corporate espionage, the exfiltration of intellectual property to narrow the technological gap with competing nations, the stealing of PII and CII data for financial gain, and defaming adversaries to further socio-political agendas.

Hackers have explored new attack surfaces as industry and country IT systems have remained vulnerable with poorly configured and outdated programs and applications. Weak applications or networks become a test field for hackers as they carry out advanced persistent threat (APT) attacks, first establishing long-term connections, then understanding the architecture of the targeted organization, and finally starting to mine sensitive data such as PII, official documents, agreements, compliance data, etc. The Anthem APT attack, which compromised almost 80 million customer PII data, is a popular example of such an attack.

It is now of utmost importance for governments and businesses to adopt a predictive approach to protecting their reputation, ensuring business continuity and protecting national interests. However, this can only be achieved by going deep into the hacker trenches to gain real-time cyber threat visibility. To this end, we need a platform that can discover evolving threats, decode and segregate valuable cyber threat insights from the vast amount of data available.

In order to beat hackers in their own game, cyber intelligence is needed for businesses to take action against unseen threats. Having a platform that allows one to predict a cyberattack is needed more than ever before. And there's one that fits the bill – CYFIRM's DeCYFIR.

Using DeCYFIR, CYFIRMA researchers analyzed data sources across deep / dark web, hacker forums and closed communities, and uncovered the following cyber-war threat scenarios.

#### • Trade wars fueling cybercrime and cyber warfare

The ongoing trade war between two of the world's largest economies – the US and China – has already created a geopolitical strain. The US has long accused China of unfair trade and theft of intellectual property. The race for political and technological supremacy has now fueled cyber warfare.

#### • Geopolitical conflicts between neighboring countries

Relations between Japan and South Korea, China and India, China and Australia have deteriorated rapidly over wartime issues and bilateral trade differences.

War hysteria, historical differences, and geopolitical supremacy will lead state-sponsored hackers to push their cyberattack threshold to a limit. Social hacktivists, political parties and large corporations will be drawn to cybercrime as a means of achieving business and political objectives, fueling the expansion of the hackers-for-hire economy.



---

### • Enhanced versions of previously used malware and attack vectors

Hackers have started to refurbish and use enhanced versions of previously used malware and attack vectors.

One such example is the BlackEnergy malware in Ukraine. Recently, this malware has been upgraded (now known as BlackEnergy 3) and sold on the dark web. It now adds the SSH keys of the attacker to the victim's machine in a list of authorized key files, which then trusts the attacker's key to secure communication. Similarly, CYFIRMA's threat intelligence algorithm caught a suspected Vietnamese state-sponsored group, OceanLotus, exploiting old vulnerabilities and using existing malware to attack opinion leaders, influencers, banks, media houses, real estate agencies, and foreign companies across a number of countries, including China, Laos, Thailand, and Cambodia.

### • Emerging and Elastic Attack Surface

New technologies such as 5 G Internet of Things (IoT), autonomous critical infrastructure, artificial intelligence, industry 4.0, cryptocurrency, cloud, virtual reality (VR), augmented reality (AR), drones and many more have also increased the attack surface.

CYFIRMA's intelligence research has revealed new attack vectors such as identity theft, fraudulent transactions, asset theft, impersonation, malicious code injection, on-boarding and off-boarding of accounts and fictitious applications that cyber criminals could use to attack financial institutions, cryptocurrency exchanges, trading platforms and retail organisations.

### • Cyber-criminals will engineer public opinion

Cyber-criminals are actively involved in changing the social and economic configuration of society by influencing public opinion, including tampering with state elections. CYFIRMA's threat intelligence revealed the escalating interests of hackers towards national apparatuses such as government policy-making agencies, rating agencies, and other organizations that can influence decision-making. The overall objective is to bring about social stratification and division.

The fact that cyber warfare is not physical compared to traditional combat warfare does not mean that it can be less harmful. We have already seen evidence of monetary and physical disruption that could cause businesses, governments and civilians alike, such as the Sony Pictures hack, the Ukrainian BlackEnergy attack on SCADA and Stuxnet. Government, businesses, and civilians all need to be protected from cyber-war chaos, and CYFIRMA's DeCYFIR provides early threat detection and containment.

DeCYFIR is a cloud-based AI (Artificial Intelligence) and ML (Machine Learning) platform for cyber security and threat intelligence.

DeCYFIR consists of a number of key modules – Threat Visibility and Intelligence, Cyber Situational Analytics, Cyber Incident Analytics and Cyber Education.

---

DeCYFIR 's intelligence-centric model prepares the organization in the event that it is caught in the middle of a crossfire. By decoding threats and applying threat intelligence, cyber operations can shift from proactive to predictive.

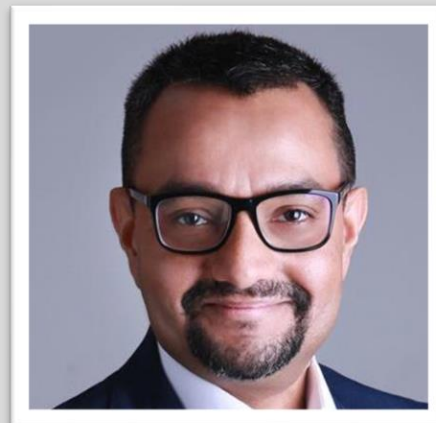
Visit CYFIRMA.com to learn how CYFIRMA can help you decode threats.

#### About the Author

Kumar Ritesh ,Founder and CEO,CYFIRMA

CYFIRMA Chairman and CEO, Kumar Ritesh, has 2+ decades of global cybersecurity leadership experience across all facets of the cybersecurity industry.

He spent the first half of his career as the head of a cyber-intelligence agency, gaining first-hand cyber threats and risks insights on a global scale before transitioning into the commercial arena as a senior executive for multi-national corporations IBM and PwC. Ritesh was also the global cybersecurity leader for one of the world's largest mining companies, BHP Billiton.



A highly dynamic executive who successfully blends technology expertise with business acumen, Ritesh has a strong track record of developing successful cybersecurity strategies, products, policies, standards, and solutions, in addition to running complex cybersecurity programs.

He has developed prototypes for data loss prevention, social profile risk assessment, web content assessment management, intelligence-led cyber risk management, and adaptive cyberthreat intelligence tools. Ritesh is also the co-inventor of two patented technologies for phishing fraud detection and protocol-aware PCB architectures.

Through his blogs and public speaking engagements, Kumar educates companies on cyber security risks, solutions and trends.

#### ABOUT CYFIRMA

Headquartered in Singapore and Tokyo, CYFIRMA is a leading threat discovery and cybersecurity platform company. Its cloud-based AI and ML-powered cyber intelligence analytics platform helps organizations proactively identify potential threats at the planning stage of cyberattacks, offers deep insights into their cyber landscape, and amplifies preparedness by keeping the organization's cybersecurity posture up-to-date, resilient, and ready against upcoming attacks.

CYFIRMA works with many Fortune 500 companies. The company has offices and teams located in Singapore, Japan and India.

Official websites:

<https://www.cyfirma.com/>

<https://www.cyfirma.jp/>



# Cyber Literacy in Post-Digital Era as Part of National Security

By Aliaksei Hapeyeu, master's degree student from Shandong University

Cyberspace in post-digital era has become not only a tool, but also a domain where people live, work, and relax. It is not bad because the development of cyber technologies underlies current progress. However, risks go hand-in-hand with opportunities. Systems interdependently connect to one another, which increases the vulnerability of disruption to whole networks. The hostile states and non-state actors may use the advantage of cheap storing and transmitting information for their own purposes. Furthermore, access to the Internet and its faculties is becoming easier (Nus.edu.sg, 2020). The diffusion of power is happening now and gives some actors incredible power to influence people's mind and shape the national role and values — the core elements of national security. The purpose of this paper is to point the problem zones of current cyber space, connect it with national security, and focus on the necessity of deep research of this phenomenon.

We consider the following questions: 1) What is post-digital era? 2) What is cyber literacy and its connection to post-digital era? 3) What is the significance of cyber literacy in national security strategy?



---

## Not digital immigrants, but digital citizens

Since the end of the XX century we started using computers and the Internet as a tool for extracting useful and necessary information, mastering it (transmitting or receiving), as access to both mastered knowledge and any information about the plans set by humanity. These achievements made it possible to create systems with a complex technical structure that allowed processing huge amounts of information compared to previous years. As a result, method of production, lifestyle, and value systems were changed.

Digital sphere was characterised by the creation and improvement of hyper communications, which included numerous mobile operators, connection speed technologies, as well as communication programs that have become prerequisites for the development of the Internet industry and cloud technologies, the emergence of new forms of information representation, i.e. the appearance of a contrasting border between the phases of social strata. Due to the rapid development of information technologies, humanity was taking great steps to improve the information world, making the distances between countries (people) minimal, simplifying people's lives through various electronic devices. It was Information Revolution where people migrated to new, digital, reality.

However, we no longer use cyber domain as a tool. Today we use cyber sphere as a space where people live, work, and communicate with one another. Bitcoin, transnational transactions, Forex trading all take place in cyberspace. From a socio-cultural standpoint, we also observe a sizeable presence of online volunteering, distance internships, or online courses. Mass media has migrated from traditional channels to online platforms like YouTube and Twitch. Sitting in the comfort of one's home, we can even travel the world via a virtual tour of Versailles or visit ancient Chinese temples. Conversely, digital disruption of an electric station is easier and cheaper than physically destroying infrastructure. Moreover, virtual operations can be executed in all areas of military warfare: in the air, on land, on the sea, and even in space (Nus.edu.sg, 2020).

In addition to it, post-digital epoch is characterised by increasing technology personalization, mobile apps, artificial intelligence, augmented reality and quantum computing, increasing the role of respected and high quality research centers, and the emergence of a new generation of more trained workforce that is constantly expanding its capabilities due to technology. The number of Internet users in the world has grown to 4.54 billion (We Are Social, n.d.), where mobile phones now account for more than half of the time we spend online — 50.1%. Recent data from GlobalWebIndex shows that we use apps in almost all areas of our lives — when we talk to friends and family, lie on the couch, manage finances, exercise, or build romantic relationships. Moreover, average person spends more than 8 hours in cyberspace today, 1/3 of a day (GlobalWebIndex, 2019).

As a result, the importance of technologies in our lives has reached new heights, and people are spending more and more time on the cyberspace. Devices and their applications are no longer just an auxiliary work tool, but a part of the citizens' lifestyle. We live in cyber domain as well as in real physical world. We have become citizens of virtual world.

---

## New cyber literacy

From the technical standpoint, the main enemy of any state and company is not a brilliant hacker-pro, but an illiterate employee/citizen who goes to all the links that come to the email, mindlessly clicks on advertising banners, rummages through dubious sites during working hours. As a result, it could steal information about customers, transactions, monitor conversations, and clutter the browser with ads. It has become much easier now because people are always in cyberspace.

I conducted a survey to see whether people are aware of cyber threats (account hacking, identity theft, bullying) through mobile apps (one of the key element of post-digital age). Respondents were people at the age of 18-64, working not in IT-sphere. Among 386 surveyed 41% are aware of it, 13% have never thought about it, and 46% unaware of the risk of cyberthreat, while 92% of the surveyed aware of cyber threat via computers.

*Table 1. Awareness of cyber threats via mobile apps and computers*

	Mobile apps	Computers
Aware	41%	13%
Unaware	46%	3%
I do not know	13%	5%

Furthermore, the more information we have, the more we rely on so-called reputational methods of evaluation. The paradox is that the incredibly increased access to information and knowledge that we have today does not give us new opportunities and does not make us cognitively autonomous. It only forces us to rely even more on other people's judgments and assessments about the information that has fallen on us. Information is only valuable if it has already been filtered, evaluated, and commented on by others. In this sense, reputation today becomes the central pillar of the post-digital age. The way the authority of knowledge is built today makes us depend on the inevitably distorted judgments of other people, most of whom we don't even know.

GlobalWebIndex reports that 90% of Internet users between the ages of 16 and 64 now watch online videos every month, which, if applied to the total number of Internet users in the world, would amount to more than half of the world's population. Moreover, 42% of users faced online insults, 32% - with the spread of rumors, 16% - with threats of physical violence (GlobalWebIndex, 2019). Carriers of extremist ideas are radicalized on YouTube, and social networks encourage the polarization of political views. Recommendation algorithms (they show what you will be interested in based on information about you and your browsing history), which work on all popular resources, contribute to the spread of such content.

---

The main terrorist threat in the United States is people who are radicalized by a variety of ideologies that they have learned from the Internet.

The best protection in this case is not to set strict regulations but to anticipate the situation in advance. We should train citizens in at least the simplest defense techniques, also known as cyber literacy - the basics of information security, following which people can protect their data, privacy, money, the flow of information, and the device itself. People know how to behave in real world and how to use computers and the Internet, but we do not know how to live there. Cyberspace is a new domain for the organization of human life that make certain requirements for it. An adult citizen in the post-digital age should understand the reconstruction of the reputational path of the information received, evaluate the intentions of those who distribute it, and calculate the plans of the authorities that confirm its authenticity. Similarly, people should know how to find, install, and work with apps to protect against cyber threats in post-digital age.

Moreover, we should move away from the "my community first" approach. The threats that arise today require joint action. The sooner communities start creating security partnerships that reflect their participation in the overall ecosystem, the faster they will start building a more sustainable society. In an ecosystem-based world, security is no longer seen as protecting one organization-it concerns everyone.

Post-digital time is a continuation, or new version, of digital time. The essence of the time is that radical changes in society begin to occur in less than a generation. We must accept that new challenges arise not once a decade, but every year, or even every month. The number and range of problems that need to be urgently addressed will continuously grow, and require appropriate new knowledge and skills of the person. One of them should be cyber literacy in post-digital world.

## National security

The foundation of any state are people and values. Almost any type of human activity has an axiological basis, since values perform a regulating and goal-setting function in the life of an individual. Through innovation companies and governments are able to use cyber space to develop a deep understanding of their audience and build permanent, personalized relationship with individuals based on their unique technological identity. Everyone knows that the Internet brings society together on a global level: it is used for creating and developing businesses, for importing and exporting goods, for recreation and relaxation, for searching for data and any information

Unfortunately, we live in the world where states and non-state actors focus on undermining the basis of their competitors. It can be done through changing the national role of the elites, shaping the ideas of the people, and influencing the inner forces of the state.

In post-digital time the role of cyberspace in shaping opinion and values is enormous. It is an area where cyber-attack can be used to produce effects similar to kinetic weapons, and where the manipulation of information and decision-making can have effects that are far more dangerous, disrupting not only virtual domains, but also negatively affecting the real world. Individual users and authors of blogs, extremists and hostile political parties have the opportunity to influence the audience via cyber area where we spend practically a half of our life. The focus is the dissemination of specially selected information



---

(disinformation). It is carried out by: sending emails; organizing news groups; creating sites for the exchange of opinions; posting information on individual pages or in electronic versions of periodicals and network broadcasting (broadcasts of radio and TV stations). An example of this is a series of civil protests in the USA in 2011 ([web.archive.org](http://web.archive.org), 2013). Its organizing force was the social network Facebook and the micro blog Twitter. It was from there that anti-government slogans and calls for civil disobedience were heard.

The most common way to use cyberspace in the interests of the conflicts is to replace the information content of sites, which consists in replacing pages or their individual elements as a result of hacking. Such actions are taken mainly to draw attention to the attacking side, demonstrate their capabilities, or are a way of expressing a certain political position. In addition to direct page substitution, it is widely used to register sites of opposite content in search engines using the same keywords, as well as redirecting (replacing) links to another address, which leads to the opening of specially prepared pages by the opposing party.

We should highlight the so-called semantic attacks, which consist in hacking pages and then carefully (without noticeable traces of hacking) placing deliberately false information on them. Such attacks are usually carried out on the most frequently visited information pages, the content of which users fully trust.

Another way to use the Internet in the interests of information warfare is to disable or reduce the effectiveness of the functioning of the structural elements of the network. The most commonly used ways to reduce the effectiveness of its individual elements are DOS attack and the introduction of computer viruses. So, the military Department of Taiwan has created about 1 thousand such viruses, which in the event of a crisis can disable the computer systems of the PRC. Their ability to break through the telecommunications network of the "enemy" was tested during the exercise.

As well as in physical world, in virtual domain of our surrounding, people, channels, articles, and websites shape our mentality. Reasonable people understand that a company of neo-Nazi on the street will not do any good but continue sitting on the extremist channels. Conscious citizens realize that believing tabloids with poor evidence and getting free money on the street is non-credible but go on reading recommendation articles and click on strange ads called "SEND US YOUR DATA AND GET FREE MONEY". We are extremely vulnerable right now because we do not have skills required to correctly identify information needed to perform a specific task or solve a problem. As a result, we are exposed to technical and informational attacks and, therefore, our values can be shaped and data can be stolen. It leads to social disintegration, and national security suffers.

Post-digital time is transforming modern civilization, and new technologies require a change in mentality. Currently, the world community is undergoing a transformation, correlated with the change of epochs and cultures. Today goods, services, and even the environment of people are individually configured. Companies and states focus on each person in every aspect of their lives, shaping the reality in which they live. We are living in post-digital time when mobility and portability, simple user interfaces, and easy accessibility to the Internet, including the use of cloud services and open web standards, as well as mobile applications with the ability to seamlessly synchronize information between different devices take place. At such critical moments, the issue of security as a basic need is always acute – the new replaces the established old and at the stage of its origin brings with it something uncontrolled and unmanageable, since the mechanisms for controlling and managing this new have not yet been formed. That is why

---

cyberlitarecy in post-digital time is so significant and must become a part of the culture of modern civilization.

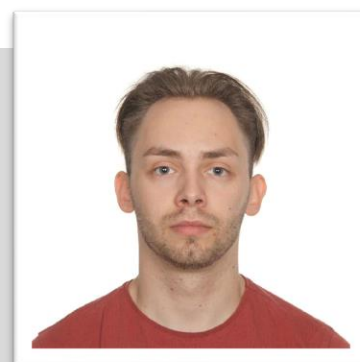
Our efforts should be aimed at developing knowledge in the field of cybersecurity, knowledge of its basic rules, and following them every day at the level of habits that become a condition for successful counteraction to cybercriminals. But it is impossible to instill lasting knowledge and form rules that a person will follow in their daily life if they do not understand why they need this knowledge and if society does not share their value and following them is atypical for the environment in which they live. Therefore, it is important not only to raise awareness, but also to create a culture of cyber literacy.

## Conclusion

Virtual world can significantly influence current issues in the physical world and, as a result, the term of national security is under attack. Initially, digital technologies provided its owners with a competitive advantage, but today such technologies are available to everyone and become a part of person's identity. Hostile actors are able to use this digital identity to develop a deep understanding of their target audience and influence it. An established trend in using mobile apps and easy access to it, expanding role of expert institutions and big amount of information has enhanced opportunity to affect people's mind. However, we can diminish the negative effects by teaching people how to behave and "live" in cyberspace. We cannot regulate cyber domain, but we can instill persistent knowledge and form rules that people will follow in their daily life and will be much better prepared to propaganda, information flow, and cyber-attacks.

### About the Author

Aliaksei Hapeyeu is a Global Shaper, Young European Ambassador, and the master's degree student from Shandong University, China. Certified International Cyber conflicts specialist by The State University of New York. Author of the article "Why we need Smart Power in Cyberspace". Aliaksei can be reached online at [aleshagapeev@gmail.com](mailto:aleshagapeev@gmail.com) and at his university website <https://en.sdu.edu.cn>



# New Research Highlights Importance of HTTPS Inspection to Detect Encrypted Malware

Two-thirds of malware in Q1 2020 was delivered via HTTPS traffic, Monero cryptominers are on the rise and more

By Marc Laliberte, Senior Security Analyst at [WatchGuard Technologies](#)

Today's threat landscape is evolving rapidly. Attackers are constantly adjusting their tactics and finding new ways to infiltrate organizations to steal valuable data. As such, businesses must remain up to date on the industry's latest threat intelligence in order to know their enemy and shore up defenses. That's why each quarter, [WatchGuard's Threat Lab](#) research team produces a report on the latest trends in malware and network attacks based on anonymized data from WatchGuard security appliances deployed around the world.

