



# CYBER DEFENSE MAGAZINE

eMAGAZINE

MAY  
2022

## In This Edition

*Vulnerable Today, Hacked Tomorrow: How a Lack of OT Cybersecurity Affects Critical Infrastructure by Ian Bramson*

*Understanding Russian Hacking Tactics to Power Up Security in the Energy Sector by Chip Epps*

*Gone Phishing: How Ransomware, Log4j, and Other Exploits Use Your Network to Catch the Big Fish by Peter Bookman*

*...and much more...*



**MORE INSIDE!**

---

# CONTENTS

<b>Welcome to CDM's May 2022 Issue</b> -----	<b>7</b>
<b>Vulnerable Today, Hacked Tomorrow: How a Lack of OT Cybersecurity Affects Critical Infrastructure</b> -----	<b>22</b>
By Ian Bramson, Global Head of Industrial Cybersecurity at ABS Group	
<b>Understanding Russian Hacking Tactics to Power Up Security in the Energy Sector</b> -----	<b>25</b>
By Chip Epps, VP of Product Marketing, OPSWAT	
<b>Gone Phishing: How Ransomware, Log4j, and Other Exploits Use Your Network to Catch the Big Fish</b> -----	<b>28</b>
By Peter Bookman, Founder and CEO of guardDog.ai	
<b>Zero Trust: It's a journey, not a Destination</b> -----	<b>32</b>
By Dr. Matthew McFadden, Vice President, Cyber & Distinguished Technologist, GDIT	
<b>5 Key Learnings from Intel's 2021 Product Security Report</b> -----	<b>35</b>
By Jerry Bryant, Senior Director of Security Communications and Incident Response at Intel	
<b>Defending Your Remote Workforce with Zero Trust Security</b> -----	<b>38</b>
By Raul Popa, CEO & Co-founder, TypingDNA	
<b>The Countdown Has Started on Secure IoT Compliance</b> -----	<b>42</b>
By Kyle Haefner, Lead Security Architect, CableLabs, Bruno Johnson, CEO, Cascoda, Joe Lomako, Cybersecurity Lead, TÜV SÜD UK test lab	
<b>Tips for Implementing HITRUST for Healthcare Providers</b> -----	<b>49</b>
By Philip Jones, Mazars, Director of Security - Chief Information Security Officer (CISO), Data Privacy Officer (DPO) for Healthcare	
<b>Why Access Control Is Critical in The Path to Cyber Insurance Readiness</b> -----	<b>52</b>
By Joseph Carson, Chief Security Scientist and Advisory CISO at Delinea	
<b>How To Establish SAP Security</b> -----	<b>56</b>
By Christoph Nagy, CEO, SecurityBridge	
<b>A Resilience-Centered Approach to Cybersecurity</b> -----	<b>59</b>
By Safi Raza, Director of Cybersecurity, Fusion Risk Management	
<b>Data-centric Security: Defense in Depth</b> -----	<b>62</b>
By Amit Shaked, CEO, Laminar	

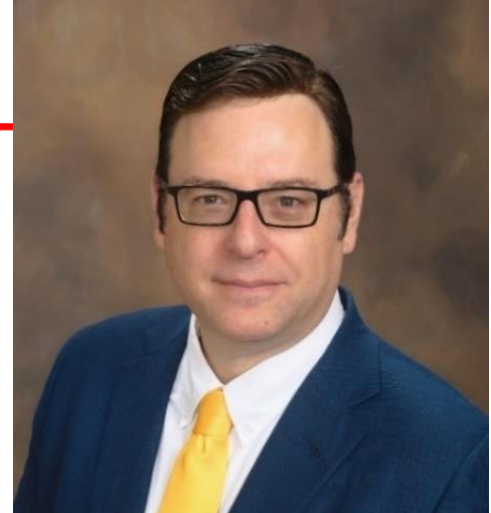
<b><i>Interview with Morten Kjaersgaard, CEO of Heimdal Security on How Cybersecurity Businesses are Tackling the Ukraine Crisis</i></b> -----	<b>65</b>
By Morten Kjaersgaard, CEO, Heimdal Security	
<b><i>True Cybersecurity Requires a Shift to A Data-Centric Philosophy</i></b> -----	<b>68</b>
By Brian Platz, CEO and co-founder, Fluree	
<b><i>The Best Cyber Security Jobs in The UK According to Data</i></b> -----	<b>72</b>
By Karim Adib, Data Analyst, The SEO Works	
<b><i>Why And How to Eliminate Security’s Biggest Blind Spot: Transport Layer Security (TLS)</i></b> -----	<b>76</b>
By Bassam Khan, VP of Product and Technical Marketing Engineering, Gigamon	
<b><i>Ethical AI - How is AI Redefining the Insurance Industry?</i></b> -----	<b>80</b>
By Antoine de Langlois, Responsible AI Data Scientist at Zelros	
<b><i>Cybersecurity’s New Frontier: Space</i></b> -----	<b>83</b>
By Duncan Jones, Head of Cybersecurity, Quantinuum	
<b><i>Drones And the Battlefield</i></b> -----	<b>86</b>
By Dr. Shaun Passley, Founder, ZenaDrone	
<b><i>Privileged Access Management as a Key Technology for Critical Environments</i></b> -----	<b>89</b>
By Dr. Heiko Klarl, Chief Marketing and Sales Officer, iC Consult	
<b><i>The Future of MFA</i></b> -----	<b>93</b>
By François Amigorena, Founder & CEO, IS Decisions	
<b><i>Cybersecurity Doesn’t Have to be a Game of Last Man Standing</i></b> -----	<b>96</b>
By John DeSimone, President, Cybersecurity, Intelligence and Services at Raytheon Intelligence & Space	
<b><i>How The Updated CMMC 2.0 Rule Impacts DoD Contractors</i></b> -----	<b>99</b>
By Dan Clarke, President of Truyo, and Jeff Sizemore, Chief Governance Officer at Egnyte	
<b><i>Bosch Aishield To Protect AI Systems and Bolster Digital Trust</i></b> -----	<b>103</b>
By Manoj Parmar, Global Program Director – AISHield at Bosch, Amit Phadke, Global Product Manager – AISHield at Bosch	
<b><i>The Land of Data-Centric Security: Before and After</i></b> -----	<b>106</b>
By Andy Smith, CMO, Laminar	
<b><i>Non-human Resources</i></b> -----	<b>110</b>
By Camellia Chan, CEO and Founder of X-PHY a Flexxon brand	

<b><i>A New Paradigm for Absolute Zero Trust and Infrastructure Resiliency</i></b> -----	<b>113</b>
By Rajiv Pimplaskar, President and CEO, Dispersive Holdings, Inc.	
<b><i>5 Reasons Why Insider Threat Should Be a Security Priority</i></b> -----	<b>116</b>
By David Barroso, Founder & CEO, CounterCraft	
<b><i>Poor Identity Management Amplifies Ransomware</i></b> -----	<b>120</b>
By David Mahdi, Chief Strategy Officer and CISO Advisor, Sectigo	
<b><i>Prevent Browser-In-The-Browser Phishing Attacks by Removing Human Input Error</i></b> -----	<b>123</b>
By Julia O’Toole, founder and CEO of MyCena Security Solutions	
<b><i>Threat Intelligence: Cyber and Electromagnetic Activities (CEMA) with Software-Defined Radio (SDR)</i></b> -----	<b>126</b>
By Brendon McHugh, FAE & Technical Writer, Per Vices	
<b><i>Cyber Security and Cloud Computing in the New Era of Remote Working</i></b> -----	<b>134</b>
By Enrique Gomez - COO GAT Labs	
<b><i>Control the Uncontrollable, The Path to Supply Chain Security</i></b> -----	<b>138</b>
By Ed Chandler, AE and Cybersecurity Lead, TÜV SÜD America	
<b><i>Defend Your Castle with Zero Trust</i></b> -----	<b>143</b>
By Peter Oggel, Chief Technology Officer, Irdeto	
<b><i>Transparency And Collaboration Between Vendors and Customers Are Key to Reducing Third-Party Security Incidents</i></b> -----	<b>147</b>
By Nick Sorensen, CEO of Whistic, Inc.	
<b><i>Responding To High-Level Cyberattacks on A Mid-Level Budget</i></b> -----	<b>150</b>
By Jesper Zerlang, CEO, LogPoint	
<b><i>Security Gotcha of Consumer and Industrial IoT Devices</i></b> -----	<b>153</b>
By Smit Kadakia, Chief Data Scientist, Seceon Inc.	
<b><i>Operational Security: How to Get Rid of Digital Footprints On The Internet?</i></b> -----	<b>158</b>
By Viktoria Sokurenko, CMO of Ukrainian start-up X-ray	
<b><i>How the Cloud Upended Security – and How Encryption Helps Restore It</i></b> -----	<b>169</b>
By Tilo Weigandt, co-founder, Vaultree	
<b><i>Public Sector Must Remain Diligent as Cloud and Ransomware Intersect</i></b> -----	<b>172</b>
By Rick Vanover, Senior Director of Product Strategy at Veeam	

@MILIEFSKY

From the

Publisher...



We'll be celebrating our 10<sup>th</sup> Year in business and of our [Global InfoSec Awards](#) and as a

Platinum Media Partner of [RSA Conference](#) on June 06 – 09 , 2022 – See You There!

Dear Friends,

The view from the Publisher's desk continues to focus on the immediacy of threats to our national and international cybersecurity. The current news often focuses on the cyber attacks which have become the war zone of today.

The continued spread of the so-called "hybrid total war" concerns all of us, as we enter a new phase of state-sponsored (whether acknowledged or not) cyber attacks. This non-nuclear means of war, reaching all sectors, all geography, and all demographics potentially targets all of the 16 sectors of critical infrastructure.

In response to the demands of our markets and partners, the scope of CDMG's activities has grown into many media endeavors to meet these growing needs. We offer Cyber Defense Awards; Cyber Defense Conferences; Cyber Defense Professionals (job postings); Cyber Defense TV, Radio, and Webinars; and Cyber Defense Ventures (partnering with investors). The full list, with links, can be accessed at:

<https://www.cyberdefensemagazine.com/cyber-defense-media-group-10-year-anniversary-daily-celebration-in-2022/>

Cyber Defense Media Group (CDMG), having launched our 10th annual cybersecurity community awards this year, continues to seek nominees for our annual young Women in Cybersecurity scholarship program for entries. Any young woman in high school who will be entering college in 2022/2023 can apply now until June 1st:

<https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-fund-for-2022/>

Readers can learn about the last two year's winner, in 2020, Annabelle Klosterman, here: <https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-winner-for-2020/> in 2021, Olivia Gallucci, here: <https://cyberdefenseawards.com/women-in-cybersecurity-2021-scholarship-winner/> who both remain an inspiration for other young women to enter the field of cybersecurity.

As in past years, a panel of judges will review each entry and choose one scholarship winner and a backup winner in case there are issues on the winner's college entry in 2022/2023. Now is an excellent time for young women to plan their future careers in cybersecurity. It's a hot field with hundreds of thousands of career openings and unlimited opportunities for those who wish to make a positive impact on today's digital world.

Warmest regards,

*Gary S. Miliefsky*

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

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



**@CYBERDEFENSEMAG**

## **CYBER DEFENSE eMAGAZINE**

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

### EDITOR-IN-CHIEF

Yan Ross, JD

[Yan.Ross@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

<http://www.cyberdefensemagazine.com>

Copyright © 2022, Cyber Defense Magazine, a division of

CYBER DEFENSE MEDIA GROUP

1717 Pennsylvania Avenue NW, Suite 1025

Washington, D.C. 20006 USA

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

All rights reserved worldwide.

### PUBLISHER

**Gary S. Miliefsky, CISSP®**

Learn more about our founder & publisher at:

<http://www.cyberdefensemagazine.com/about-our-founder/>



## **10 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](#)**  
**[PROFESSIONALS](#) [VENTURES](#) [WEBINARS](#)**  
**[CYBERDEFENSECONFERENCES](#)**

---

# Welcome to CDM's May 2022 Issue

## From the Editor-in-Chief

Once again, this month the Editor's Welcome letter provides an overview of the topics and trends in the articles for the issue. As always, the articles reflect the authors' perceptions of the most pressing cybersecurity matters of the day.

The challenges and responses of the cybersecurity community are growing, as evidenced by the unusually large number of articles being submitted, reviewed, and published; this month we are pleased to include 40 impressive articles, all relevant to the most pressing cybersecurity issues of the day.

A brief review of this month's Table of Contents will demonstrate the breadth and importance of the topics chosen by our contributors and brought to you, our readers, to support your own cyber endeavors.

We live in an ever-changing and dynamic world of cyber players, both offensive and defensive; the importance of cyber endeavors in both domestic and international affairs, especially as an alternative to physically destructive physical warfare, continues to grow.

The central role Cyber Defense Magazine plays in the breadth of activities conducted by the entire Cyber Defense Media Group means that we always select and publish the most actionable intelligence from the most knowledgeable writers in the field.

Wishing you all success in your cybersecurity endeavors,



Yan Ross  
Editor-in-Chief  
Cyber Defense Magazine



### About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at [yan.ross@cyberdefensemediagroup.com](mailto:yan.ross@cyberdefensemediagroup.com)



# SPONSORS







# CYBER DEFENSE CONFERENCES



## ***THREE EVENTS IN ONE***

**Orlando, Florida, USA | October 27-28, 2022**

***One of the most exclusive, fun and educational CISO conferences of the year!***

*Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world renowned expert - meets 100 top cyber defense companies in an intimate, high value two day summit*

**[www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com)**



# **RSA**<sup>®</sup>Conference

---

## **San Francisco**

---

**Moscone Center & Digital | June. 06 - 09, 2022**



**REGISTER NOW**





# THE SECRETS OF HARDENING ACTIVE DIRECTORY

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

**GET YOUR FREE eBook**

Get <https://cionsystems.com/>



DATATRIBE

# CYBER STARTUP FOUNDRY

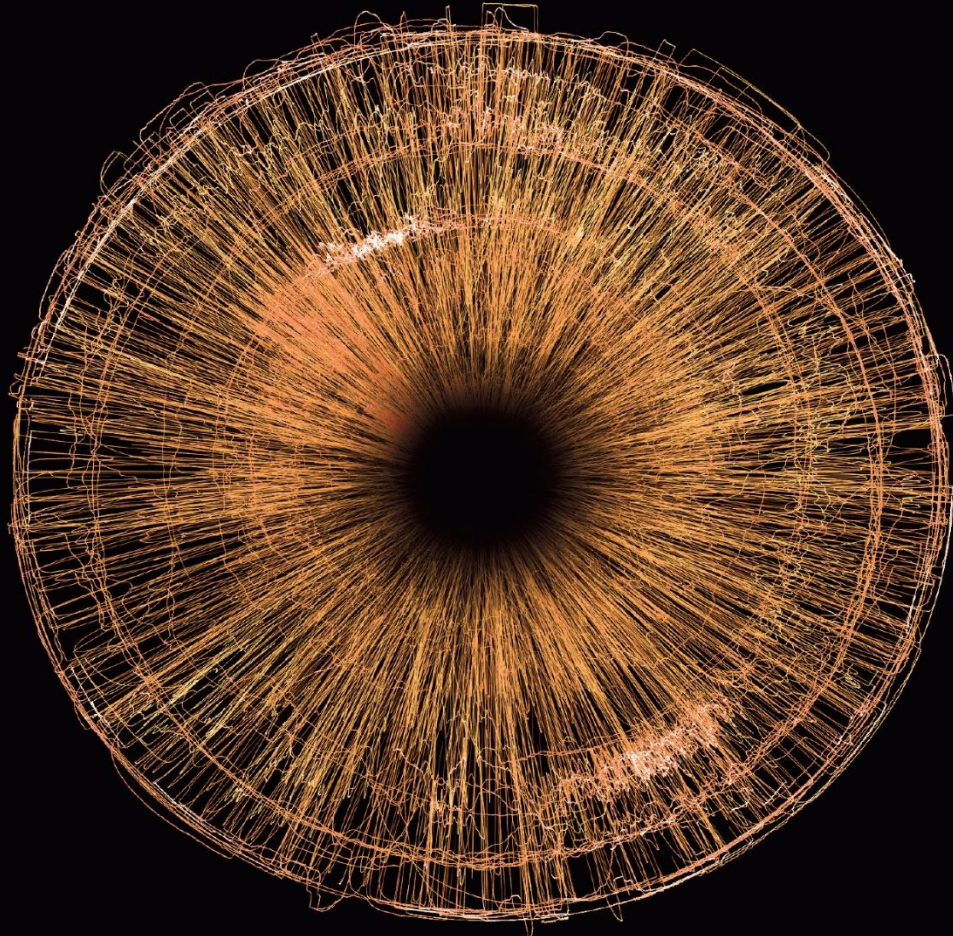
Forging dominant companies  
from nation-state domain expertise

CAPITAL | RESOURCES | GUIDANCE | SUCCESS

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



JOIN THE TRIBE  
DATATRIBE.COM



# Record Every Packet. See Every Threat.

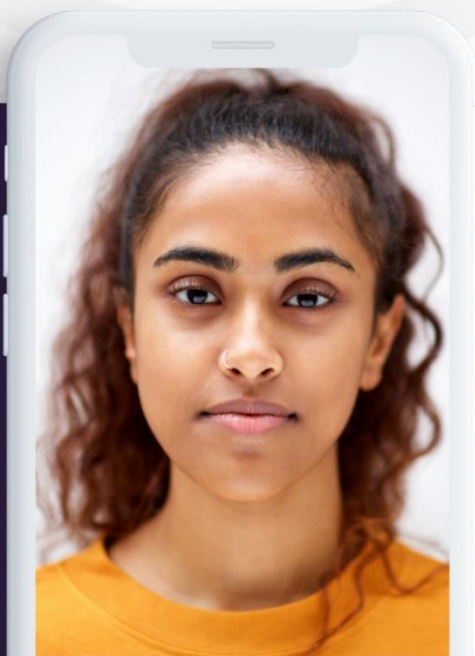
Capture the evidence as it happens.  
Because there are no second chances.

[endace.com](http://endace.com)



# Close the loopholes in passwordless logins with identity-based authentication

Defeat phishing, data breaches and ransomware while improving your user experience.



## Experience BlockID

Use biometric authentication with flexible levels of identity assurance to secure workforce account access and eliminate the risk and inconvenience of passwords.

[www.1kosmos.com/demo](http://www.1kosmos.com/demo)

We monitor the  
**DARKWEB**  
so that your  
**BUSINESS** has  
no stops





# Award-Winning, Secure File Transfer & Automation

▶▶ **Supports All Major Transfer Protocols**  
FTP, FTPS, SFTP, HTTP, HTTPS, AS2, Email, SMB, CIFS, NFS

▶▶ **Best In Class PGP Automation**  
Encrypt, decrypt, sign or verify encrypted files with a simple checkbox

▶▶ **Cloud Integration**  
Connect To A Range Of Cloud Storage Providers (Amazon S3, Microsoft Azure, Box, Citrix ShareFile, Dropbox, Google Cloud, Oracle Cloud and more)

▶▶ **RepliWeb Replacement**  
RepliWeb reached End of Life on 01/31/2022. This platform is no longer being supported. Our software, Diplomat MFT, is an ideal alternative to this popular solution.

▶▶ **FREE TRIAL**  
We offer a no obligation, free trial or demo. Please visit our website for more details or call us on: (210) 985-0985



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



# CYBER CRIMINALS DON'T GIVE A \$#!T:

But we do, and we're  
here to help!



## SCADAfence

The Most Comprehensive  
OT & IoT  
Cyber Security Platform For  
Critical Infrastructure &  
Enterprises

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

- About your project's scope.
- It's managed by a third party.
- It's a legacy system.
- It's "too critical to patch."
- About your outage windows.
- About your budget.
- That you've always done it that way.
- About your go-live date.
- It's only a pilot/proof of concept.
- About non-disclosure agreements.
- It wasn't a requirement in the contract.
- It's an internal system.
- It's really hard to change.
- It's due for replacement.
- You're not sure how to fix it.
- It's handled in the Cloud.
- About your Risk Register entry.
- The vendor doesn't support that configuration.
- It's an interim solution.
- It's [insert standard here] compliant.
- It's encrypted on disk.
- The cost-benefit doesn't stack up.
- "Nobody else could figure it out."
- You can't explain the risk to "The business."
- You've got other priorities.
- About your faith in the competence of your internal rules.
- You don't have a business justification.
- You can't show return on investment.
- That it's supposed to be "Air Gapped."

# 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)



# 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



**“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)

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

# ARTICLES



## Vulnerable Today, Hacked Tomorrow: How a Lack of OT Cybersecurity Affects Critical Infrastructure

By Ian Bramson, Global Head of Industrial Cybersecurity at ABS Group

Did you know almost 50% of ICS (Industrial Control Systems) organizations don't have dedicated 24/7 security to manage Operational Technology (OT) incidents should a cyber event occur? While this fact may not be common knowledge to organizations, hackers have been readily exploiting this gap, as seen in incidents such as the Colonial Pipeline shutdown or the Oldsmar, Florida water treatment plant breach. Adversaries have learned that targeting ICS can result in quicker and higher payouts because of the potential to disrupt operations, prompting threat actors to focus on ICS targets. Ransomware attacks have proven very effective for OT systems just as with IT systems and are now being used as a weapon in international politics. As the conflict between Russia and Ukraine continues, adversaries are looking to gain real-world advantages from these kinds of cyber attacks. The pro-Russia hacking group Conti recently released [a statement](#) stating, "We are going to use all of our possible resources to strike back at the critical infrastructure of an enemy." This should be a warning bell for any organization involved in critical infrastructure to be on high alert and consider themselves a potential target. All of this begs the question: are organizations prepared to detect and respond to a cyber attack on their OT systems?

### New SANS report highlights lack of preparedness

Despite known and increasing threats, many organizations have not made OT cybersecurity a priority. A recent report from the SANS Institute titled "[Threat-Informed Operational Technology Defense: Securing Data vs. Enabling Physics](#)", found that only 22% of security technology managers have the visibility needed to defend against modern threats. If an organization is creating a response plan after an attack

---

occurs, then they are already too late. Keeping your response plan ready for implementation at a moment's notice and your staff current on the procedures for addressing an attack enables a swift and unified response, yet 40% of those surveyed have not run incident response exercises in the last 18 months. On the positive side, although it appears many OT environments are not well positioned to detect or respond to an attack, many companies do have investments planned. The research reveals that 52% of respondents rank increasing visibility into control systems and implementing ICS specific network security monitoring (NSM) as top priorities in the next 18 months.

## Why is OT cybersecurity lagging behind?

Attacks on the OT environment are not entirely new, with notable incidents like the Stuxnet attack in Iran dating back 12 years. But there is still a perception gap between senior decision makers and those on the front lines about the importance of a robust cybersecurity program in OT. In the SANS report, 35% of participants indicate such a gap between senior management and OT/ICS cybersecurity front line teams. This gap manifests itself as lack of investment in OT cybersecurity programs which means security teams are resource challenged and running on threadbare budgets.

The expertise required to manage OT cybersecurity programs is highly specialized. An effective program requires experience in both cybersecurity and the industrial environment within which the systems operate. Too many organizations take a "copy and paste" approach, applying the same principles and techniques from IT environments to OT, which have drastically different concerns, processes and equipment. Attacks on these OT systems go beyond data and into physical spaces and deal with networks of legacy equipment installed at different times and with varying levels of technological capabilities. As a result, a dedicated team of experienced professionals is needed to better protect the security of the system and the people working inside of it. However, the survey found that currently 47% of ICS organizations do not have internal, dedicated, 24/7 security response teams.

## Taking steps to close the gap

Getting in front of this challenge requires change from the top down. To close the gap between front line teams and senior management organizations, decision makers can take several different steps:

- Appoint a Chief Information Security Officer (CISO) who can oversee OT/ICS security from a senior executive position, guaranteeing OT security professionals have a voice in the boardroom to help prioritize security initiatives.
- Educate the board of directors on common misconceptions surrounding OT security. This means making sure they understand that OT security can't be copied from IT, that being compliant does not mean being secure, and that this is a quickly evolving space where solving the last attack won't prepare you for the next one.
- Run OT-specific tabletop exercises regularly to keep team members from different levels of the company on the same page regarding a response to an attack. ICS incident response teams must

---

understand the control system processes, the engineering, industrial protocols, safety factors, and ICS-specific cyber threats and maintain response plans that fit their organization.

- Employ an active cyber defense cycle (ACDC) whereby they can secure, maintain, monitor for and respond to threats. This repeatable process is driven by human cyber defenders who have both the necessary engineering knowledge of the OT environment and a background in cybersecurity defense. An active defense keeps security personnel engaged in identifying vulnerabilities and takes a more proactive than reactive approach with the focus on understanding not just the last attack but looking ahead to the next one.
- Bring in a third-party organization to aid in identifying vulnerabilities, setting up a robust security program, and advising on maintaining OT protection moving forward. These experts can provide support for companies as they make key hires and set up an in-house cybersecurity program.

## Cybersecurity now or forever hold your peace

OT environments are still playing catch up in terms of cybersecurity as 45% of survey participants estimate threats to their control systems are at high risk. And they're right. The effect on operations, human safety and the environment could all prove costly when OT systems are exploited.

Many companies are not prepared for the potential onslaught of attacks that could be headed their way. While many are coming around to the necessities of building a more robust cybersecurity program for their OT environments, they are fighting an uphill battle to prepare for these attacks. Threat actors are actively plotting their next OT/ICS attack, looking to disrupt critical infrastructure either for profit or political gain. Without a proper plan for how to identify, respond to and recover from an attack before the attack occurs, organizations could find themselves in costly and dangerous situations.

### About the Author

Ian Bramson is Global Head of Industrial Cybersecurity at ABS Group and a recognized leader in the emerging threat landscape of attacks on industrial operations and critical infrastructure. With more than 20 years of experience in cybersecurity and technology, Ian works directly with executives in the energy, industrial and maritime sectors to help minimize their cybersecurity risks. Ian can be reached online through his LinkedIn page at <https://www.linkedin.com/in/ianbramson/> and at our company website <https://www.abs-group.com/>







# Understanding Russian Hacking Tactics to Power Up Security in the Energy Sector

By Chip Epps, VP of Product Marketing, OPSWAT

Every critical infrastructure sector depends on energy to operate, yet the energy industry reports one of the highest rates of cyber incidents. Operational Technology (OT) is often the target of cyber criminals given that it controls the critical physical processes within industrial facilities, and gaining control of it can cause catastrophic damage. Coupled with the critical nature of these environments is the vulnerability of aged legacy systems that operate on air-gapped and isolated OT networks which require physical access to manage and deploy system updates.

Recent news coverage on the indictment of Russian spies for conducting a global hacking campaign that targeted hundreds of energy organizations has intensified the ongoing conversation about the security of critical infrastructure, especially since one of the targets of this campaign hit close to home at a nuclear facility in Kansas. While the indictment was retroactive to the activities that occurred between 2012 and 2018, the six-year hacking campaign serves as a great case study for industry leaders in the energy sector to understand the attack vectors and learn how to prevent threats to OT in the future.

## A Watering Hole of Tactics

The first tactic used by the Russian hackers is known as a “watering hole attack,” or a “drive-by attack.” This type of attack lures victims to a website that looks similar to known vendors’ websites, but it is

---

actually spoofed and contains malicious files through application updates. A layered approach is important for threat mitigation for this type of attack, and there are many best practices that energy organizations should adopt.

The first step would be to implement Remote Browser Isolation (RBI) solutions to prevent malware from being delivered to the user's endpoint. Additionally, scanning all files that are downloaded to both the IT and OT networks within the organization, and then using either static scanning for known malware, or sandbox dynamic analysis which can detect malicious behavior in unknown files, are effective ways to stay ahead of threats. Organizations can also introduce URL/domain reputation and sandboxing capabilities to detect network communications to known bad hosts as part of the behavior analysis.

Further, proper network architecture and complying with NERC and NRC requirements can help prevent the propagation of threats from entering the OT domain. Safeguarding the OT network also entails network segmentation using unidirectional gateways and a protocol break to ensure OT assets are protected from outside threats.

While the above prevention protocols are best practices, hackers may still find their way into networks, so it's important to deploy intrusion prevention systems right before critical assets, such as PLCs, RTUs and other industrial appliances.

Finally, an organization can deploy automated workflows to scan for malicious links and file scanning to prevent human error.

## A Chain of Attacks

As we've seen with SolarWinds and Log4j compromises, software supply chain attacks are another common tactic used by cybercriminals and one that has been leveraged by the Russian espionage groups. In this case, the hackers worked to hide malware in software updates used by systems that control the equipment in power plants.

To mitigate this common type of attack, organizations should adopt a zero-trust philosophy and consider software updates from third-party vendors to be suspect and thoroughly inspected until considered safe. This entails disabling automatic software updates in OT networks, validating all updates in a test environment prior to delivery in production, checking software against known malware and vulnerabilities and running them through dynamic analysis, and inspecting the software component's country of origin for compliance.

As U.S. legislation and global conversations on contingency planning for attacks on critical infrastructure evolve—and as these types of cyber incidents increasingly play out—the security of the energy sector should be at the top of everyone's mind and mitigation list.

---

## About the Author

Chip Epps is the VP of Product Marketing at OPSWAT. He joined OPSWAT in 2021 with a 15+ year security career in both Product Management and Product Marketing, having been CISSP certified. He's focused primarily on emerging product categories and associated go-to-market strategies spanning security domains including Endpoint, Datacenter, Network, Gateway, Cloud, IAM, SOAR and Threat Intelligence. Prior to a career in security, Chip spent 10+ years in IT operations and service delivery across numerous market segments including Healthcare, Finance, and Government, being ITIL certified. Chip received his BME (Mechanical Engineering) from Georgia Tech, was certified Chief Engineer by Naval Reactors (submarine qualified) and obtained his MBA with a focus on new ventures from University of San Diego.



Chip can be reached at [chip.epps@opswat.com](mailto:chip.epps@opswat.com) and at our company website <https://www.opswat.com/>.



## Gone Phishing: How Ransomware, Log4j, and Other Exploits Use Your Network to Catch the Big Fish

Ransomware and Log4j are the latest examples of the ways cyber criminals leverage security weaknesses to spread onto networks and steal or extort large paydays.

By Peter Bookman, Founder and CEO of guardDog.ai

### Phishing for the Big One

In order to keep yourself and your company safe, it's important to understand the psychology of a cybercriminal and their objectives. The Internet is like a vast ocean, and like fisherman, these criminals are hunting for the best spots to catch the biggest fish. They aren't interested in the small fish, per se, but in how they can use the smaller prey to catch the bigger ones. They are after a giant payday, and the bragging rights to go along with it. So, they troll for vulnerable targets and develop the best lures they can, to exploit the opportunities they find.

Perhaps you think, "it will never happen to me." You'd be wrong. A report from Cybersecurity Ventures predicts global ransomware damage costs will reach \$20 billion this year, which is 57x more than in 2015. The report notes this equates to a ransomware attack on a business "every 11 seconds in 2021."

Log4j just emerged on the scene and is already being referred to as the largest vulnerability in history with *hundreds of millions of devices affected*. It is expected to take years to fully address and resolve.

Let that sink in.

---

There are mobile device management solutions (MDM) that offer some security capabilities, but they are often exploited at the network level and unaware of the activity (I recently wrote here about how MDM isn't enough). Gaining control of a device is not enough to achieve their goals. Cyber criminals use these entry points with the strategy of *spreading over your network* to gain total control. They need the kind of leverage they can use to extort the level of payday they're after.

Accessing and spreading on the network is the common denominator most of these attacks require to succeed. This is where the opportunities lie to stop the thieves in their tracks.

## Casting the Best Lure

Ransomware, phishing, and many other exploits are about using the right bait to compromise a device, get onto a network and spread. Many of these count on human behavior to help them along, like an innocent click on a link in an email.

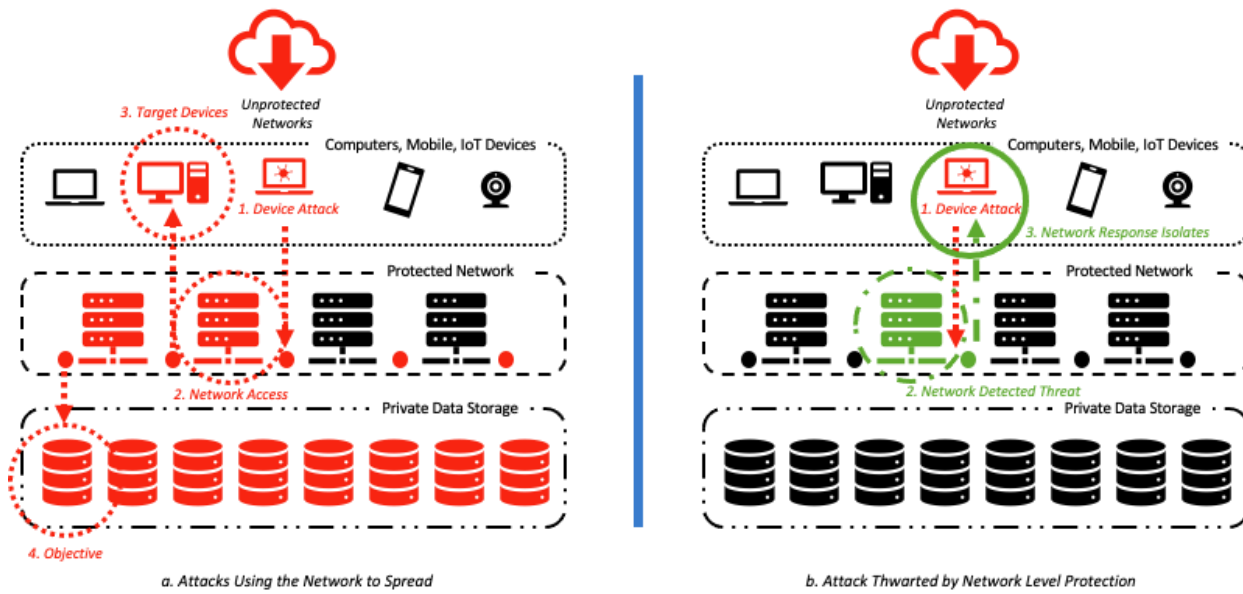
These types of threats typically appear to come from a friendly brand you know and trust like a bank, a streaming service, or any known brand you might trust. The email may claim your subscription will automatically renew at some higher rate, unless you call now to deal with it. It might say your password has been changed and if you changed it ignore the message, but if you didn't, *click here to reset your password!*

Perhaps you are a customer; perhaps not. The criminals likely don't know and don't care. To them, it's a numbers game. They are fishing for a victim. The hacker is an imposter, but what they send you may look and seem very real. They aim to get you in an urgent state of mind, so you'll respond and engage quickly without thinking it through. In the reality of things, brute force is not a common way cyber criminals get access to confidential information. They look for a weakness they can exploit more easily, such as fooling someone into aiding in the attack from the inside. This is how they get you.

Regardless of cyber security policies or training, anyone can make a human mistake and accidentally compromise their device. Who hasn't clicked on a link in an email at some point?

Log4j is even more scary. It uses a popular open-source logging solution prolific across many software deployments to spread. Simply viewing a pixel in a chat window, for example, could infect another machine – with no other action required. This exploit relies on running a certain version of Java and the way Log4j2 libraries can be exploited.

Further complicating things is the fact that most software doesn't contain a bill of materials, hence the possibility of it taking years to find and correct all the vulnerabilities. In the chart below on the left, we see a device attack has successfully leveraged the network to infect other devices and gain access to all private information. On the right, we see suspicious activity from a device that was detected and then isolated at the network level, preventing the spread.



## Force Them to Cut Bait

There is much we can do to secure devices from attacks, such as adding virus protection software, device management solutions, EDR, and other protections, but these solutions aren't aware of what's happening at a network level. Once the criminal targets and infiltrates your device, then what? If you have part of your team accessing secure information from unsecured external networks, then what?

Investment in network level protection is a must, to identify a threat that is attempting to spread and stop it before it gains a foothold. Network aware solutions can see patterns and traces these threats leave as they attempt to spread. With the right cyber security strategy in place, you can minimize the damage from an attack and potentially stave off the disaster of losing control of private information and having it held for ransom.

Deploying methods that monitor networks, detect threat patterns, and respond to them in a timely manner is the key to keeping the attack surface low and halting an attack's progress when it's found an entry point. You could accomplish this by using professional cybersecurity services from MSSPs, or by deploying a product that offers AI-based network-oriented autonomous countermeasures flexible enough to work with distributed work environments, which is an approach we use at the company I direct, guardDog.ai.

To keep pace with cyber criminals, you will need to invest in a variety of tools, talent, and strategies to keep them at bay. Every company should build a comprehensive cyber security plan that maps out how you will respond to threats at the administrative, technical, and physical level. A great plan maps your workflows and ties policies and protocols together to ensure you are responsive and can adapt to changing conditions.

This is increasingly important as businesses must comply with many new State and Federal regulations now in effect, with many more on the way. Many of these regulations provide safe harbor, but only if you

---

are complying according to a written plan at the time an incident occurred. The fines are steep for being negligent or for doing nothing at all.

The bottom line is that you must build a cyber security practice that is adaptive and responsive to avoid being taken by the bad guys.

### **About the Author**

Peter Bookman is Founder and CEO of guardDog.ai. Bookman has 25 years' experience leading teams and disrupting markets with numerous exits. He is credited as an inventor to 14 patents in both software and hardware intellectual property.

Peter can be reached online at @pbookman and at our company website <http://www.guardDog.ai/>





## Zero Trust: It's a journey, not a Destination

By Dr. Matthew McFadden, Vice President, Cyber & Distinguished Technologist, GDIT

In a year marked by significant cyber events – the White House's Executive Order on Improving the Nation's Cybersecurity made it clear that maturing our cyber defenses is a priority for our country. The Executive Order (EO) highlights the need for cybersecurity modernization – specifically through advancement toward zero trust and migration to secure cloud services.

Zero trust is a cybersecurity framework developed around the concept of “never trust, always verify.” It requires all users, whether they are inside or outside an organization's network, to be continuously validated to access applications and data. This is assessed against five key pillars: identity, devices, network and environments, applications and workloads, and data.

### Where to Start?

The Cyber EO requires all Federal agencies to develop a detailed plan to implement a zero trust architecture. The Office of Management and Budget and Cybersecurity and Infrastructure Security Agency (CISA) published its final version of zero trust strategy in January, which provides roadmaps for agencies to transition to zero trust models and securely migrate to cloud services over the next two years.

Here are some steps to consider in the process:

- Define the protect surface: Everything starts with the data; you can't defend what you don't know you have. The first step is to conduct an audit of the data, applications, and other services you use within your network. Identify these elements, determine where they reside, and start categorizing them by value and risk.



- 
- Map data transaction flows: A critical component of zero trust is preventing adversaries from moving laterally in your environment to access other assets. It's critical to understand how and where data flows – across all five key pillars. With a map of your environment, you can create enforcement points throughout your architecture to secure, manage and monitor devices, users, applications, and other network activity.
  - Architect the environment: Define the technology capabilities you need to defend the protect surface and data transaction flows across the five key pillars. For example, from an identity perspective, implementing identity, credential, and access management solutions (ICAM) will enable you to track user identities across the network and ensure access is limited to only those who can verify they need it.
  - Create policies around access: Consider who needs access to what data and applications, and what security standards must their devices meet to gain access.
  - Monitor and maintain: Define how you will monitor and maintain your environment going forward to assess your protect surface and enforce policies. Automated decisions around trust, such as looking for suspicious network activity and shutting it down at machine speed, are needed at scale – and investments are necessary.

These five steps named in the guidance, which must be met by the end of Fiscal Year 2024, closely align with the five pillars of the Zero Trust Maturity Model published by the CISA. <https://www.cisa.gov/zero-trust-maturity-model>

## The Importance of Partnership

As agencies modernize their cybersecurity programs, they must approach every decision – across technology, process, and people – with a zero trust mindset. It's important that agencies seek an industry partner with holistic, enterprise-wide experience and expertise across all five zero trust pillars to help guide them on their journey.

Agencies need a partner who has the required capabilities as well as proven experience developing reference architectures. Trusted partners in the cyber industry know that cyber is not a singular part of the mission – it's the thread that connects every endpoint, network, and person.

GDIT, for example, has worked with the Defense Information Systems Agency (DISA) on its ICAM program, to identify efficiencies, facilitate strong authentication to cloud services, provide authorization services with role-based access, and enable better and faster audits of users and resources. This program is a critical pillar of the Department of Defense's (DoD) ultimate push toward a zero trust architecture.

Agencies can also look to trusted partners to leverage zero trust architecture to modernize their infrastructure and secure their move to the cloud. As the DoD continues to migrate its users to the Defense Enterprise Office Solution (DEOS), the cloud-based environment that will deliver collaboration services to the DoD, zero trust architectures will provide an added layer of security and authentication to support rapid migration.

Opportunity Ahead

---

While advancing toward a zero trust architecture is a challenging undertaking for our government, it is a necessary evolution to help us meet today's sophisticated cyber threats head-on. Ultimately, zero trust will serve as an enabler for broader digital transformation, making it easier and more secure for agency users to work productively and safely from any device, from any location.

The requirements and timelines outlined in the Cyber EO are ambitious, representing a monumental shift across how government networks are secured, software is procured, and cyber teams operate and collaborate. It's important to get started today. Take small steps, make forward progress, iterate over time, and use lessons learned to make informed decisions for the future. And you don't need to do it alone – seek out a partner who can support you every step of the journey.

### **About the Author**

Dr. Matthew McFadden spearheads cyber strategy for GDIT's Federal/Civilian, Defense, and the Intelligence & Homeland Security divisions and develops advanced cyber capabilities and offerings to solve cyber missions. He represents a cyber workforce of more than 3000+ professionals, 30+ cyber alliances, and programs supporting the largest cyber operations and unique cyber missions in the federal sector.





## 5 Key Learnings from Intel's 2021 Product Security Report

By Jerry Bryant, Senior Director of Security Communications and Incident Response at Intel

As security threats continue to get more complex, attackers are increasingly targeting hardware to exploit software. As a result, secure hardware has become a priority for much of the industry as vendors work to provide trusted foundations to protect data and empower software to deliver greater protection and functionality. We know that system trust is rooted in security and if hardware isn't secure, then a system cannot be secure. Achieving the levels of hardware security needed to mitigate new attacks requires a variety of elements – such as a security-centric approach to product development, investments in technology and research, collaboration with academia, bug bounty programs and more – all working in concert. But it also requires vendors to proactively seek out and mitigate security issues, and to share what they've learned.

In this article, I'd like to share what Intel has learned as a result of its [2021 Product Security Report](#).

The report is designed to share the latest data and information around Common Vulnerabilities and Exposures (CVEs) disclosed by Intel in 2021 (through internal research, work with researchers and academia, and through various bug bounty programs). But first I'd like to note that Intel also helped drive the creation of the community-driven Hardware Weakness Enumeration (CWE) that resulted in the 2021 CWE most important hardware weaknesses list – this includes 98 total hardware weakness patterns

---

across 12 categories. For example, some of the top hardware weaknesses include CWE-1189 Improper Isolation of Shared Resources on System-on-a-Chip, CWE-1191 On-Chip Debug and Test Interface with Proper Access Control, and CWE-1231 Improper Prevention of LockBit Modification. The complete list can be found [here at MITRE](#).

Now let's dive into five key learnings from the Intel 2021 Product Security Report:

1. 226 total CVEs were mitigated in 2021. Intel's proactive product security assurance efforts discovered 93%, which is a percentage increase year-over-year since 2019. This occurs through red team events, extensive internal and external code reviews, and through collaboration with external researchers who report vulnerabilities to Intel's bug bounty programs.
2. Of the 226 CVEs, Intel employees found 50% of them (or 113 CVEs). And of the remaining 113 CVEs reported by external researchers, 86% (or 97 CVEs) were reported through Intel's Bug Bounty program. Intel's efforts to internally identify and mitigate vulnerabilities has continued to increase over the last three years.
3. 77% of hardware/firmware vulnerabilities were found by Intel (up from 69% in 2020), while 70% (down from 83% in 2020) of software issues were found by external researchers. This is the result of continued investment by Intel to harden the security of its products, plus additional collaboration with researchers through new programs like [Project Circuit Breaker](#), an expansion of Intel's Bug Bounty program.
4. Collaboration with external researchers remains essential to Intel's security assurance strategy, contributing to the discovery of CVEs across a variety of categories. That data is then fed back into Intel's security development lifecycle (SDL) and helps inform where to focus additional efforts such as hackathons.
5. Intel compared CVE counts to AMD in two primary areas: CPUs and Graphics. Of the 16 Intel CPU and 51 Graphics vulnerabilities found in 2021, 25 were discovered internally by Intel (and 42 were found through Intel's Bug Bounty program). According to AMD's publicly available information, 31 AMD CPU and 27 Graphics vulnerabilities were disclosed in 2021 and all were attributed by AMD to external sources. Notably, Intel and AMD share 23 of the Graphics CVEs, as these were issues reported through Intel's Bug Bounty program, but the affected graphics components were AMD parts integrated into Intel products.

Intel continues to heavily invest in security assurance. This includes its Security Development Lifecycle (SDL), which guides the company in applying privacy and security practices across hardware and software (including firmware) throughout the product lifecycle. Furthermore, the community of security researchers from around the world continues to contribute to improving the security of Intel technology through Intel's [Bug Bounty program](#). And just recently the company announced [Project Circuit Breaker](#), the next expansion within its Bug Bounty program comprised of a community of elite hackers hunting bugs in firmware, hypervisors, GPUs, compromising chipsets, pwning processors and more.

---

As with any broad technological hurdle, security challenges cannot be fully addressed by a single institution acting alone. As a result, Intel participates in, and often leads, a wide range of additional efforts to help advance the state of security across the industry. These include working toward technology standards with the Trusted Computing Group, Confidential Computing Consortium, 3<sup>rd</sup> Generation Partnership Project, NIST, ISO and others. Intel is also active in the academic community through awards programs and research sponsorships. And finally, the company has led an effort with [MITRE](#) and others in the community to develop the Hardware Common Weaknesses Enumeration (CWEs) and share learnings with others by participating in special interest groups as part of its membership in the Forum of Incident Response and Security Teams ([FIRST](#)).

To read the entire Intel 2021 Product Security Report, [click here](#). Or, if you want to watch Intel's Chips and Salsa video podcast break down of the report, [click here](#).

#### About the Author

Jerry Bryant is a Senior Director of Security Communications and Incident Response at Intel where he focuses on strategy and ecosystem enablement. Before joining Intel in 2019, Jerry was a Principal Security Program Manager in the Microsoft Security Response Center (MSRC) where he focused on industry and government engagement. Jerry has a wide range of experience including starting a web application development company and working in the manufacturing industry as an expert in process control and defect reduction. He has also been heavily involved in the Forum for Incident Response and Security Teams (FIRST) PSIRT SIG.





# Defending Your Remote Workforce with Zero Trust Security

By Raul Popa, CEO & Co-founder, TypingDNA

To truly understand zero trust, you must rethink your mindset of cyber security. For years, security teams followed a simple code: “Trust, but verify.” But with zero trust, security is far less laid back — guided by a more skeptical philosophy of “Never trust. Always verify.”

The beauty of this security approach is how well it works in the new work-from-anywhere environment. Zero trust does not care if an employee is logging in from the office, at home, or from a local Starbucks — making it the ideal solution for defending the millions of employees now working remotely.

In this article, we’ll walk you through the basics of zero trust security, the key role of continuous authentication, and why zero trust is critical for protecting against today’s modern threats.

## What is zero trust?

Simply put, zero trust functions on the philosophy that because attackers can live both inside and outside the network, no person should be fully trusted even if they’ve authenticated themselves at the front door with a username and password.

---

[Zero Trust Architecture](#) treats every user, device, and application as a potential threat to the company, limiting user access to only what is needed, and continuously searching for anomalous or suspicious activity — assuming that a breach is imminent or has likely already occurred.

A drastic change from the old model of “perimeter thinking” where users were typically only authenticated once to access the network. With zero trust there is no assumption that what was trusted to get into the network should be trusted to access everything that’s inside.

Let me paint you a scenario to illustrate why this concept is so important.