Our latest [Internet Security Report](#) included many key findings and best practices that midmarket organizations and the managed service providers that support them can use to ensure that their defenses are up to the task of fending off today's most prevalent security attacks. Let's dive in:

1. Two-Thirds of Malware is Encrypted, Invisible Without HTTPS Inspection. An incredible 67% of malware is delivered via HTTPS traffic. This means that organizations without security tools that can decrypt and examine HTTPS traffic will miss a full two-thirds of security threats! We also found that 72% of the malware delivered via encrypted HTTPS was new or "zero day," meaning no antivirus signature exists for it and it will not be blocked by legacy signature-based antimalware methods. Not only are two out of every three pieces of malware in the wild delivered through an encrypted channel, but that malware is also more difficult for traditional antivirus to detect!



---

This data clearly shows that HTTPS inspection and advanced behavior-based threat detection and response solutions are now requirements for every security-conscious organization. Many IT and security teams are unenthusiastic about setting up HTTPS inspection because it requires extra work with certificates on individual endpoints – it's not just a feature within security tools that can be switched on and off. HTTPS inspection can also slow down the throughput of some network security tools, so some organizations aren't able to maintain high network speeds while inspecting encrypted traffic. While I'm sympathetic to these concerns (especially for midmarket businesses with limited IT and security expertise), letting this traffic through a firewall without inspecting it is no longer a safe option and there are network security platforms that offer HTTPS inspection while maintaining good network speeds. Given the magnitude of the threat, the only reliable approach to defense is implementing a set of layered security services that include advanced threat detection methods and HTTPS inspection.

2. COVID-19 Impacts Security in a BIG way. Q1 2020 was only the start of the massive changes to the cyber threat landscape brought on by the COVID-19 pandemic. Even in just these first three months of 2020, we saw a dramatic rise in remote workers and attacks targeting those individuals. Phishing attempts increased, and the greater number of employees operating outside the traditional network perimeter led to more attacks aimed at remote desktop technologies. We strongly recommend that all organizations follow phishing best practices and make sure to secure remote access technologies by requiring employees to use a mobile VPN and not exposing services to the internet that shouldn't be. Additionally, companies should deploy secure MFA as an additional protection layer against password-based attacks.
3. Cryptominers are on the rise. Five of the top ten domains (identified by our [DNS filtering service](#)) distributing malware either hosted or controlled Monero cryptominers. This sudden jump in cryptominer popularity could simply be due to its utility; adding a cryptomining module to malware is an easy way for online criminals to generate passive income.
4. Flawed-Ammy and Cryxos malware grow in popularity. The Cryxos trojan was third on WatchGuard's top-five encrypted malware list and also third on its top-five most widespread malware detections list, primarily targeting Hong Kong. It is delivered as an email attachment disguised as an invoice and will ask the user to enter their email and password, which it then stores. Flawed-Ammy is a support scam where the attacker uses the Ammy Admin support software to gain remote access to the victim's computer.
5. Ancient Adobe vulnerability surfaces as top network attack. An Adobe Acrobat Reader exploit that was patched in Aug. 2017 has appeared in WatchGuard's top network attacks list for the first time. This vulnerability reappearing several years after being discovered and resolved illustrates the critical importance of regularly patching and updating systems.
6. Attackers use reputable domains to launch spear phishing attacks. Three new domains hosting phishing campaigns appeared as top attacks. These domains convincingly impersonated digital marketing and analytics product Mapp Engage, online betting platform Bet365 and an AT&T login page (this campaign is no longer active at the time of the report's publication).

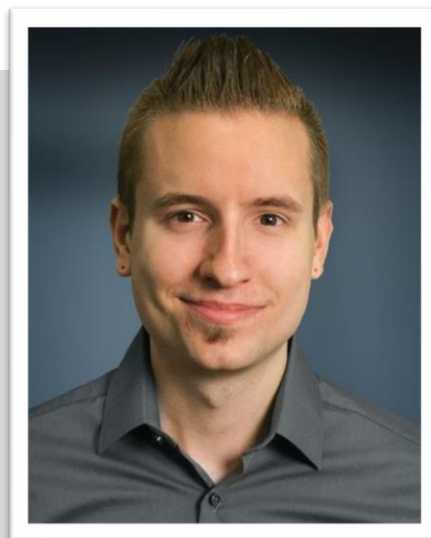
---

In conclusion, our latest analysis on malware and network attack trends show a clear need for organizations to decrypt and inspect secure web traffic and to deploy modern anti-malware technologies that use behavior-based or machine learning techniques to detect malware that signature-based solutions will miss. As the wide variety of threats and techniques present in our other findings indicate, organizations should implement a layered security approach with multiple, overlapping security services including strong endpoint protection, mobile VPN, multi-factor authentication and more to better protect employees working from home during the current crisis and beyond.

#### About the Author

Marc Laliberte is a Sr. Security Analyst at WatchGuard Technologies. Marc joined the WatchGuard team in 2012. Specializing in networking security technologies, Marc's responsibilities include researching and reporting on modern information security trends. With speaking appearances and regular contributions to online IT publications, Marc is a thought leader providing security guidance to all levels of IT personnel.

Marc can be reached on Twitter at @XORRO\_ and at our company website <https://www.watchguard.com>.





## Protecting a Mobile Workforce with Hybrid DNS Security

By Ashraf Sheet, Regional Director, Middle East & Africa at Infoblox

The future of the workplace is undoubtedly a remote workforce, accessing the corporate network via mobile devices and the cloud. This is likely to cause a few sleepless nights for the teams traditionally responsible for managing network security on-premise.

With remote working, data breaches will become commonplace. Networks will be infiltrated with malware due to an increase in roaming or off-network access.

### Vulnerable and unsecure

At the root of many of these breaches, and the damage and stress that accompanies them, lies the DNS, or domain name system. Often referred to as the address book of the internet, DNS sits at the heart of every organisation's IT network, translating domain names into machine-readable IP addresses. Despite most internet communications relying on DNS, however, it is inherently vulnerable and not sufficiently secured, resulting in weaknesses that can be exploited for criminal ends.

DNS is used by a high percentage of malware to carry out campaigns such as communicating with C&C servers, holding data to ransom or serving as a pathway for data exfiltration. Due to its position at the



---

core of the network, however, DNS is often the first part of an organisation's infrastructure to see the majority of malicious activity and should, therefore, be considered an organisation's first line of defence.

By collecting and analysing data from DNS queries, an effective enterprise DNS security solution will provide essential context and visibility that will alert IT teams to any anomalies, enable them to report on which devices are joining and leaving the network, and ultimately allow them to resolve problems more quickly.

Many DNS security solutions are focused on on-premise networks, however, and aren't sufficiently suitable for remote workers and offices, much of whose workloads are held in the cloud.

### The mobile options

Meeting the demand for greater speed and mobility means that internet traffic from mobile workers tends not to be backhauled to an organisation's network via corporate points of presence such as servers or routers. As a result, DNS traffic to and from an organisation's mobile users will not generally be visible to corporate security monitoring.

The growing shift towards a more mobile workforce makes it important, therefore, for organisations to adopt a hybrid approach to DNS security that will protect both on-premise and mobile users; a combination of on-premise DNS security as mentioned above, and one of the following approaches to maintaining DNS security in a mobile environment.

Agent software, for example, can be installed on a mobile device and reroute DNS traffic to a cloud-based DNS security solution that can monitor client-side behaviour to detect malicious or suspicious DNS activity. And in cases where it isn't possible to install an agent, configuration settings on a mobile device can be set to proxy mobile device traffic through services often referred to as cloud access security brokers, or CASB. However, while CASB services are able to monitor HTTP traffic from mobile devices, the implantation of an additional DNS proxy solution is required to reroute DNS queries to a cloud-based DNS security solution which can then monitor and block suspicious activity.

What's more, a combination of both client agent and proxy approaches, integrated with threat intelligence to assure the detection of DNS tunnelling and other advanced targeted threats, can provide broad coverage across a variety of devices and external services.

### DNS as an asset

If not given proper consideration within an organisation's security plans, DNS can provide an easy point of entry for malicious actors intent on disrupting networks, and accessing and exfiltrating sensitive information. And the problem is growing. As sophisticated cybercriminals continue to develop new

---

techniques and tactics to exploit vulnerabilities in DNS services, the increasing demand to support a growing mobile workforce opens up additional attack vectors.

DNS services and data can be used as an asset in the security chain, however. By taking a hybrid approach of on-premise DNS security together with a cloud-delivered solution, organisations are able to protect not just the users within their corporate network, but also those based in branch offices, and those who increasingly opt to work remotely.

#### About the Author

Ashraf Sheet is Regional Director MEA at Infoblox. He is a network and security expert and has held various progressive roles including senior security consultant, leader for Managed Security services and head of Security Business Unit for local and multinational companies.

Ashraf can be reached online at (asheet@infoblox.com) and at our company website <https://www.infoblox.com/>





## Unstructured Data, Unsecured Data

The Data You Overlook Needs Protection Too

By Deborah Kish, EVP, Marketing & Research, Fasoo, Inc.

Sensitive unstructured data is everywhere, it means different things to different businesses and comes in two forms. Unstructured data that:

1. Is used for analytical purposes.
2. Resides in file formats such as Microsoft Office, text files, images and CAD/CAE format.

The second form is often overlooked, can cost your business its competitive advantage, and subject you to regulatory fines if stolen or leaked. In a world where a pandemic has wreaked havoc on employers and employment, this sensitive unstructured data is at highest risk mainly because it covers more surface area, continues to grow rapidly, and is quite often invisible to the enterprise. Therefore, it is important to know what and how much of it you have in typical office file formats. More importantly, understand how to and why it is important to protect it.

The Organization for the Advancement of Structured Information Standards (OASIS) has published a standard for unstructured information management. The standard indicates that "...unstructured information represents the largest, most current and fastest growing source of knowledge available to



---

businesses and governments worldwide.” Therefore, it is believed that more than 90% of an organization’s data is unstructured rather than data stored in traditional databases. We know it exists and we know it is growing but we also know that most businesses typically don’t take measures to protect it. Most feel it is a “hard to tackle” task to find unstructured data and get it under control and tamed, let alone protected.

The reason why it is often overlooked is because the risks associated with unstructured data generally are not taken into consideration. The risks are for:

- Privacy or Industry Regulatory Compliance
- Intellectual Property Protection

### Privacy or Industry Regulatory Compliance

When employees create files that contain sensitive information, copies of those files naturally proliferate. There will be multiple versions of the files and sharing of those versions between employees via e-mail and network file shares. It’s rare that employees will go back and delete these files later and anything sent via e-mail may be archived in .pst files; file shares will be backed up to various media. This not only creates a larger attack surface, but will add significant complexity should an organization face litigation and discovery requests from data subjects. Organizations that are subject to the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) will struggle to satisfy data destruction demands and the “right to be forgotten”. If an organization handles cardholder data, it’s crucial to keep credit card numbers within Payment Card Industry (PCI) controls – something rarely applied to unstructured data due to cost and complexity.

The Norwegian Supervisory Authority (Datatilsynet) is an example of non-compliance to GDPR and fee assessments “due to insufficient technical and organizational measures to ensure information security”. In July 2020, the authority found that the Municipality of Rælingen was in violation of articles 32 and 35. The company did not conduct a DPIA and prior to the start of the processing it had not taken adequate technical and organizational measures in accordance with Article 32 of the GDPR, resulting in an increased risk of unauthorized access to the personal data of the pupils. Also, and still under investigation, in the UK, British Airways is potentially facing a fine of £183.39M from an incident that compromised approximately 500,000 customer’s personal data. There are several examples, but not having technical measures in place is very common across violators.

### Intellectual Property Protection

When thinking about how unstructured data is expanding your threat surface, think about who is the threat. Unstructured data in files is an attractive and easy target for internal threat actors with limited protection. Let’s face it, when a data theft story breaks out, it is typically not because a cyber-criminal stole a bunch of Word files from a folder on someone’s laptop. Instead, it is the insider saving information on a USB drive or taking a screenshot of sensitive information in a spreadsheet. This is costly to the

---

business because in most instances, it is information that has been sold to competitors, or used to expose explicit information for political purposes or gain.

A couple of examples of insider theft include the [Sony hack](#) where an employee in Human Resources had salary information on 30,000 Deloitte employees and publicized it; and the [Morgan Stanley](#) employee who stole account information from 350,000 of its wealth management clients and posted some of the information on the internet. [GlaxoSmithKline](#) had IP, trade secrets and presentation data compromised in two ways; documents emailed from inside GSK to private email accounts, using USB and other storage devices and copied onto personal devices. This particular incident also led to mounting legal fees and a \$500m fine to the victim in all of this, GSK. These examples are just a blip on the map, but should serve as reminders that businesses must know that sensitive information in files exists, is protected appropriately, and that only the right people can access them. Not to mention the responsibility of the business to protect the information if it is subject to industry or privacy regulatory mandates. Put simply, unauthorized access or loss of sensitive data can compromise competitive advantages, damage the brand, and expose the organization to significant regulatory penalties and even litigation.

As most businesses are focusing on securing structured databases and identity and access management, they must also include unstructured data in their data security initiatives. But before even thinking about moving forward, you need to assess your own situation and then you can move forward with a plan to first understand what sensitive unstructured data you have. It's not as hard as you may think.

#### Where Do You Start? Know the Data. Control the Data.

Your current governance, risk and compliance (GRC) policies may be a little outdated. Now is the time to take them out, dust them off, and update them to include sensitive unstructured data. With privacy regulations rapidly changing, it is important to not learn privacy through impact and avoid being the victim of a violation. It is difficult under the best of circumstances to respond to a DSR or incident from a structured database, but even more challenging with information that is unstructured. Knowing where your sensitive unstructured data is and what it is will be a critical part of your GRC policy. Getting there is not as daunting as you might think and in just a few steps, you will be on your way to high visibility, control, protection and improved response time to incidents and DSRs. Business unit by business unit, talk to the person in charge and ask:

1. What documents do you create or work with that contain sensitive information?
2. Where do these documents reside?
3. What applications do you use that contain sensitive data that you may download into reports or other documents?
4. Do you upload documents into applications, file shares, content management systems or any other external application or information system?
5. Is this data shared internally, and if so, how and with whom?

---

6. Is this data shared externally, and if so, how and with whom?

This is an important part of the process, because it will give you more insight into the kind of data you have. It will also provide you with an opportunity to implement some best practices of how the data is handled and protected and automate critical functions such as discovering and classifying documents that contain sensitive information.

About the Author

Deborah Kish is Executive Vice President of Marketing and Research at Fasoo. She is responsible for leading Fasoo's research and product strategies in the unstructured data security and privacy space. Fasoo provides unstructured data security and enterprise content platforms that enable our customers to protect, control, trace and analyze critical business information while enhancing productivity. Fasoo has successfully retained leadership in the unstructured data security market by deploying enterprise-wide solutions globally, securing millions of users.



Deborah can be reached online at (deborahkish@fasoo.com, @deborah\_kish, linkedin.com/in/deborahkish.) and at our company website <http://www.en.fasoo.com/>





## Securing the Weakest Links in Today's Public Cloud Environments

By Avi Shua, CEO, Orca Security

The demand for cloud security is continuing to explode, with short-term needs being accelerated by the shift to remote work during the pandemic. According to [Gartner](#), the Cloud Security market is projected to grow 33 percent by the end of 2020, as deployments and threats increase in tandem.

Public cloud security is fundamentally a shared responsibility, and as adoption grows, organizations must remember that just one gap in cloud coverage can lead to devastating data breaches. Missed cloud workload vulnerabilities happen because most organizations depend on installing and maintaining individual security agents across all their assets. But this intensive effort is easier said than done, as our latest research confirms.

### Top Vulnerabilities in Public Cloud Environments

According to the [Orca Security 2020 State of Public Cloud Security Report](#), organizations are lacking in three key areas for securing their cloud assets running on AWS, Azure and GCP. These areas include securing frontline workloads, minimizing lateral movement risk to internal servers, and improving weak

---

authentication and password protections. As organizations continue to make easy security mistakes in their public cloud deployments, hackers are finding new ways to wreak havoc on companies most valuable assets, and their customers.

We have seen many recent examples of data breaches resulting from easy-to-prevent cloud misconfigurations. I like to point to last year's data breach of a Mexico-based media company, Cultura Colectiva, which had 540 million Facebook records stored on an open S3 bucket—accessible to anyone on the internet. Equifax is another example of a high-profile company that suffered a massive data breach in 2017 due to a neglected, unpatched web server, resulting in a \$700 million fine from the FTC.

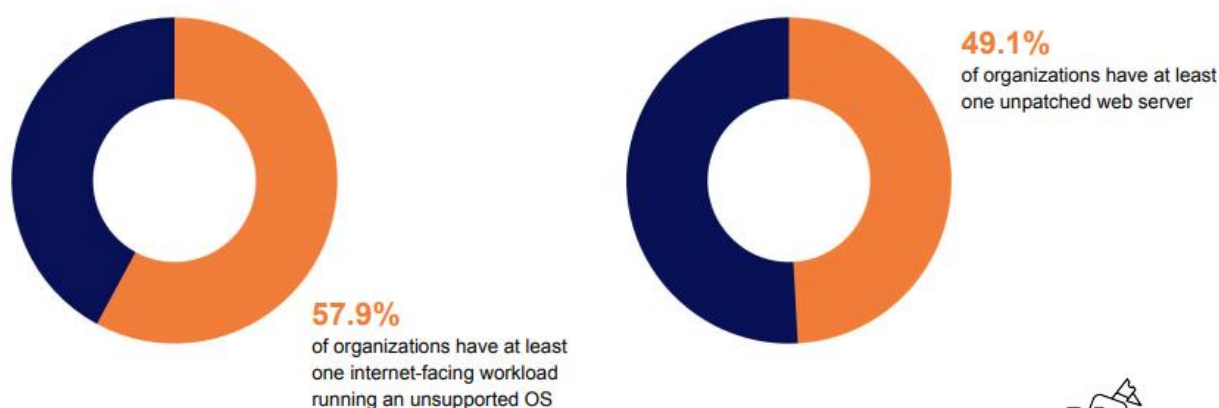
With these examples, let's take a closer look at the most common vulnerabilities found in organizations' public cloud estates, and the steps they can take to prevent future data breaches.

### Neglected Workloads are the Weak Link

For organizations migrating on-premise workloads to public cloud environments, our research found that the security of internal workloads is much worse than frontline workloads. More than 77 percent of organizations surveyed have at least 10 percent of their internal workloads in a neglected security state. This means that the application's operating systems were either left unpatched or unsupported by current updates. Meanwhile, nearly 60 percent have at least one neglected internet-facing workload that falls into the unsupported OS category. Furthermore, 49 percent of organizations have at least one unpatched web server within their public cloud environment.

Orca Security 2020 State of Public Cloud Security Report

## Weak Link: Neglected Workloads



Orca Security © 2020

---

These findings are key to understanding the mechanics of a data breach. Attackers find weak links through vulnerable frontline workloads and execute lateral movement, to progressively move through the network and find more sensitive assets. According to our research, nearly 81 percent of organizations had at least one neglected, internet facing workload.

Tip: Assume breaches will happen and look for lateral movement risks. Attackers will use secrets, credentials and keys stored on breached servers to move laterally. Don't wait for them to find these attack opportunities – search for these risks beforehand to remove or tighten, as applicable.

### Poor Password Security Creates Authentication Issues

Companies must also pay close attention to the authentication and verification methods used to grant permission to frontline and internal workloads. Today, there is no excuse for organizations that do not implement basic authentication protocols like multi-factor authentication (MFA).

Sadly, this is not the case, as we found that 23 percent of organizations have at least one cloud account that does not use multi-factor authentication for the root account (super admin user).

Weak passwords and credentials also remain an issue for organizations to ensure the security of their public cloud environments. More than 5 percent of organizations have at least one workload using an easy-to-guess or leaked password, which is either a simple derivative of an existing password or has been detected in a previous breach.

Orca Security 2020 State of Public Cloud Security Report

---

## Weak Link: Authentication Issues

---

Weak security authentication is another way attackers breach cloud environments. We found that **23.5%** of organizations have at least one cloud account that doesn't use multi-factor authentication for the cloud provider root account (super admin).

Another type of weak authentication is the use of non-corporate credentials. **19.3%** of organizations have at least one internet-facing workload accessible via non-corporate credentials.



**23.5%**  
of organizations have at least one cloud account that doesn't use multi-factor authentication for the cloud provider root account



**19.3%**  
of organizations have at least one internet-facing workload accessible via non-corporate credentials



Orca Security © 2020



The use of personal credentials in the workplace is also a concern. According to our findings, 19 percent of organizations have at least one internet-facing workload accessible via non-corporate credentials. Given that there are a staggering 15 billion consumer credentials floating around the dark web, companies should urge their employees not to use personal credentials in the workplace to prevent attackers from leveraging stolen credentials to access their networks.

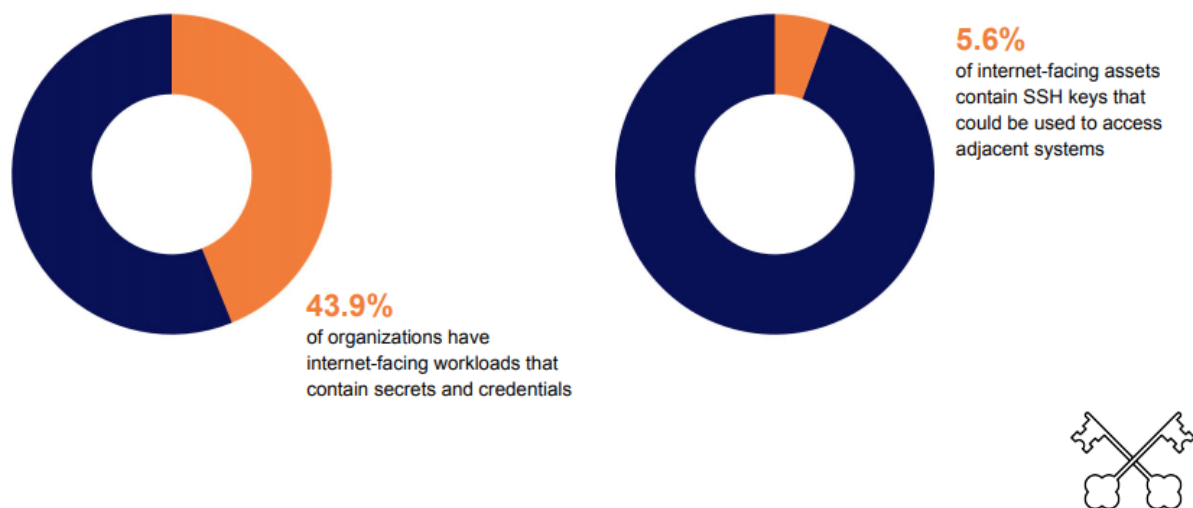
Tip: Breaches mostly stem from simple errors such as stolen root account passwords with no MFA. IT teams must get the basic security protocols in place before advancing to more advanced capabilities.

### Hackers Know Internal Servers Are Vulnerable

It is no secret among hackers that internal servers are often less protected than external internet-facing servers. Once attackers gain access to an organization's cloud estate, they can expand rapidly in search of sensitive data and assets such as passwords and authentication tokens.

Orca Security 2020 State of Public Cloud Security Report

## Finding the Keys to the Kingdom



Orca Security © 2020

We found that while only 2 percent of neglected, internet facing-workloads contain customer information, 44 percent contain secrets and credentials including clear-text passwords, API keys, and hashed passwords.

These authentication tokens and credentials are valuable for attackers, which they leverage to execute lateral movement across networks in search of crown jewel data. And we found that nearly 6 percent of internet-facing assets contain SSH keys that could be used to access adjacent systems.

---

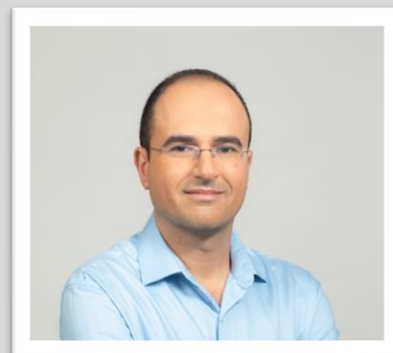
Tip: Cloud security is only as good as its coverage. IT teams must make sure to cover 100 percent of their cloud assets, as attackers will always find a way to breach an organization's weakest link.

### Mistakes Will Happen

It is important to remember that mistakes will happen. However, in the age of the cloud, there is no excuse to not know what vulnerabilities you have. Embrace that cybersecurity is no longer confined to IT departments, but also extends to sales and marketing teams who are accessing the data. Understand, monitor and embrace these security risks while implementing tools that help you react quickly.

#### About the Author

Avi Shua is the CEO and co-founder of Orca Security. He invented the patent-pending SideScanning™ technology upon which Orca Security is built. SideScanning™ uses novel, out of band, zero impact integration with the cloud virtualization layer to gain full visibility into those risks that matter most—vulnerabilities, malware, misconfigurations, weak and leaked passwords, lateral movement risk and improperly secured customer data. Learn more at [Orca.Security](https://orca.security/).



Avia Shua can be reached online at [Twitter](https://twitter.com/orcasec) and at our company website <https://orca.security/>

Author Social Media URLs- 1) LinkedIn - <https://www.linkedin.com/in/avishua/>  
2) Twitter (Orca Security) - <https://twitter.com/orcasec>  
3) Twitter (Avi Shua) - [https://twitter.com/shua\\_av](https://twitter.com/shua_av)





## Compliance in A Connected World

By Kirsty Fisher, CFO, Titania

In 2019, [Microsoft](#) made waves at its annual Black Hat conference in Las Vegas, where it confirmed its discovery of a [malicious hacker group](#) which was using common Internet of Things (IoT) devices to carry out widespread corporate attacks. The way in? Internet connected devices including a VOIP phone, a Wi-Fi office printer and a video decoder, with compromised devices across multiple customer locations. But these are just a few of the numerous examples of hackers exploiting the so called 'Internet of Things' in recent years. Kirsty Fisher, CFO at [Titania](#) explains.

Many of these hacks could have had potentially serious consequences had they gone undetected. For example, in 2017, the Food and Drug Administration (FDA) issued a warning about implantable cardiac devices, which they'd found to be at risk of attack. Used to monitor and control heart function, including heart attacks, vulnerabilities meant hackers could control shocks, alter pacing and deplete the battery.

Tech analyst company IDC predicts that in total there will be [41.6 billion](#) connected IoT devices by 2025. With no central security standards or compliance frameworks underpinning the proliferation of IoT devices, individuals and businesses remain exposed for the near future.

But what makes the Internet of Things and the risks associated with connected devices different from the traditional internet? Largely, the human factor. The IoT doesn't need people to work. It provides technology, media and telecoms companies with the opportunity to create new products and applications, which rely on sensors collecting, reviewing and acting on data. Popular with increasingly tech savvy



---

homeowners, who want the latest smart app-controlled lighting and heating system or interactive media device, the opportunity for suppliers to create new revenue streams is huge.

However, the challenge with this automation is that it creates a huge wealth of sensitive data, which is then being shared amongst more people. Even the [FBI](#) has put out warnings about the risks, highlighting to people that hackers can “use those innocent devices to do a ‘virtual ‘drive by’ of your digital life.” Businesses are also being targeted through IoT devices as an entry point, with Microsoft and other tech giants highlighting attacks where access to secure networks has been gained via printers and VoIP systems amongst other connected devices.

### The business challenges

As networks become increasingly complex and the growth of the Internet of Things shows no signs of slowing, the challenge of keeping businesses cyber secure and minimising risk is greater than ever.

Spanning the public and private sector from smart cities and transport initiatives to healthcare and smart home/consumer applications, yet with no central standards in place, the onus is very much on those in the IoT ecosystem to work together to create as secure an environment as possible for the time being.

While there is some sector-led collaboration taking place, many organisations are looking to those in technology, media and telecommunications to take the reins and lead the way. Like many large organisations, in the past, businesses in these sectors may have implemented different cyber risk strategies appropriate to a particular department, country or product. With the increased threat from the IoT and new ways in which data is being used and connections to networks made, many are now revising cyber strategies to sit at a corporate, organisation wide level. They are also paying more attention to preventative strategies, trying to predict IoT cyber threats before they happen, minimising attacks that do take place and continuity planning for how they will restore services as soon as possible.

### The way forward

Despite the very real cyber security threat posed by the IoT and the complexity of the networks and parties involved, there is concern that too much control over data could stifle innovation. Many pioneers in the cyber security sector are suggesting the answer lies in the development of more secure devices and improvements in internet security to go alongside this.

Speaking on this issue, [Philip Reiting](#), President of the not for profit, Global Cyber Alliance neatly summarised the issue: “We must move from the Internet of Things to the ‘Secure Internet of Secure Things’. First, we must build (more) Secure Things – devices, software and services with few vulnerabilities, that are securely configured and automatically updated. Of critical importance, cloud services must come with security embedded and not as an up-sell.

---

“Second, we need the Secure Internet – automated collective defence must be built into the network, so that the Internet ecosystem can react as the body does, recognizing infections and fighting them off. We must build Internet Immunity.”

### Back to basics

Of course, while the industry calls for standards to be developed and the security of devices to be improved, businesses who want to use connected devices without compromising cyber security shouldn't be alarmed. Like the approach some of the larger tech and telcos companies are taking, businesses of all sizes can put in place simple, organisation-wide preventative measures to minimise risk to their businesses as well as solutions to help them identify and respond quickly to threats.

Rather than neglecting your core network and putting the focus just on to connected devices, you should seek to improve the security of your network holistically as a weakness in one part can of course impact the rest. To minimise your attack surface and prevent adversarial intrusion by hardening your network, businesses should not underestimate the power of good cyber hygiene. A study by the [Online Trust Alliance](#) (OTA) estimated that 93% of cyber security incidents – large and small – could have been avoided if the business in question had basic cyber hygiene practices in place.

In short, cyber hygiene is the continuous cycle of carrying out routine checks on an organisation's network, endpoints and applications to identify and fix any network vulnerabilities, protect against cyber threats and maintain online security. Best practice such as deleting old user accounts, firm-wide policies on access and passwords, back up of data, securing physical and cloud databases, checking routers and networks, might seem obvious, but keeping on top of the basics really is the key to cyber hygiene and minimising the risks associated with security breaches.

### Time for change?

Many organisations let basic cyber hygiene practices slip through lack of time and resource, not due to absence of expertise. Indeed, over the last decade many new risk management frameworks have been introduced to combat this; for example, in 2014 in the US, the Federal Government introduced its best practice DHS CDM, or 'Continuous Diagnostics & Mitigation' program.

To comply with this framework, agencies are expected to audit their entire enterprise every three days. In practical terms, if you had 500 devices connected to your network, you'd be carrying out nearly 61,000 audits every year. For a bigger organisation with 25,000 devices, that'd be over 3 million vulnerability audits every year. Even if you're not aiming for CDM levels of network security, with the number of core network devices increasing across organisations, it's not a problem that can be fixed by simply solving the [shortage of skilled cyber security professionals](#) in the industry.

Then add to this the need for resources dedicated resources to analyse the threat intelligence needed for effective threat detection and response – and the scale of the cyber security challenge is laid bare.

---

## So, what's the answer?

Early threat detection and response is clearly part of the answer to protecting increasingly connected networks, because without threat, the risk, even to a vulnerable network, is low. However, ensuring the network is not vulnerable to adversaries in the first place is the assurance that many SOC's are striving for. Indeed, one cannot achieve the highest level of security without the other.

Even with increased capacity in your SOC to review cyber security practices and carry out regular audits, the amount of information garnered and its accuracy, is still at risk of being far too overwhelming for most teams to cope with.

For many organisations the answers lie in accurate audit automation and the powerful analysis of aggregated diagnostics data. This enables frequent enterprise-wide auditing to be carried out without the need for skilled network assessors to be undertaking repetitive, time consuming tasks which are prone to error. Instead, accurate detection and diagnostics data can be analysed via a SIEM or SOAR dashboard, which allows assessors to group, classify and prioritise vulnerabilities for fixes which can be implemented by a skilled professional, or automatically via a playbook.

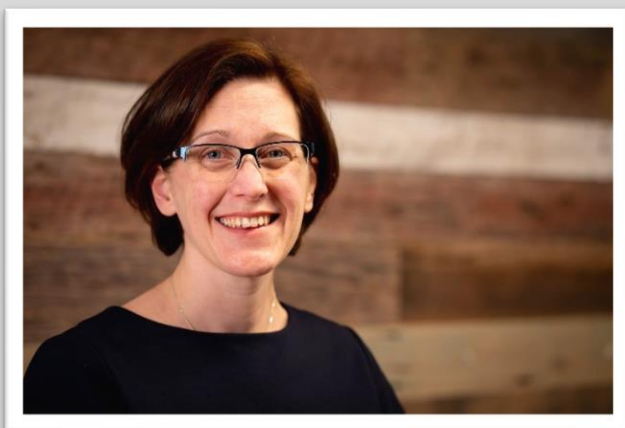
The right automation platforms ultimately provide the capability to check more devices across more networks more frequently, which is essential in combatting the risks that IoT brings. If you're investing in making your network more sophisticated by adding the latest connected devices, it is only wise to make sure that they are secure and also, through regular checks and good cyber hygiene, your core network is as secure as it possibly can be and not exposed to preventable attack.

For more information, please visit: <https://www.titania.com/>

### About the Author

With a strong track record in establishing efficient and effective business operations, Chartered Accountant Kirsty Fisher joined Titania as Chief Financial Officer in 2018. In the short time she has been a part of the business, Kirsty has implemented robust management controls across all departments, using her independent financial judgement to lead Titania and the entire team through significant Organisational Transformation.

Kirsty can be reached online at @TitaniaLtd on Twitter and at our company website <https://www.titania.com/>







# Defending Ever Expanding Networks and IT Systems

Architecture at Scale is Needed

By Trevor Pott, Product Marketing Director, Juniper Networks

How many systems must an information security professional defend? For most people, the numbers involved are abstract concepts. We think we understand them, but when confronted with them in a tangible form, we are constantly surprised by how much our perception differs from reality. Today even the smallest enterprises operate at scales that are simply beyond our ability as humans to truly comprehend.

There's a considerable gap in capability between small business IT and enterprise IT. For example, it is entirely feasible – and even reasonable – to meet all of a small organization's file storage needs using a bare-bones secure cloud storage provider like Sync.

It would be rank madness to do this for an organization with 10,000 employees. When you get to the scale of a military, there are strong arguments to be made that, if used as the organization's only storage solution, such an approach would constitute criminal negligence.

Scale matters. As scale increases, inevitably, so does complexity. There is no getting around this.

So how many systems must an information security professional defend? All of them. Given the scale of our increasingly interconnected world, that's quite the problem.

---

## The evolution of network management and automation

In the beginning, we managed everything by hand. Each system on our networks was a pet, loved and cared for, unique amongst all other systems. Eventually, the number of systems under management became too large for this approach to management, and so administrators turned to scripting. Common tasks were automated. Each administrator could manage a larger number of systems.

Eventually, people who had a large number of scripts packaged them into the first IT management applications, and manual IT gave way to management centralization. Scripting and #CommandLineLife was replaced by policies, profiles and templates. The number of systems a single administrator could manage exploded, and this is where most organizations are today.

Unfortunately, that scale thing keeps coming back 'round again. Despite the management magnification capabilities afforded administrators by today's policy-driven management applications, larger organizations are hitting very real scaling problems. 100% of administrator time is being tied up with policies, profiles and templates. Worse, in many cases the relevant IT teams are already at their maximum size: adding staff does little to increase the number of systems that can be managed.

## Holistic architect wanted

If there is one thing I would like every single network defender to keep in mind for the next decade, it is that there is no network edge anymore. The days of hunkering down behind our perimeters are long past.

"Hybrid IT" and "multicloud" – including all flavors of modifying buzzwords – is no longer novel. It is simply how IT is done today. A single organization's IT can span multiple infrastructures. On-premises IT blends neatly into infrastructure, software and services provided by multiple public cloud providers, while edge computing has quietly become an ordinary fact of life that we don't even pay much attention to anymore.

That dispersed, complex vision of a modern network exists without even beginning the conversation about mobile and remote workers, IoT, or the intricacies of interdependence that exist both upstream to our supply chain, and in the provisioning of IT to downstream customers. Unfortunately, in many ways, we are our own worst enemy, and we – both as IT practitioners and as vendors – create many of the security problems that will haunt us in the coming years.

Our innate need to categorize, to segment and to simplify may well be looked upon as the security threat of the 2020s. Our need to keep bringing complexity down to something we can fit in our brains stands in the way of making holistic architectural – and thus security – decisions about the implementation of IT across these many and varied infrastructures.

---

## Think outside the network

The persistence of a siloed mentality, complete with an insistence on treating network segments as though they had perimeters (and as though those perimeters mattered) consistently limits our thinking. This puts us at risk. The compromise of the most minor system can lead to the compromise of significantly more important systems, and an inability to think holistically will ultimately lead to compromise.

Consider, for example, the caching of credentials. In many cases, merely logging into a system with administrative credentials once (and then forgetting to wipe the cache) is enough to leave a copy of those credentials on the system in question. That cache can be exploited by attackers to then compromise other systems that are part of the network and which share those credentials.

In this manner the compromise of a small edge node located on the other side of the world could result in a devastating compromise of central databases. What's worse, these sorts of compromises happen not because anyone along the chain of responsibility between those two systems does anything wrong, but because their areas of responsibility were so disconnected that the security implications of how doing something to A would affect B were never even considered.

## Machines managing machines managing machines...

This is the challenge of the 2020s. In order to cope with perpetually increasing scale we must begin to turn the definition and daily management of policies, profiles and templates over to machines. Machine Learning (ML), Artificial Intelligence (AI), and other Bulk Data Computational Analysis (BDCA) tools are a must.

Initially, these tools will make suggestions, and automate very simple tasks - the sort of things we're seeing from AIOps vendors today. But this is only the beginning; in order for the networks of tomorrow to even be possible, virtually everything that IT administrators do today must be done by BDCA tools without any form of human input.

This is not about replacing IT personnel. It isn't about an attempt to save money. The problems we're running up against are the limits of human capability.

Humans can only hold so many things in working memory at a time. Call it a RAM limit, if you will. We can only conceive of so many nodes on a network. We can only wrap our minds around so many permissions interactions. Enterprise networks are already bigger than we can fit in our brains, and that means we are running up against human limits in terms of even being able to architect these networks, let alone defend them.

For security to be effective, it needs to be holistically integrated into network architecture decisions. Network and security are inseparable, and the challenge of the next 10 years is going to be redesigning how we represent these networks for human consumption, and how we translate human-scale architectural and security decisions into the practical application of configuration for a literally incomprehensible number of systems that, even for small businesses, can span the entire globe.