Let’s say an attacker steals a user’s credentials and “legitimately” authenticates with their username and password. They get through the front door and discover a folder of highly sensitive corporate data, like source code, HR data, or internal emails — downloading its contents threatening to expose it in a ransomware attack. To avoid this scenario, traditionally you have two moves:

- Force the user to re-authenticate every few minutes to ensure only legitimate users are accessing the network at all times. But this comes at a steep price: costing you money in lost productivity, and increased Help Desk calls — not to mention some pretty frustrated employees.
- Or, allow them to authenticate themselves seldomly, like once a day... which certainly makes for happier users, but leaves your company vulnerable to greater threats.

With a zero trust approach, you would apply a “never trust, always verify” approach — continuously checking the user’s access — even once they’ve authenticated at the front door. As a result, significantly reducing the chances of a data breach.

### Continuous authentication: a key component of zero trust

A core part of the zero trust model is continuous authentication — the need to solve for what happens in-between security checks. This means that to achieve true zero trust, organizations must constantly authenticate user identities throughout a user’s entire engagement with a network, service, or device—rather than just once at login.

This is especially critical for remote workforces, where insider threats and negligent employee behavior present a real risk for companies when employees handle sensitive or privileged information in insecure work-from-anywhere environments. In just the last two years, there was a [44% increase in insider threats incidents](#).

It’s important to remember that insider threats include both malicious insiders who *purposely* steal data, money, or other assets, as well as *negligent* insiders — usually employees making a human error such

---

as falling prey to a phishing attack or sharing their devices with an unauthorized user. These individuals can potentially misuse access to networks and assets to intentionally or unintentionally modify, delete, or disclose sensitive information. Organizations must take action to protect this sensitive data.

## Device sharing may be your company's biggest threat

With millions of employees shifting to remote work at the start of the pandemic, an unexpected new threat entered the picture. Danger was no longer limited to hackers or external forces. The threat was inside, and company devices like laptops and desktops were now at risk of being accessed by family members living in the same household.

While sharing company devices with family members may *seem* innocent, ignorance can cause real harm. A single wrong click on a phishing link, or unauthorized access to sensitive company or customer data can lead to serious consequences.

Companies from highly regulated industries such as medical, finance, legal, customer service, and human resources have to follow strict standards to safeguard customer and company data. Protecting these endpoint devices is critical. Employers must find continuous authentication solutions that allow employees to constantly prove their identities throughout the day without it being a burden.

To achieve zero trust with a remote workforce, two core rules must be followed:

1. Identify the user *before* they enter the system with Multi Factor Authentication (MFA). [Corporate Vice President Ann Johnson from Microsoft's Cybersecurity Solutions Group](#) said "The entire principle of zero trust is that you trust nothing. That's the first thing that we tell organizations: they must use multi-factor authentication for 100% of employees 100% of the time. That is the first control to put in place as part of that Zero Trust architecture".
2. Continuously authenticate the user throughout the day, especially when they're accessing privileged data. If continuous authentication is added on top of the MFA-secured login process, it adds an even greater layer of security by continuously checking that the logged-in user is the one operating under granted access at all times — even in-between standard and front-door security checks. This way, even if the login is compromised, access to crucial information is denied by applying a second, continuous layer of secured authentication.



---

## Can you afford not to have zero trust?

In a work-from-anywhere environment, company devices are more vulnerable than ever before. As millions of employees now work remotely, companies must make sure that only authorized users are accessing the company's endpoints.

Any business which handles customer data on employees' devices should be able to tell at any time throughout the day whether unauthorized users are accessing the company endpoints — with processes in place to flag suspicious behavior and take action.

Companies looking to protect against such insider attacks must limit privileges to internal structures and apply a [zero trust policy](#) where the identity of any actor can be verified at all times.

### About the Author

Raul Popa is the CEO, Co-founder, and Data Scientist at TypingDNA — an award-winning cybersecurity startup that authenticates people by the way they type on computers and mobile devices. Typing biometrics technology is currently being used in our suite of Continuous Authentication and 2FA products. Raul and TypingDNA have won multiple awards and were featured in TechCrunch, Forbes, VentureBeat, TheNextWeb, ProductHunt, FinancialTimes, and other top publications. Raul was recognized in the Top 60 AI Influencers from Eastern Europe and was featured in the Top 100 New Europe list of influencers. As a tech innovator Raul speaks about AI, Biometrics, Identity Access Management and entrepreneurship at global events such as TEDx, Applied Machine Learning Days, World Summit AI, International Biometrics Summit, Future of AI (at European Parliament), How To Web, TechFest, any many others. Connect with Raul on [LinkedIn](#) and [Twitter](#), or at <https://www.typingdna.com/>





## The Countdown Has Started on Secure IoT Compliance

By Kyle Haefner, Lead Security Architect, CableLabs, Bruno Johnson, CEO, Cascoda, Joe Lomako, Cybersecurity Lead, TÜV SÜD UK test lab

Internet of Things (IoT) security, like global warming, is one of the few things that can be said to have global awareness, global initiative, and a growing but disjointed global consensus. Governments of the world have recognized that IoT security is a priority problem. In response, they've developed security baseline guidance, and drafted and passed legislation to increase IoT security. Manufacturers have realized that building security and privacy into devices adds real value to their brand. This is since consumers are increasingly aware of the importance of security and privacy in the devices they own and, as such, will make purchase decisions based on enhanced security and privacy features.

The challenges facing the industry now lie in navigating a patchwork of regulations that are currently vaguely defined with no clear guidance for certification of compliance. The countdown timer for compliance has already started.

### Requirements and Provisions to Be Considered

Legislators in North America and Europe have been developing standards for IoT security. For example, the European Telecommunications Standards Institute (ETSI) has updated the Radio Equipment Directive (RED), which establishes a regulatory framework for placing radio equipment on the market.

---

ETSI adopted a Delegated Act of the RED, activating Articles 3(3)(d), (e) and (f) for certain categories of radio equipment to increase the level of cybersecurity, personal data protection and privacy.

The update mandates cybersecurity, personal data and privacy protection for devices that can:

- 3.3d: communicate over the internet, either directly or via any other equipment;
- 3.3e: process personal data, traffic data or location data;
- 3.3f: enable users to transfer money, monetary value or virtual currency.

These [provisions](#) become mandatory on [1st August 2024](#), at which point manufacturers of radio connected devices must be compliant or face potential action.

In the U.S., the National Institute for Standards and Technology (NIST) has released a three-pronged approach split between manufacturers, federal agencies and consumers.

For manufacturers, NIST provides guidance in the form of the NISTIR 8259 series. [NISTIR 8259A](#) is the IoT device cybersecurity core baseline that focuses on capabilities such as device identification, device configuration, data protection, logical access to interfaces, software update and a catch-all for logging and cybersecurity state awareness. [NIST 8259B](#) covers non-technical requirements such as documentation, information queries from customers, information dissemination, and education and awareness.

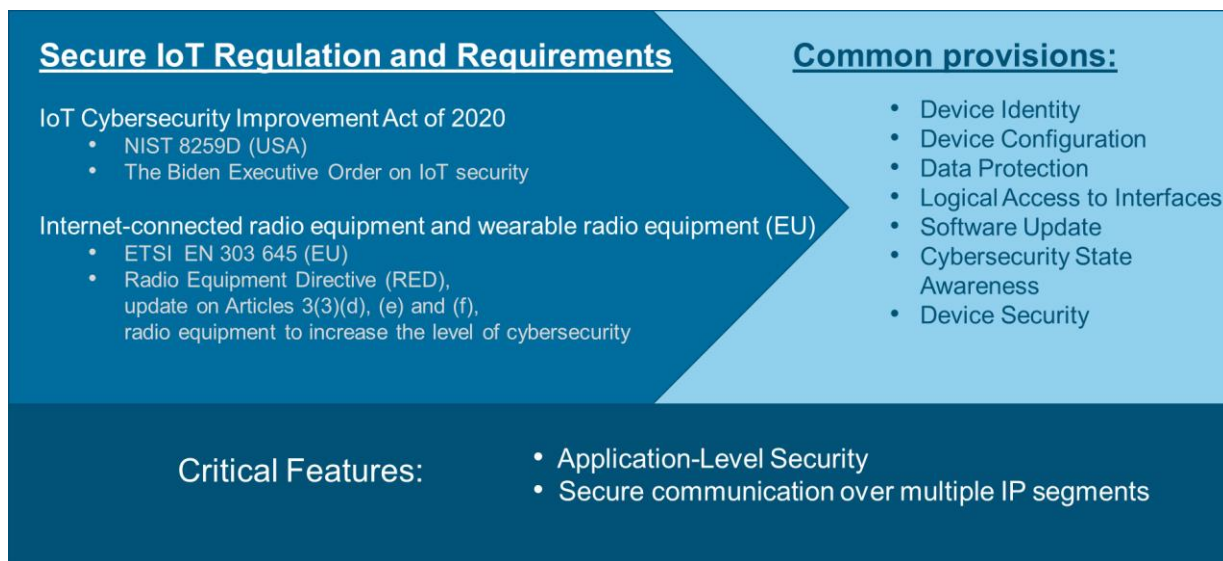
For federal agencies, NIST provides guidance in [SP 800-213A](#) on the use and management of IoT devices. This publication provides detailed requirements similar to categories in [NISTR 8259A](#), however with more specific requirements under each device capability.

For consumers, NIST, in coordination with the Federal Trade Commission (FTC), has been assigned by [President Biden's Executive Order 14028 on Improving the Nation's Cybersecurity](#) to provide criteria on consumer IoT device labeling. This aims to give manufacturers guidance and standards on how to label consumer devices in terms of their capabilities both physical and cyber.

Additionally, the U.S. Federal Communications Commission (FCC) in June of 2021, released a [notice of proposed rulemaking and notice of inquiry](#) with the focus of improving the adoption of cybersecurity best practices in consumer electronics.

While there has not been an official call for a cybersecurity certification in the U.S. similar to the RED in Europe, judging by releases from NIST, FTC and the FCC, signs are beginning to point in that direction.

The primary requirement categories seen in Figure 1. below.



**Figure 1. [IoT Security Landscape](#)**

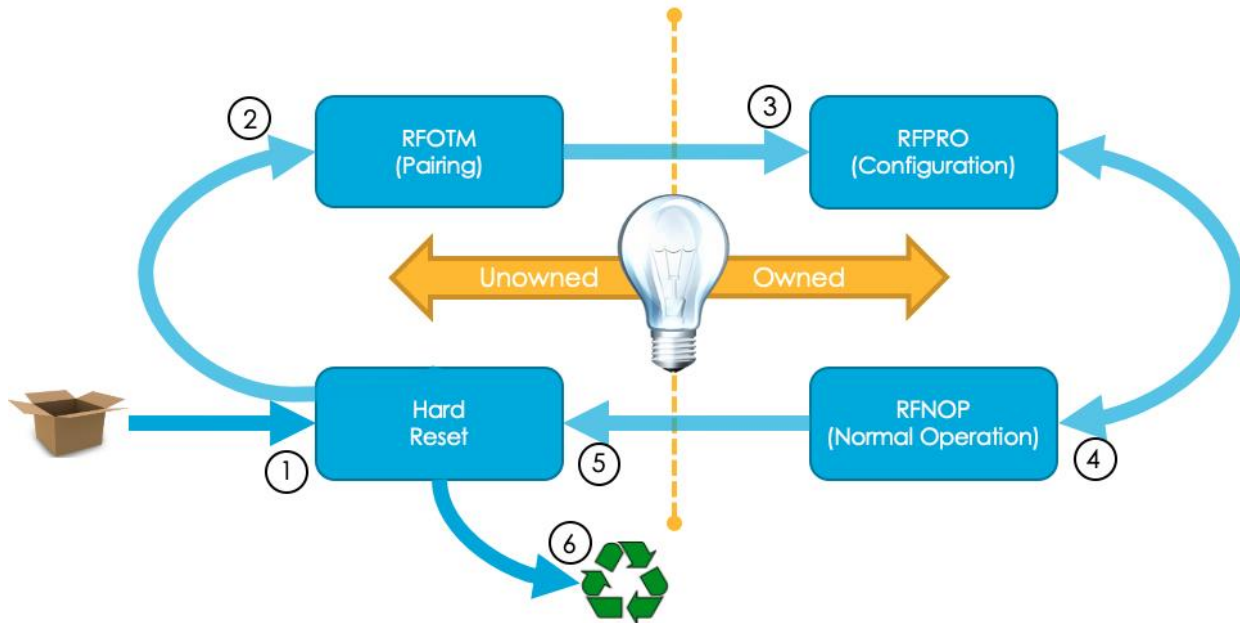
These legislations cause challenges for manufacturers, operators, and installers of IoT devices.

## The Secure Device Lifecycle

A secure device lifecycle is the foundation of all secure device ecosystems. Manufacturers, operators, and installers of IoT devices will need to build upon this foundation to comply with the guidelines and regulations listed above. Stakeholders should be incorporating the secure device lifecycle into their business plans and processes now.

A secure IoT device lifecycle involves both hardware, software, and the ecosystem infrastructure required to support the device and associated services. Secure device lifecycle management shown in Figure 2. below encompasses all of the processes from the manufacture of the device where cryptographic identity is fused at the factory<sup>①</sup>, to provisioning operational credentials onto the device<sup>②</sup>, configuration at

deployment site<sup>③</sup>, ongoing secure updates during normal operation<sup>④</sup>, and finally secure data wipe<sup>⑤</sup> at decommissioning<sup>⑥</sup>.



**Figure 2. [The OCF Secure Device Lifecycle](#)**

### Challenges for Manufacturers

For manufacturers, the timeline for meeting the EU's RED provisions is short, especially given that the average hardware time-to-market is one and a half to two years – and this is without ongoing supply chain issues. Additionally, developing embedded devices with protections for keying material can take extra time and some manufacturers will need to retool their production lines to accommodate the extra steps of burning key material to the chips.

### Challenges for Operators

Consumers expect that their smart devices are manageable wherever, whenever and on any device. To meet this expectation, manufacturers should ensure that their ecosystem offering includes secure communication both proximally, but also to the cloud and over multiple IP segments. Operators should build out and refine security technologies such as Public Key Infrastructure (PKI) to authenticate,

---

authorize and account for devices within their ecosystems – and do so in a way that creates simple and seamless user experiences.

## Challenges for Installers

Depending on the use case, the installation process can include a mix of the system integration, application engineering, and the IT administration function. As with manufacturers and operators, installers need to develop suitable technical training and management processes to allow for the appropriate provisioning of secure devices. The provisioning process ensures access rights and privileges for individual users so as to ensure a seamless user experience while maintaining security.

## Answering the Call

For several years, manufacturers, vendors and internet operators have been working through various standards organizations to build secure IoT specifications that bring much of the best practices of running secure connected systems into the domain of secure connected and *constrained* systems.

There are now mature internationally recognized secure IoT communications standards that can help support the requirements set forth by the EU RED and the US NIST. By using such protocol standards, many of the challenges related to IoT security can be overcome.

However good the communications standard, organizations at every level of the IoT supply chain still need to implement appropriate management processes and ensure that their workforce has sufficient training to facilitate a seamless transition to a more secure world.

Governments are moving at an increasing pace to protect the security of networks from vulnerable and insecure devices – as can be seen with the above directives and guidelines coming from both the EU and US. Specific requirements directly tied to legislation are at best poorly defined and vague, and yet at the same time specific deadlines for conformance have already been set. This puts manufacturers in a difficult position in determining conformance of product lines with lead times that can stretch into multiple years.

The best option right now is to plan to build devices that can meet a majority of the requirements established in ETSI and NIST. It is impossible to foresee what legislation will require, but it is easy to guess that it will be based at least in part on currently established IoT security baselines. Manufacturers must not delay; the clock is ticking.

---

## References

“EN 303 645 - V2.1.0 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.” 2020. ETSI.

[https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303645/02.01.00\\_30/en\\_303645v020100v.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf)

“Executive Order on Improving the Nation's Cybersecurity.” 2021. The White House.

<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

“Federal Communications Commission FCC 21-73 Before the Federal Communications Commission Washington, DC 20554 In the Matter of.” 2021. Federal Communications Commission.

<https://docs.fcc.gov/public/attachments/FCC-21-73A1.pdf>

“NIST Internal or Interagency Report (NISTIR) 8259A, IoT Device Cybersecurity Capability Core Baseline.” 2020. NIST Computer Security Resource Center.

<https://csrc.nist.gov/publications/detail/nistir/8259a/final>

“NIST Internal or Interagency Report (NISTIR) 8259B, IoT Non-Technical Supporting Capability Core Baseline.” 2021. NIST Computer Security Resource Center.

<https://csrc.nist.gov/publications/detail/nistir/8259b/final>

“NIST Special Publication (SP) 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog.” 2021. NIST Computer Security Resource Center.

<https://csrc.nist.gov/publications/detail/sp/800-213a/final>

“OCF - Specifications.” n.d. OPEN CONNECTIVITY FOUNDATION (OCF). Accessed March 3, 2022.

<https://openconnectivity.org/developer/specifications/>

---

## About the Authors



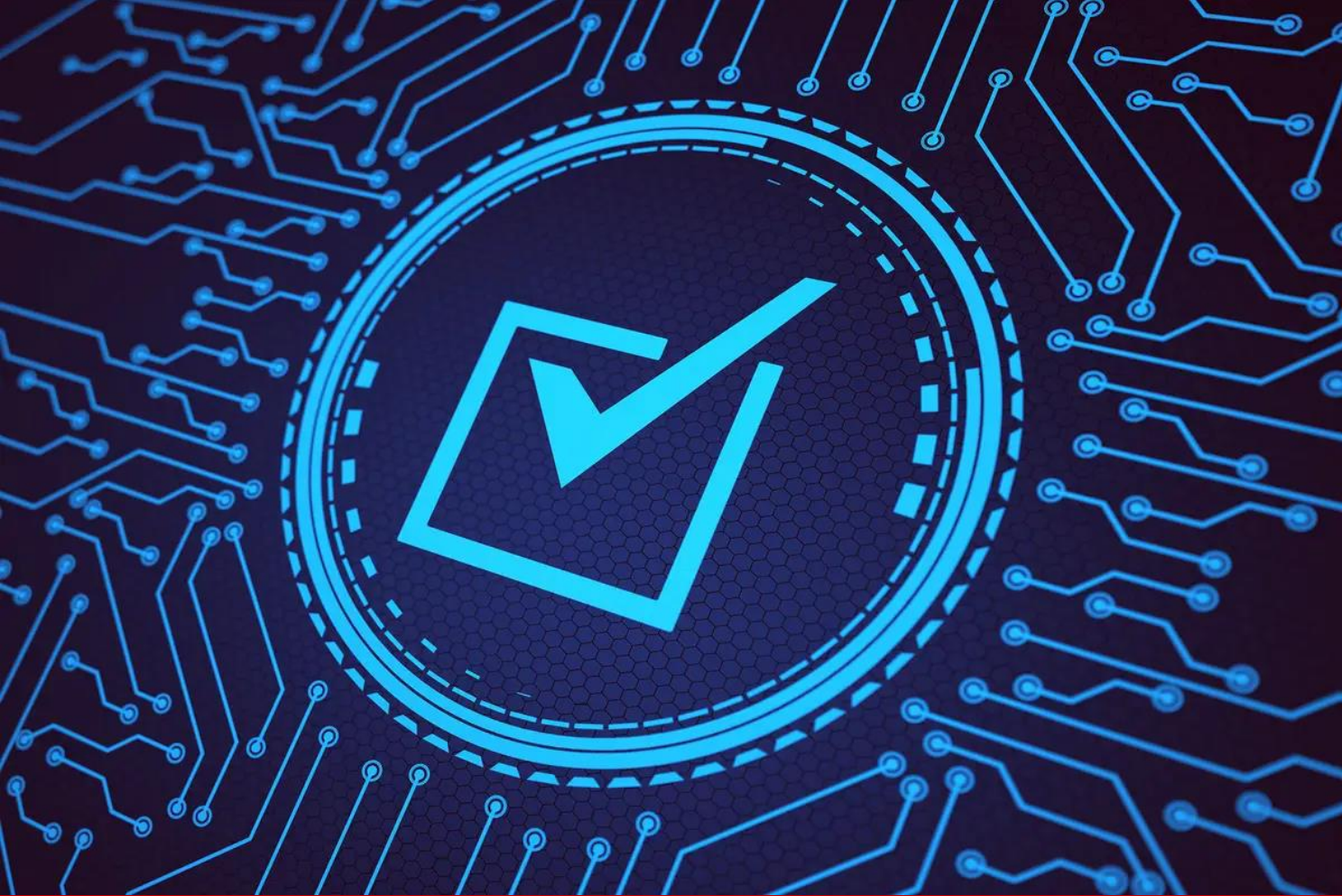
Kyle Haefner, PhD is a Lead Security Architect at CableLabs. He also chairs the Core Security work group of the Open Connectivity Foundation (OCF).

Bruno Johnson is the CEO of Cascoda. He also chairs the Marketing and Communications work group of the Open Connectivity Foundation (OCF).



Joe Lomako heads the cybersecurity team in TÜV SÜD's UK test lab. He has a 25-year background in IoT and wireless connectivity compliance and certification.





## Tips for Implementing HITRUST for Healthcare Providers

By Philip Jones, Mazars, Director of Security - Chief Information Security Officer (CISO), Data Privacy Officer (DPO) for Healthcare

The need for effective and quality healthcare services has never been more apparent than during the global COVID-19 pandemic when our health infrastructure was put to the ultimate test. We learned that these life-critical services need continual technology investment to meet evolving patient needs, such as the exploding demand for telehealth solutions we've seen in the last two years. However, increased technology brings increased data privacy concerns, especially in legacy healthcare systems, as cybercriminals look to exploit vulnerabilities within patient data storage.

In fact, according to a [2021 Verizon Data Breach Investigations Report](#), the health industry is one of the sectors experiencing the highest amount of data breaches. As of mid-February 2022, there have already been [almost 500 confirmed health care breaches](#).

One initiative meant to combat this is the Health Information Trust Alliance ([HITRUST](#)), a commonly accepted and highly recommended security framework that guides organizations on establishing controls to meet regulatory compliance and build a security program to protect operations from attacks. It was founded to help organizations secure operations, manage risk, and solve nuanced issues plaguing today's healthcare industry. HITRUST demonstrates healthcare compliance along with a NIST risk score

---

that effectively measures IT operational risk and guides organizations to improve their overall security posture.

An organization can demonstrate its compliance with HIPAA and other laws through HITRUST certification. Here are a few key areas to address when preparing for a HITRUST certification, which can help your organization stay prepared and protected from the onslaught of cyberattacks against the healthcare space:

- **Multi-Factor Authentication (MFA).** You will be hard-pressed to find a cyber-insurance carrier that provides a policy without MFA. MFA requires a UID/PW and a second verification to sign in, typically through an application, phone, or email. MFA will need to cover remote user access, remote access email, all privileged accounts, and insurance companies are starting to require MFA to access backups.

*Pro Tip* – Email notifications can cause access problems. When possible, use a phone application such as Microsoft Authenticator for a higher level of security.

- **Monitoring and Detection.** Suspicious activities on systems, networks, and security devices are correlated and analyzed to detect possible attacks and prevent or reduce damage to operations.

*Pro Tip* – With most covered entities low on staff and technical expertise, consider hiring a managed security service provider (MSSP) with a retainer for digital forensics in the event of an incident.

- **Breach Incident Response Plan** - An incident response program will cover detection, notification, communication, and coordination. Training and clearly defined responsibilities are essential in any response plan.

*Pro Tip* – Perform regular tabletop exercises with different groups within the organization and your outside consultant to build awareness and confidence.

- **Backup and Disaster Recovery** - Regularly backup copies of information and software and tie them into a disaster recovery plan. Completing a business impact analysis (BIA) and including standard operating procedures (SOPs) to bring systems online is also an essential part of this process.

*Pro Tip* – Hire a firm with expert knowledge to help build a cloud-based solution. A solid business continuity plan using a cloud service provider will dramatically reduce complexity and response time.

Cybersecurity concerns and data protection should be top of mind for healthcare organizations, and it is essential to reassess current cyberattack prevention measures as often as possible. Becoming HITRUST

---

certified is only one part of a complex cyber protection puzzle, so it is essential to consult with an advisor to ensure you are effectively protecting your patients' data.

### About the Author



My name is Phillip Jones and I am the Director of Security - Chief Information Security Officer (CISO), Data Privacy Officer (DPO) for Healthcare at Mazars U.S. I have built multiple privacy programs ranging from startups to major international organizations. I have guided multiple board of directors through tough and complex compliance of security and privacy regulations.

Prior to joining Mazars US, I held several leadership positions in Privacy/GDPR, U.S. regulatory compliance, and cybersecurity of both prestigious consulting firms and technology organizations, including U.S. Navy Intelligence, IBM and Booz Allen & Hamilton.

Philip Jones can be reached online at [Philip.jones@mazarsusa.com](mailto:Philip.jones@mazarsusa.com) and at our company website <https://www.mazars.com/>



## Why Access Control Is Critical in The Path to Cyber Insurance Readiness

Combatting the challenges of cyber insurance

**By Joseph Carson, Chief Security Scientist and Advisory CISO at Delinea**

Cyber insurance is just like any other insurance policy. It helps businesses to offset costs related to damages from cybersecurity incidents like ransomware and data breaches. In the last 10 years, cyber insurance has become critical for almost every company that has a digital presence. This is because businesses are increasingly looking for some sort of financial security against potential cyber threats, such as ransomware, that are just lurking around the corner.

However, businesses face a frustrating challenge when it comes to getting covered, mostly due to soaring prices and a long list of complex eligibility criteria which will assess them against a range of different security controls and best practices.

The only solution in this case is increasing cyber insurance readiness and ensuring that best practices are implemented across the organisation to demonstrate effective risk management. A key component for mitigating risk lies in ensuring effective identity and access controls are in place to keep pace with more stringent cyber insurance standards.

---

## Cyber insurance policies: changing requirements

The cyber insurance industry is relatively new. In fact, before 2010, cyber insurance companies hardly existed outside Europe and America. Today, it's a \$7.6 billion industry, and it's expected to grow [to over \\$36 billion by 2028](#). This is evidently because digitalisation has become a core requirement across almost every industry.

As digital and interconnected businesses are increasing rapidly, so is the presence of cybercriminals across this space. With the added 'convenience' of the dark web and advanced automated tools, cybercriminals can launch attacks with almost minimal effort and resources or simply choose cybercrime as a service by giving the attackers the target you want them to attack.

This growing need to protect the digital space and interconnected organisational networks has paved the way for cyber insurance companies to emerge as a unified umbrella of financial protection. However, such increasing threat vectors are also the reason why cyber insurance providers have to set up a long list of complex criteria before granting coverage to organisations.

The high demand and rising cost of claims in the current market are also driving up premiums. [According to reports](#), coverage prices increased by 130% in the US and 92% in the UK in the fourth quarter of 2021 alone. Prices are also expected to keep rising this year due to the ongoing inflation in the global economy, as well as due to the financial impact of the Covid-19 pandemic.

## What are the cyber insurance requirements?

Cyber insurance companies provide coverage based on an organisation's cybersecurity capabilities and infrastructural readiness. If a company's cybersecurity infrastructure is not up to the mark, insurance providers will assume a certain risk factor in providing coverage. With cyberattacks becoming almost inevitable, it also comes down to how well-prepared companies are in preventing or mitigating the impact of such attacks.

There is no specific industry standard yet for cyber insurance, and it changes based on the provider and different policy premiums. Some insurers base their criteria on the general standards set up by government regulators, while others have their own evaluation metrics.

However, most insurance providers consider three major factors of cybersecurity readiness - network firewall, antivirus, and access security control.

They are also likely to ask in-depth questions about a company's risk management practices and security controls. For example, they might want to know how the company monitors potential threats or authenticates user access.

These factors are essentially the pillars of cybersecurity readiness and provide an accurate framework for insurance providers to assess the security infrastructure of their clients. In terms of access control, a more definitive criteria would be privileged access management (PAM).

---

## Managing “privileged access” to monitor credential usage behaviour and potential risks

The majority of all cyberattacks are targeted at end-users. It's often easier for cybercriminals to exploit a user's lack of awareness, rather than targeting highly secured and encrypted systems. That's why access control is one of the most important aspects of cybersecurity, and cyber insurance providers often check if an organisation has put in place common security controls to minimise risk. Among these are automating password management, protecting privileged accounts, limiting privileged access, and implementing multi-factor authentication. Making privileged access a core part of your strategy is one of the best practices that can help to demonstrate that you're taking cyber security seriously.

If we look at the list of [cyberattacks from 2022](#) alone, more than half of all incidents are due to credential leaks. It is becoming increasingly important to regulate who has access to your data and devices, particularly in larger organisations, where data is often stored in layers and different databases are managed by different departments. When access is not restricted, a single credential leak could expose the entire system.

Access control acts as a doorway between attackers and the core information system. Efficient access management can restrict attackers from inflicting significant damage, or even prevent such attacks entirely.

Privileged access management doesn't only help build cyber insurance readiness, but it's beneficial for the company as a whole. Large clusters of privileged credentials pose a serious threat to business networks. Having an automated solution that authenticates and assesses credential access in real-time can significantly reduce the risks of a security breach.

It also helps to efficiently set up and manage different levels of access to cloud platforms, including authentication, authorisation, and monitoring. For example, if a user is not authorised to access a certain file or segment on the network, the PAM software can instantly report the incident and suspend all access, eliminating certain cyberattacks or data breach attempts before they turn into a cyber catastrophe.

In short, PAM solutions designate special access to internal users of organisations to secure their applications and network infrastructure. If a standard user can gain access to private or confidential data this becomes a security threat, which is why privileged access management is critical for a company's network security. Such solutions can protect companies from both internal and external threat actors, by monitoring all administrative access and reporting any unusual behaviour.

When it comes to getting insured, you'll have to play the convincing game. Insurance providers need to be assured that your organisation is more than capable of defending against potential threat actors and security incidents, and PAM solutions go a long way in providing that assurance.

---

## Why cyber insurance matters?

Cyberattacks are becoming increasingly common and frequent. By having any aspect of your business on the cloud, you are attracting hundreds of illicit threat actors who want to exploit your valuable data and information. Having cyber insurance can give businesses financial security against such threats in the digital space.

Access control management doesn't just reduce the risk to your business from internal and external threat vectors, but also allows organisations to meet eligibility requirements for financial protection if the worst happens and a breach does occur.

### About the Author



Joseph Carson is Chief Security Scientist and Advisory CISO at Delinea Joseph. He is a cyber security professional and ethical hacker: over 25 years' experience in enterprise security specializing in blockchain, endpoint security, network security, application security & virtualization, access controls, privileged account management. Certified Information Systems Security Professional (CISSP), cyber security advisor to several governments, critical infrastructure, financial, transportation, maritime industries.

Joseph can be reached online at @joe\_carson and at our company website [delinea.com](https://delinea.com)



## How To Establish SAP Security

By Christoph Nagy, CEO, SecurityBridge

Malicious external cyber-threats certainly grab the headlines and leave businesses with no doubt as to the potential havoc they can cause. However, what can inflict almost equal pain and what are statistically more prevalent are internal threats, both unintentional and nefarious. 84% of cybersecurity leaders have identified employee error as the leading source of cyberthreats. Additionally, nearly 74% of businesses have experienced security issues because their workers have violated internal rules.

It makes sense that businesses should therefore safeguard crucial data and systems from their own employees by establishing Systems, Applications, and Products (SAP) security. This is a crucial procedure for any organization to protect itself from both internal and external threats.

### Align user access with the organizational needs

SAP security can help you to maintain data confidentiality within your organization by limiting the access of each system user with respect to their role. Within this system, employees will only be permitted to accomplish processes and gain information if the actions fall within their established scope of duties and responsibilities.



---

If you want to establish SAP security within your organization, then firstly align the access for each employee with their role within the organization. Once that's determined, it's crucial that the corresponding access and restrictions can be identified within the system. Furthermore, individuals with the most high-risk roles within the organization will have to be identified and given the greatest level of security.

### Involve key players in promoting better security

After you've figured out which employees need to be authorized, you need to educate them as to their roles in the system. Our article on the "Art of SAP Security" emphasizes that [training end-users and developers](#) is critical to the proper implementation of security measures. Additionally, you also need to create an SAP team that will oversee training the end-users and monitoring any activity.

To ensure that they can properly manage the SAP system, a company's IT professionals and developers can be [upskilled through a cybersecurity degree](#) that focuses on technical skills such as network security, security log management, to name a few. It's also essential for these professionals to develop skills in data security, risk analysis, and cloud migration to best equip themselves to protect your organization.

### Constantly monitor the users within the SAP system

The SAP system protects your information and processes by managing the access of internal and external entities through automated measures. Although the servers, security logs, and system communications go some way to securing your data, it's still vital to monitor and track every movement within the system.

One interesting article on increasing SAP security emphasizes that the operators in your SAP team need to examine the permissions and authorizations automated within the system. Taking this a step further, your team can also oversee your SAP security by carrying out segregation of duty (SOD) checks to ensure that end-users are staying within their authorized roles. Tracking the movement of both the systems and the end-users is essential so that no unauthorized individuals can pass through.

### Keep the system up-to-date by managing patches

Cyber criminals' techniques are increasingly more sophisticated, and SAP security systems should anticipate new threats in advance. To keep these systems updated, security patches are constantly being launched for businesses to integrate with their existing programs. However, speed-to-security is essential for an up-to-date SAP security system.

SAP bugs are quickly weaponized by cyber criminals, with one intelligence report stating that critical SAP vulnerabilities are exploited by attackers within three days of their release. Therefore, ideally businesses need to download SAP patches as soon as they become available to prevent breaches, this however rarely happens. Therefore real-time threat monitoring is such an essential defense asset.

---

## Emphasizing organizational protection

An SAP security system is one of the stalwarts of defense against both internal and external security threats – particularly as the world (and so many business practices) continue to go digital. By controlling access to your organization’s systems, you can protect confidential information and maintain the integrity of your business.

### About the Author



Christoph Nagy has 20 years of working experience within the SAP industry. He has utilized this knowledge as a founding member and CEO at SecurityBridge—a global SAP security provider, serving many of the world's leading brands and now operating in the U.S. Through his efforts, the SecurityBridge Platform for SAP has become renowned as a strategic security solution for automated analysis of SAP security settings, and detection of cyber-attacks in real-time. Prior to SecurityBridge, Nagy applied his skills as a SAP technology consultant at Adidas and Audi.



## A Resilience-Centered Approach to Cybersecurity

By Safi Raza, Director of Cybersecurity, Fusion Risk Management

If there was ever a year for an organization to ensure its cybersecurity was robustly planned, prepared and tested, this is it. With the probability of a cyberattack at its highest ever level, there were a record number of attacks recorded in 2021. According to recent [Check Point Research](#), overall attacks per week on their client corporate networks grew by 50% when 2021 was compared with 2020.

The reputational and financial damage an unexpected cyberattack can inflict is widely recognized, and yet there are multiple examples of companies that have fallen foul of appropriate cyber protection. One example was when computer hardware giant Acer suffered a security breach which resulted in them having to pay a record-breaking \$50m USD. The cybercriminal group REvil went on to leak stolen data online. Also, when Microsoft's Exchange Server was attacked in March 2021, it affected millions of Microsoft clients with 60,000 private companies disrupted in the US alone, as well as nine government agencies.

Cybersecurity burnout is one of the many reasons for lapses, with low morale among cybersecurity professionals at an all-time high, and pandemic-induced employee turnover becoming more common according to the [Chartered Institute of Information Security](#) (research here: <https://bit.ly/3CrNFMK>). The current conflict in Ukraine further heightens the risk of cyberattacks, and now is the time for all

---

organizations to review their cybersecurity policy and processes to ensure they are robust and resilient enough to prevent cyberattacks and avoid any disruption to business operations.

### **Building resilience and trust through better cyber-hygiene**

Cyber-hygiene is one aspect of a strong and resilient cybersecurity policy that is vital if businesses hope to counter attacks that could leave them exposed to financial losses. Insurance underwriters are clear that businesses must do everything they can to mitigate the risk of those losses or potentially leave themselves “uninsurable.”

A range of technology capabilities is now available, and a combination of different options should be employed for the most effective cyber security. These options could include the integration of AI, machine and deep learning systems, all of which can help protect the data security chain in a more reliable way than human beings can. Antivirus/malware software, firewalls, regular updates of apps, web browsers and operating systems can all contribute to good cyber-hygiene.

The best cyber-security solution should also include disaster recovery or business continuity planning that outline how the organization could recover from any cyber-attacks. Preventative methods are also critical, such as educating employees and providing specialist training so that they remain vigilant and attentive to potential IT security issues within the organization.

### **Investment in the future**

Heads of businesses should evaluate every aspect of their current cyber security frameworks, and understand fully where their weak spots are and what risk level they bring with them.

This increased requirement for enhanced protection will require investment to ensure security and future resilience - and this is the time for organizations to spend more than ever on cyber security. Next generation firewalls or Firewall as a Service (FWaaS) have helped create stronger defenses that has led to the nature of attacks changing. Phishing attacks have increased by 110% year on year (according to the FBI), and it is one of the main threats that will need to be addressed. Even the most sophisticated anti-phishing programs are unable to defend in the way that they should, with many phishing emails able to get through IT security walls, presenting a real and dangerous threat.

As well as financial investment, organizations must invest so that security can be updated and kept in check on a regular basis. This will require a culture shift as security takes more of a central role, including frequent interactive cyber security simulations and skill sharing events. Employees must be embedded within an organization’s security culture and feel ready to report anything they notice to the IT teams, allowing them to then investigate and mitigate any risks.

---

## The importance of immediate action

Operational resilience is key for any organization's future success, and there is no room for complacency. Hackers and cybercriminals constantly adapt their methods and will happily exploit any vulnerability, so companies must be alert to new technology to protect themselves and help build and safeguard customer trust. It's essential to implement this protection now to ensure your business is prepared for inevitable future disruption and be able to do business as usual in the event of the unexpected. Those businesses that take immediate action will be in the best position for future success. Ongoing readiness will translate into resilience and those organizations who can ensure their operational resilience will continue to deliver on their brand promise - no matter what disruption they may face.

### About the Author

Safi Raza, who has more than 15 years' experience in information security, is Director of Cybersecurity at Fusion Risk Management. Prior to joining Fusion, Safi spent 14 years at Rosenthal Collins Group, where he spent eight years in training and six years in information security. Safi was responsible for overseeing the e-Trading Services Department where he helped introduce, adapt and support new and improved trading technologies

Safi can be reached online at: <https://www.linkedin.com/in/safiraza/> and at our company website <https://www.fusionrm.com/>





## Data-centric Security: Defense in Depth

By Amit Shaked, CEO, Laminar

Last year, organizations saw the highest average cost of a data breach in 17 years, with costs rising from [\\$3.86 million USD](#) in 2020 to \$4.24 million USD in 2021. As a result, overburdened security teams are consistently trying to stay on top of the latest threats, vulnerabilities and hacker tactics.

Complicating matters even more is the rapid adoption of the public cloud, which has surged from \$270 million USD in 2020 to an estimated [\\$397 million USD](#) in 2022. This fast-paced digital transformation gave way to the rapid development of digital products and services. Unfortunately, the cloud has also blurred the security perimeter and opened up more opportunities for attackers to exploit data.

While chasing down cyber adversaries and attempting to reduce the opportunities for hackers to attack seems like the right step to take, many security teams are missing the point: the data itself.

### Be Your Data's Guardian in the Cloud

Data has gone from a commodity to a currency. As a result, it is just as valuable for attackers as it is for business. Having a solid understanding of the latest cyberthreats is important, but just as critical of an issue is that security teams are almost blind when it comes to data residing in public cloud infrastructure due to the sprawl of cloud services and pace of change for devops.

### And how can you protect what you can't see?

There are three critical steps that security teams must put into motion if they want to maintain efficient and adequate visibility of sensitive data within public cloud environments and ultimately bolster security posture.

---

## 1. Find a Cloud-Native Security Tool

In cybersecurity, there is no one size fits all solution. However, the cloud is an ever-changing environment which means the solutions must change too. Solutions can now be built into an organization's public cloud infrastructure to combat data breaches by autonomously discovering data stores and continuously analyzing and remediating risks or leaks. Too often do data security professionals and leaders find themselves unable to see the full picture of their data. Ensuring your security solution can integrate with cloud infrastructure allows for a seamless transition and visibility, identifying data that resides in the shadows.

With the ever-expanding public cloud, and how bloated with data they are becoming, CISOs everywhere are scared about their unknown and unprotected data stores. Criminals are capitalizing on this and repeatedly breaking through these systems due to the rapidly changing landscape - our defenses must adapt.

## 2. Monitoring and Protecting Your Treasured Data

As previously mentioned, a company's sensitive data can and will be copied and backed up. It is an organization's responsibility to ensure that this data can be properly monitored and protected. This responsibility can only be achieved by understanding the data, where it is, and where it is going. Security relies heavily on known variables hence a solution without full visibility compromises the entire organization's security posture.

Whether accidentally or intentionally, human error can cause devastating losses both financially and socially for a company. Up to [85 percent](#) of data breaches now have a human element. All organizations must understand data exposure, who is within their system and why they should be accessing public cloud data at all times, otherwise organizations risk losing their treasure trove.

## 3. Always Have A Plan

The "Achilles heel" in cybersecurity is too often, a leadership team with their heads in the sand. Far too many organizations believe themselves to be immune to the current ransomware crisis looming over industries across the board. It is essential to have an incident response plan and team in place. Excruciating detail should be provided for the roles that each core pillar of an organization should play during an ongoing crisis. Proactive monitoring of the crown jewels allows security teams to be notified of abnormalities and access risks that was not possible a few years ago. This Zero-Trust approach to data allows for less human error and more power into security operation centers.

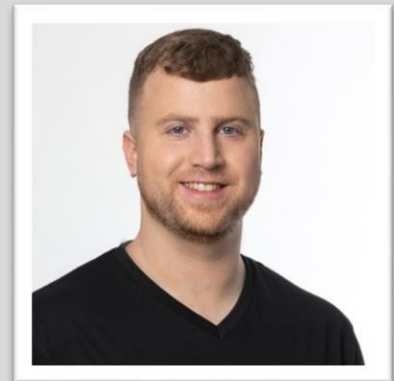
---

## A Data Centered World

Accepting that technology is fluid and ever-changing will dramatically assist security teams and leaders when it comes to protecting an organization. The cloud is here to stay, and it is being relied upon even more as the pandemic ensues and teams continue to work off-site. Thus, finding the appropriate solution for an organization's security needs must become a foundational level priority moving forward. Personal and corporate data should be protected as the treasure trove it truly is. Efficient and effective Public Cloud solutions should be able to monitor and protect data silos, revealing what data is hiding in the shadows. It is important to remember that it is incredibly costly for business and reputation if cyber adversaries sell their treasure trove of data to the highest bidder.

### About the Author

Amit Shaked, CEO, Laminar. He is also the Founder of Laminar which started in 2020.







## Interview with Morten Kjaersgaard, CEO of Heimdal Security on How Cybersecurity Businesses are Tackling the Ukraine Crisis

By Morten Kjaersgaard, CEO, Heimdal Security

### 1. How are cybersecurity companies reacting to the Russia-Ukraine conflict and what would be the best approach, in your opinion?

Reactions really seem to vary with the focus of the business. Intelligence companies are scrambling to find actionable threat intelligence on Russian activity, whilst SOC teams are staying readily attentive to the increased number of alerts coming through.

As for [Heimdal](#), we are really focused on continuing to stay proactive, which we also strongly believe is the right approach. Hence, my opinion remains the same - companies need to focus on proactively increasing the defensive posture of their infrastructure, rather than waiting for their adversaries to find gaps in it. Our current product development also tries to support just that, with technology that continuously makes it easier to manage your environment and easier to prevent attackers from penetrating it in the first place.

### 2. How are cybercriminals reacting to this conflict? Who are they targeting most now?

State-sponsored actors are increasingly targeting each other at the moment and the objective is to have the upper hand in actionable intelligence on the other party. We clearly saw that with the imposter

---

situation against UK parliament members, but it is certainly something we also see happening for all major EU countries.

However, there is also a heavily increased number of attacks on private businesses, which are a key source of potential technological secrets, as well as financial means to funding a war. Attacks on businesses have already quadrupled from 2021-Q4 levels and we expect this is only the first wave.

### **3. Do you believe that cyberattacks, that have become a part of modern warfare, can have a direct, decisive impact on the battleground? What's your opinion about the hackers that "turn good"**

There is absolutely no doubt that cyber warfare can have a direct impact on slowing ground advances, so cyber warfare is now a direct part of war planning. As you can imagine, it would be tremendously difficult to get aircraft off the ground if control systems are not working and also hard to communicate rapidly if your infrastructure is not working optimally.

As for "hackers turning good", I think we can all only applaud those who stand up for those who are less capable of protecting themselves in any situation, and that also applies here.

### **4. How does this conflict affect local markets and their spending?**

Overall, we are currently seeing increased cybersecurity spending across the board. Governments across EU and the United States are increasingly pushing both state, municipalities and private businesses for increased security measures and rightly so. The current security situation is drastic and requires heavy investment and overhaul, as the IT Security area is not always the first priority when budgets are made.

### **5. What do you think will be the long-term consequences of this conflict for the cybersecurity market? Is Heimdal Security preparing for possible consequences, cementing existing products or maybe anticipating the need for something new?**

Heimdal is continuously trying to focus on our proactive approach, which in the current state is highly beneficial, as CIOs scramble to get in front of what is happening at the moment. A lot of security vendors are reactive, which both apply to Intelligence players, antivirus vendors, and SOC teams.

Our focus has always been to close the gaps before they are exploited or predict attacks before they happen – as we do with our unique AI-driven Predictive DNS. More recently we have been focusing on making IT management even easier for IT admins and giving them tools to work faster than the attack will ever be, even on a mass scale. We can't disclose more than that at the moment.

---

## About the Author

Morten Kjaersgaard is the CEO of Heimdal Security, a leading European provider of cloud-based cybersecurity solutions based in Copenhagen, Denmark. He has a degree in Corporate Marketing and prior to Heimdal, he spent his years at the top of the IT industry as CCO of BullGuard Ltd and CEO of a large Danish IT Reseller. Morten has previously been on several company boards and is a frequent event speaker and an Internet Security evangelist. He can be reached online at <https://www.linkedin.com/in/kjaersgaardmorten/> and on our company website, <https://heimdalsecurity.com/blog/author/morten/> .



# DATA-CENTRICITY



## True Cybersecurity Requires a Shift to A Data-Centric Philosophy

By Brian Platz, CEO and co-founder, Fluree

### A target-rich environment

While news of cyber attacks emanating from Russia's invasion of Ukraine has been [sparse](#), some experts say cyber conflict has been a constant in the battle theater [since the war's onset](#). Others [caution](#) that Russian President Vladimir Putin could launch a severe cyber campaign at any moment. Then there are those who say what we've witnessed to date presages the [future of cyber warfare](#).

Beyond the war in Ukraine, cyber attacks worldwide dropped precipitously [in February](#) — roughly 5.1 million records breached — compared to January's total of about 66 million records breached, [according to](#) IT Governance, a United Kingdom-headquartered company.

To illustrate the challenge over the course of a whole year, consider the 1,001 data breaches in 2020 [tracked by](#) Statista that affected 155.8 million.

---

The paucity of public fissures within the cybersecurity realm during the past several weeks combined with Russia's ongoing aggression has created a certain amount of tension among those who fear the worst is still to come.

Yet, that doubt also has created the opening for a conversation that cybersecurity professionals should be having — one that could prove revolutionary in the field regarding how we think about protecting data.

Vulnerabilities remain manifold. Today's global data architecture is one with a virtually unlimited surfeit of targets, including emails and texts due to information sharing by friends and colleagues; social media posts; and other types of communication among organizations and businesses. Literally every API represents a potential vulnerability. Akami's [2020 State of Internet Security Report](#), in fact, found that 75% of all financial services industry cyber attacks targeted APIs. The result is a system of countless data silos, each with a discrete surface ripe for attack.

Perhaps counterintuitively, despite being the grand prize hackers seek, data remains unprotected. Instead, security investment continues to be concentrated in online infrastructure.

The rise of cloud-computing has coincided with the mushrooming of the numbers and types of devices connected to clouds. Such personal devices and corresponding WiFi networks represent another category of at-risk information.

## Today, applications manage security — that's backwards

Security should be executed by the data itself — security would be baked into the data itself in such a way that security and data become inseparable. Protective structures around data would become unnecessary. Data-management responsibilities, in other words, shift to the data tier from the application tier.