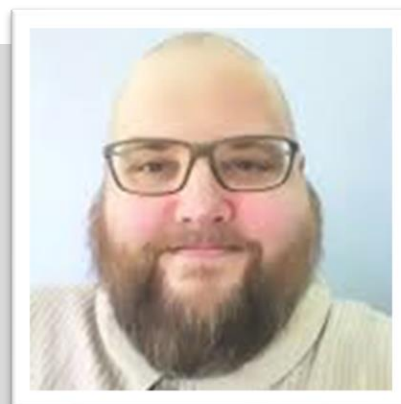
---

Vendors will build – are building – AIs to take on the day-to-day. This, while fantastically difficult, is still the easy part. The hard part is convincing organizations – and certainly individual administrators within those organizations – to give AIs that kind of power. The jump from basic BDCA tools and suggest-o-tron ML agents all the way to AIs which make judgment calls about which policies to craft and apply is, psychologically at least, a pretty big deal. To say nothing of the legal and regulatory implications.

In the end, the latest strains of malware or who is hacking whom is not the problem. The problem – the real problem – is architecture at scale. What is needed are the tools to take the intelligent, experienced, and capable IT staff that organizations already have and empower them to operate at that level. The robots can handle the rest.

#### About the Author

Trevor Pott is the Product Marketing Director for Juniper Networks. He shares all the ways that Juniper's technologies can help organizations of all sizes defend their data, meet regulatory requirements, and advance the organization's own goals while doing so.





## The “New Normal” – Navigating Remote Work and Security in the COVID-19 Era

By Bill Delisi, CEO of GOFBA

There are many “new normal” that apply to different parts of life and certain industries. For cybersecurity, a core change to the landscape is the impacts of remote work and security issues both during and after the COVID-19 era.

Unfortunately, the willingness of SMBs to encourage remote work, conflicts with a general lack of preparedness among staff and security teams for the related cybersecurity challenges. [According to a June 2020 study from IBM](#), which found among other issues that “more than 50% of respondents don't know of any new company policies related to customer data handling, password management and more.”

To rectify the vulnerabilities that come with remote work, SMBs need to increase training and mandate the usage of the proper tech tools. Here are some other considerations.

### Phish, Vish, and Smish – The Need for Training

Phishing schemes continue to wreak havoc during COVID-19, as hackers consistently prey on people's fears. During the early days of the pandemic, there was a rush of scams about COVID-19 testing, or fake

---

alerts about someone needing to pay fake bills during quarantine. As the pandemic continues, there's more phishing schemes produced that tout false vaccine news or encourage people to donate to phony charitable organizations. Employees need training that helps them to spot the hallmarks of phishing emails, including misspelled words or links in the email, urgent language, or a request for the recipient to submit personal information. Remind employees that deleting emails is always a sound best practice, or at the very least screenshotting the content and asking the security team to review.

In addition to phishing training, security should also detail the dangers of vishing and smishing scams. Vishing social engineering attacks involve tricking someone to provide private information through a phone call, for example through the common ruse of an automated message urging the recipient to call their "financial provider." Text and SMS messaging is under attack from "smishing" which hackers use to send alerts and requests for information, for example a text might pretend to come from Amazon and direct people to update shipping and credit card information. Security teams should provide information about these scams to staff, which should include visual examples of each type. Remote workers are especially at risk for these types of attacks due to often using their own device to access both corporate and personal networks and email platforms, which increases the number of suspicious messages they receive.

### The Right Tech and Protections

SMBs that stick with remote work for the long haul will need to devote resources to shore up security. A first step is to provide staff with their own laptop or workstation preloaded with the proper malware software, firewall protection, and various company protocols. What about BYOD? As remote work becomes the standard, many firms will curtail BYOD due to staff using their own devices for riskier behaviors, in terms of cybersecurity threats. There are multiple issues regarding BYOD data storage and movement through various devices. Many firms will find it is easier to avoid potential privacy issues with BYOD by issuing corporate phones and laptops. There is also the device support and updating headaches with BYOD, and corporate devices bring uniformity to updates and device-specific policies.

Further protections for remote work include mandating the use of encryption software for all employee-produced data, which creates a layer of protection from theft or loss of the device. Employees should also use encrypted internet connections, and for the optimal protection consider end-to-end encrypted email and file sharing tools used in tandem with VPNs or remote desktops. Remote workers will adjust to using VPN connections while at home or on the road. They'll need explicit company policies and best practices about using the VPN, including; staying updated with VPN patches and configurations, 100% adherence to using the VPN, and knowing when to disconnect from the VPN when utilizing bandwidth for non-work purposes (video streaming, etc.).

Remote workers should also utilize two-factor authentication for all company passwords. They need context for why this extra step is necessary and to understand any risks to such authentication. For example, the ways social engineering attacks can still exploit two-factor authentication.

### Monitoring

As remote work expands into multiple sectors and types of roles, firms will start to implement more intensive monitoring. This will include web camera feeds during work hours, real-time keyboard logging, and live shared screen views. Such initiatives bring about a host of privacy concerns, especially for workers sharing their Wi-Fi or devices with family members. Employers instituting monitoring will need to create written policies, so employees are aware of the extent of such efforts and their implications. On



---

the security front, monitoring should check remote workers' adherence to best security protocols, such as usage of VPNs, or risky search behaviors. To combat risks during work times, employers will turn towards secure search engines and communication platforms such as [GOFBA](#) which provide intelligent filtering for pornographic, violent, and potentially malware-ridden internet content.

Many SMB owners and managers are not eyeing a return to office buildings and commutes. A May 2020 survey from Intermedia found [57 percent of SMBs](#) that instituted remote working due to COVID-19 said they will likely allow such arrangements in the long term. The survey found business owners noted increases in employee availability, and boosts to both job and life satisfaction as positive reasons for remote work, along with the corresponding lowered overhead costs. There are multiple benefits for remote work, if companies increase their training, technology, and policies to protect company data from cybersecurity risks.

#### About the Author

Bill DeLisi is one of the world's most authoritative experts on cybersecurity. He is currently the Chief Executive Officer, Chief Technology Officer and a founding member of the Board of Directors for GOFBA, Inc. DeLisi has more than 30 years of experience in the computer industry, including holding the position of Chief Technology Officer at several companies. He has worked closely with Microsoft Gold Certified Partners, helping pioneer "cloud" computing and creating security infrastructures that are still in use today. DeLisi is responsible for the development of proprietary technology that serves as the backbone of GOFBA's platform and has over 30 certifications with Microsoft, Cisco, Apple, and others, which includes the coveted Systems Engineer with Advanced Security certification, as well as expert status in Cloud Design and Implementation.

Bill can be reached via email at [bill@gofba.com](mailto:bill@gofba.com) or on his company website [www.GOFBA.com](http://www.GOFBA.com).





## Do Not Forget to Securely Lock Your Data in Microsoft Teams

By Johanna Reisacher, Marketing Manager, Secomba GmbH

More and more employees work from home. As a result, in the last months the demand for Microsoft products, especially Microsoft Teams, has increased. Therefore, in many companies and organizations, a large amount of business data travels back and forth across different teams and channels in Microsoft Teams every day. This data must be protected just as reliably as all other data used in the company.

Up until now, it has not been possible to protect data with end-to-end encryption directly in Microsoft Teams. The German encryption software Boxcryptor offers a solution to this privacy concern.

In the following, we will explain why you should use end-to-end encryption to protect your data. We will show you what the Microsoft Teams integration of the encryption software Boxcryptor looks like.

### Data Protection and Encryption in Microsoft Teams

Video files, audio files, information that you share while chatting or in private messages, and files that you store privately for yourself or for common collaboration in a project group — there is a lot of data that accumulates during the daily use of Microsoft Teams.

---

All of this data is encrypted by Microsoft, both in transit between different devices, users, or data centers, and at rest, with standard technologies.

Microsoft offers to encrypt your data, but that is exactly why Microsoft also remains in possession of the keys to your data. This enables Microsoft to access all data stored and used in Microsoft Teams in plain text. Theoretically, Microsoft employees with bad intentions could access sensitive company data. Apart from that, Microsoft might be forced by authorities on the basis of laws such as the CLOUD Act to provide access to sensible data. Companies that want to store their data according to the zero-knowledge principle have only one choice; they must apply additional protection. Zero knowledge encryption does not allow anyone except the owner of the data and authorized teams in an organization to access the data in plain text. Files are already encrypted on the user's end device before being uploaded to the cloud. So "readable" data never leaves your device.

### The Boxcryptor App — Features and Functions

The encryption solution Boxcryptor offers end-to-end encryption based on a combination of AES-256 and RSA. It has been on the security market for almost ten years. Since July 2020, the software solution is available as an integration in Microsoft Teams, to Boxcryptor Company and Enterprise customers.

Through end-to-end encryption, your data is protected from prying eyes. Nobody can access the data; neither Boxcryptor, nor Microsoft, or any other third party.

The software is cross-cloud, which makes it well suited for a multi-cloud strategy. In total, Boxcryptor supports more than 30 cloud solutions besides OneDrive and SharePoint. NAS systems and local data can be encrypted as well.

Boxcryptor can be directly integrated into Microsoft Teams, similar to other apps. The combination of Boxcryptor and Microsoft Teams offers a user-friendly surface for secure and efficient collaboration in teams and companies.

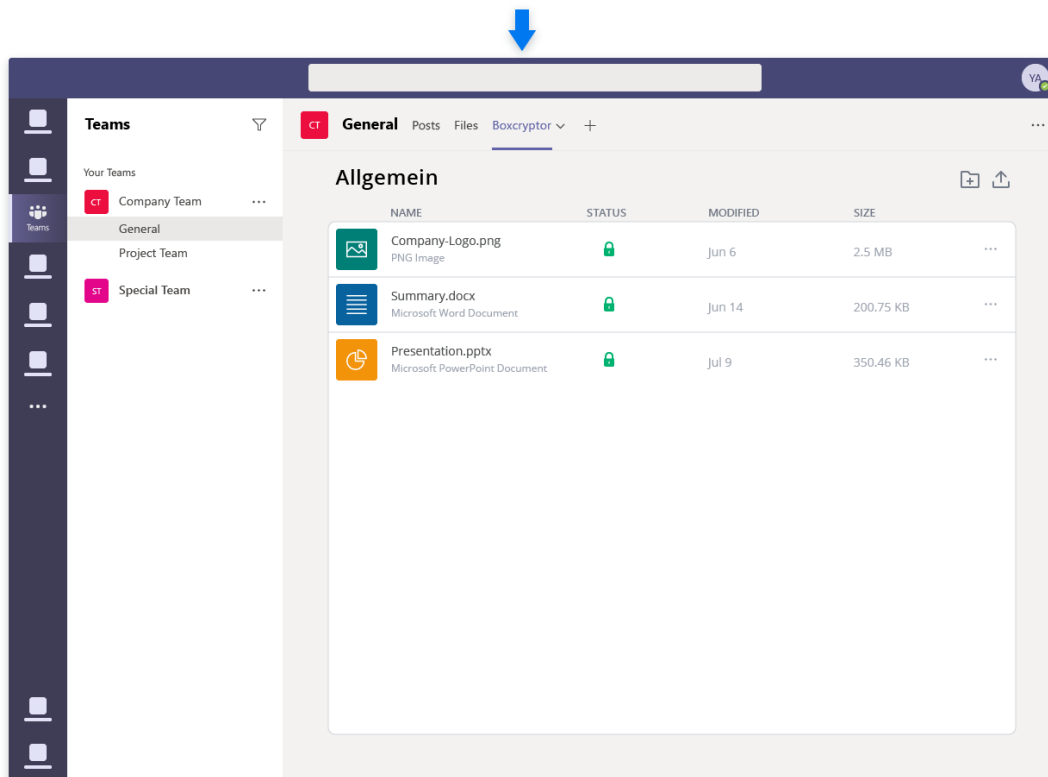
### Three ways to Store End-to-End Encrypted Data in Microsoft Teams

Companies can use the app in Microsoft Teams in three different ways. First, as a so-called "Channel App" in channels of different teams. Second, as a "Personal App" for the user's individual data. Third, employees can share encrypted files with their team directly in the chat area of a channel.

Before first usage company administrators have to download the Boxcryptor app on the website [www.boxcryptor.com/en/microsoft-teams/](https://www.boxcryptor.com/en/microsoft-teams/). Soon it will be also possible to install the app via Microsoft AppStore.



## 1. Secure Team Collaboration with the Channel App



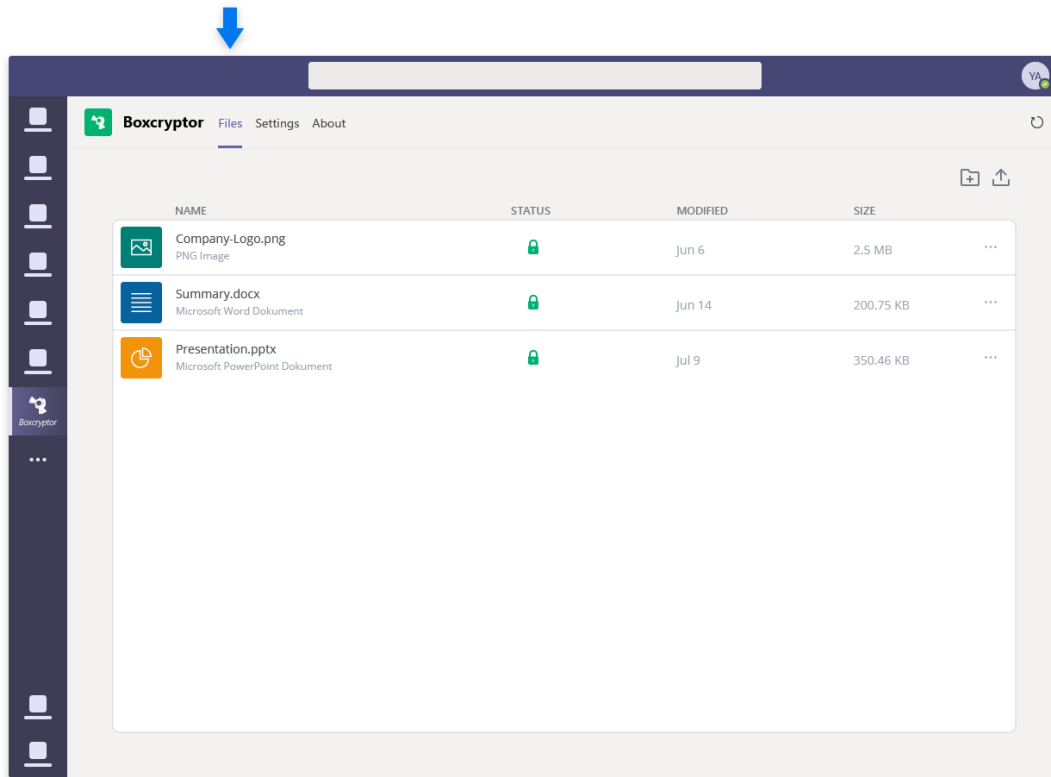
Boxcryptor for Microsoft Teams: Channel App

You can easily integrate Boxcryptor into a channel in your team through adding a new app in the selected Team Channel by clicking on the “+” symbol on the horizontal menu bar. After successful sign-in, the Boxcryptor folder will be displayed as a new tab.

The permission to view the files in the new encrypted folder is initially held exclusively by the person who creates the folder. Other people must first obtain permission before they can access files.

In the Boxcryptor tab, teams are able to view encrypted folders and files, to upload and download files in encrypted or unencrypted mode, and to delete or rename them. You can also create new encrypted folders and preview PDFs and image files.

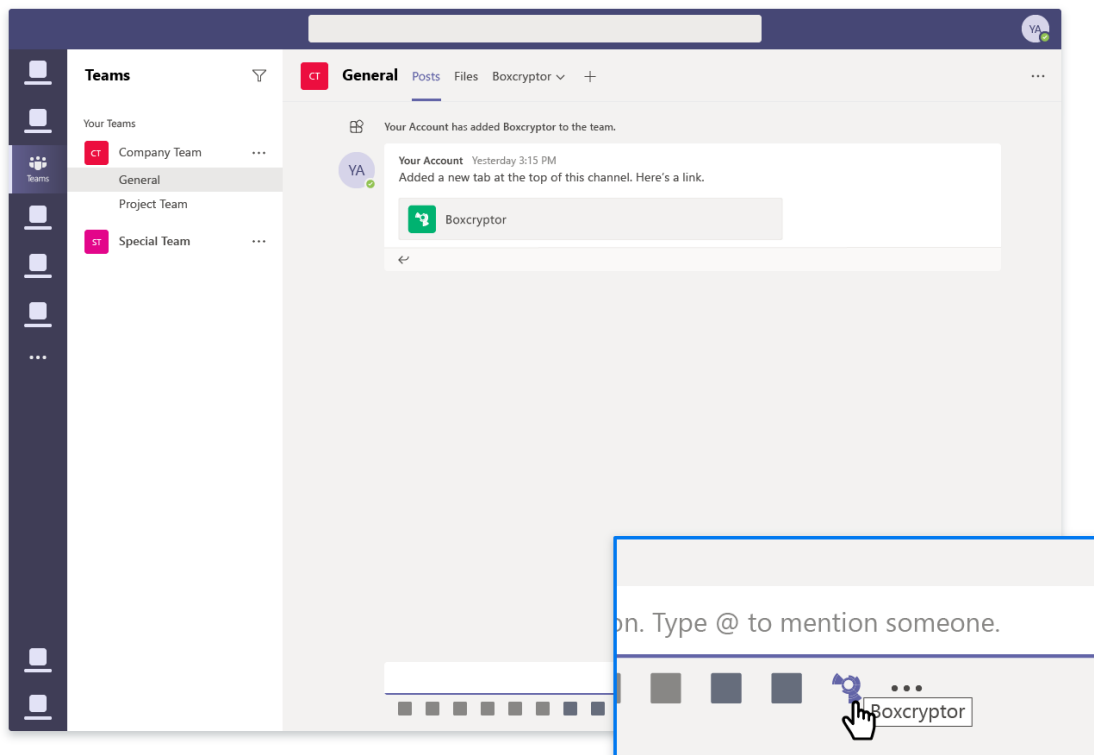
## 2. Boxcryptor's Personal App for Privacy of Your Data in Microsoft Teams



Boxcryptor for Microsoft Teams: Personal App

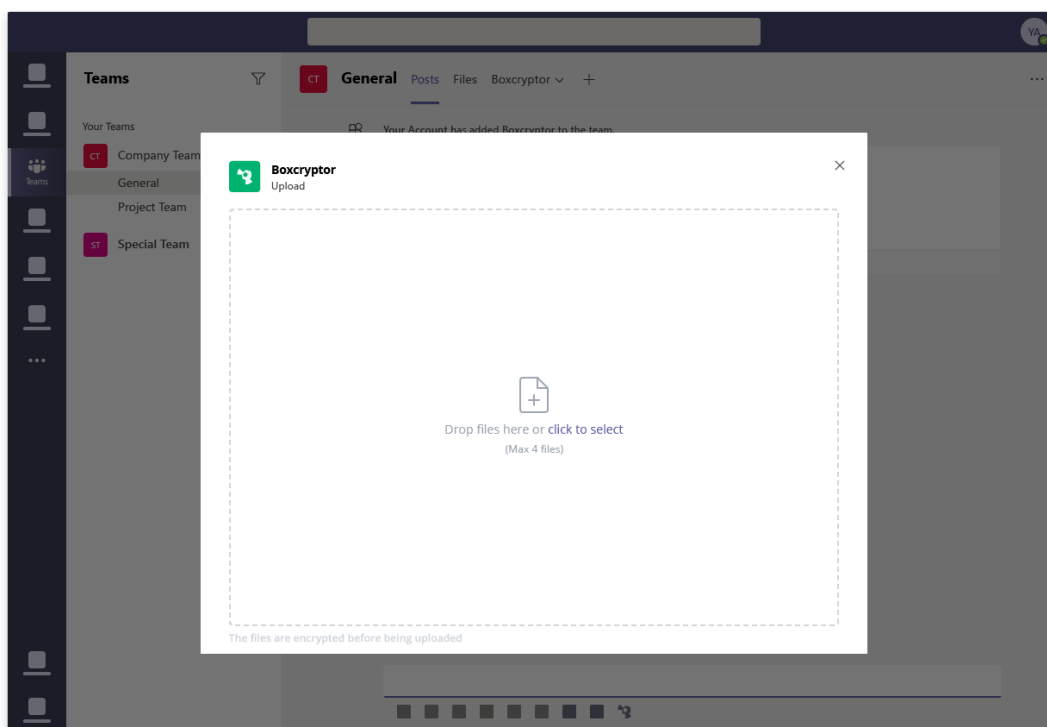
Boxcryptor's personal app gives team members the option to store encrypted data in their private OneDrive folder. This app is for data which is not supposed to be shared with the whole team. Integrate the app by clicking "more apps" in the left, vertical menu bar. Afterwards the app will be pinned on the vertical personal menu bar in Microsoft Teams.