And personnel overseeing various aspects of data — data-governance leaders, for example, should reach across the aisle and engage with data-management and data-security leaders to develop a set of data-centric policy enforcement guidelines.

To borrow a phrase from a July 2020 [post](#) on the blog of NetApp, a hybrid cloud data services company headquartered in California: "Security controls should be as close to the data as possible."

Think about it as a matter of data quality control.

---

This could take many forms. One might be that members of several departments within a company would be allowed to view information in different areas of that business, but only certain department members would be permitted to update department-specific data. Another could be that everyone may view university or college course catalogs, but only a school administrator would have the power to edit the information in those catalogs.

Both instances are examples of data defending itself.

As information travels among storage systems, applications and various business contexts, its protection remains intact — no matter the type of network or application security. The data itself controls permissions and rules regarding identity and access. Those permissions and rules exist throughout the information's lifecycle.

## Benefits of data-centric security

When security exists within the data tier, rewards include the mitigation of data theft and loss, improved governance and compliance strategies and fewer surfaces vulnerable to attack combined with greater delivery velocity.

Current requirements of security logic being re-implemented throughout apps, data lakes, middleware and APIs becomes obsolete. Instead security logic is automated and scalable. That solves a problem identified in the [2021 Verizon Data Breach Report](#) that found that increased automation boosts offensive attacks as much as it moves the needle on defense.

Compliance naturally incorporates into whatever is the overall governance strategy. And, developers no longer expend time and energy on security and governance activities. Their sole responsibility is to build better applications and APIs.

Effective data-centric security policies succeed in three areas: management, tracking and protection. The first enables organizations to define policies determining the access to, the contribution of and use of data by whom. Tracking establishes a data supply chain monitoring system as it moves through systems and users. The final piece closes the deal by imposing protocols for identity and access.

The paradox of more regulations that oversee data, including the European Union's 2018 [General Data Protection Regulation](#) and the 2018 [California Consumer Privacy Act](#), is that more information than ever is being shared by more people and organizations than ever. The exchange and brokering of data has become commonplace. Such a complex data supply chain screams for more robust security.

---

Keys to the solution are pairing identity with rules to make data-centric security as impervious as possible. Part of this approach includes a maxim that recently has gained more traction among cybersecurity experts: Verify but never trust. Verification relies on provable cryptographic identities connected to a variety of authorizations. Those rules work because they may be complex and arbitrary. Enforcement proceeds from database connections, answering questions such as, Is the user linked to the data? Or, are the user and data linked to the identical organization?

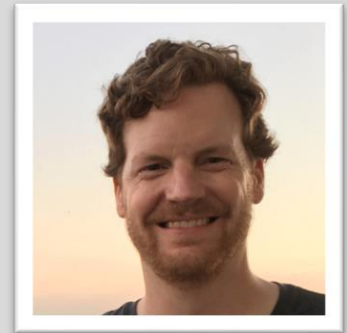
The more rapid adoption of data-centric security as a best practice, the quicker today's arguably innumerable information vulnerabilities will disappear. And, gone will be the reports of data breaches that the populace has accepted as normal and routine.

#### About the Author

[Brian Platz](#) is co-founder and CEO of Fluree PBC, a North Carolina-based public benefit corporation focused on transforming data security, ownership and access with a scalable blockchain graph database.

Platz was an entrepreneur and executive throughout the early internet days and SaaS boom, having founded the popular A-list apart web development community, along with a host of successful SaaS companies.

Previous to establishing Fluree, Brian co-founded SilkRoad Technology which grew to over 2,000 customers and 500 employees in 12 global offices. Brian can be reached online at [@bplatz](#) and at [www.flur.ee](#).





## The Best Cyber Security Jobs in The UK According to Data

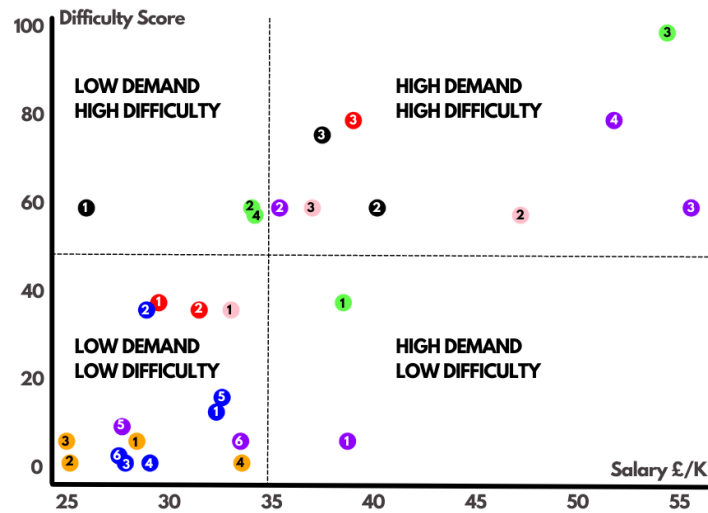
By Karim Adib, Data Analyst, The SEO Works

According to a report commissioned by the UK government, 82% of job openings advertised online across the UK require digital skills. The same study attributes a 29% higher salary and a 59% reduced risk of redundancy (due to automation-led obsolescence) for these digital jobs. Not only does this illustrate the importance of digital skills - it also suggests that job openings that do not require digital skills are dwindling and paying less.

While digital industries are booming and demand has never been higher, some niches are easier to break into than others, and some niches pay higher than others. The Digital PR team at The SEO Works gathered data on the average salary from top UK job boards Glassdoor, indeed, and Prospects to reveal some of the most in-demand digital jobs along with how difficult it is to get started in them. Here are the findings.



# Digital Jobs: Salaries vs Difficulty



**Key**

**DATA SCIENCE**

- 1) Data analyst      2) Data Scientist      3) Database Administrator

**DIGITAL DESIGN**

- 1) Animator      2) Audio Engineer      3) Copywriter
- 4) Graphic Designer      5) VFX Artist      6) Video Editor

**DIGITAL MARKETING**

- 1) Digital PR Executive      2) PPC Executive      3) SEO Executive
- 4) Social Media Marketer

**GAME DEVELOPMENT**

- 1) Game Artist      2) Game Designer      3) Game Developer

**INFORMATION TECHNOLOGY**

- 1) Technical Support Officer      2) Network Engineer      3) Systems Analyst

**SOFTWARE DEVELOPMENT**

- 1) Applications Developer      2) Applications Analyst      3) Blockchain Developer
- 4) Machine Learning Engineer      5) Web Designer      6) Web Developer

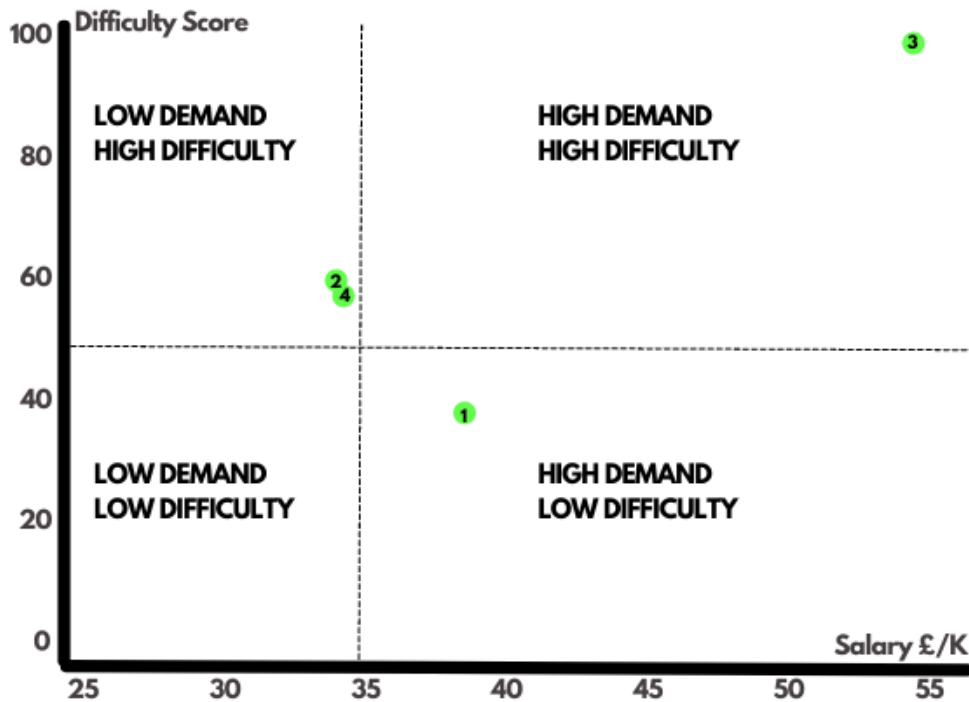
**SOFTWARE SECURITY**

- 1) Cyber Security Analyst      2) Forensics Computer Analyst
- 3) Penetration Tester      4) Software Tester



The data shows that the digital industry has opportunities catering to a variety of skill sets as well as a variety of interests. At a glance, it is not surprising to see a correlation between salaries and job ‘difficulty’ (how many years of training/experience are required), whereby easier jobs tend to pay less, and more ‘difficult’ jobs pay more. Here are the findings for the cyber security industry.

# Cyber Security : Salaries Vs Difficulty



## SOFTWARE SECURITY

1) Cyber Security Analyst

2) Forensics Computer Analyst

3) Penetration Tester

4) Software Tester



**Cyber security: One of the toughest digital industries to get into, but not without extra benefits.**

A huge advantage of many digital careers is that it's possible for anyone to get most if not all of the skills they need online. This is not the case with cyber security, but this is not necessarily a downside. It might be harder to get into cyber security, but the demand is there and you will be compensated handsomely for your hard-earned knowledge. This is why Cyber Security Analyst has the overall second best difficulty to salary ratio in the study and Penetration Tester is ranked as the second best-paid job on the chart. When technology exists, so does the need to keep this technology safe.

---

## Penetration Tester Is Well-Renumerated, But It's The Hardest Job To Get Into

Penetration Tester is the second-highest paid job on the chart with an average salary of £54,000. This relatively high salary is because getting into penetration testing needs a university degree as well as 2-4 years of experience in the industry. This means on average it takes 5-6 years to be able to become a Penetration Tester - a high bar to entry when compared with, for example, a job in Digital Marketing. The demand is clearly there, but is it worth pursuing compared to other cyber security jobs, like being a Cyber Security Analyst, which offers a much better demand to difficulty ratio?

## Cyber Security Analyst is a great career choice due to its difficulty to salary ratio

When looking at a job, you want to consider how tough a career is to get into versus how much the skills you get will be worth. This is why when we compare being a Cyber Security Analyst to other digital jobs it comes out as the second best career choice on the chart. The reason this ranked so well on the difficulty scale compared to other jobs in the cyber security sector was that a lot of companies do not require a university degree to apply. However, it will be difficult to find information online to get you to mastery level.

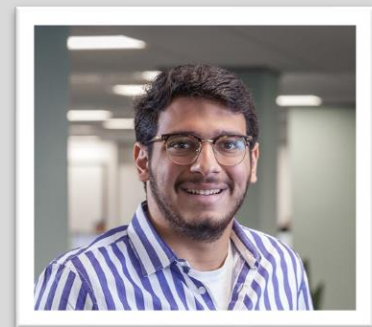
## Is Cyber Security the Industry for You?

This chart is one way to consider your future career, but such a big decision is never as straightforward as it might seem at first. So, do not let the chart dictate too much about what you want to go for. One thing is for certain, however - demand for cyber security professionals is strong, and that shows no sign of changing anytime soon.

### About the Author

Karim Adib is a data researcher and analyst at The SEO Works. His background in civil engineering and marketing allows him to combine data analysis with storytelling to create data-led pieces.

Karim can be reached online at @karimadib99 on Twitter and at our company website [seoworks.co.uk/services/digital-pr-agency/](https://seoworks.co.uk/services/digital-pr-agency/)





## Why And How to Eliminate Security's Biggest Blind Spot: Transport Layer Security (TLS)

Gigamon VP breaks down how to eliminate TLS, and considerations for a decryption and encryption approach

By Bassam Khan, VP of Product and Technical Marketing Engineering, Gigamon

Many who work in IT are still of the mindset that encrypted traffic means safe traffic. That's a dangerous generalization. Encrypted traffic simply means it's private, and private communications does not equate to safe communications.

Security teams' use of encryption continues to grow steadily for legitimate privacy and protection purposes – and unfortunately, is growing even faster for nefarious purposes. While most network-based analysis tools benefit from inspecting decrypted traffic, risk grows exponentially with each tool that receives clear text traffic, since the tool itself can be compromised. Decryption is not a binary decision and there are several options for how to decrypt.

Further, to address significant blind spots like Transport Layer Security (TLS), security teams should consider a decryption and encryption approach. Whichever path your organization chooses, the most important step is to document and communicate your approach and the decision factors leading to it.

### Encryption and Decryption

The good

Network traffic encryption is critical for securing networks from unauthorized access and data theft. By encrypting your network traffic, you can prevent others from being able to see or steal the data passing

---

through your network. In addition, increasing adoption of TLS encryption helps protect against “man-in-the-middle” attacks and other malicious activities.

### The bad

With its growing adoption, threat actors are turning to encryption as their default method for operating and remaining undetected. From command and control, to malware insertion, to data exfiltration – encryption allows adversaries to do their work without fear of being caught. Additionally, encryption allows for longer dwell times and insert encryption malware on as many hosts as possible for a ransom payout, exfiltrating sensitive data and intellectual property for a double extortion. Most current tools, including Suricata and Snort rules, are useless against encrypted payload.

### The ugly

There are a few key challenges to consider when decrypting network traffic. First, decrypting the data can open up privacy concerns. In addition, decrypting the traffic may violate compliance requirements or even require re-architecting the network and datacenter infrastructure. Finally, decrypting the traffic is central processing unit (CPU)-intensive and places significant strain and bandwidth reduction on the tools that are used to decrypt it.

By understanding these challenges, organizations can better plan for and mitigate them.

## TLS Traffic Inspection With Network Detection and Response Solutions (NDRs)

Modern network detection and response (NDR) solutions can function solely on encrypted traffic using only Secure Sockets Layer (SSL)/TLS traffic metadata, such as:

- **Server Name Indication (SNI) certificate attributes:** Helps identify when the entity was registered, who owns the entity, and suspicious attributes like randomness, name/typosquatting, and uncommon top-level domain.
- **Cipher Suite – JA3 / JA3S:** Helps find suspicious encrypted session’s “Hello” connection. Detection-based solutions that rely solely on IP address and known bad domains are often ineffective; these two fields can change at any point or malware could be constantly morphing its command-and-control infrastructure. JA3 and JA3S, which are hashes of how the encrypted connection was established, are less likely to change – therefore, frequently changing JA3 and unknown JA3s are suspicious.
- **User agent:** Helps identify the user agent (i.e., browser). This data can be useful to differentiate automated systems used for web advertising and marketing purposes, versus a more nefarious intent.
- **Certificate info:** Think through when the certificate was issued. A few day-olds issuance that is a few days past expiration is considered as concerning as it is for 10 years past expiration.

---

While it's possible to make detections on encrypted traffic metadata, these techniques have their limits. For the level of threat detection you want, NDRs need to work with both traffic metadata and the full content of packets, which provides access to unified resource identifiers (URIs), parameters, responses code, user-agent, request and response body, files, and much more. With this rich data set, analyzing intrusions over hypertext transfer protocol (HTTP) can be more straightforward. Therefore, the combination of encrypted traffic metadata and decrypted payload analysis provides the maximum number of data points for threat detection.

## Choices For Decryption

### Do nothing

Even though it might be easy to say "don't do this," for some organizations, traffic decryption may not be an option. This could be due to reasons like compliance requirements, corporate policy, tools overload, current datacenter architecture, cost, or others.

If this is your path, your most important step is to over communicate the reasons and risks associated with this approach.

## Decryption by each tool

This is the easiest approach because most tools will have a built-in decryption feature. You just turn it on, and the tool will do the work for you. There are three things to think about when using this approach.

1. If a tool is deployed inline, it becomes a single point of failure. If the tool goes down, the entire flow downstream will break.
2. This approach will not work with TLS 1.3, which requires a "man-in-the-middle" inline deployment.
3. This is the most expensive approach. Decryption is a resource intensive function that can dramatically degrade the tool's performance and throughput.

## Dedicated decryption appliance

Another option is to use a standalone appliance that decrypts and forwards traffic to all the other tools. A decade ago, this was more common, but people stopped using it because decrypting traffic is not the end goal. The end goal is inspecting network traffic safely.

---

## Centralized Decryption and Smart Traffic Brokering

Visibility fabrics (also known as packet brokers) provide security, flexibility and cost-efficiency needed for decrypting traffic by:

- Allowing for centralized “decrypt once, feed many tools” deployment model
- Conforming to any policy regarding plain text access
- Offering masking of personally identifiable (PII) data
- Maintaining IP and URL “blacklists” where sensitive traffic from trusted sites is kept encrypted, like employee personal banking and healthcare websites
- Eliminating the need for physical wiring changes when modifying decryption policies
- Supporting TLS 1.3 through an inline deployment, utilizing both inline tools and out-of-band traffic tools

Finally, it is a good idea to review the National Security Agency's (NSA) [advisory on TLS decryption](#). This advisory advocates for a centralized decryption model.

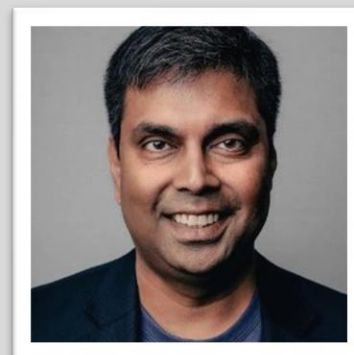
## Wrapping Everything Together Through Increased Visibility

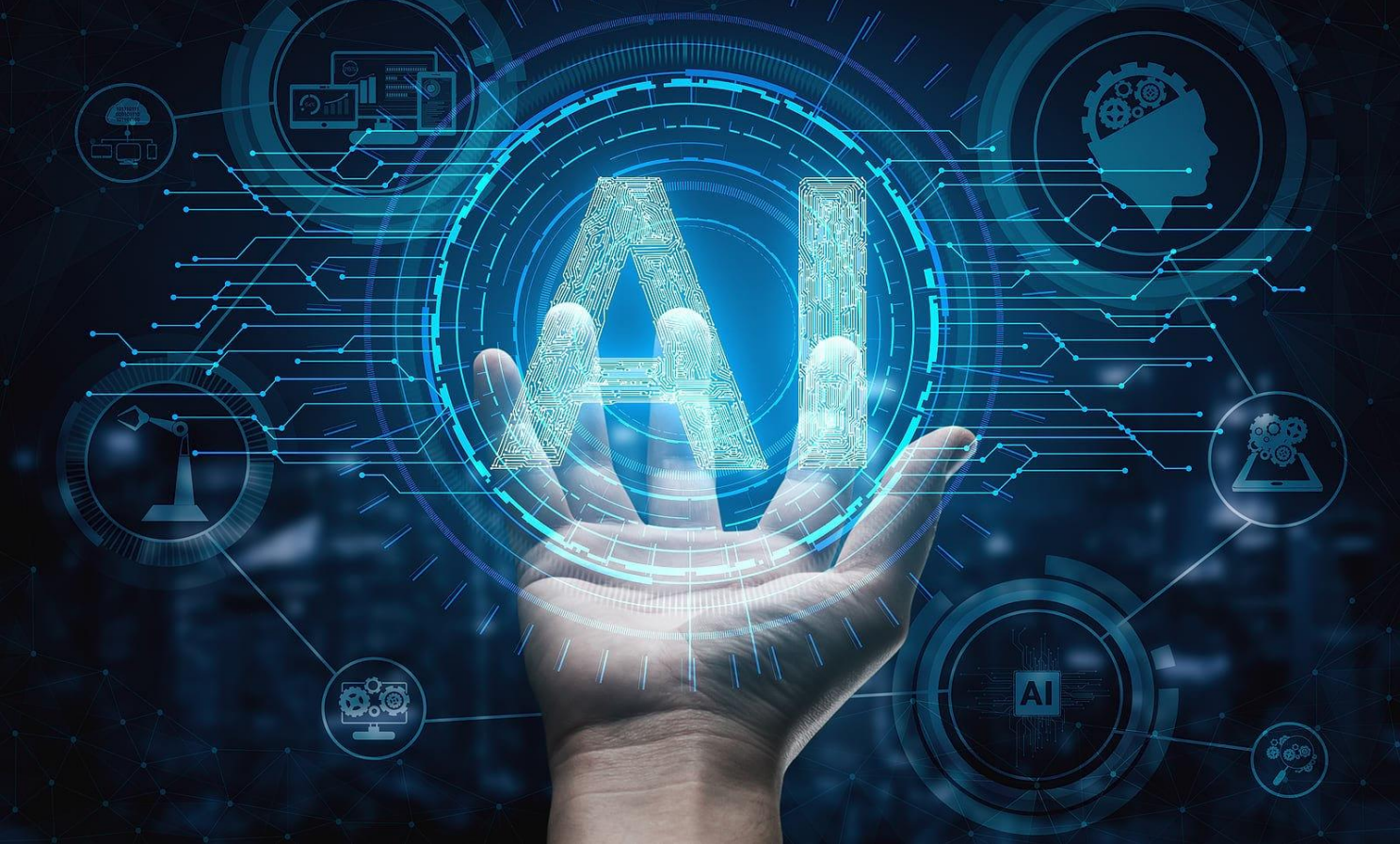
From a larger level, in order to eliminate the blind spots that come with TLS, in addition to a number of other security vulnerabilities – network visibility is critical. Visibility can be useful in tasks such as decrypting data, which can be done more selectively based on traffic type, destination tool, and industry-specific requirements. These types of capabilities also provide flexibility for teams to configure data in any way they need, and also support the agility necessary for changing the configuration quickly if policies change.

No matter what decryption method you choose, it is important to communicate the reasons and trade-offs with upper team management. Key security decision-makers at your organization need to understand the implications of decrypting network traffic and feel aligned with your team’s approach. Otherwise, you may not have their support when that day comes.

### About the Author

Bassam Khan is the Vice President of Product and Technical Marketing Engineering at Gigamon. He brings 20 years of experience managing products for security, cloud and collaboration technology companies. Prior to Gigamon, he held executive positions at ControlUp, AppSense, PostPath, Cloudmark and Portal Software. Bassam can be found on [LinkedIn](#), [Twitter](#), and on our company blog at <https://blog.gigamon.com/author/bassam-khan/>.





## Ethical AI - How is AI Redefining the Insurance Industry?

By Antoine de Langlois, Responsible AI Data Scientist at Zelros

When Cybersecurity meets Artificial Intelligence, companies and organizations have many new challenges and potential threats to consider. Here are some examples of how AI can help combat a cyber-attack.

### Adversarial attack

In the case of a Vision ML model, tasked to detect a panda, you can modify the input image to fool the algorithm into predicting a gibbon. While the image remains strictly identifiable as a panda for the human eye. It could fool an autonomous car into mis-identifying a stop sign with a speed limit road sign, with critical consequences. It can also be developed for speech recognition. Here again the sound change could not be detected by human ears but will fool the speech recognition device

To counter adversarial attacks, companies need to retrain the algorithm to ensure it detects and flags anomalies by proactively detecting the breaches and retraining the algorithm helps minimize such attacks. To have a robust model, companies can also “sample with noise” to help prevent a future adversarial attack.



---

## Data Poisoning

Data poisoning happens when some samples of the data used for training the algorithm are manipulated to make it provide a malicious prediction triggered by specific inputs, while remaining accurate for all the other inputs.

This Data Poisoning manipulation is done before the model training step. Zelros has [Ethical Report standard](#), collecting a dataset signature on the successive steps of modelization is precisely to check and prove afterwards the data has not been tampered with. This standard can be adapted by other companies as a best practice when using AI responsibly.

## Privacy

When an individual or a group have very specific features within the dataset used to train an algorithm, their identity may be compromised. To avoid an individual identity to be revealed as part of the training data and thus a risk on their privacy, organizations can use specific techniques such as federated learning. It amounts to training individual models locally and federating them on a global level, to keep the personal data locally. As a general advice, detecting specific samples of outliers and excluding them from the training is also a good practice.

## Bias Bounties

As for classical software, sharing details of an AI algorithm can become a liability if it is exploited with malicious intent, since it provides insights on the model structure. A countermeasure, evoked by Forrester as a trend for 2022 are bias bounties, which will help AI software companies strengthen their algorithm robustness.

**“At least 5 large companies will introduce bias bounties in 2022.”** - According to Forrester: [North American Predictions 2022 Guide](#)

Bias bounties are becoming a prime tool for ethical and responsible AI because they help ensure your algorithm is as unbiased and as accurate as possible, thanks to having more people review it.

## Human Behavior

Before considering malicious activity to access our Data or manipulate the AI tool used, companies ought to pause and just consider the Personal Data we as people willingly (even if not knowingly) share. Our CyberSecurity main weakness is our proclivity to disseminate knowledge of our identity and activity. Artificial Intelligence or even basic data gathering tools have given this behavior consequences that may prove critical.

Let's take an old example for reference, with the geo localization data openly shared on a social network:

---

<https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>

Although from 2018, it shows how individual scraps of data may be gathered to provide powerful insights on an individual Person identity and behavior.

These insights can then be leveraged by AI tools to categorize 'potential customer targets' and act on that intel. A more recent reference may be The Social Dilemma documentary about the world of the "attention economy" built on this Personal Data gathering. To limit the impact of our Human behavior, nothing beats culture and scientific awareness. Data Science acculturation is a key for more security on our private data but also for more fairness in AI models, as detailed in the first topic of this [article](#).

"AI tools may be too powerful for our own good": When provided data on customers, a Machine Learning model may learn much more than we would like it to. For example, even if the gender is not explicit in customer data, the algorithm can infer it through proxy features, when a Human could not (at least on that amount of data, in such a limited time).

For that aspect, analyzing and monitoring the ML model is crucial.

To better anticipate the algorithm/model behavior and prevent discrimination through proxies, a key element is diversity: Having multiple reviewers with complementary input through their individual cultural/ethical background. Organizations can also request algorithmic audits by Third parties, to take advantage of their expertise and workforce diversity if the team themselves lack diversity.

## References:

*To develop for Insurance domain + North America reference:*

Link with [American NAIC \(National Association of Insurance Commissioners\) principles](#) compliance challenge: Fair and **Ethical** / **Accountable** / Compliant / **Secure**, Safe, Robust

*Sources for adversarial attacks (very technical - not for the article but for sourcing reference):*

- *Vision adversarial attack >* [https://openaccess.thecvf.com/content\\_CVPR\\_2020/papers/Duan\\_Adversarial\\_Camouflage\\_Hiding\\_Physical-World\\_Attacks\\_With\\_Natural\\_Styles\\_CVPR\\_2020\\_paper.pdf](https://openaccess.thecvf.com/content_CVPR_2020/papers/Duan_Adversarial_Camouflage_Hiding_Physical-World_Attacks_With_Natural_Styles_CVPR_2020_paper.pdf)
- *Speech adversarial attack >* <https://arxiv.org/pdf/2110.09714.pdf>

## About the Author

Antoine de Langlois is Zelros' data science leader for Responsible AI. Antoine has built a career in IT governance, data and security and now ethical AI. Prior to Zelros he held multiple technology roles at Total Energies and Canon Communications. Today he is a member of Impact AI and HUB France AI. Antoine graduated from CentraleSupélec University, France.

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





## Cybersecurity's New Frontier: Space

By Duncan Jones, Head of Cybersecurity, Quantinuum

Ground-to-space communication is not an area that immediately comes to mind as a target for cyber attacks, and yet securing reliable communication to and from spacecraft is an imperative effort for all space organizations. In fact, NASA has [dubbed](#) security against malicious attacks on their communications “a major issue.”

How major, you might ask? Well, maybe even life threatening.

According to NASA's published research on [Reliable and Secure Space Communication Protocols](#), if hackers can intercept or modify the content of communications, not only is the success of the mission at stake, but lives could be lost as well.

This cyber risk comes as space exploration hits new heights. Last year saw [more space launches](#) than any year prior, with companies relying on space to explore new ways to improve life on Earth in fields such as medicine and chemistry. Growing numbers of researchers are also looking to low-Earth orbit to prove scientific theories developed on Earth will hold true in zero gravity.

The issue of protecting ground-to-space communication networks has only deepened as hackers wield ever more sophisticated methods to crack security systems and intrude on communication networks. This endless arms race is forcing cybersecurity professionals to constantly evolve their defensive tactics, and it's only going to get worse in the future. In the coming decade or so, bad actors will get hold of the most powerful tool to shatter cybersecurity that we know of: powerful quantum computers.

---

Quantum computers perform a type of computation that leverages the properties of quantum mechanics. While traditional computers operate on zeros or ones (known as “binary”), a quantum computer can operate on values that are a mixture of zero *and* one. Quantum computers encode this data in quantum bits – qubits – that can be linked together through a process called entanglement. Superposition and entanglement, along with another quantum principle called interference, translates into unbelievable processing power. When sufficiently powerful quantum computers are available (which experts [estimate](#) may be within the decade) cyber criminals can harness these machines to process massive calculations quickly, making many of today’s encryption techniques easily broken.

So what can space-focused organizations do to prepare themselves for such potentially devastating attacks? It turns out the answer may be fighting fire with fire.

In addition to embracing quantum-resistant cryptographic algorithms, such as those being [standardised by NIST](#), organizations can turn to quantum itself to strengthen cybersecurity. Products in this space use the properties of quantum mechanics to achieve stronger security guarantees than their classical counterparts. An example of this is the generation of cryptographic keys, which can be enhanced using the raw unpredictability of quantum behavior. While traditional computers utilize methods of random number generation to create encryption keys that are effective, they aren’t entirely random. But because quantum computers are built on the properties of quantum mechanics, which exhibits non-deterministic behavior, keys created with these systems are nearly perfectly random.

One example that demonstrates this combination of newer algorithms paired with quantum technology comes from [Axiom Space](#). Currently, the company is designing the core layer of infrastructure for low-Earth orbit operations, as it builds the commercial successor to the International Space Station (ISS). The firm has partnered with [Quantinuum](#), a full-stack quantum computing company, to secure communication for commercial customers using the ISS and, later, its successor spacecraft.

More specifically, Axiom Space is using Quantinuum’s solution [Quantum Origin](#), a cloud-hosted platform that generates the strongest cryptographic keys in the world, from a verifiable quantum source. Quantum Origin provides Axiom Space certainty that datasets derived from a range of their activities in space, such as manufacturing, experiments in microgravity biology, or gene sequencing are more secure. In its first use, Axiom sent a message encrypted with quantum-enhanced keys from the ISS, which read: “Hello Quantum World.”

When it boils down to it, investing in strong, cutting-edge security allows for space organizations to charge forward unhindered in their efforts to expand our relationship with space indefinitely. Companies worldwide are injecting millions of dollars to commercialize space with a budding [space tourism](#) industry. Some moguls even predict the advent of humans becoming a [multi-planet species](#) in the near future. As countries across the globe gravitate their eyes towards the promise of space, hackers will follow – so cybersecurity protection must beat them there.

---

### About the Author

Duncan Jones is Head of Cybersecurity at Quantinuum. He leads a team developing advanced cybersecurity products based on quantum technology, which deliver value today. Duncan has 14 years of experience in cybersecurity, particularly in hardware security. He has held senior technical and product-focused roles across multiple global technology companies. Duncan Jones can be reached online on [LinkedIn](#) and at <https://www.quantinuum.com/>.





## Drones And the Battlefield

How Drones Are Transforming Military Operations

By Dr. Shaun Passley, Founder, ZenaDrone

Recent years have seen a substantial increase in drone spending within the military sector. It's a cycle of development: innovations in the technology have led more people to adopt it, which has encouraged more innovation. It's a system that stimulates growth and improvement at all levels, and the economic potential of this field is wide open.

One of the main reasons drone technology has been so widely embraced in the military industry and beyond is that it is much quicker and more efficient with search and rescue. These are essential military operations, and having them completed more efficiently will allow more lives to be saved. And given that military operations on the front lines are naturally dangerous, drones can help soldiers from putting themselves into harm's way in the line of duty.

Technological developments have allowed an increase in drones' maneuverability and flight speed. An increase in the number and quality of propellers with which drones are equipped has led them to fly much quicker and cover a substantially wider search area than a person could on foot. This means better surveillance, better reconnaissance, and a significantly better response to any situations that may arise, sometimes even before they occur.

The cameras used by drones have also substantially improved over the years. These cameras now produce high-quality images that give operators an eye in the sky that they would not have had access

---

to before. The capability of drones to transmit live imagery to their operators is also valuable because it allows teams to be deployed for an appropriate response much faster and more accurately than traditional intelligence.

Thermal imaging capabilities in drones are indispensable for military operators. When conducting surveillance and reconnaissance, it is crucial to thoroughly understand the situation, or else lives could be lost. Especially when working at night, it can be difficult to see all of the surroundings, which can also serve as a hiding place for people who may be threats.

The battery life of these drones has considerably increased, which permits them to undertake much longer missions. Because of their increased capacity, drones have become a much more feasible solution. Whereas they used to be just a short-term alternative for certain tasks, they have since become a legitimate way of conducting an entire portion of a mission. It's a much safer and more convenient alternative.

These tools allow drones to provide a situational assessment for military operations. Before deploying troops, reconnaissance can establish enemy positions, forecast weather, map out terrain, and explore other variables. This information can be integral in devising an approach and protecting soldiers from potential harm, and it is much more reliable than most forms of intel, which can be outdated.

Drones can also help determine the aftermath of combat. The images produced by drones can be used to find survivors and identify deceased and see if the target of an offensive campaign was successfully hit. Often, these battle sites can be dangerous after combat, especially when there may be some surviving enemy combatants still waiting to attack, so this provides a much safer alternative to an on-foot exploration of the rubble.

Furthermore, the military can outfit drones with certain modifications that allow them to become offensive tools in and of themselves. Some of the offensive functions for which drones can be enabled include suppressing an enemy's air defense and disrupting their communications. Without these essential functions, the enemy is at a substantial disadvantage, giving the offense a prime opportunity to attack.

However, there are some critics of the use of drones in military operations. They argue that distancing the human element can result in decisions that aren't fully informed. But on the other hand, it tends to reduce the reactivity of any given situation. With boots-on-the-ground troops, it is essential to decide in split seconds. Although not always the case, drones can provide operators with the information and time they need to develop a better response.

But as drone technology continues to improve, many of these concerns will be alleviated. Innovation is all about solving problems, and so as things continue to improve, a lot of these issues will be resolved.

---

Efficiency and safety will continue to be improved, and as a result, the prevalence of these tools will grow even further.

### About the Author

In addition to being the Founder of ZenaTech, which owns the [ZenaDrone](https://www.zenadrone.com/) technology, Dr. Shaun Passley is also the Founder of EPAZZ, Inc., and has had the privilege to head eight different companies. With an MBA from Benedictine University, an undergraduate and graduate degree from DePaul University, a graduate degree from Northwestern University, and a doctorate from Benedictine College, Shaun's creativity and entrepreneurial spirit enable him to identify key market opportunities and successfully launch new ventures. He is responsible for EPAZZ, Inc.'s software and product development which includes the design, research, and development of ZenaDrone and future products and services. First Dr. Passley can be at our company website <https://www.zenadrone.com/>







## Privileged Access Management as a Key Technology for Critical Environments

By Dr. Heiko Klarl, Chief Marketing and Sales Officer, iC Consult

Closed gas stations disrupted flight schedules, a nationwide state of emergency: In May 2021, a ransomware attack on the Colonial Pipeline –which provides 45 percent of the East Coast’s fuel supply – plunged the region into chaos. The attack was orchestrated by hacker group DarkSide, who first stole around 100 GB of data, then compromised the billing system, and finally shut down the pipeline for good. Only after the payment of 75 bitcoin (at that time, around \$4.4 million) did the company receive a slow decryption tool and was back up and running on May 12. That same day, President Joe Biden signed an Executive Order to strengthen cybersecurity to prevent such cases. But of course, companies can do a lot to protect themselves without executive help. At the top of the list: strong protection for identities and accounts, especially those with privileged access rights.

The Colonial Pipeline hack and the government's prompt response illustrate how dangerous inadequately protected IT infrastructures are and why it is paramount to comprehensively control the access to these networks. This is especially true for critical infrastructures – i.e., organizations that are so vital that their destruction would have a debilitating impact on physical or economic security, public health, or safety. To prevent scenarios like the one above, more and more organizations are implementing Zero Trust strategies and protecting their users with powerful Identity & Access Management solutions. And they are right – a robust IAM strategy is a great foundation for a strong identity-centric security solution. But by itself, IAM will not prevent attackers or malicious insiders from moving laterally through the network

---

via compromised accounts and servers to gain additional rights and maximize their damage potential. For this, dedicated Privileged Account Management (PAM) is required.

## What Is PAM?

When it comes to protecting identities and accounts, the so-called 'least privilege principle' has always been an important best practice: It ensures that each authenticated user is only granted the minimum level of privileges sufficient to perform their intended task. This ensures that even if an attacker gains access to a user account, the maximum damage they can cause is limited by the privileges of the user in question: For example, if a user only has read access to selected resources, the risk is relatively manageable. For optimum protection, it is also recommended to assign privileged roles (i.e., roles with particularly extensive rights) only for a brief period and never permanently. This just-in-time access will help companies minimize the attack surface of critical network functions.

## Additional Recommended Measures

Most vendors support this basic PAM solution with a wide range of additional technologies, and at first sight, the strategies of the manufacturers differ in many details. However, closer examination reveals many common traits and key components:

- High-level Tier 0 or Tier 1 resources, such as domain controllers, require the highest degree of protection. As a result, most vendors grant privileged access to them only in an isolated environment and protect access with robust Multi-Factor Authentication.
- Equally strict are the requirements to access the identities and credentials of SaaS admins and privileged business users. Here, the focus lies on robust Password Management strategies, e.g., enforcing strong passwords and automatic regular password changes.
- It should always be possible for critical credentials for infrastructure accounts, DevOps accounts, and SSH key pairs to be stored in secure vaults.
- To ensure additional cyber resilience, most vendors recommend further measures such as red team exercises or enhanced auditing and reporting features.

## Which Solution Fits Best?

When evaluating the PAM market for the first time, the wide selection of available solutions can look a bit intimidating. To find the right product for their organization, identity leaders should ask themselves the following key questions:

- Which assets and accounts are we looking to protect? Which specific risks are we looking to mitigate?
- Are we facing a true greenfield project? Or do we already have standalone PAM solutions in use in certain areas or even an enterprise-wide legacy solution with which we are not satisfied?

- 
- Which legal and industry compliance regulations do we have to consider?
  - Do we favor a cloud-native, hybrid, or on-premises approach?

Experience shows that internal teams often struggle to fully answer these questionnaires and to finally decide, without external advice, whether CyberArk, Delinea or Onedidentity, to name a few, are the best fit for their business.

## Start Your Project with a Workshop

Therefore, it is often worthwhile to discuss the project with a vendor-independent consultant or system integrator at an early stage. They should be familiar with the products of various leading manufacturers and help assess which solution will fit best into an organization's architecture. For a successful kickoff, a comprehensive, free PAM workshop is recommended to explore the status quo and define concrete goals for the project. It should help:

- define key priorities and business goals of the PAM migration
- evaluate existing solutions and analyze existing performance gaps
- assess the current PAM maturity
- outline existing dependencies (e.g., legacy systems and required customizations)
- develop a structured PAM approach

This kind of workshop will help the organization grasp the project in all its complexity, ensure support from all relevant stakeholders and, thus, set the course for successful implementation.

As a prime target of multiple modern cyberattacks, privileged accounts require special attention and dedicated protection. Strong Privileged Access Management (PAM) ensures that users are always only granted a minimum level of privileges for their specific task and provides additional protection layers like Multi-Factor Authentication, strong Password Management and Secure Storage Vaults for critical keys. PAM migration is a complex task, though, and internal security teams should strongly consider onboarding an external specialist to set the stage for a successful implementation.

---

## About the Author

### Dr. Heiko Klarl, Chief Marketing and Sales Officer, iC Consult Group

Dr. Heiko Klarl has been active in Identity and Access Management (IAM) for over fifteen years. He seeks to bridge the gap between business and IT in order to create holistic solutions: all the way from the customer's strategy to technological implementation. To date, he has successfully completed a wide variety of IAM projects in a variety of industries, including automotive, banking, and logistics.



As Chief Marketing and Sales Officer of iC Consult Group, he is passionate about understanding the challenges of his customers and working with them to find the best-fit solution.

Heiko can be reached online at [heiko.klarl@ic-consult.com](mailto:heiko.klarl@ic-consult.com) or <https://www.linkedin.com/in/heiko-klarl/> and at our company website <http://www.ic-consult.com>

# Multi

# Factor



## The Future of MFA

Going Beyond Privileged Accounts

By François Amigorena, Founder & CEO, IS Decisions

Given the current global cyber threat landscape, multi-factor authentication (MFA) is one of the most effective ways to prevent breaches and protect network data. But although MFA adoption has accelerated since the pandemic, it's still slow to takeoff. Why? For MFA adoption to really become widespread, organizations must grasp the true value of MFA and how to implement it effectively.

### MFA Adoption is Slow

In their everyday lives, most people ignore two-factor authentication (2FA), or hesitate to apply 2FA for, mostly, the same reasons: they have misplaced confidence in passwords, are frustrated or confused about setup, or they're just lazy. A case in point: less than 10% of Google users have enrolled in 2FA.

This reluctance has propelled several tech giants to make MFA mandatory: Salesforce now mandates MFA, 2FA will gradually become mandatory for all Google users, and Amazon.com Inc.'s Ring has already made 2FA mandatory.

Unfortunately the same attitude exists in the workplace, with enterprise MFA adoption still low.

---

## Why Do Organizations Hesitate to Adopt MFA?

A few persistent common MFA myths make many organizations reluctant to adopt MFA. Many view MFA as best-suited only for:

- Very large organizations.
- Privileged accounts, like: Windows local administrator accounts, domain admin accounts, Active Directory service accounts, and anything that has rule over a major part of the network environment.

First of all, the question of whether or not to apply MFA actually should have nothing to do with your organization's size. Whether a small business or a global enterprise, your data is just as sensitive, and should be just as well protected.

But should MFA really only apply to the most privileged accounts?

## Is Protecting Privileged Accounts Enough?

The idea behind “privileged accounts” belongs to a certain security approach called privileged access management (PAM). Within this approach, securing the login of your privileged accounts is the first step to securing access.

PAM ties into an old-school, perimeter-based security approach, when the login security of the “average” user account wasn't as important as those privileged accounts. Even so, PAM certainly has a place for monitoring and securing privileged accounts like Active Directory administrator accounts.

But the modern enterprise faces a different cyber threat landscape today, even compared to as recently as two years ago. Factors like the rapid shift to remote work, and many organizations' hurried transition to a hybrid environment including both the corporate network and the cloud, call for a new approach.

## Least Privilege Is as Relevant as Ever

The principle of least privilege limits user access to the sets of data, applications and systems that they absolutely need. It's been around for years (Microsoft was writing about it 30 years ago), but as the risk of attack increases today, least privilege is more relevant than ever:

- An external attack leverages user accounts to gain control over endpoints, to move laterally within the network and, ultimately, to acquire targeted access to valuable data.
- Insiders exploit their own granted access or other compromised accounts to wield data and applications for malicious purposes.

The point is, least privilege is about more than privilege. In essence, the principle has always been about preventing the compromised use of an account with access to valuable data.

---

## The Real Value of MFA

In a modern organization, every user has attributed access rights and privileges. For the purposes of logon security, that makes all users some sort of privileged user. Organizations can reduce risks by [extending login security as far down the “non-privileged” path](#) as possible, to as many users as possible.

This leads us to the real value of MFA: protecting any account with access to critical data, applications, and systems.

## Special Considerations for Deploying MFA to All Users

When rolling out MFA to any number of users, preparation is key. Obviously, applying MFA to all users will likely require more planning than if you were applying MFA to only your privileged accounts. Remember these six key points for a smooth MFA deployment:

- Securing logins significantly improves your security stance
- MFA is not just for privileged users
- MFA doesn't have to be frustrating for IT departments
- MFA must balance user security and user productivity
- Educate and empower your users to support MFA
- Management commitment and buy-in is key

## The Future of MFA: Protecting All Users

Tech giants may push some organizations to adopt MFA, but a real increase in MFA adoption will require a fundamental shift in organization's security approach. The more organizations understand the value of applying principles of least privilege and privileged account management to all accounts, the more they will understand the advantage of securing logins across all users. Organizations will put more effort into finding a balance between employee productivity and security. And when they do, get ready to see the demand for granular, customizable MFA explode.

### About the Author



François Amigorena is the founder and CEO of [IS Decisions](#), a global software company specializing in access management and MFA for Microsoft Windows and Active Directory environments. A former IBM executive, François is also a member of CLUSIF (Club de la Sécurité de l'Information Français), a non-profit organization dedicated to information security.

Francois can be reached online via [LinkedIn](#) and at our company website <https://www.isdecisions.com/>



## Cybersecurity Doesn't Have to be a Game of Last Man Standing

Nor should tackling cybersecurity be a solo mission. Leaning into partnerships and changing where security investments are made may be critical to a more secure future.

**By John DeSimone, President, Cybersecurity, Intelligence and Services at Raytheon Intelligence & Space**

We all understand the principles of the game “tag.” One player is “it” and everyone else is left running around to fend for themselves to avoid being tagged. There are no trusted alliances, every person is in it for themselves, and everyone is a potential enemy.

In the world of cybersecurity, playing solo is the worst tactic to take, and too many organizations rely on this outdated approach. Instead, they should prioritize strategic partnerships and investments in tools that will keep their organization accountable – this is the differentiator between proactive businesses and the ones waiting to be attacked.

### Collective defense is key

Cybersecurity is not a game of tag, nor is it a game of last man standing. In the realm of security and defense, having partnerships, alliances, and people on your team is critical to developing a holistic security strategy.



---

Historically, closing people out and maintaining privacy seemed like the default solution to any security concern, but we're learning through time and experiences that security can operate in a quid-pro-quo style and information sharing is vital to building a well-informed security strategy.

Bringing together leaders with assorted backgrounds lends itself to a diverse security strategy for businesses and governments. People from differing industries have unique perspectives and problem-solving experiences, which leads to more solution generation and a robust security plan.

Some of our newest government cyber leaders work seamlessly together despite having varying backgrounds. They are developing mandatory cybersecurity standards, working to combat ransomware, and overall will build a stronger offensive and defensive cyber program thanks to their mixed backgrounds in security.

## Technology as a security partner

We also will continue to see the impact of digital transformation in the world. There are over [21 billion devices](#) on the internet a day, each producing its own share of data. The growing IoT environment has created more vulnerable attack surfaces. The more collaborative we become, the quicker we adapt to agile attackers.

In addition, data will become increasingly complex and new business operations (like an influx of [remote workers](#)) are making it even more necessary to strategically share vulnerabilities and information amongst trusted partners. However, human error will always persist and some functions like [critical infrastructure](#) and [personal data](#) should be safeguarded at a level higher than other entities.

Organizations committed to enhancing their cybersecurity stance must also be willing to invest in scanning and remediation tools. How can employees and companies protect what they do not know exists?

Companies recognize that they do not need more end-point protection devices, as they are not holistic solutions. Scanning tools and software with sensing capabilities are more cost-effective investment, and they give both organizations and governments the ability to actually see where compromised attack surfaces are so they can act accordingly and reinforce vulnerable areas.

Paring these software investments with skilled CISOs and chief data officers is an ideal way to fortify a security initiative and continuously audit company weaknesses and strengths.

We will see a continuum of maturity and cyber readiness in every industry. Your organization could be at the forefront if they walk away from the game of Tag and move on to proactive investments and tactical partnerships. The time to enhance your business's cybersecurity posture cannot be put off until tomorrow.