### 3. Sending Encrypted Files in the “Posts” Tab



Boxcryptor for Microsoft Teams: Message Extension





Boxcryptor for Microsoft Teams: File upload via Message Extension

As soon as Boxcryptor has been added to a Microsoft Teams channel, there is another feature available in the “Posts” tab of your channel: You are able to share encrypted files with the entire team, by selecting the Boxcryptor logo below the team conversation. You can upload up to four encrypted files of your choice. Anyone who has Boxcryptor authorization in the channel can open the file which is now displayed as a post, and read it in plain text.

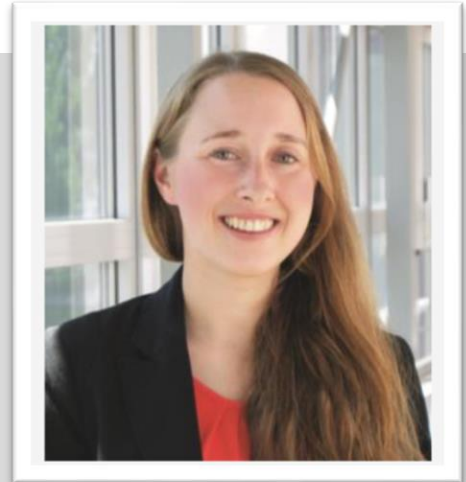
### A glance into the future

There are still limitations if you want to protect your data in every possible scenario in Microsoft Teams. For example, it is not yet possible to encrypt data end-to-end in a private channel or the individual and group chats. Also, Boxcryptor only supports the Microsoft Teams client apps and not yet the browser application. The long-term ambition is an application that gives companies the ability to encrypt business data in any Microsoft Teams application scenario without having to give away the key to their own data.

---

### About the Author

Johanna Reisacher is a Marketing Manager at Boxcryptor | Secomba GmbH. After five years of working for an IT publishing house, she has joined the team of Secomba GmbH in March 2020. Johanna can be reached online at <https://www.linkedin.com/in/johanna-reisacher/> and at our company website <https://www.boxcryptor.com/>





# Building Secure Software Right from the Start: Four Steps for an Effective AppSec Strategy

By Joanne Godfrey, Security Evangelist, ZeroNorth

Companies are rushing to launch digital transformation initiatives and roll out new software products and services at greater speed than ever before. But one false move, such as releasing vulnerability-riddled software that facilitates the loss of company or customer data, can destroy your business.

The easiest way, by far, to protect your business and your customers is to design and build software products that are secure from the start. With software now defining and driving all businesses, the need for an AppSec program has never been more critical. But ramping up an AppSec program is not a simple process. You need time, staff, expertise, not to mention budget, all of which are generally in short supply right now. You also need to figure out a strategy for the program, one that supports your own specific business needs, culture and resources. This strategy should encompass four core components: the ends, the means, the how and the why.

## The Ends: Figuring out what to protect

Not all data and their respective applications are of equal value. Some are internal facing, some are external facing, some utilize customer data, some are informational, etc. So, the first thing to do when ramping up an AppSec program is to consider which are your most valuable assets. Is it your intellectual property? Sensitive customer data? Financial data? You'll also need to understand how this data is used and by which applications, all within the context of your business. So, if your new web app is driving revenue and it's offline, that's bad for your business' bottom line. But what's far worse and much costlier is a breached application that allows malicious actors to gain access to the network and your private customer data.



---

It seems like “what’s worth protecting and what’s not” should be an obvious and easy question to answer, but such an assumption often leaves this important question unasked. If you ask different teams within your organization, you’ll probably get surprisingly varied answers. Through inclusive dialogue with business owners, risk, compliance, security and engineering, you’ll need to determine the value and criticality of your assets—as well as the applications that use them. In turn, this assessment will drive the means and ways you protect them.

### The Means: Lining up the right tools for your AppSec program

There are many technologies and techniques on the market today to protect your critical data and applications, as well as infrastructure. But building secure products from the outset is by far the easiest and most cost-effective way to proactively protect corporate and customer data, not to mention brand reputation. This requires running AppSec scans to discover vulnerabilities during the different stages of the software development lifecycle (SDLC), then analyzing, correlating and prioritizing the data from these scans so developers can easily remediate vulnerabilities as quickly as possible.

So, the second component of an effective AppSec program is to line up the right tools to discover and manage vulnerabilities in your business-critical applications. Selecting the right scanning tools will depend on the languages and frameworks in your application portfolio, performance requirements and budget, as well as how these tools are implemented throughout your specific SDLC. The tool selection and deployment process alone can take many months. It also requires some level of expertise in both security and development technologies and processes, together with a deep understanding of business priorities – time you may not have right now. Moreover, if implementation is a heavily manual process, it’s unlikely the tools will be used consistently—which defeats the purpose.

One way to overcome some of these hurdles and trim down the timeframe needed to ramp up an AppSec program is to use open source security scanning tools. Many open source security scanning tools deliver powerful capabilities. They are free and readily available, making them a practical choice for companies seeking to implement an AppSec program quickly and with little perceived effort. But regardless of whether you’re using commercial and/or open source AppSec tools to gain real value quickly, you’ll need to be able to centrally orchestrate and manage these disparate tools. You’ll also need to find a way to correlate and prioritize findings in order to make the data actionable and operational for security and development teams.

### The Hows: Facilitating productive collaboration between security and development

This leads us to the third component. There needs to be—or you need to build—a committed relationship between the security team responsible for finding security vulnerabilities and the engineering team who actually remediates the issues found.

---

We often hear the engineering team isn't super interested in having the security team run assessments during build pipelines. Or, they don't want to be told about the litany of security issues discovered because of the deep backlog they already have. They don't have the time to deal with this additional work. They have been hired to deliver software, not secure code.

This is where perceptions—and, indeed, job definitions around application security—need to change. It's also where both teams must get on the same page regarding risk. There needs to be an understanding that application security vulnerabilities are a risk to the business in the same way as financial risk or market risk. Which applications should be scanned, when they should be scanned, what vulnerabilities gets fixed, when should they be fixed and how they get fixed must be aligned with what's best for the business. Moreover, vulnerability data must be delivered to developers in an easily consumable and useable format—without unnecessary “noise”—so they can quickly and easily focus on fixing the source of the problem, all without disrupting their existing development processes. Ultimately, by working collaboratively with security, the engineering team can become more efficient and effective, producing higher quality code from the get-go.

### The Whys: Communicating effectively with executives

As with every relationship, business or personal, communication is key. And it's not just about communicating; it's about how you communicate—the tone, the frequency, the language you use.

The fourth component of a successful AppSec program is about effective communication. Salient AppSec information must be communicated to business executives and application owners in terms they can relate to, such as potential loss of revenue; reputation and brand impact; criticality of security vulnerability (high-medium-low); time and cost of remediation (together with the impact of time lost on other strategic initiatives); penalties as a result of a compliance violation and legal implications. Obviously, the timing of this communication is important too. The earlier you flag a security problem with a business-critical application, the quicker it can be addressed. This way, you can hopefully avoid any meaningful impact to your business.

Moreover, communication must be a two-way street. Actually, it must be a three-way street when it comes to security. There must be clear lines of communication from the security team to business decision makers around application security risk. Executives must then assess the cost of that risk to the business and communicate the criticality and priority back to security and engineering teams. These human interactions are critical, and no amount of technology can replace them.

Over time, the business changes, the economic environment changes, people and their perspectives change, breaches happen. And any of those things can be a tipping point in changing perceptions around application security. But to stay competitive while growing business—all within a volatile threat landscape and unpredictable economy—one thing remains constant. Security teams, engineering teams and business executives must work hand-in-hand to understand, assess and mitigate risk. They must continuously measure the impact and results of the program—and then iterate and iterate. The success of your business depends on it.

---

### About the Author

Joanne Godfrey serves as Security Evangelist at ZeroNorth. Previous to this, she was a Senior Product Marketing Manager at IBM Security. She has also held management level positions at Egress Software Technologies, AlgoSec, and Bradford Networks (acquired by Fortinet). She holds a MA in Modern History from University of London and a BA in International Relations, Political Science, and Business from The Hebrew University. Joanne can be reached online at: <https://www.zeronorth.io/>





# VIRUS ALERT

Please select an option:

Safe Mode

Safe Mode with Networking

Safe Mode with Command Prompt



## How to Close the Door on Ripple20 Vulnerabilities by Combining Local Security with Software Defined Perimeters

By Don Boxley, Co-founder and CEO, DH2i [<https://dh2i.com>]

Cyber security researchers at the independent security research group [JSOF](#) recently discovered at least 19 security vulnerabilities that are found at the base of almost all Internet of Things (IoT) products. The zero-day vulnerabilities were found in a TCP/IP software library that Treck, Inc. developed — the software library is widely used in IoT devices, and the supply chain amplifies the vulnerabilities. According to the researchers, this series of vulnerabilities — dubbed "[Ripple20](#)" not for the number of vulnerabilities but for their impact and ripple effect on internet-connected devices in 2020 — affects “hundreds of millions of devices (or more) and include[s] multiple remote code execution vulnerabilities.”

On the JSOF website, the researchers spell out just how high the inherent risks are in this situation, giving the following as examples of potential consequences of these 19 vulnerabilities. Attackers could:

- Steal data off of a printer
- Change an infusion pump's behavior
- Create malfunctions in industrial control devices
- Hide malicious code within embedded devices that stays there for years
- Enable outside entry into network boundaries

---

On June 16, 2020, recognizing the validity and danger of these [vulnerabilities](#), the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a critical security [advisory](#). "A remote attacker can exploit some of these vulnerabilities to take control of an affected system," CISA warned, noting that these affect "Trek IP stack implementations for embedded systems." You can read a July 15 update to this advisory [here](#) that provides a detailed overview of each of the 19 vulnerabilities.

The CERT Coordination Center at Carnegie Mellon University's Software Engineering Institute (SEI) also published a [Vulnerability Note](#) about this issue, stating that most of the 19 vulnerabilities "are caused by memory management bugs" and "likely affect industrial control systems and medical devices." The SEI summarized the situation by stating that "a remote, unauthenticated attacker may be able to use specially-crafted network packets to cause a denial of service, disclose information, or execute arbitrary code."

In short, many cyber security experts believe that we have just begun to discover the magnitude of the danger that Ripple20 represents, and even with fixes and patches from the manufacturer, the problem won't go away easily. There are two potential solutions: local security solutions and software-defined perimeters (SDP). While some local security solutions have proven ability to provide endpoint security for hybrid environments and cloud-based security to protect data as it moves from cloud to cloud and within clouds, deployed alone they may not be able to do the trick.

It's the same with SDP solutions, which can hide the IoT devices from the general public, by use of SDP's micro-tunnels at the application-level. These give network administrators the ability to segment users and devices at the application level rather than the network level. The benefits of this include diminishing the threat of lateral network attacks. SDP achieves this outcome by setting strong limits on remote users, allowing them access only to the applications they require, with no need for access control lists or firewall policies.

SDP also enables IoT devices and gateways to communicate with directly to one another by providing discreet, private and secure network communications over untrusted networks, such as the public internet via User Datagram Protocol (UDP). Companies can thus gain secure connectivity by using randomly generated, non-standard UDP ports for on-demand micro-tunnel communications, requiring only one UDP message channel between IoT devices and gateways. This helps to secure IoT devices leaving no open ports, all but eliminating any surfaces that could remain vulnerable to network attacks.

SDP solutions are also multi-cloud ready, since placing all operations in a single cloud server is risky. SDP software allows for spreading workloads across more than one cloud, which works because of the application-specific micro-tunnels that tie them together. This also reduces risk in case of outages, allowing companies to shift operations as needed from cloud to cloud.

Despite the advantages of SDP, though, if the IoT devices with vulnerabilities from the Trek TCP/IP stack are accessible over the local area network, then the devices will still be vulnerable to attacks. At the end of the day, SDP is a transport layer that can provide private and hidden paths for exclusive data hideaways, but local security for such protected destinations is still local. This is why users need to layer both solutions. When local and SDP solutions are paired, together they present a virtually unassailable defense, which will help safeguard the companies that use this double-tiered strategy from suffering the consequences that can result from Ripple20 vulnerabilities.

---

### About the Author

Don Boxley Jr is a DH2i co-founder and CEO. Prior to DH2i ([www.dh2i.com](http://www.dh2i.com)), Boxley spent more than 20 years in management positions for leading technology companies, including Hewlett-Packard, CoCreate Software, Iomega, TapeWorks Data Storage Systems and Colorado Memory Systems. Don earned his MBA from the Johnson School of Management, Cornell University.







## Funding Schemes and Cyber Security

By Milica D. Djekic

What a lovely day; you are just searching your web for some online business opportunities or you are reviewing the cyberspace to get the stipend for your student's service. Here we go! The option simply appeared on your screen and you are reading carefully about the requirements you need to meet in order to become the part of that project. Yet, there are still a lot of the stock market businesses that would offer you the chance to make some investments in order to collect the good profit at the end of the year. So, you can put several thousand dollars into that site and they would promise you that they would pay you a million after some period of time. Lucky you! So, all you need to become a millionaire is to do some internet research, do smart investment and wait for that money to land on your bank account. Indeed, such a thought can make you being so excited and probably extremely happy, so no one would blame you to get proud on yourself for such a clever decision in your life.

The time would go on; you would wait and begin dreaming what you can do with your first million dollars in your life. The cyberspace is so full of stories how the people became rich over night and literally, many would believe that goes like so. That's why the folks would feel the bless finding some investment

---

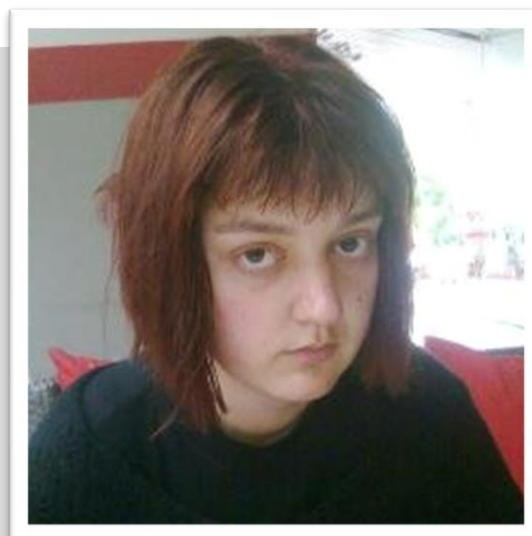
platforms that would also be marketed on the other webpages as so trusted and competitive. The point is that does not go like that! To make your first million dollars you need to work hard for many years and there are no investments platforms that would take the few thousand dollars from you and return you the millions at the end of the season. Even if you save the money in some legal banking it's clear that the interest rates could be only several percents out of total and that's so rational.

So, the next times when you discover the funding website think twice before you make any transaction on. Maybe it's the best to report that case to the authorities as they could advise you what to do then. The heaps of those platforms could serve for collecting the funds for terrorism or another serious offense. The law enforcement agencies would use their security researchers that would provide so skillfully written reports about such web locations and once the policing members get such information they would try to dig deep in order to figure out who got behind such a business. The reason why those websites would appear at so many places across the web is the marketing and nothing else. The scheme is usually like that the investment platform gurus would maintain a plenty of websites and they would use them to leave the impression of the trusted organizations. There would not be the obvious correlation between those websites, but they all would support that funding option.

The role of cyber defense in such criminal schemes could be to do some tracking of the money transactions and try to trace the main bank account as well as the purposes of such gathered funds. In other words, there is no money without hard work and if you want to show your brightness be intelligent as security researcher is and just aware your local authorities about your findings. They would know what to do and apparently, you would be in safe hands, 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, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.





## Media Content Captured on Mobile Is Driving Compliance Problems

Photos, Videos, and Other Multi-Media Content Captured by Employees Are Easily Shared and Rarely Governed

By Josh Bohls, CEO, Inkscreen

Recent headlines are once again demonstrating the consequences of employees inappropriately leaking photos from mobile devices, and are shedding new light on a problem that security and compliance experts have warned about for years. Multimedia content captured on employee devices is left unmanaged and all too easily and inappropriately shared.

In one high profile case, a first responder leaked extremely sensitive photos of the Kobe Bryant helicopter crash site. Clearly it is within the scope of a first responder to document the scene - this is done in any situation from a simple fender bender to a home burglary or a tragic and gruesome event such as a helicopter crash. The photos and videos are critical to document the scene and will be used in many different ways.

In another (and more positive) example, the capture of images on mobile devices has emerged as a helpful component of patient care delivery in some segments of healthcare, particularly during the COVID-19 pandemic. All patient content is of course subjected to HIPAA regulations, CCPA and GDPR protections, and other liability-laden considerations. Yet, even regulatory requirements, stringent

---

organizational policies and laws governing the care and confidentiality of evidence and personal health data are sometimes not enough to prevent leaks of content captured on or shared with mobile devices. Similarly, insurance companies frequently require content captured by employees and consumers to validate a claim, and if the situation results in litigation, the photos may be presented as evidence in the trial.

Unfortunately, whether due to human nature and an individual's drive to share interesting content, malicious device hacks, or through inadvertent leaks, the unauthorized sharing of sensitive mobile content is a major gap in many organizations' security, compliance and risk frameworks.

The reality is that in just about every sector, employees often take photos or videos for their job using the default camera app on their personal or company issued phones. As a result, potentially sensitive photos, documents and videos captured by an organization's employee could easily get that organization caught up in privacy breaches and legal actions.

Employees with law firms, healthcare providers, insurance companies, other regulated industries, and intellectual property/design-led environments (such as automotive development departments for example) routinely take photos or record videos as part of their job. The best and most effective, proactive approach to protect content captured on or shared through employee mobile devices is for the organization to adopt a solution to protect and manage this content.

All of these factors elevate the priority that these photos and videos be managed and controlled. It is imperative that organizations who collect and handle sensitive media - such as law enforcement, healthcare organizations, and law firms - have systems in place to protect the content. The risks and consequences of ignoring this problem are immense. The company may be subjected to regulatory fines, the evidence may not be admissible in court, and victims can certainly cite the harms caused by the public release of such content, as was the case with Mr. Bryant's crash.

IT and security teams need to mandate that employees use apps that enable the organization to protect, manage, and control business content collected on mobile. The new mobile mantra should be: capture media content securely.

One approach that security-aware organizations are taking to protect against leaks is selecting and deploying an enterprise mobility management (EMM) platform such as MobileIron UEM or Microsoft Intune. With or without an EMM, an important step to securing and safeguarding mobile multi-media content is mandating that employees use a managed camera app for all relevant document scans, pdfs, images, audio and video recording, etc.

Such market-proven managed mobile capture solutions let the organization invoke a wide range of policies and controls to protect sensitive corporate data. The best managed mobile capture solutions further extend these protections with compliance features that notify compliance departments, IT administrators or other designated recipients in the event that an employee attempts to share captured content to an unauthorized app or cloud provider, take a screenshot of a protected photo, or other actions that violate the established container and data leak prevention (DLP) policy.



---

Such leak prevention and insider threat logging and alert systems protect all involved – including the subject, the employee and the organization.

The use of employee devices to capture content is now de facto across the workplace. Secure content capture via a mobile capture solution lets organizations sharply reduce the risks inherent with the practice, protects the organization's compliance, and safeguards the privacy and welfare of all involved.

#### About the Author

Josh Bohls is the CEO and Founder of Inkscreen, a pioneer in secure mobile media content capture and governance.

Josh First Name can be reached online at ( [jbohls@inkscreen.com](mailto:jbohls@inkscreen.com) and @inkscreen) and at our company website <https://www.inkscreen.com/>





## Weaknesses of Biometric Authentication

By Mark Perkins, MS, CISSP, IT Manager

In today's digital world, knowing who is on the other end of the wire is more important than ever. Democratization of digital technology and proliferation of Internet access, in addition to the transformation from physical to virtual has created a new era of criminal activity. Currency, for example, can be simply transferred from one account to another. Digital documents requiring multiple signatures can be completed simultaneously on different continents. These conveniences come with a risk. Without physical verification, how do you know who is on the other end?

IAAA, or Identification, Authentication, Authorization, and Accounting, is an essential function in cybersecurity. To identify and verify who a person is, what they have access to, and logging what was done is extremely important. With quantum computing, passwords—even complex passwords—are too easily cracked. Multi-factor authentication can be implemented to mitigate this risk. One of the strongest methods of multifactor authentication is biometric authentication.

---

“Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who he says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database.” (Haughn, 2020)

There are several different types of biometric authentication, and new technologies are being developed every day. Facial scanning and fingerprint scanning are common and found on most smart phones and personal devices. There are many other types, however, such as retina scanning, iris recognition, and palm vein scanning and hand geometrics. Artificial intelligence has allowed new methods to be developed, such as keystroke rhythms. “Identifying or authenticating people based on how they type is not a new idea, but thanks to advances in artificial intelligence it can now be done with a very high level of accuracy, making it a viable replacement for other forms of biometrics.” (Constatin, 2017)

“Unlike the Personal Identification Numbers (PIN) and passwords, biometric data is nearly impossible to guess and is unique to a single person.” (Thompson, 2018) Although it may seem that biometrics are foolproof, they are not. “No one method is without limitation and there is still a way to go until biometric authentication methods become affordable and trusted enough for widespread adoption.” (Thompson, 2018)

Unless you write down your PIN number or password, it is statistically improbable that it would be guesses by a human. Passwords are encrypted with a one-way hash. Fingerprints, unlike passwords, are left on everything you touch. The issue is further compounded by the massive stockpiles of fingerprints in the hands of US authorities, with more than 31 million in a Department of Homeland Security biometrics database as of 2014 and more than 34 million belonging to civilians also in an FBI database as of 2010. (Sputnik International, 2018) History has shown that our government networks are susceptible to compromise. Even more interesting, machine learning has made it easy for researchers to develop “a technique to create so-called DeepMasterPrints: fake fingerprints designed to trick scanners.” (Newman, 2018)

Iris scans are considered highly reliable and are extremely accurate, however the cost of equipment required to get the detail necessary to validate the scan is very high. “Large companies, agencies or Governments can afford that price, but the general public can’t afford to pay that price. Some say that it costs five times higher than fingerprint scanning which is more readily available to the general

---

public.” (Mehedi, 2018) This barrier of entry may encourage a potential user to select a less secure method of authentication. Retina scans also utilize the eyes, however the method used has issues regarding cleanliness and privacy.

“Fingerprints and facial scans are seen as an enhanced additional layer of security, but they rely on database storage just like any other type of data.” (Ikeda, 2019) On a lower level, essentially these biometric values are converted into numbers via complex algorithms and stored in a database on an on-premise server or in the cloud. If the servers and databases are not properly secured, encrypted, or protected with effective perimeter security, the data can be accessed. Values can be changed or deleted. “Unfortunately, leaking of biometric source information is the inevitable next step in a long line of security blunders. With any authentication method, from passwords to advanced biometrics, security is only as strong as its weakest link.” (Ikeda, 2019) The real danger in this situation is unlike a password, biometric data cannot be changed, and once it is compromised the end user is not able to change them.

Security has seen many evolutions in my career. From password, to username and password, to multifactor authentication, to biometrics, to biometrics augmented with artificial intelligence. As information security has become more robust and complex, so have the tools to thwart these methods. All cybersecurity strategies have strengths and weaknesses. One must evaluate their respective environment and determine the best strategy.

#### About the Author

Mark Perkins, MS, CISSP is an IT Manager at a Food and Active Pharmaceutical Ingredient Manufacturer of a globally traded company. He is currently completing his Ph.D. in Information Technology.





---

## References

- Constatin, L. (2017, Jan 27). AI-Based typing biometrics might be authentication's next big thing | PCWorld. Retrieved from PCWorld.com: <https://www.pcworld.com/article/3162010/ai-based-typing-biometrics-might-be-authentications-next-big-thing.html>
- Haughn, M. (2020, July 19). What is biometric authentication? - Definition from WhatIs.com. Retrieved from SearchSecurity.TechTarget.com: <https://searchsecurity.techtarget.com/definition/biometric-authentication#:~:text=Biometric%20authentication%20is%20a%20security%20process%20that%20relies,of%20the%20biometric%20data%20match%2C%20authentication%20is%20confirmed.>
- Ikeda, S. (2019, August 27). CPO Magazine. Retrieved from CPOMagazine.com: <https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/>
- Mehedi. (2018, Jan 18). 25 Advantages and Disadvantages of Iris Recognition - Biometric Today. Retrieved from BioMetric Today: <https://biometrictoday.com/25-advantages-disadvantages-iris-recognition/#:~:text=The%20key%20disadvantages%20of%20iris%20recognition%20are%20the,cost%20of%20the%20iris%20devices%20are%20fairly%20high.>
- Newman, L. H. (2018, November 17). Machine Learning Can Create Fake 'Master Key' Fingerprints | WIRED. Retrieved from [www.wired.com](https://www.wired.com/story/deepmasterprints-fake-fingerprints-machine-learning/): <https://www.wired.com/story/deepmasterprints-fake-fingerprints-machine-learning/>
- Sputnik International. (2018, 12 31). Biometric Weakness: Many Fingerprint-Protected Devices Can Be Hacked - Report - Sputnik International. Retrieved from Sputnik International: <https://sputniknews.com/science/201812311071134102-Fingerprint-Protected-Devices-Hacked-Report/>
- Thompson, E. (2018, January 9). Understanding the Strengths and Weaknesses of Biometrics - Infosecurity Magazine. Retrieved from Infosecurity Magazine: <https://www.infosecurity-magazine.com/opinions/strengths-weaknesses-biometrics/>
- TransUnion. (2020, July 19). BioMetric Authentication | What is BioMetric Authentication | TransUnion. Retrieved from TransUnion Corporation Web Site: <https://www.iovation.com/topics/biometric-authentication>



## 5 Ways to Avoid Security Automation Pitfalls

By Joe Partlow, CTO at ReliaQuest

Amid an enterprise attack surface that is more complex than ever, many security teams have turned to automation to boost threat detection and response. When implemented correctly, security automation can help increase visibility and control over an ever-expanding environment and across the entire security lifecycle.

One of automation's major benefits is that it saves time and energy by replacing manual or repetitive, low-value processes. For example, it can consistently execute operational tasks like process or service restarts or quickly automate incident response processes.

However, some enterprise leaders have unrealistic expectations for automation. They treat it as a cure-all that can replace analysts and other team members. But without the right combination of people, processes and technology to use automation effectively, enterprises could end up investing more resources than they realize in new efficiencies. There are a few strategies and guidelines security teams should keep in mind before they make such an investment.

### Use Automation to Elevate, Not Replace, Human Experience

While automation can streamline workflows and help execute security tasks at scale, it cannot replace a security team. In fact, getting the full value of automation relies on having mature processes and teams

---

in place. Every organization is different, so automation must be used uniquely by every organization. Only a seasoned security team that understands the specific environment can implement automation and continually update playbooks. There is no “set it and forget it” strategy.

### Focus on Automation That Enables Business Continuity

A risk-based approach is often most effective when investing in automation. Enterprises can work with peers and stakeholders to think through how business priorities have changed over the last few months amid shifting workplace processes. Evaluate key priorities, like the rising importance of securing cloud and SaaS applications, as well as any changes to the roles or responsibilities of employees accessing sensitive data and from what location. From there, enterprises can determine the biggest risks to the business and redouble efforts where it will have the biggest impact.

### Apply Automation to What You Know

Automation is best used for specific processes that a security team knows and trusts, instead of applying it to every source in the environment. Automation not only requires intimate knowledge of incident response processes, but it also requires insight and access into the integrated systems. For example, if you want to trigger a vulnerability scan on a target host, even apparently innocuous steps to gather contextual information about hosts become challenging without a deep understanding of the process you want to automate, your organization’s policies, and the system you are integrating.

### Get Creative to Streamline Processes

With IT and security teams stretched increasingly thin, automation is often most effective when used to complete routine tasks to free up time for teams to focus on more important business priorities. Try looking at automation and its potential uses creatively, beyond just running scripts.

For example, automation can be used when differentiating between suspicious insider events and harmless ones. One way to do this is to use automation to continuously simulate common red team or adversary tactics that will quickly identify what risks may be present or gaps in security coverage. By automating these tasks, enterprises can identify where the greatest user risks are and address them by tuning alerts or providing employee training.

### Use Automation to Add Context to Data

Data overload is a persistent problem among security teams, who often rely on disparate tools that collect and store data in many different locations. Some teams attempt to solve this problem by funneling all of their data into a single, searchable repository. But this method can involve a lot of manual, time-consuming process that defeats the goal of greater efficiency.

---

Instead of trying to manually sift through and parse data, security teams can deploy automation to correlate data from across multiple sources, and separate relevant alerts from irrelevant data and false positives. This can help security teams make better decisions and remove the blind spots that are barriers to decision-making. By using automation to organize data, teams gain context around workflows and gain the background for choosing which plays to run against which events.

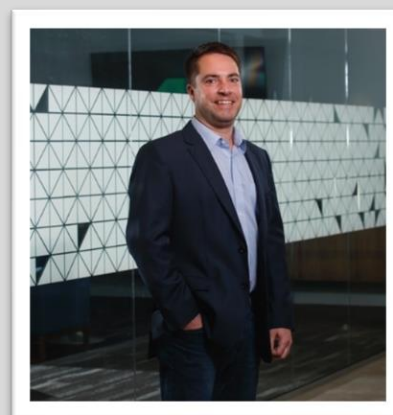
## Final Thoughts

Many automation and orchestration solutions are not intended for companies just starting out down the automation path. They require customers to develop and maintain code in order to create plays and playbooks, versus allowing them to focus on which playbooks to run, and when. Furthermore, they tend to focus on the automation of response rather than look holistically at the security lifecycle, from detection and investigation through remediation and even threat hunting.

It is important for businesses to explore any opportunities to improve efficiencies, particularly as security budgets decrease going into 2021 to account for economic uncertainty. By thinking both broadly and practically about the role of automation, enterprises can make their team's efforts to keep their environment secure both more efficient and effective.

### About the Author

Joe Partlow is the CTO of ReliaQuest, a leader in enterprise cybersecurity, where he oversees all new research and development efforts and new product initiatives. Joe has been involved with infosec in some role for over 20 years; mostly on the defensive side, but always impressed by offensive tactics. Current projects and interests include data analytics at scale, forensics, threats, security metrics & automation, red/purple teaming and artificial intelligence.







# Manual vs. Automatic Cybersecurity Testing: What's the Difference?

By Tamir Shriki, Customer Operations Manager, XM Cyber

In the context of cybersecurity, if you want to protect something, you need the ability to test its defenses. It's the only way to maintain visibility into the true state of your security posture.

The key question, however, is this: How does one get the best and most comprehensive test results? Poor testing may offer little more protection than no testing at all.

For most organizations, it boils down to two choices: Manual tests and automated tests. The former are conducted by people, and the latter by machines. Both have their relative strengths, and both can work together to create a sum that is greater than its individual parts.

## How Manual and Automated Tests Differ

Manual security tests often take the form of red team exercises or penetration tests. Let's take a closer look at these two concepts:

- Penetration tests are designed to uncover any and all vulnerabilities and configuration issues within a computer system. While a vulnerability test or assessment simply identifies security gaps, penetration tests go a step further and exploit these newfound vulnerabilities to discover

---

the full range of impact a breach could have on the system or organization.

- Red team exercises are similar in nature but go beyond the scope of a penetration test. During these exercises, a red team of security professionals (acting much like ethical hackers) will attempt to penetrate a computer system and exploit any vulnerabilities they find. The red team often faces off against a second team of security professionals (dubbed the "blue team") who are tasked with countering the red team and protecting the security environment. Red team exercises often last longer and are greater in scope than penetration tests, with red team members employing social engineering and other techniques to mimic advanced adversaries.

Following manual testing, reports are compiled and detailed remediation or mitigation guidance may be offered.

Automated testing, on the other hand, is typically done with a wide range of tools and applications. Let's take a minute to review two of the most common: Vulnerability scanners and breach and attack simulation platforms.

- Vulnerability scanners are a widely used tool that helps identify and classify security gaps within a network, application, equipment etc. These automated tools can be run quickly and efficiently to spot vulnerabilities that match those listed within its database.
- Breach and attack simulation (BAS) platforms also identify vulnerabilities but take things a step further by also exploiting the vulnerabilities they find (with no impact to production) to fully understand the risk these vulnerabilities pose. A BAS platform acts much like an automated red team, launching continuous simulated attacks and providing prioritized remediation guidance once security issues are identified.

### Is One Approach Superior to the Other?

Manual and automated testing are not in opposition, and often work well together. Each approach described above does have its own characteristics that may or may not make it the right fit for each environment, however.

Penetration tests and red team exercises go well beyond the scope and mandate of a conventional vulnerability scanner. These manual tests, which may be staged over weeks and include top-level cybersecurity talent, are typically much more rigorous and more likely to uncover vulnerabilities that are not widely known or catalogued. In addition to detecting a much narrower range of vulnerabilities and offering a much more limited window into the current security posture, a vulnerability scanner will often return many false positives -- contributing to a phenomenon called alert fatigue, which is one of the more common reasons why breaches succeed.

There is, however, one significant edge a scanner possesses: It's automated and costs little in the way of resources, relatively speaking. As vigorous and in-depth as a good pen test or red team exercise may be, it is also time-consuming and expensive. Most organizations can only afford to stage them quarterly or yearly. This creates a problem, as any changes that occur during the periods between manual tests can create new vulnerabilities. Because manual tests are a snapshot of a point-in-time, they are inherently unable to provide ongoing visibility into the strength of one's security posture.

---

One solution to this problem is to merge person and machine, using scanners to augment pen tests and provide coverage during periods between manual testing. Doing so can help overcome the innate limitations of both approaches. However, the aforementioned BAS platforms also provide an elegant solution to this longstanding problem.

That's because BAS platforms offer the best elements of both approaches: The precision and depth of a manual pen test combined with the continuous coverage of a vulnerability scanner. By constantly probing for new threats (based on the world's most comprehensive threat directory, MITRE ATT&CK), and simulating the most likely techniques and attack paths used by adversaries, an advanced BAS platform acts a permanent, hyper-vigilant red team -- one that never needs a day off or takes a break.

### The Takeaway

Manual and automated testing differ in many key respects, yet they both can work together effectively to ensure that an organization's security posture is sufficiently robust. By incorporating advanced vulnerability scanning -- and cutting-edge new solutions such as BAS platforms -- organizations no longer have to make compromises. Instead of opting for deep but infrequent coverage (manual tests) or shallow but continuous coverage (conventional automated scanning), it's possible to have the best of both worlds -- and enjoy the peace of mind afforded by thorough and ongoing security testing.

#### About the Author

Tamir Shriki is a Customer Operations Manager at XM Cyber. Tamir has held various positions in the cybersecurity industry and managed major customer escalations. He has a strong background in network security, virtualization, AV, IPS, sandboxing, BYOD, mobile access technologies, and encrypted communication protocols.







# Privacy Shield Revoked

What This Means for EU-US Commercial Data Transfers

By Dan Piazza, Technical Product Manager, Stealthbits Technologies

On July 16th, the European Court of Justice (ECJ) [struck down the EU-US data privacy agreement named Privacy Shield](#), which many organizations rely on to transfer data between the EU and the U.S.

Privacy Shield was enacted in 2016 as a replacement for the Safe Harbor Privacy Principles, which were also struck down by the ECJ in 2015. In addition to being a replacement for the Safe Harbor Privacy Principles, Privacy Shield was designed to protect the fundamental rights of data subjects in the EU whose personal data is transferred to the U.S. for commercial purposes.

The primary goals of the Privacy Shield framework were:

- Strong data protection obligations on companies receiving personal data from the EU
- Safeguards on U.S. government access to data
- Effective protection and redress for individuals
- An annual joint review by the EU and U.S. to monitor the correct application of the arrangement



---

Under GDPR (EU's [General Data Protection Regulation](#)) Privacy Shield aimed to act as a safety mechanism that ensured personal data transferred out of the EU received the same protection in the U.S. as it did while in the EU.

### Privacy Shield Declared Invalid

In the ECJ's ruling, it found two major issues with Privacy Shield:

1. U.S. privacy and surveillance laws “are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law.”

This indicates U.S. agencies, like the NSA, have excessive access to personal data transferred out of the EU, which does not align with GDPR standards (i.e. not “essentially equivalent” to EU protections). In addition, certain U.S. laws, such as the Foreign Intelligence Surveillance Act, don't align with GDPR either.

2. Privacy Shield required the U.S. to have an ombudsperson responsible for handling requests and concerns from EU data subjects regarding their data that's been transmitted from the EU to the U.S.

The ECJ found this mechanism “does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law”.

Ultimately the ombudsperson didn't have enough authority to assist EU data subjects with bringing legal action to court regarding personal data.

### How This Impacts Organizations Using Privacy Shield

Companies using Privacy Shield for EU-US data transfers can no longer use this framework, as it was immediately invalidated as of the ECJ's July 16th ruling. With that said, there are two common alternatives to Privacy Shield.

[Standard Contractual Clauses \(SCCs\)](#) are contractual terms which the sender and receiver of data agree to, which ensures both parties are following GDPR standards when data is transferred between the EU and another country (such as the U.S.). [Binding Corporate Rules \(BCRs\)](#) can also be used in lieu of Privacy Shield, if SCCs don't meet an organization's needs.

---

However, SCCs and BCRs aren't as easy to use as Privacy Shield. U.S. organizations that transfer data from the EU must now conduct analysis to determine if they can meet the legal requirements to protect data from U.S. surveillance. This is in direct conflict with the ECJ's Privacy Shield ruling, which found U.S. federal intelligence and surveillance agencies, as well as U.S. laws, currently make this difficult.

In addition, organizations using SCCs or BCRs need to legally guarantee "U.S. law does not impinge on the adequate level of protection" for transferred data. If this legal standard cannot be met, then an organization's data transfers from the EU must be immediately suspended.