---

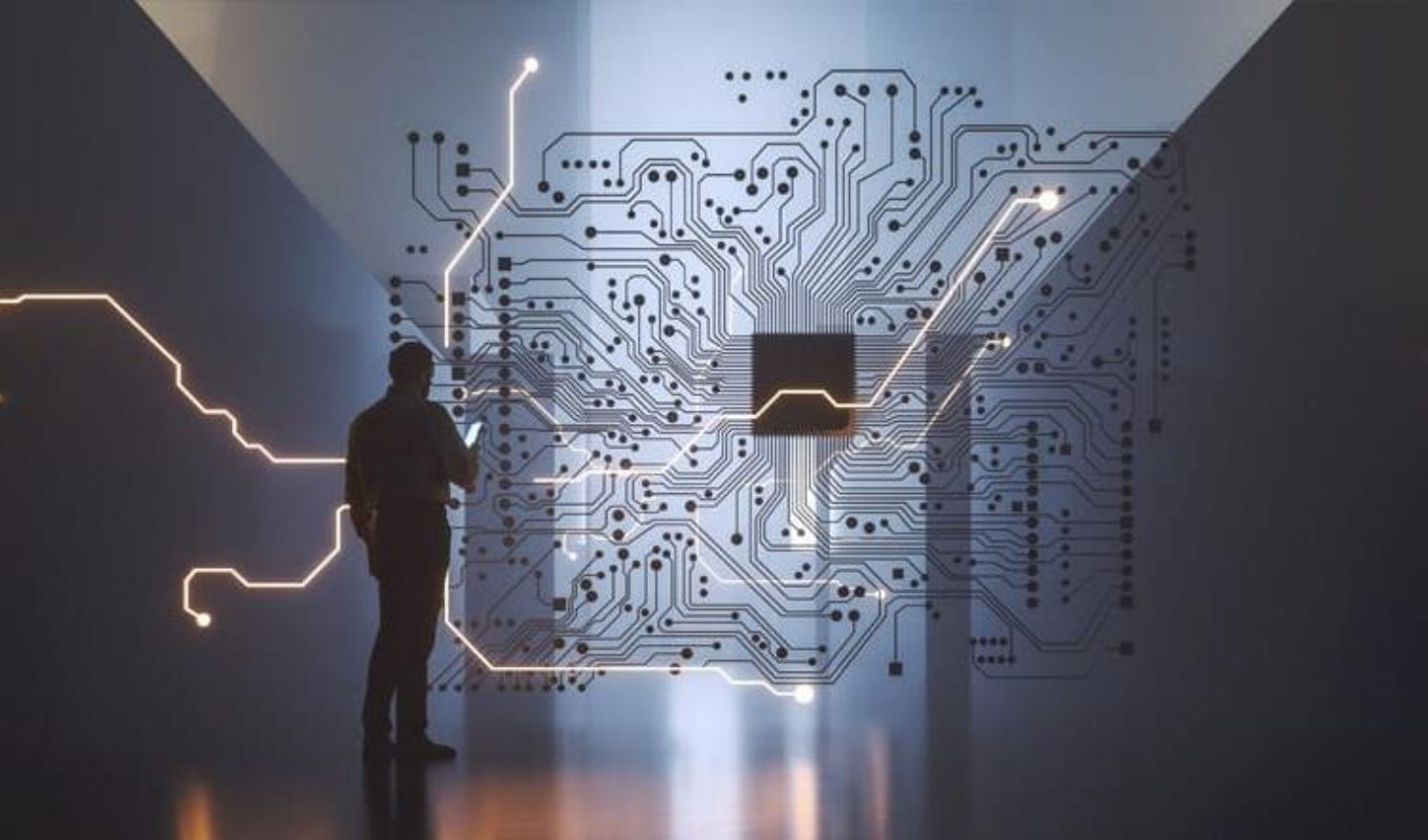
## About the Author

**John DeSimone** is president of Cybersecurity, Intelligence and Services for Raytheon Intelligence & Space, a business of Raytheon Technologies. Most recently, DeSimone led the business' Cybersecurity and Special Missions organization where he oversaw strategy and operations for the cybersecurity solutions and services business.

Before joining Raytheon in 2016, DeSimone served as an executive vice president of delivery and operations at CSRA Inc. He also served as vice president and general manager of Computer Sciences Corporation's North American Public Sector Enterprise Services group.

DeSimone earned a bachelor's degree in computer science from Columbia University in New York and attended the Motorola Chairman's Leadership Institute at the Kellogg School of Management at Northwestern University.





# How The Updated CMMC 2.0 Rule Impacts DoD Contractors

What Small Businesses Must Do to Stay Compliant

By Dan Clarke, President of Truyo, and Jeff Sizemore, Chief Governance Officer at Egnyte

Every year, the Department of Defense (DoD) relies on hundreds of thousands of entrepreneurial businesses to provide critical technologies and innovations that help support the men and women who are working to protect the US. Equally, DoD contracts are often the lifeblood for many of those private-sector businesses.

More recently, those companies—known as the defense industrial base (DIB)—have been the target of increasingly sophisticated cyberattacks. In an effort to safeguard against those attacks, the DoD initially introduced the NIST 800-171 standard to protect the confidentiality of controlled unclassified information (CUI). That program allowed defense contractors to self-attest, however after review, the department discovered a majority of contractors could not pass their audits.

To put an enforcement ring around compliance, the DoD introduced the Cybersecurity Maturity Model Certification (CMMC) program in 2020. That framework was updated in November 2021 and requires all contractors within the DIB that handle CUI to certify, if they want to continue working with the department. But, as with any government program, there's some gray area and contractors must understand where they fit in.

---

## The evolution of CMMC

The CMMC is part of the DoD's effort to secure its supply chain and protect its DIB contractors from cybersecurity threats who have increasingly been the target of frequent and complex cyberattacks. The program was designed to provide assurance to the DoD that DIB contractors could adequately protect CUI, and the requirement includes any information that may flow down to subcontractors in a multi-tier supply chain.

When the interim CMMC 1.0 rule went into effect, it was met with mixed reviews. Some applauded it, while others felt it was far too stringent because of its assessment requirements for very small contractors that manage CUI—and that continues to be a major barrier.

Initially, all DIB contractors were required to undergo an audit by a third party, referred to as C3PAO (CMMC 3rd Party Assessor Organization). Now, under CMMC 2.0, only organizations that manage Federal Contract Information (FCI), that they've classified as Level 1, may self-attest. All other DIB contractors that handle CUI—Level 2 and 3—must pass an audit by a C3PAO. Self-attestation is not an option for those businesses.

The problem with this requirement is that there simply aren't enough auditors to meet the demand. Backlogs of audit requests have grown, and will continue to, as there is no assessor ecosystem in place today to accommodate requests. The DoD and the CMMC Accreditation Board (AB) are working to correct the backlog, however.

## What CMMC 2.0 means for small businesses

While the number of security tiers to be achieved was reduced from five to three tiers in the transition from CMMC 1.0 to CMMC 2.0, it also put a heightened priority and urgency on contractors and subcontractors to become certified to continue their work with the DoD. Though contractors who process CUI will require C3PAO certification, at least 140,000 additional subcontractors who process only FCI have the ability to perform self-assessments.

The ability to self-assess, however, can be a double-edged sword as it places the onus on those companies to confirm that they are audit-ready and compliant. For smaller companies that typically don't have security or privacy experts on their teams, self-assessment will represent a significant undertaking, and most don't know where to start.

## How small businesses can prepare

The first step is to determine the scope of the business's CMMC auditable environment. It is imperative to understand where FCI and CUI data is processed within the contractor's environment, then to build a security strategy around it.

For the Level 1 contractor, controls that are required to be compliant consist of 17 practices that fall under six domains:

- Access Control
- Identification and Authentication
- Media Protection

- 
- Physical Protection
  - System and Communications Protection
  - System and Information Integrity

These are collectively known as basic safeguarding requirements for FCI, as defined in the Federal Acquisition Requirements (FAR) clause 52.204-21. Which controls you decide to implement first is also a critical decision as it will help to set your course for compliance.

Many businesses that are seeking CMMC L1 certification will begin with who has access to what data, how they access it, and what they are authorized to do with that data. This would take you through Access Controls and Identification & Authentication first, as an example.

With those criteria, create a timeline and map to compliance. Again, this will require an understanding of where FCI and CUI data lives within your organization. Take into account structured and unstructured data, who has access to that data, how it is used and how it circulates through the business, as well as any vendors or partners that you interact with. You will also need to establish a confidential and protected environment for authorized users to collaborate and access FCI and CUI. The audit evidence or collected artifacts that demonstrate compliance to the requirements also need to be contained within the protected environment.

Having a clear picture of where all of your data lives and who has access to it, will enable you to identify where you need to implement security safeguards. The level-of-effort for this activity is typically a very time-consuming and manual process for many organizations, especially if they don't know where to look and don't have processes, vendor products or in-house scripted automation processes to assist in the data discovery process. The good news is that there are now cost-effective automation tools available to smaller businesses—it's just a matter of finding one that will support the data discovery process and walk you through the process of becoming audit-ready.

Whether performed manually or supplemented by the use of an automation tool, the time to start preparing is now. Though the official enforcement date for CMMC 2.0 has been somewhat of a moving target, it's tentatively set for 2025, and you need to get ahead of the curve. This is mission-critical since DoD is prioritizing a speedier rollout.

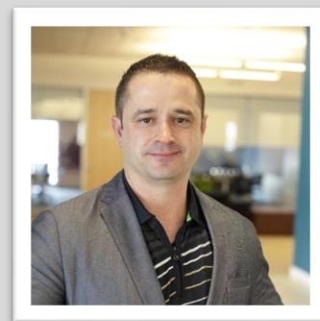
---

## About the Authors



**Dan Clarke** is the President of Truyo, an automated consent and data privacy rights management platform. He has more than 30 years' experience in technology and business leadership, and is an experienced data privacy advisor with deep expertise in the privacy landscape. Dan can be reached at [truyo.com](https://truyo.com).

**Jeff Sizemore** is the Chief Governance Officer at EgnYTE, a cloud content security and governance platform, where he is responsible for the strategy and execution of EgnYTE's Secure and Govern solution. Jeff has an extensive background in data protection, specifically in encryption, key management, data loss prevention, and identity and access management. Jeff can be reached at [egnyte.com](https://egnyte.com).





## Bosch Aishield To Protect AI Systems and Bolster Digital Trust

**Bosch AIShield was recently unveiled at CES 2022 as an industry-first & patented AI Security SaaS offering to protect AI systems against emerging security threats**

**By Manoj Parmar, Global Program Director – AIShield at Bosch, Amit Phadke, Global Product Manager – AIShield at Bosch**

Every organization wants to protect its valuable digital assets like data and information, but what about AI algorithms? Successful exploitation of AI algorithms can cause financial loss, reputational damage, loss of competitive advantage, and loss of intellectual property. For example, a malicious breach of pricing algorithm for an e-commerce company can result in attackers causing financial loss to the retailers/sellers and negatively impacting the platform's brand reputation. Similarly, a heavily invested medical diagnosis AI algorithm, when stolen or attacked, could lead to loss of niche competitive advantage and loss of patient data. Similar challenges & threats have also been highlighted recently by [enisa](#) (EU agency for cybersecurity) and [NIST](#) (National Institute of Standards & Technology) with Bosch being a key comment contributor to the later. Bosch has been researching & working on this as well since 2020.

According to Bosch, majority of organizations are struggling to address the challenge of securing models. Suppose one want to protect their algorithm. In that case, they must check the latest research related to an adversarial aspect of AI, find the right people with the proper knowledge of AI and security, figure out how to use open-source research in the development of algorithms, and then understand how to integrate with the development workflow easily and intuitively. Lack of addressing these challenges results in unanswered questions such as - how often your algorithm is really under attack? What is the true financial

---

value of AI models, and what if they are stolen? What's the impact of the AI model attack on brand reputation and customer trust?

Therefore, the need of an hour is to create a last layer of defense for AI models to plug in the newer attack surfaces.

[Bosch AIShield](#) brings hacker-level vulnerability assessment and security hardening to the organization's AI-powered devices and cloud solutions. The product provides a SaaS-based

tool with UI so that every AI stakeholder (e.g., data scientist, ML engineers, product managers, security engineers) can benefit from our patent-powered deep technology. With a few clicks, AI stakeholders can get vulnerability assessment reports, generate, and deploy customized defense mechanisms, and get real-time notifications on real-time threat detection.

“Bosch is committed to make AI trustworthy and build digital trust in AI. AIShield is an important product offering towards that. It protects AI systems against emerging threats from adversaries. AIShield makes AI security accessible to all and bolsters Digital trust in AI”, says Krishnamurthy Vadiraj, Head Technology & Innovation, BGSW.

Bosch AIShield also offers out-of-the-box native automation support so that organizations can achieve scale rapidly. With a minimum configuration, it can be easily, effortlessly, and hassle-free way integrated into the MLOps (ML workflows) leveraging our API offerings. Bosch AIShield takes an AI model and sample data as an input and calculates the vulnerability score of a model using our intelligent attack framework and attack database. The attack database is foundational and constantly updated through our research and open-source intelligence. Bosch AIShield identifies relevant attack vectors and, using them, calculates the vulnerability score. This score prioritizes the most critical vulnerabilities and creates a defense mechanism against attacks as a remediation response. Bosch AIShield generates a deployable version of the defense model and real-time attack notifications. The notifications are designed to be easily be integrated by industry-leading Security Incident and Event Management services. The user interface provides intuitive visualizations and detailed reports. Bosch AIShield also offers consulting services to help the organization navigate the security landscape of AI. With Bosch AIShield's rich end-to-end security offering, even small security teams and AI/ML developers can ensure AI systems are monitored and protected.



---

## About the Authors

Amit is a seasoned software professional and an experienced product manager with varied experience of 9+ years in building products for the international automotive market. He currently is Global Product Manager for AIShield and has experience managing diverse distributed teams. One of his past roles as Executive Assistant to Senior Vice President of Innovation has given him keen insights into the innovation journey of an empowered captive center of a large MNC tasked with building products for the globe. He has completed an executive education certificate program from UCLA, Anderson School of Management (PGP Pro). His areas of interest are Product Management, Innovation, Strategy, and Agile Development.



Manoj's role is Global Program Director – AIShield® at Bosch. He is an award-winning, experienced, seasoned Technologist. He has been working at Bosch for more than 13 years. His responsibilities include building a global product at the intersection of AI and Cybersecurity to safeguard AI systems and leading the AI Security Initiative for Bosch Group. Manoj's journey is inspirational and transformational across automotive, two-wheeler, and digital domains to deliver customer-focused business values. Along with his teams, he has built several innovative products and solutions using multiple classical and emerging technologies.



He has filed 20+ patents and has published 13+ research papers. He is a mentor for deep tech startup events. He has also been a guest speaker for technology, innovation, and entrepreneurship.

He is a recipient of the Chevening Cybersecurity Fellowship 2021 by the UK Government's FCD Office. Zinnov awarded him Technology Role Model Award 2020. He is a founding member of MITRE ATLAS. He holds engineering and management degrees. He has also completed the Corporate Startup program from UC Berkeley and M.Sc. in Innovation and Entrepreneurship from HEC Paris.

He is a lifelong learner and enjoys cooking, reading, and jogging.

To learn and engage more on Bosch AIShield, please visit:

[Bosch AIShield Webpage](#)

[AIShield Product listing on Azure Marketplace](#)

[AIShield with Azure Sentinel on Marketplace](#)



## The Land of Data-Centric Security: Before and After

By Andy Smith, CMO, Laminar

Data protection and cloud security have enterprises running around a giant hamster wheel. They know that they are practically blind when it comes to where sensitive data is in the cloud and how well it's protected. Meanwhile, data protection teams are crying out for a way to gain a complete and accurate view of their data. It doesn't seem like such a tall ask, considering that data is at the center of cloud transformation—no matter how you slice it. Yet, still, some companies are living in the renaissance period of cloud security and blissfully unaware of their assets in the cloud.

### Setting the Scene

If innovation were a Hollywood movie, data would be the lead actor. Data is inarguably the most critical piece of the puzzle when it comes to innovation within the modern cloud-first enterprise. Most business leaders have wrapped their heads around this concept and recognize the facts; they agree that: In order to give my developers and data scientists the tools they need to innovate, our data must be democratized and we must be able to support new applications on the cloud. While most businesses understand that data is important, that it's critical to protect and that it is a source of differentiation, they often fall short of understanding what exactly is involved in effective data security. Especially when it comes to sensitive data stored in the cloud, many security teams are still in the dark.

This misunderstanding—or possibly misinformation—leads enterprise leaders to rely on traditional methods of data security. Outdated technology hasn't adjusted to the new cloud-native environment. This means that data security and privacy workflows, reviews, committees and assessments are all manual. Herein lies a tremendous growth opportunity.

---

We could discuss the problems with current approaches until we're blue in the face. Problems of [alert fatigue](#), [FUD](#), [friction with developers](#) and of course exposure to [data exfiltration and security risks](#) are holding organizations back from reaching their full “cloud potential.” While recent approaches, like [Cloud Security Posture Management \(CSPM\)](#) tools, have brought some useful capabilities for cloud infrastructure—such as VMs, containers, etc.—they don't address the needs of data security teams who have been left in the dust. Traditional data security solutions and manual processes haven't adjusted to the new cloud-first environment, which makes the work of the modern analyst much more challenging, and, most significantly, has positioned them as “gatekeepers” rather than “enablers” of business and innovation.

## Stuck in the Past

Legacy data security suites have left enterprises ignorant to what sensitive and regulated data they have in the public cloud. This impacts several components of a data security strategy. First, teams are left conducting manual, periodic interviews with application owners to identify sensitive data stores that are out of date (usually days later) as the cloud environment is agile and dynamic as developers and data scientists can make copies of data anytime they want. This is all in a failed effort to determine where their sensitive data lives in the cloud. They're stuck in a “trust but no verify” approach that is completely manual and unable to keep up with the speed of the cloud.

Second, when securing and controlling cloud data, they often rely on written policies with little to no enforcement. Instead of automated approaches to enforce policies, they have to trust that developers will understand standard policies and properly implement them. They are involved in laborious compliance audits of policies, which can easily leave gaps. Lastly, legacy data loss protection (DLP) solutions only cover email, endpoint and on-premises infrastructure, which means data security teams have limited to zero visibility into potentially ruinous data leaks in IaaS and PaaS environments.

Third, security teams may be thought of by others within the organization as a hindrance to business and innovation. While leadership can preach all day to stakeholders and marketing about the importance of security, there can be a disconnect between security teams and other decision-makers when it comes to acting on the platitude. Security might seem like a great idea “when we get to it,” but when it comes to enacting security best practices, leadership might not want to risk possible disruption that would slow or even stop a project. Without the right tools in place, security teams can feel like they are fighting an uphill battle, which can be discouraging and lead to neglect of pertinent issues just to reduce friction with colleagues.

## A Place in the Future

Where does this leave the modern enterprise that wants to gain a complete and accurate view of all assets on the cloud to move innovation forward? A cloud-native, data-centric approach will take

---

organizations from the past to the future of data management and protection. Let's break down the components of a forward-thinking, modern approach to cloud security.

### **Eat, Sleep, Breath Cloud**

There's no arguing that cloud is integral to most businesses today. Thus, a modern data management approach must start by integrating fully with the public cloud itself, using modern, cloud-native approaches. Within virtually every enterprise are hundreds of technologies and apps that store, use and share data in the cloud. These tools can be managed by cloud service providers (AWS S3 buckets, Google Cloud Storage, Azure Blob Storage, etc.), IT (AWS RDS) and even developers or operations teams (database that runs on an EC2 or a Kubernetes node). Furthermore, each technology is configured and used differently on a daily basis. These architectures are complex, dynamic and constantly changing, which increases risk dramatically over legacy data management.

For this reason, a cloud-native tool or application is critical for companies seeking a place in the future. A cloud-native tool or application is designed to capitalize on the characteristics of a cloud computing software delivery model. They utilize the cloud service provider's (CSP) native APIs that are designed to meet these needs. While cloud-native data security solutions aren't mainstream yet, they're gaining traction among larger, established organizations that recognize their unmatched value and their unique ability to discover, classify, secure and control the data that lives in the cloud more deeply.

### **Full Visibility**

If security teams don't know where their sensitive data is, who has access to it and can't understand the risk posture associated with certain assets, how can they expect to know about leaks and vulnerabilities in a timely manner? Gaining that deep, all-encompassing visibility into every piece of organizational data stored in the cloud—whether that data asset is managed by the cloud provider, if it's a formal data store or in compute or if it's public or isolated—and continuously monitoring the movement and management of that data is the most effective way to stay nimble and reduce the attack surface. For companies living in the "future" of cloud data management, this means connecting security tools directly with their cloud account to agentlessly scan the entire cloud environment and autonomously discover all data stores. Autonomous solutions are critical as cloud environments are agile and dynamic where security teams and even application developers are not aware of the typically thousands of data assets in their cloud accounts. Many data management solutions will automatically scan known datastores with the right credentials to gain access, but only autonomous solutions discover ALL resources without knowledge of the environment. Achieving this level of visibility without disrupting workflows is huge in terms of moving security teams away from a gatekeeper persona to business enablers.

---

## Putting the Pieces Together

Collecting and analyzing all data assets is just the first step toward a more advanced, forward-thinking approach to data security in the cloud. Modern cloud-native solutions are also able to autonomously scan all of those discovered pieces of data to understand where to focus first—the most sensitive data and the most critical issues—and present that information to security analysts. Cloud-native tools can also autonomously scan audit logs, network flow logs and various data sources in order to build a profile for every data access point. A cloud-native, agentless approach allows data security teams to detect leaks and remediate them faster by monitoring unwanted data access in real-time by analyzing access logs for anomalous activity. Cloud security teams are no longer stuck in an environment of alert fatigue and burnout because they finally have eyes on all of their sensitive data at any given moment.

Without the right tools, today's security professionals will continue to live in fear of the unknown, like unknown data repositories (what we call shadow data) that can be targeted with the least odds of detection. Security teams are afraid of being out of the loop and susceptible to breaches. This creates tension between security teams and the rest of the enterprise. But with the right tools, security teams can champion digital transformation and innovation and truly become heroes within their organization.

### About the Author

Andy Smith, the CMO of Laminar. He is a marketing and product leader and can be reached online at <https://www.linkedin.com/in/andysmithcmo/> and at our company website [laminarsecurity.com](http://laminarsecurity.com)





# Non-human Resources

How to close the weakest link in your cyber defenses

By Camellia Chan, CEO and Founder of X-PHY a Flexxon brand

Every cyber security professional knows that human error is the common factor behind the majority of successful cyber breaches. Software patches that are not updated, thoughtless clicking on phishing emails, tweaks to software configurations, or 'personalized' re-settings of anti-virus software are all too often the innocuous start of a cascading, expensive and reputation-damaging security breach.

The extent of that human error – whether caused by malicious intent or straightforward carelessness – has most recently been quantified by the World Economic Forum (WEF). In its Global Risks Report 2022, it calculated that [95 percent](#) of all security issues can now be traced to human error.

Of course, cyber security professionals are also extremely aware that our industry as a whole is understaffed and under-resourced. Nearly 20 percent of the WEF's network of academic, business, government, civil society and thought leaders believe that cybersecurity failure will become a critical threat to the world in the next two years. At the same time, there is a 3 million gap in the number of cyber professionals needed worldwide.

## Remote insecurity

The potential for human error has been greatly exacerbated by the pandemic and the accelerated dependence of both individual organizations and entire economies on digital systems.

Rapid digitalization accompanied by remote, and now hybrid, working has led to a proliferation of platforms and devices to make remote working possible. The corporate network has become more diffuse, its boundaries have gotten fuzzier, and sensitive data is routinely shared with a wide range of

---

intermediaries, from cloud service providers to data aggregators and APIs, among others. The attack surface is greatly expanded.

The widespread adoption of cloud-enabled services and networks itself has also changed the typical threat vector. Threats can now flow from cloud to machine level, putting endpoint devices and their operating systems in the direct line of fire.

At the same time, remote workers are sending corporate details over their residential networks, using the same laptop and the same weak password for both personal and professional applications.

## Costly inaction

With no clear barrier between work and home, a familiarly informal ‘office’ setting, and even a more relaxed dress code, the psychological factors that keep workers ever vigilant easily morph into cyber fatigue and ‘what’s the worst that can happen?’ mindset. Which is why, even with the most robust infrastructure and policies in place, major corporations can still fall.

The pandemic has certainly increased the opportunities for human error to cause indescribable damage to corporate systems. But even as a new form of normalcy returns to corporate life, the opportunities created for cybercriminals will continue to grow. The expansion of IoT-enabled devices, edge-computing, 5G and blockchain-enabled applications present new opportunities and new threats.