*The European Data Protection Board (EDPB) also [posted a FAQ](#) regarding this Privacy Shield ruling. Per this FAQ, GDPR Article 49 derogations may also be means for completing certain data transfers.*

Ultimately, organizations that previously used Privacy Shield need to reevaluate if their data transfer processes meet GDPR standards. Although this is no small task, the following steps are essential:

### Locate Personally Identifiable Information

Organizations need to know what personally identifiable information (PII) they're storing, and where it's located. Due to improperly provisioned access, it's possible that users have moved PII data to unexpected locations.

### Remediate Stale Personally Identifiable Information

Once personal information is no longer needed for regulatory or business purposes, it should either be securely archived or deleted outright.

### Audit and Control Access to Personally Identifiable Information

Overprovisioned and improperly granted access raises an organization's risk for a data breach. Users should only have access to the data required to perform their daily tasks, and admins should only have elevated privilege when needed.

### Be Able to Respond to Consumer Data Subject Access Rights (DSAR) Requests

Organizations must be able to quickly respond to consumer DSAR requests. This involves gathering all PII related to a data subject, providing that information to them, and potentially deleting that information.

---

## How Software Solutions Can Help

Software solutions and automation can help with these steps, including Data Access Governance (DAG) software to locate personal information, remediate stale data, and resolve overprovisioned access, as well as Privileged Access Management (PAM) software to enable secure, task-based administrative access delivered just-in-time and with just-enough privilege.

## Moving Forward Without Privacy Shield

A [joint statement](#) between the U.S. Secretary of Commerce and the EU Commissioner for Justice was released on August 10th, stating the two sides are working towards a new agreement.

“The European Union and the United States recognize the vital importance of data protection and the significance of cross-border data transfers to our citizens and economies. We share a commitment to privacy and the rule of law, and to further deepening our economic relationship, and have collaborated on these matters for several decades.”

This statement doesn't offer any specifics, and until more details are released organizations shouldn't assume a new Privacy Shield is coming soon. Even if a new framework gets put in place, unless there's drastic changes to how the U.S. government treats data privacy then it's likely the new agreement will get struck down by the same EU court.

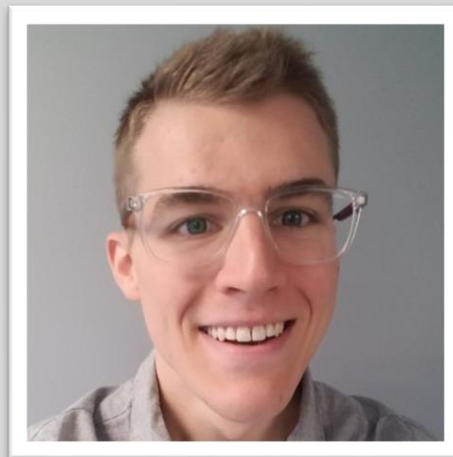
In the meantime, organizations that need to keep the flow of data open between the EU and U.S. will need to utilize either Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

This is an unfortunate reality, but things can only improve once the U.S. government starts to take data privacy more seriously. State-level laws, such as the California Consumer Privacy Act (CCPA) and New York SHIELD Act, are steps in the right direction. However, it's clear the U.S. needs federal data privacy regulations on par with the EU'S GDPR. Until then, arranging a successor to Privacy Shield, and more importantly making it stick, remains a challenge.

### About the Author

Dan Piazza is a Technical Product Manager at Stealthbits Technologies, responsible for File Systems and Sensitive Data in their Data Access Governance solution, StealthAUDIT. He's worked in technical roles since 2013, with a passion for cybersecurity, data protection, storage, and automation. Stealthbits is a cybersecurity software company focused on protecting sensitive data and the credentials attackers use to steal that data.

Dan can be reached online at [linkedin.com/in/danieljpiazza](https://www.linkedin.com/in/danieljpiazza) and at our company website <https://www.stealthbits.com/>





## Automotive Cybersecurity Is Not One-Size-Fits-All. Here's How Oems And Tier 1s Can Tailor Their Approach to Meet the Needs of The Market

*OEMs, Tier 1s and key supply chain players all differ in their approach to cybersecurity, opting for strategies that align specifically with their needs. Chief Product and Marketing Officer Nathaniel Meron outlines the benefits of visibility-first cybersecurity, and how this new approach will allow for intentional, tailor-made cybersecurity policies based on individual needs.*

By Nathaniel Meron, Chief Product and Marketing Officer, C2A Security

### Introduction

Building a production-ready vehicle isn't as straightforward as it sounds. Heightened consumer expectations, increased demand for computerised, connected vehicles, and the persistent [top priority of personal safety](#) all exert pressure on stakeholders in mass vehicle production to get it right. Recently, cybersecurity has emerged as a central sticking point in this narrative: can cars truly be safe, reliable or road-ready without being fully secure, and resilient against attack?

As a result, OEMs and Tier 1 suppliers have hastened to adopt cybersecurity strategies, leading to fragmented [supply chain communications](#) and a multitude of approaches across the industry, neither of which account for the different cybersecurity strategies required for each vehicle. While the industry is



---

looking to address this challenge, albeit gradually, the best approach is one that will see the automotive industry building a tailored cybersecurity approach from the ground up. Instead of aiming for a one-size-fits-all cybersecurity solution, key automotive stakeholders should embrace their differences through a visibility-first concept that will enable each OEM to plan and execute a tailor-made cybersecurity policy based on unique needs.

### Can a customized approach really be cost-effective?

OEMs and Tier 1 suppliers differ in their approach to cybersecurity, as do their needs. While some are focused on the deployment of basic passive security solutions, others have advanced to active measures, each with their own approach: some OEMs and Tier 1s think that one-dimensional protection will suffice, while others are building multi layered defense mechanisms. Though these cybersecurity end-goals are certainly important, the process of getting there is even more so. Today's cybersecurity solutions undoubtedly provide real value to the ecosystem, but are inhibited by their inability to scale easily and support different variants of vehicle models, and how each vehicle on the road may need a different configuration. Automotive manufacturers need a diverse toolbox to protect different systems from the vast array of potential attacks.

These tools must be as [flexible as the approach itself](#). With a supply chain fraught with complication and the sheer volume of vehicle makes and models, it's essential that solutions be scalable enough to accommodate customizations for all industry manufacturers. Although the number of requirements for effective, scalable cybersecurity solutions is high, their cost doesn't have to be. In fact, an approach that creates visibility across the vehicle lifecycle will produce cost savings. Streamlined communication means less overhead and a reduced risk of recalls, while solutions that are easily integrated into any system cost less in the long-term, particularly those that work with any hardware solution.

Though security requirements may change throughout the vehicle lifecycle, OEMs must be able to orchestrate, change and update security across all different models and variations, quickly and effectively.

### Security by design, customized to the automotive industry.

A tailored approach to cybersecurity embodies a new meaning of "security by design" for the automotive industry. No, one OEM can't act as its own supply chain, but it can tailor its implementation strategy to match the architecture of its vehicle. Key players in the automotive industry have already started to master the art of vertical integration. Tesla's rapid-fire approach to innovation has served its purpose well: they are the only automotive manufacturer to build everything from [seats to computer processors](#) themselves, with great success. This same principle can be applied to automotive cybersecurity. While suppliers will undoubtedly still be involved in the process, how can OEMs vertically control cybersecurity by leveraging a solution such as the one deployed by Elon Musk, and Tesla?

Typically, for any OEM, cybersecurity principles remain the same. Security and safety goals are still aligned, but the means of implementation are fundamentally different due to the solutions, vehicle

---

architecture or networks within the vehicle. Take network perimeter security as an example: perimeter components are vulnerable to remote cyber attacks, meaning there are too many potential weak spots residing in the network. Sometimes, there is no isolation between those perimeter networks to inner safety systems at all - making fraught networks, with many potential weak spots, even more vulnerable to attack. Therefore, OEMs need to apply additional layers to enhance security. A scalable, tailored, and visible cybersecurity lifecycle management solution that overlays existing solutions will address all of these needs seamlessly, creating optimal security for the vehicle and a cost-effective, streamlined approach for each OEM.

### Visibility enables OEMs and Tier 1s to customize their approach to cybersecurity

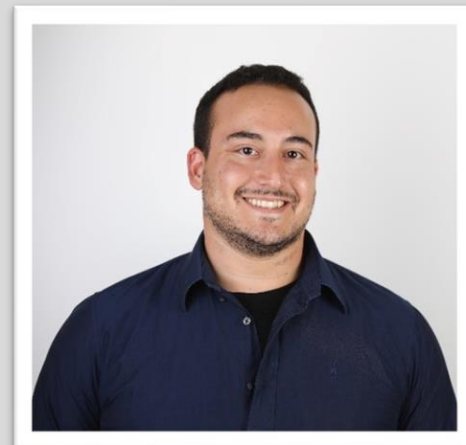
A transparent cybersecurity lifecycle management platform will give the automotive industry the visibility required to perfect cybersecurity posture and achieve their cybersecurity and safety goals. This visibility-first approach means that all OEMs and Tier 1s can practically address cybersecurity requirements of each individual vehicle at scale, regardless of make or model, streamline communication across the supply chain, and reduce the overall cost of cybersecurity per vehicle.

Visibility means security by design customised to the industry and its unique needs. While one OEM can't own their entire supply chain, they can now own all communications across it and prioritise cybersecurity management throughout the vehicle lifecycle. OEMs will be able to orchestrate change and update security across all different car variants, quickly and effectively. The result will be cost-effective cybersecurity for every make, model and individual vehicle, even as cars and trucks become more connected and complex.

---

## About the Author

Nathaniel is passionate about bringing new technologies to market to solve real problems, joining his first startup at the age of 20. With C2A Security, Nathaniel is bringing that same passion to help automotive OEMs and Tier 1s overcome the cybersecurity risks presented by today's sophisticated connected vehicle architecture with new levels of visibility and control. With Nathaniel's support and direction C2A has announced a joint solution with NXP, collaborated with Marvell as a strategic partner, added an additional security control to Vector's AUTOSAR basic software, joined the the AUTOSAR alliance as the first and only Israeli start-up partner, expanded the company's IP portfolio and completed a \$6.5M USD funding round.



An international speaker, Nathaniel has presented at a number of conferences globally including: the Consumer Electronics Show (CES), OurCrowd Global Investors Summit, Collision Conference, MOVE Mobility London, EcoMotion Tel Aviv, and Mondial.Tech among others.

For all of his work at C2A Security, Nathaniel draws upon his extensive experience as a team leader and officer of an elite unit in the Israeli Intelligence Corps. He holds a B.Sc. in Electrical and Electronics Engineering and an MBA, both from Tel Aviv University.

Nathaniel can be reached online at [C2ASecurity@antennagroup.com](mailto:C2ASecurity@antennagroup.com) and at <https://www.c2a-sec.com/>



# Mapping Automation to the MITRE ATT&CK Framework

By Chris Calvert, vice president, product strategy, and co-founder, Respond Software

As major enterprises race to digitize their IT and line of business infrastructures, cybersecurity has become an imperative, both from a business and regulatory perspective. Yet these same forces of digitization and the rise of software have proliferated vulnerable points of access to sensitive information that malicious actors are able to access.

To remedy these challenges, the MITRE Corporation, a global technology standards non-profit, developed the MITRE ATT&CK knowledge base. Its objective was to give cybersecurity professionals a way to systematically categorize and mitigate adversary behavior.

With the vast assortment of tactics and techniques being used by attackers, the MITRE ATT&CK framework provides a way to catalog these methods and understand them. The framework itself, as a result, is large and complex, describing more than 500 activities, which can make it tricky to navigate.

How can organizations defend against all of these activities at all times? The answer lies in aligning automation with the MITRE ATT&CK framework.

## Understanding the MITRE ATT&CK framework

The ATT&CK framework offers security teams detailed and highly specific information on how enterprise IT environments can be compromised and provides actionable insights into attacker behavior. Red teams or pen testers can emulate all of the attack scenarios discussed in the ATT&CK framework. The framework helps security analysts understand the “how” and “why” of particular malicious activities by focusing on attackers’ actions. The ultimate goal of the framework is to provide a comprehensive overview



---

of each possible attack technique as a foundation for security teams to develop a defense plan against. If you can protect your network against every technique catalogued by the knowledge base, your environment is essentially secure.

The MITRE ATT&CK framework categorizes attack tactics based on 12 different columns of data outlining the different tactics that an attacker can use. The adversary will use multiple tactics in different phases of the cyber-attack life cycle. Each phase consists of behaviors, which are a set of techniques. Techniques, in turn, use varying sets of procedures. Therefore, the initial tactic to gain a foothold in your environment is connected to one or more techniques followed by another tactic with its techniques. And so on, until the adversary has reached their objective or has been stopped.

### Setting up the SOC: The more, the merrier

Since it's possible for any one vendor's solution to miss particular attack techniques, it's imperative to create a SOC with multiple overlapping systems and failsafes. Implementing solutions from a variety of vendors brings a breadth and depth of information that can prevent security holes. For instance, integrated reasoning and decision engines monitor and decide like a human expert analyst at the scale, speed and consistent depth of analysis of a machine, fully scoping all relevant malicious activity and incidents.

Known as decision automation, this process can pull all of the relevant information about a network IPS event; an approach that is difficult to accomplish successfully with just a rule or playbook. Decision automation can consider all the context relevant to the tactics and techniques outlined by the MITRE ATT&CK framework, including suspicious patterns in the date and time, the attack category and severity and Source IP/port and Destination IP/port. The solution asks more than 100 questions to decide whether the event is malicious and assigns a score in a probabilistic mathematical equation.

Decision automation maximizes MITRE ATT&CK coverage by cross-correlating disparate sensor data and information to detect, investigate and prioritize security incidents automatically. It maximizes sensor grid investments because security teams don't have to tune their sensors. It can understand the attack from a broader and deeper perspective because it's able to simultaneously investigate, correlate, reason and decide like a human analyst would, but with a deep memory of all current and past incidents.

### Decision automation in action

Let's consider a real-world example. At the beginning of a holistic attack, decision automation software received telemetry from the endpoint protection product or the antivirus. It saw that there was a malicious executable detected or remote access Trojan. It was categorized as a low-severity event, and the telemetry said that the infection had been cleaned. The same thing happened on another asset. Since the decision automation software will gather the threat intelligence, the asset criticality of the internal

---

assets, the account criticality, the vulnerability status and much more, it gathered the information, regardless of whether or not it was escalated as an event.

Two hours later, traffic was seen from both of these servers out on malicious domains and endpoints external to the company environment. So, the software investigated, gathered information, reasoned, scoped, prioritized and escalated this into an incident. This may have been missed by a human analyst because the data that came in said there was a low-severity infection that had been cleaned.

But this is all part of the same big attack story, and the software understood that. It had the deep memory to remember a past incident and be able to tie it into additional data that was gathered and to create an incident.

This is done without the need for rules and playbooks. A SIEM by itself, for instance, needs playbook programming for it to operate and function normally. It also doesn't have the consistent depth of analysis, speed and scale of a machine, scoping in all relevant malicious activity into instance, which may have disparate pieces that are not put together into the big-picture view.

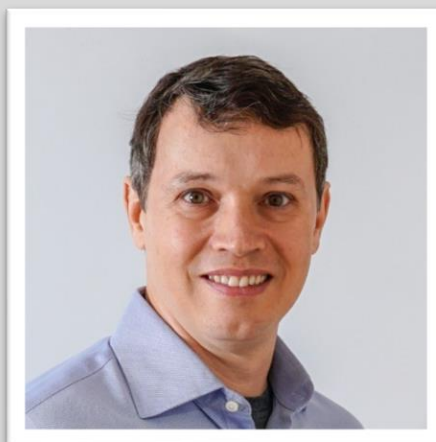
### A hybrid security partnership

The MITRE ATT&CK framework is a practical and useful knowledge base, and it underscores just how complex and vast the attack landscape has become. It's not realistic to expect human security analysts to cover even a small number of attack methods, let alone all of them.

As a result, decision automation is a modern necessity for organizations that want full coverage against all attack types. It makes deeply analytical decisions about what's likely to be worthy of further investigation, which then get passed on to the human analysts in a hybrid partnership that covers all the bases.

#### About the Author

Chris Calvert, vice president of product strategy and co-founder, Respond Software. Chris has over 30 years of experience in defensive information security; 14 years in the defense and intelligence community and 17 years in the commercial industry. He has worked on the Defense Department Joint Staff and held leadership positions in both large and small companies, including IBM and HPE. He has designed, built and managed global security operations centers and incident response teams for six of the global Fortune-50. As he often says, if you have complaints about today's security operations model, you can partially blame him. It's from his firsthand experience in learning the limitations of the man vs. data SecOps model that Chris leads product design and strategy for Respond Software.



Chris can be reached on twitter at @respondsoftware and at our company website

<https://respond-software.com/>



## Cyber Liability Insurance – Safe Bet or Sales Gimmick?

By Darren T. Kimura, [Spin Technology](#)

~~WORD COUNT: 745/600-1000~~

The threat of ransomware is rising rapidly. Each day, we see more stories about companies overtaken by this type of cyberattack. [Garmin](#) and [Canon](#), two well-known consumer brands, are the most recent examples of organizations that paid large sums of money to criminal organizations to regain access to their company data. In Garmin's case, the demanded ransom was over \$10 million, which doesn't include wasted company time and resources, customer loss, legal fees, fines, or the amount paid to an organization to negotiate with the hackers on their behalf. Even organizations with tight security protocols can be affected – cybercriminals are becoming increasingly sophisticated in their methods as the payout for ransomware creeps higher.

While an attack on a large organization is costly, ransomware for a small or medium-sized business can be disastrous as well. The majority of all cyber-attacks aren't directed at multi-million-dollar companies; they're leveraged against smaller businesses that may not have the resources to dedicate to creating a fully secure environment for their data. In fact, a recent study showed that [60 percent of SMBs](#) will suffer a data breach at some point, and 70 percent are targets for ransomware. Even more shocking – 86

---

percent of ransomware victims had antivirus protection. Unfortunately, in some cases, prevention is not enough.

### What is cyber liability insurance?

Cyber liability insurance is a specialty insurance line intended to protect businesses (and the individuals providing services from those businesses) from Internet-based risks (like ransomware attacks) and risks related to information technology infrastructure, information privacy, information governance liability, and other related activities. These types of threats are generally excluded from traditional commercial liability policies or are poorly defined. It's often a logical step in protecting data once an organization has already put in place the necessary and recommended security and privacy protocols to protect against data theft.

### Does my organization need cyber liability insurance?

Despite being the primary target for most ransomware attacks, 80 percent of SMBs do not have cyber insurance protection. Many SMBs falsely assume they don't need the coverage if they don't do payment transactions. But the reality is that cybercriminals are using social engineering and phishing scams to steal personally identifiable information (PII) and to gain access to networks and accounts. This type of loss can create liability for the company and require expensive forensics and remedial actions – including alerting thousands of customers by mail and purchasing identity theft protection for them after-the-fact. And if hit by a ransomware attack for example, it can mean total lockout of data sets, systems, accounts and more (if proper backup protocols are not in place) – that cost can be catastrophic.

### What coverages does my business need (and what does it cost)?

The amount of insurance needed truly depends on your business size. In many SMBs, \$100,000 is often enough. However, when evaluating the amount of coverage, it's wise to remember that the cost of a ransomware attack is often more than just the ransom itself. For example, one 50-employee company was hit by a ransomware attack, which cost them \$6,000 in ransom. However, it also cost \$15,000 for forensics, \$20,000 in legal fees, \$12,000 in fines, and \$20,000 in data recovery. While the initial sum demanded was manageable, the total expense was more than \$73,000. The cost of the policy itself can range from a few hundred dollars up to several thousand dollars a year, depending on requested coverage.

### What exactly does it protect the company from?

Most policies protect from e-theft, ransomware, telecommunications theft, and social engineering fraud. Social engineering fraud refers to the transfer of money or securities to a person or account beyond the insured entity's control by an employee. This can help protect the organization from cybercrime generated within the infrastructure of the business (insider threats). Having insurance that protects the organization from both internal and external threats is the best way to ensure an unforeseen incident will be covered.



---

### Is there coverage beyond the base policy?

For many organizations, having a cyber liability policy is a safeguard above and beyond their current insurance policies. It's an explicit certificate dedicated to aiding the recovery process should a cyberattack occur. This approach is forward-thinking, as cyberattacks of all kinds continue to rise across the board. Relying on a blanket corporate policy to cover cybercrime is a risky venture. These types of policies often include language and loopholes that may exclude payment for certain types of disaster like acts of war as an example. The first step in securing company data should be the protection of that data and the engagement of policies and technology to prevent an attack in the first place. However, cyber liability insurance is an additional precaution that's recommended in case the unthinkable occurs.

#### About the Author

Darren is the Executive Chairman and Chief Revenue Officer at Spin.ai. He holds 13 patents and his expertise covers Cybersecurity, IT, Software, Big Data, and Networking. Darren is based in Palo Alto, CA.



The background is a dark blue gradient with a grid of faint white lines. Overlaid on this are several concentric circles and arcs, some of which are composed of small white dashes, resembling a stylized clock or a data visualization. Binary code (0s and 1s) is scattered throughout the image, particularly along the arcs and in the corners. A semi-transparent yellow rectangle is centered horizontally and vertically, containing the word "EVENTS" in large, bold, black capital letters.

# EVENTS





# GSX

GLOBAL SECURITY EXCHANGE

POWERED BY ASIS INTERNATIONAL

**21–23 SEPTEMBER 2020**  
ATLANTA, GA | [GSX.ORG](https://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](https://GSX.org)**.

**REGISTER WITH CONFIDENCE » [GSX.org/CDM](https://GSX.org/CDM)**

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



# CYBER SECURITY

FOR CRITICAL ASSETS | EUROPE

6th - 7th October 2020

— Virtual Event —

FREE with code:

CDMVIP

Join Us Online at Cyber Security for Critical Assets European Summit This October

The 7th annual Cyber Security for Critical Assets Summit brings together 100's of IT & OT security leaders from across the Oil & Gas, Energy, Utility, Power, Water, Mining, Healthcare & Chemical industries for 2-days of insight building and expert knowledge exchange on 6th - 7th October. Join us online to hone your skills in areas including:

- Steps to ensuring business continuity during the COVID-19 pandemic
- Transforming your cyber security strategy to keep up with Industry 4.0
- Modelling an OT SOC
- Incident response and disaster recovery for critical systems
- Addressing the human element of cyber security
- Designing, operating and managing risks to ICS and their assets
- Governance in OT environments
- And, more!



Speakers include CISOs, VPs, Heads of IT & OT Security at: Maersk, Ofgem, Iberdola, NATS, Ansaldo Energia and more...



Andy Powell  
CISO  
Maersk



Cristian Cucu  
CIO  
Nuclearelectrica



Mark Chaplin  
Principal  
Information Security Forum



Sandra Heissenberger  
CISO  
City of Vienna



Marc Samson  
CISO  
ENGIE Services BeLux



Stuart Okin  
Head of Security Privacy  
& Resilience  
Ofgem



João Domingues Agostinho  
Cyber Security Chairman  
Trans Adriatic Pipeline



Claudio Bolla  
Group Information Security  
Director  
INEOS



Mikael Vingaard  
Specialist Industrial Security  
Danish Energy Agency



Andrew Cocking  
Information and Cyber  
Security Manager  
NATS

This is a one-of-a-kind opportunity for critical infrastructure leaders across Europe, to come together and safeguard their assets. View the agenda and secure your place for FREE using the discount code: CDMVIP at: [europe.cs4ca.com](https://europe.cs4ca.com)



# ISAF | CyberSecurity

## 9<sup>th</sup> International Cyber Security, Information & Network Security Exhibition

OCTOBER 08<sup>th</sup>-11<sup>th</sup>, 2020

Istanbul Expo Center (İFM) - Türkiye




[www.isaffuari.com](http://www.isaffuari.com)

T. +90 212 503 32 32 - [marmara@marmarafuar.com.tr](mailto:marmara@marmarafuar.com.tr)

**MARMARA**  
TANITIM FUARCILIK  
[www.marmarafuar.com.tr](http://www.marmarafuar.com.tr)

 /marmarafuar

 /isafexhibition

 /company/marmara-fuar



# CYBER SECURITY FOR CRITICAL MANUFACTURING | USA MANUSEC

October 13th-14th 2020

— Virtual Event —

FREE with code:

CDMVIP

Join Us Online at Cyber Security for Manufacturing USA Summit This October!

Cyber Security for Critical Manufacturing Summit launches online this October, uniting 100's of manufacturing security leaders from America's: **Transport, FMCG, Food & Beverage, Machinery, Chemical, Pharmaceutical & Automotive** industries.

The agenda boasts an A-list speaker line-up as well as an educational edge that reveals the most up-to-date insights for mitigating risks and safeguarding critical manufacturing processes. Join us online to hone your skills in areas including:

- Managing cyber risks in the era of smart production
- Launching an OT security operations centre
- Overcoming the challenges of network design and security in manufacturing environments
- Building high-performing security teams
- Employing a Strategic Approach to Managing Shared Supply Chain Risks
- Developing, implementing and testing OT disaster recovery plans
- And, more!

**CPD  
CERTIFIED**  
The CPD Certification  
Service

Speakers include CISOs, VPs of IT & OT Security, Heads of Automation at **Pepsico, GSK, Nexteer, Kraft Heinz, Tesla Motors...**



Arun DeSouza  
CISO  
Nexteer



Arvin Verma  
Cyber Risk Management  
Specialist  
Pepsico



Lisa Tuttle  
CISO  
SPX Corporation



Michael Elmore  
VP OT Security  
GSK



Chandra Brown  
CEO  
MxD



Ismail Guneydas  
Cyber Security  
Assurance Manager  
Tesla Motors



Ricardo Lafosse  
CISO  
Kraft Heinz



Yancho Gerdjikov  
Regional Security Lead  
Nestlé



Brandi Johnson  
Sr. Manager, Cyber Risk  
Management  
Toyota



Scott Reynolds  
Manager, Industrial  
Security  
Johns Manville

This is a one-of-a-kind opportunity for manufacturing security leaders across USA, to come together and safeguard their assets. View the agenda and [secure your place for FREE](#) using the discount code: **CDMVIP** at: [usa.manusecevent.com](https://usa.manusecevent.com)



**THE INDUSTRY'S LARGEST  
INDEPENDENT AI GOVERNMENT EVENT**

2nd Annual

# **aiworld | GOVERNMENT VIRTUAL**

**OCTOBER 28-30, 2020**

**1,100+**  
ATTENDEES

**120+**  
SPEAKERS

**85+**  
SPONSORS

**50+**  
CONFERENCE  
SESSIONS

**Save 20% 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](https://AIWorldGov.com)**

# QUBIT CONFERENCE **SOFIA** 2020

3<sup>rd</sup> Cybersecurity Community Event

**29**OCTOBER/ 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**

EXHIBITION  
**20/23**  
LE BOURGET

**2020**

CONFERENCE  
**19**  
PARIS



[www.euronaval.fr](http://www.euronaval.fr)



# 5<sup>th</sup> BRAND PROTECTION CONGRESS



**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 Magnificent petronas twin towers & shoppers paradise that is Kuala Lumpur , Malaysia.*



# **6<sup>th</sup> BRAND PROTECTION CONGRESS**



**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](mailto:info@worldbigroup.com)

**WORLD BI**  
CONFERENCES | SUMMITS | WEBINARS





[www.egyptdefenceexpo.com](http://www.egyptdefenceexpo.com)

[@egyptdefenceexpo](https://www.instagram.com/egyptdefenceexpo)

[/egyptdefenceexpo](https://www.facebook.com/egyptdefenceexpo)

[@visitedex](https://www.tiktok.com/@visitedex)

[#edex2020](https://twitter.com/visitedex)

## THE 2<sup>ND</sup> 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

Supported by

Organised by





A night cityscape with a network overlay. The image shows a dense urban environment at night, with city lights and building silhouettes. Overlaid on this is a complex network of white lines connecting various points, resembling a digital or cyber network. The text 'CYBERSECURITY KNOWLEDGE. WHEN YOU NEED IT.' is prominently displayed in the center in a bold, white, sans-serif font. The entire graphic is framed by a thick blue border with a slight 3D effect.

# 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](https://rsaconference.com/cyberdefense-2020)



# HELP PROTECT AMERICAN INTERESTS IN CYBERSPACE

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working on the front lines safeguarding Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll find a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.



**AFCivilianCareers.com/CYBER | #ItsACivilianThing**

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.





# 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\*\*](https://www.goanywhere.com/think-like-a-hacker) to get a free copy of our cybersecurity guide.



**GO ANYWHERE®**  
Managed File Transfer





DATA PROTECTION WORLD FORUM

PRIVACY | TRUST | RISK | SECURITY

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

**Rowena Fell**

Global and EMEA Risk Assurance  
Operations Leader - Ernst & Young

**Flavius Plesu**

Head of Information Security  
Bank of Ireland UK

**Steve Wright**

Data Privacy and Information  
Security Officer - John Lewis

**Marloes Pomp**

Head of Blockchain Projects  
Dutch Government



**SEE THESE SPEAKERS FOR FREE**

*Use our code 'CYBERMAGFREE'*

**#CYBERBYTE**  
**@ROSSOWESQ**





---

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](mailto:marketing@cyberdefensemagazine.com)



# CYBER DEFENSE TV

## INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here...we've launched [CyberDefense.TV](https://www.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.

### The Interviews

These anticipated "CEO Hotseat" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Miliefsky**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. [www.cyberdefense.tv](https://www.cyberdefense.tv)

## Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

[By signing up, you'll always be in the loop with CDM.](#)

---

Copyright (C) 2020, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

All rights reserved worldwide. Copyright © 2020, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

### Cyber Defense Magazine

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

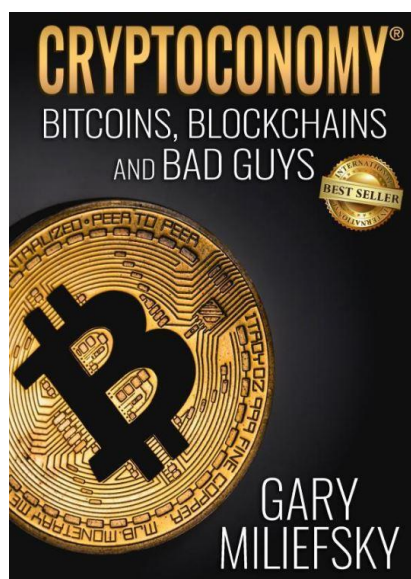
NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)  
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 09/02/2020



# TRILLIONS ARE AT STAKE

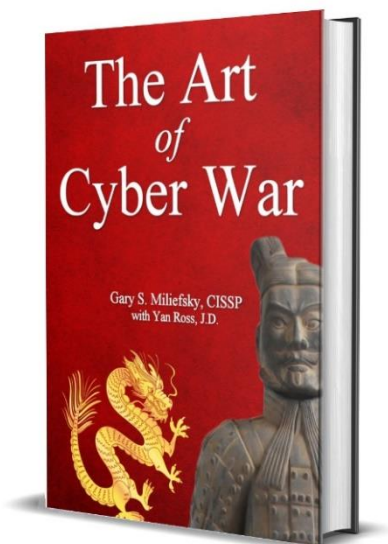
**No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES**

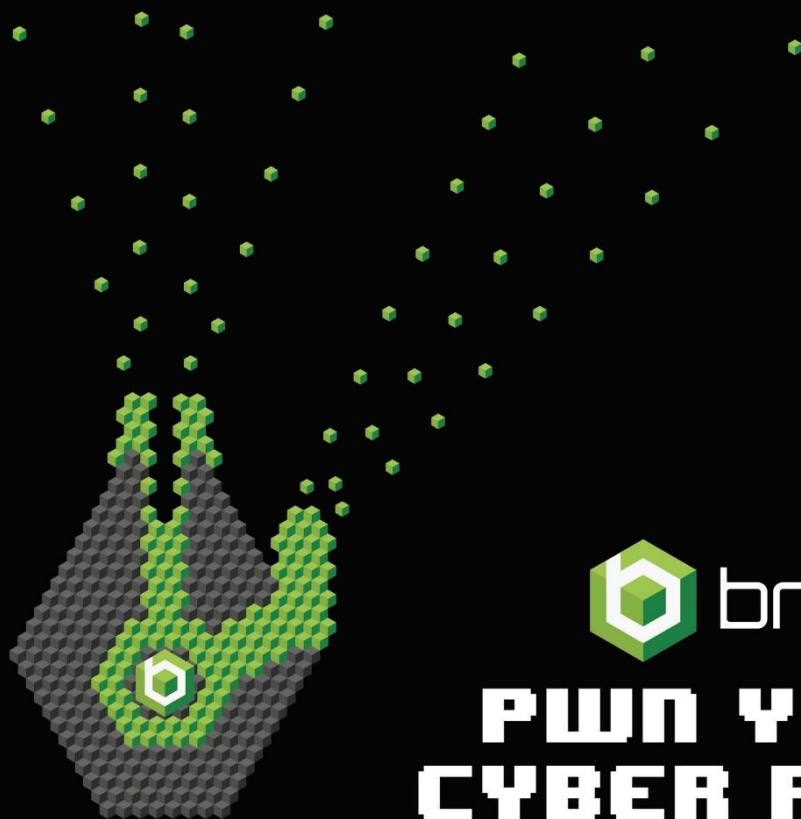
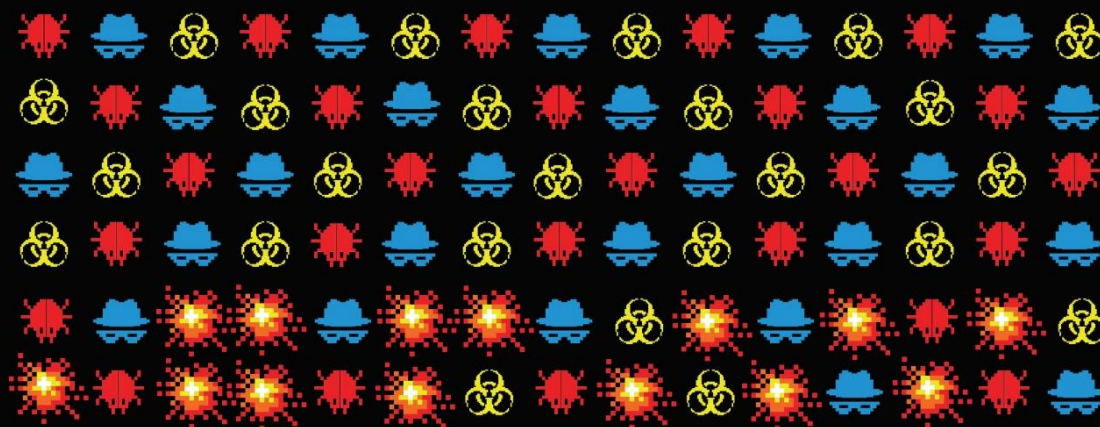
Released:



<https://www.amazon.com/Cryptoeconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH>

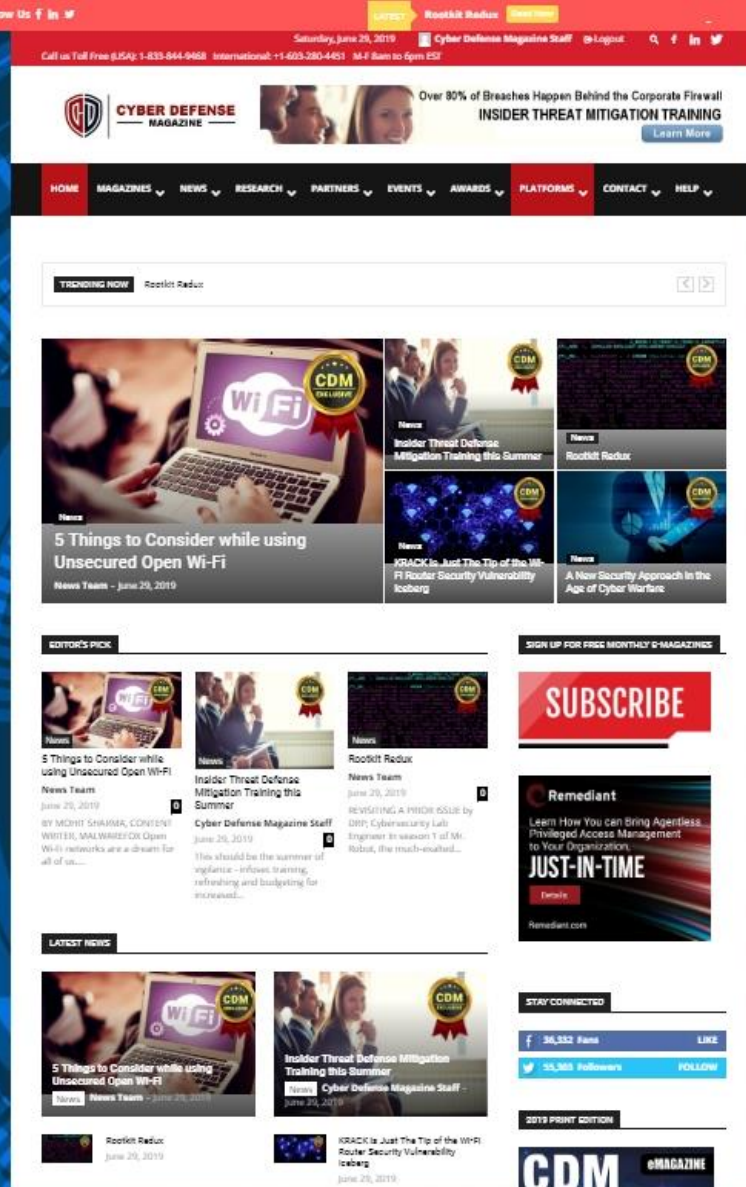
In Development:





**PWN YOUR  
CYBER RISK**





## 8 Years in The Making...

### Thank You to our Loyal Subscribers!

We've Completely Rebuilt [CyberDefenseMagazine.com](http://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](http://CyberDefenseMagazine.com) up and running as an array of live mirror sites. **Millions of monthly readers and new platforms are here:**

[www.cyberdefensewebinars.com](http://www.cyberdefensewebinars.com) and brand new [www.cyberdefenseventures.com](http://www.cyberdefenseventures.com)



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



### Be Part of the Experience!

Call **800.733.3976** or visit [smartmanufacturingexperience.com](https://smartmanufacturingexperience.com)



## 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**



**SECURITY SERVICES  
LEADER**



**LEADER IN MANAGED  
SECURITY SERVICES**



**SECURITY COMPANY  
OF THE YEAR**



**#1  
ON THE**



**TOP 10  
ON THE**





# CDM

**CYBER DEFENSE MAGAZINE**

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

## eMAGAZINE

[www.cyberdefenseemagazine.com](http://www.cyberdefenseemagazine.com)


"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert



**ALWAYS FREE  
NO STRINGS ATTACHED**



A night cityscape with a network overlay. The image shows a dense urban environment at night, with city lights and building silhouettes. Overlaid on this is a complex network of white lines connecting various points, resembling a digital or cyber network. The text 'CYBERSECURITY KNOWLEDGE. WHEN YOU NEED IT.' is prominently displayed in the center in a bold, white, sans-serif font. The entire graphic is framed by a thick blue border with a slight 3D effect.

# 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](https://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.



**cythereal.com**



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