As these essential business tools converge and connect, as virtual 3D spaces become networked and pervasive, users – employees – will be asked to navigate inherent security vulnerabilities in complex, decentralized systems without sophisticated onboarding capabilities or structured security policies.

## New vulnerabilities

On the offense, attacks proliferate as cyberthreat actors continue to take advantage both of more aggressive attack methods and lower barriers to entry. For example, ransomware-as-a-service (RaaS) gives non-technical criminals the ability to successfully penetrate a corporate network.

Now that malware can be powered by AI, the low-skill, high-reward model of cyber criminality is set to increase – particularly as the expansion of cryptocurrency usage keeps ransom payments away from scrutiny by regulated banks and law enforcement agencies.

As physical supply chains become more digitalized, those same criminals have discovered new vulnerabilities to exploit. The weakest link in any system may no longer be the error of an employee but at some technology provider or other third party down the supply chain. Cyber-attacks are therefore no longer exclusively aimed directly at a big corporation’s infrastructure, but at the smaller less well protected companies that support and supply them.

---

## Beyond software

Today, most cybersecurity depends on software defenses, but business leaders and their cybersecurity professionals need to update their arsenal if they wish to protect their devices and their data. By design, firmware has a better view of the system—and a greater ability to protect it. As such, security at the that level of the storage drive is the best way to minimize attacks.

This is what an AI-infused solid-state drive (SSD) can do. The AI element provides intelligent, intuitive and immediate defense by detecting anomalies in data-access patterns that typically indicate ransomware, cloning attacks, physical drive theft, and even other side-channel attacks.

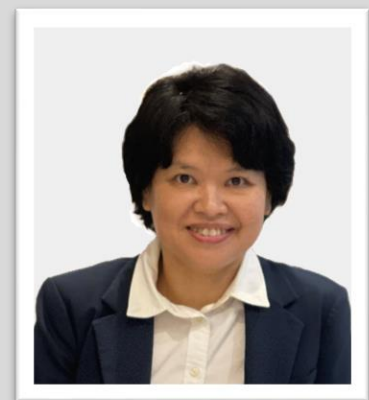
Embedding AI at the firmware level, where it sits close to a user's data, ensures real-time threat detection and protection against zero-day exploits. Data within the drive is closely protected 24/7 – making it an ideal solution for complementing software-based defenses at every participant in a supply chain.

What's more, when developed on a zero-trust framework, only authorized and authenticated personnel can access the content within, which further serves to protect users, applications, and data from external threats. As to the SSD itself, hardware sensors can provide real-time physical protection should employee's device be stolen, lost or tampered with.

Leading OEMs are already implementing this kind of technology in the latest models, and we can realistically expect more to arrive as businesses seek secure devices that diminish the impact of human error by minimizing the amount of human intervention needed to keep data safe. In a constantly evolving, multi-threat world, it is the last – and very necessary – line of defense.

### About the Author

My Name is Camellia Chan and I am the CEO and Founder of Flexxon. Camellia Founded Flexxon in 2007 and has over 20 years of experience in the Electronics Manufacturing industry. As the CEO and founder of Flexxon, Camellia oversees the company's business development and growth, industry partnerships, and expansion to regional and global markets. Under her leadership, Flexxon has become a world-leading brand in providing NAND flash storage solutions across sectors; specifically in four niche areas – Cyber Security, Industrial, Medical, and Automotive (CIMA).







**ZERO**

**TRUST**

## A New Paradigm for Absolute Zero Trust and Infrastructure Resiliency

By Rajiv Pimplaskar, President and CEO, Dispersive Holdings, Inc.

### How Secure is your Public Cloud?

Public cloud is an IT model where 3<sup>rd</sup>-party-managed on-demand computing and infrastructure services are shared with multiple organizations using the public Internet. Over the last decade public cloud services and SaaS applications have exponentially grown to become mainstream across governments and enterprises worldwide. This phenomenon, coupled with the unprecedented shift of people working from home during the COVID-19 pandemic, have “de-perimeterized” the corporate network and eroded IT’s control over infrastructure.

Erosion of control and the rise of new and emerging threat actors have led to an “implicit trust” problem with the network. Implicit trust occurs where a public cloud or network resource is “trusted” on a de facto basis without meeting the burden of proof for earning that trust. Implicit trust can be very dangerous as information is most vulnerable for a data breach or malware infection when it’s in motion. As we’ve seen on multiple occasions over the last two years, network resources are prime targets for unauthorized access, insider threats, code and injection attacks, Man-In-The-Middle (MITM) attacks, privilege escalations, as well as lateral movement.

The public cloud can also become a gateway for attacks by Nation state threat actors. The current geopolitical events are a stark reminder of the security risks and fragility of business resiliency when relying on public cloud infrastructures across different countries. Unquestionably, an evolved paradigm for both securing corporate users, sensitive data and resources and assuring underlying infrastructure resiliency is no longer a luxury – it is essential!

---

## Zero Trust and The Achilles Heel of Session-level Encryption

Central to any zero trust strategy is the belief that organizations should not automatically trust anything inside or outside its perimeters. Rather, they must verify anything and everything trying to connect to its systems before granting access. While incredibly relevant for today, most zero trust approaches stop at the network as they rely on traditional cryptographic protocols to keep communication secure and private.

Transport Layer Security (TLS) is a common cryptographic protocol that operates at the session layer (layer 5) of the Open Systems Interconnection (OSI) model and is designed to provide communications security over a computer network. Once the client and server have agreed to use TLS, they negotiate a stateful connection by using a “handshaking procedure” with an asymmetric cipher to establish not only cipher settings but also a session-specific shared key with which further communication is encrypted using a symmetric cipher. Applications generally use TLS as if it were a transport layer, even though applications using TLS must actively control initiating TLS handshakes and handling of exchanged authentication certificates.

The danger of solely relying on this approach is that unfortunately, modern threat actors can operate underneath the session layer (at the network and the transport layer - layers 3 and 4 respectively) and intercept, as well as harvest all data (including the shared secret). Threat actors with these capabilities may have powerful economic and / or Nation state motivations and the luxury to play a “long game.” Their focus may not be decryption but, disruption or capturing data in transit for replay attacks and / or future analysis. Nation state actors have evolved tremendously and now possess powerful compute and coordinated resources available at their disposal that can reframe a traditional cryptographic math problem into a much more insidious (yet much simpler) database lookup one.

Finally, the next decade will determine the outcome of the ongoing war for quantum computing supremacy, now being waged between the world’s superpowers. Quantum computing, while inherently very useful, changes the game dramatically when it comes to protection rendered by conventional IPsec or TLS encryption. The Quantum Alliance Initiative at the Hudson Institute highlights some sobering facts about the potential cost of a quantum computing attack noting that, a single attack on the banking system could cause \$1.9 trillion in overall damages on the financial systems. An attack on cryptocurrency would cause a \$3.3 trillion blow to the United States economy.

## Lessons From the Past – Introduction of Spread Spectrum in the Radio Frequency (RF) world

Interestingly, a similar problem was first identified and subsequently solved in the last century after World War II in the context of radio guidance systems for Allied torpedoes that used spread spectrum and frequency hopping technology to defeat the threat of jamming and interception by the axis powers. The principles of this work are incorporated into today’s Bluetooth, GPS and 5G technology.

Military communication systems strategically “spread” a radio signal over a wide frequency range several magnitudes higher than minimum requirements. The core principle of spread spectrum is the use of noise-like carrier waves and, as the name implies, bandwidths much wider than would be required for simple point-to-point communication at the same data rate. The use of the spread spectrum delivered several benefits:

- Resistance to jamming (interference)
- Resistance to eavesdropping
- Multiple access capability or code-division multiple access (CDMA)

---

## Absolute Zero Trust – The Modern Paradigm

The Internet as well as cloud operators can learn a great deal from the RF world and leverage the proven battlefield concepts of RF frequency hopping and spread spectrum communications to securing TCP/IP communications regardless of the level of trust with the underlying infrastructure.

Secure communications technologies are now available that can establish dynamic virtual active/active multipath networks with rolling encryption keys and granular access controls. In addition, orchestration, control and data planes can be separated, thereby further protecting data flows from potential interception and future analysis. Managed attribution can also keep virtual endpoints, users and network resources obfuscated, making them virtually impossible to detect. Finally, proper access control and device posture checking can be implemented to prevent unauthorized access.

Such networks can be both intelligent and predictive, enabling dynamic routing and management capability with smart deflection and redirection of traffic from impacted resources and network nodes to mitigate against availability issues and DDoS attacks. Importantly, performance can be enhanced, even across high latency, low bandwidth environments, enabling alternative communication pathways such as mobile hotspot, ADSL, broadband, satellite, MPLS, LTE, and others to maintain business continuity—even in the face of primary network disruption.

Zero trust and infrastructure resiliency can certainly be achieved, but only if the appropriate safeguards are implemented and all existing vulnerabilities mitigated. Combining the lessons of the past with technologies and measures we now possess can provide the needed security and protections against even the most aggressive and skilled bad actors.

### About the Author

Rajiv Pimplaskar is the President and CEO of Dispersive Holdings, Inc. A zero trust industry leader, Rajiv is passionate about growth, driving innovation and scaling SaaS cybersecurity companies. Rajiv has two decades of experience across product, go-to-market, and sales and until recently was the CRO for Veridium US, LLC. Prior to Veridium, he held sales, corporate development, and technical roles at Cloudmark (acquired by Proofpoint), Atlantis Computing (acquired by HivelO) and Verizon. He has an MBA and master's degree in computer science from Widener University in Pennsylvania and a bachelor's degree in electrical engineering from the University of Pune in India.



Rajiv can be reached online at [rajiv@dispersive.io](mailto:rajiv@dispersive.io), <https://www.linkedin.com/in/rajiv1p/>, and at our company website: [www.dispersive.io](http://www.dispersive.io).



## 5 Reasons Why Insider Threat Should Be a Security Priority

By David Barroso, Founder & CEO, CounterCraft

Whether it's the purported 36% of employees that can still access to systems or data of an old employer after leaving a job or the 49% that have shared their login details for some reason<sup>1</sup>, inside actors are definitely one of the most concerning threats to your cybersecurity.

Oftentimes, CISOs can overlook insider threat as an issue belonging to another department, such as IT or HR. However, statistics show it is one of the biggest security issues in any organization. The 2022 Cost of Insider Threats: Global Report <sup>2</sup>reveals that insider threat incidents have risen 44% over the past two years, with costs per incident up more than a third to \$15.38 million.

Insider threat is not limited to employees stealing data from your organization. An insider threat needs to include your supply chain, former employees and any individual that has inside information about security processes and practices.

Here are the top reasons why detecting and preventing insider threat should be a priority on your to-do list:

---

<sup>1</sup> <https://www.isdecisions.com/insider-threat-persona-study/>

<sup>2</sup> <https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats>

---

### **1) An insider with trusted access can have high impact with a relatively low execution cost, meaning they can affect organizations of all sizes and industries.**

This is inevitable— organizations need to trust their employees to be able to carry out various tasks. This trust spreads over a number of roles from temporary workers and contract staff to IT administrators, individual contributors, lawyers, auditors, third party contractors, and employees both current and past...all of them can turn into a malicious insider.

### **2) We are even more vulnerable to insider threat as we shift to the cloud.**

According to the 2021 Insider Threat Report by Cybersecurity Insiders<sup>3</sup>, 53% of cybersecurity professionals believe that detecting insider attacks has become harder since shifting towards the cloud. If insider threat was an issue before, as businesses and organizations move to the cloud, it has become even more pressing. Insiders with temporary or permanent access to the cloud environment (IaaS, SaaS, PaaS) can wreak havoc.

### **3) Sensitive data is particularly vulnerable**

Sensitive data is the major target by insider threat actors. Once they access this data, they can sell it, make it public, or use it for blackmail.

### **4) Breaches often occur over an extended period of time.**

Time to detection is a real struggle when it comes to insider threats. The majority (some studies show over 70%) of insider breaches are discovered after months or years. The lost data and intellectual property grows exponentially over time. Organizations need a plan that provides for real-time detection of potential insider threats early on in the threat cycle.

### **5) Internal systems' safety is at risk.**

The access an insider threat has is often wide and deep. They have the potential and the capability to exert wide-ranging sabotage, damaging internal systems, data, and even critical services.

---

<sup>3</sup> <https://www.cybersecurity-insiders.com/portfolio/2021-insider-threat-report-gurucul/>

---

## Recognizing Insider Threats

The first step in preventing insider threat is to notice risk factors. Insider threat has some widely accepted indicators, including employees:

- whose jobs are in danger
- who disagree with a company policy or have exhibited activist behavior
- under financial distress
- leaving the company
- who work at odd hours
- who seem to be experiencing unexplained financial gain
- with suspicious travel patterns

Staying aware of these general indicators of insider threat can help organizations take a big step towards mitigating the effect these insiders can have on your business's security. Knowledge is power, and in this case simply paying attention to the actions of employees can be enough to raise a red flag.

## So, How To Deal With Insider Threats?

Technically speaking, insider threats are a challenge that many security programs aren't able to take on. A user with legitimate access and knowledge of an internal network is simply undetectable by traditional security software standards. Insider threat actors often do not exhibit the malicious patterns and signatures from known threat actors. So, is there a tool to help find them?

In this case, deception technology is one of the best ways to detect threatening internal behaviors. Being able to generate high fidelity alerts is a critical capability when you are swamped in millions of security events per day. Decoy servers and files that act as breadcrumbs are created and deployed within an internal network. These decoys and breadcrumbs are designed to be documents that have no business being accessed. Therefore, by definition, anyone interacting with the decoys is, at minimum, snooping around where they shouldn't be and potentially out to do damage to the company. This means the alerts given by deception technology within an internal network are high fidelity, preserving teams' resources and helping analysts to do their job well.

When it comes to creating the type of decoys and deception "campaigns" that will attract insiders and attackers, the most important factor is that they be realistic. It's always a good idea when evaluating deception technologies to ask about the technology behind the decoys. Are they deployable across multiple endpoints? Can you deploy them externally, on internet-based platforms? Are they high-interaction? Can the activity on them be collected and analyzed in real time? The answers to these questions will reveal how effective the deception technology can be.

---

Shaping a defense against insider threats is possible, and a well-designed deception technology campaign is one of the only ways to achieve it.

### About the Author

Entrepreneur, serial tech inventor, and visionary David Barroso is the CEO and founder of CounterCraft. Prior to founding the business and developing the Cyber Deception Platform, he was instrumental in the set-up of ElevenPaths, Telefónica's flagship cybersecurity business, and led the cybercrime division at a leading pure-play European cybersecurity company. Barroso is recognised globally for his contribution to the industry as a captivating speaker, lecturer and thought leader, regularly found leading the debate about emerging threats at Black Hat and RSA conferences, among many others.

After 15 years in the cybersecurity arena, quantifying cyber risk remains central to Barroso's inclination for research and development. His knack for innovation in response to emerging threats and his exceptional ability to guide stakeholders towards delivering advanced cybercrime, threat intelligence, and active defense solutions underpin his position as founder at CounterCraft.



### David Barroso, Founder & CEO CounterCraft

David Barroso can be reached online at (EMAIL ([dbarroso@countercraftsec.com](mailto:dbarroso@countercraftsec.com)), TWITTER (<https://twitter.com/lostinsecurity>), LinkedIn (<https://www.linkedin.com/in/davidbarroso/>)) and at our company website <https://www.countercraftsec.com/> and Social Media (TWITTER (<https://twitter.com/countercraftsec>), LinkedIn (<https://www.linkedin.com/company/countercraft/>) and YOUTUBE (<https://www.youtube.com/c/CounterCraftSec>))

# IDENTITY AND ACCESS MANAGEMENT



## Poor Identity Management Amplifies Ransomware

By David Mahdi, Chief Strategy Officer and CISO Advisor, Sectigo

While ransomware *is* malware, security leaders must go beyond legacy anti-malware approaches to mitigate risk. Ransomware is a data-centric threat; that is, ransomware preys on corporate data. Cunning and successful ransomware attacks hijack user access with an aim to encrypt sensitive files, stealing data. So, if ransomware is all about the data and the hijacking of user access to get to the data, then the more data a user can access, the more attractive target the user is for the attacker.

Ransomware is a multi-faceted cybersecurity issue, and best practice dictates using email security and antivirus, in addition to other tools to fend it off. Indeed, while these are good best practices, IT leaders need to undergo a crucial perspective change when it comes to ransomware and understand it isn't solely a traditional malware problem. Bad actors want access to data, and they gain access by compromising user accounts, or in other words, by compromising the identity layer of an organization. Without considering the importance of identity and data access, organizations will remain vulnerable to attack.

Yet, organizations and security leaders can't simply lock down identity and data access to prevent ransomware. Typically, IT departments tend to over privilege users to avoid interrupting business. While this approach generally helps day-to-day operations, it's also precisely what allows bad actors who breach the perimeter to run amok throughout the environment. If a highly privileged user and their associated accounts have a lot of access, when compromised, the amount of damage could be catastrophic. Focusing on identity and data security in terms of right-sized access will significantly reduce the attack surface for many threats, including ransomware.

With that in mind, enterprises must focus on establishing and maintaining trust for every single identity in their environment, both human and machine (software, bots, devices, applications, etc.). Otherwise known as identity-first security, the aim is to mitigate the damage from identity and data-centric attacks, such as ransomware.



---

## Right-Sized Access and The Least Privilege Principal

Once trust is established with a digital identity, security leaders must then think about right-sized access. That is what that identity (or user) needs access to in order to fulfill its role requirements. Simply put, the path forward would be to leverage a [“least privileged”](#) approach, as reflected on the website of the U.S. Cybersecurity and Infrastructure Security Agency.

Of course, ransomware attacks can still occur even with a least privilege or right-sized access approach. As such, behavior monitoring that focuses on identities and data is critical. By constantly gauging normal, anomalous, and malicious behavior, security leaders can achieve a better balance of security and business agility. The goal is to ensure that users and machines have the access they need, but that there is a safety net if a security issue occurs (i.e. insider attack, ransomware, or other threats).

## Establishing Digital Trust for Digital Identities

Enterprises need a clear method of verifying and establishing digital trust for all (thousands or hundreds of thousands) types of identities, ensuring only valid and trusted users and machines can log into networks.

One proven way to establish digital trust in identities is by leveraging public key infrastructure (PKI) digital certificates. This technology has been around for decades and remains the most secure way to provide authentication and continuously prove identity, especially as the volume of both human and machine identities continues to rise. Certificates, issued by Certificate Authorities (CAs), provide validation that the user or machine is trusted and secure. PKI uses cryptographic keys to authenticate identities and is much more reliable than passwords or other traditional forms of authentication. When it comes to fending off ransomware, using PKI-based identities can and should act as the baseline for digital identities. Rooting digital identities in digital certificates, for humans and machines, ensures that identity-first security has a strong foundation.

[Gartner, which first coined the concept of identity-first security in 2021](#), describes the approach as putting “identity at the center of security design.” This way of thinking is a major step forward in cybersecurity because it replaces the legacy and dated approach of the walled fortresses pre-pandemic that left organizations feeling secure behind firewalls.

## Connecting Identity-First Security to Data Security

While there are several best practices to employ from an overall identity-first security perspective, let’s focus on data security. Data can take many forms, structured (databases), unstructured (i.e. files) or semi-structured. Regardless of the data type, knowledge about the data, its risk, sensitivity levels, and therefore classification should be established. Understanding the risk and classification levels of data should then be aligned to the overall identity-first security strategy. Ultimately, it will help security leaders understand what kind of data their users and machines have access to. Leveraging data access governance (DAG) tools are one approach to help close the data-access gap. However, DAG tools are

---

only as good as the trust in identities that they leverage to control corporate data access. As such, security leaders must start with establishing trust in digital identities, as we discussed above.

## Identity-first Security Is the Most Important Line of Defense for Ransomware Attacks

It's impossible to stop all cyberattacks, regardless of how much time, money, or labor enterprises pour into security. However, establishing digital trust for every identity – both human and machine – in company environment and ensuring right-sized access can limit the damage done by the attackers who break through.

Going forward when we think about ransomware, we need to recognize that at its core it is an identity and data access issue. Ransomware wants access to data, and it will typically compromise accounts/user identities to gain access to that data. So, rather than worrying about just malware detection, security and business leaders looking to improve their chances of coming out of a ransomware attack unscathed should establish strong identity-first and data security strategies. This includes knowing where all the sensitive data resides, and monitoring user and machine access to that data in order to mitigate ransomware and other cunning cybersecurity attacks.

### About the Author

David Mahdi is the Chief Strategy Officer and CISO Advisor of Sectigo. In his role, David leads the company's overall strategy, direction, and M&A efforts to expand its leadership in the digital trust space. With 20+ years of experience in IT security, most recently serving as Vice President and Analyst in Security and Privacy at Gartner, David has helped large organizations tackle digital transformation projects in the digital trust, identity, cryptography, and cybersecurity spaces.

David can be reached online at (David.mahdi@sectigo.com, @davemahdi, linkedin.com/in/dmahdi.) and at our company website: <https://sectigo.com/>





## Prevent Browser-In-The-Browser Phishing Attacks by Removing Human Input Error

**How companies can combat the threat of new browser-in-the-browser phishing attacks by taking back control of network access and password distribution.**

**By Julia O'Toole, founder and CEO of MyCena Security Solutions**

In 2022, the greatest threat vector is phishing attacks, which are responsible for more than 80% of all breaches to individuals and organisations. These are a result of misused or stolen passwords; hackers, despite their name, don't "hack in", but instead log in using credentials phished via social engineering. This potential for an error in judgement on the individual's side can have great ramifications for whole organisations.

Cyber attackers are also getting smarter in how they breach organisations. In mid-March 2022, a novel phishing technique called browser-in-the-browser (BitB) attacking was uncovered by an Infosec researcher, which uses simulated browser windows and other authentication service providers to steal login credentials.

BitB attacks act as an extension to existing clickjacking or user-interface redressing that alters the appearance of browsers and web pages to trick users to bypass security controls. With this technique, an entirely fabricated replica is created – a user thinks they are seeing the real popup window, but it's just faked within the page.

---

“Very few people would notice the slight differences between the two,” according to the report. “Once landed on the attacker-owned website, the user will be at ease as they type their credentials away on what appears to be the legitimate website.”

## Remove Danger by Retaking Control

It's up to businesses to remove the danger presented by BitB phishing attacks by ensuring that employees can no longer create, view or type passwords to access the company files, apps and systems. This amounts to taking back access control and removing the risks of human error from the network access process.

To the untrained eye, which is likely to be the majority of workers, these types of phishing attacks are dangerous yet impossible to spot. All it takes is for one unsuspecting employee to make a mistake and it compromises the entire network.

Attacks like these aren't for quick cash payouts. Actors will sit inside your system and wait to cause the most damage. All the while, the user continues working without realising they've unwittingly given their credentials away.

This type of attack has been utilised in the past. In 2020, cybercriminals used similar BitB techniques on the video game digital distribution service Steam to gain access to consumer credentials. Whilst this may cause damage to individuals, what we're seeing now is a more aggressive assault on an organisational level. For the safety of your business, it's time to take back responsibility and start controlling your own access.

## Password Managers are Not the Solution

While some have recommended using a password manager and Single Sign-On tools to circumvent the problem, as they automatically input passwords without falling for the replica windows, this still presents major issues.

Centralising multiple passwords behind a manager's master password does nothing to prevent access fraud. It only centralises access information for hackers in a breach scenario. This was the case of the Lapsus\$ group who, after infiltrating Okta's network, were able to easily find an Excel document filled with LastPass administrators' passwords to access Okta's customers.

Password managers and Single Sign-on tools may provide a surface layer of convenience for users, but in the event of a breach also offer their company's keys to the kingdom on a silver platter. Instead, access segmentation and encrypted passwords distribution is a more effective solution that completely removes the potential threat of human error or fraud from the equation and safeguards access integrity.

Additionally, businesses might see the appeal in doubling down with multi-factor authentication (MFA) methods as a precaution. But their initial loss of access control means that not even MFA can guarantee the legitimacy or integrity of access. Cyber attackers have found many ways to infiltrate those as we've

---

seen recently through known vulnerabilities in MFA protocols. Relying on MFA merely postpones an inevitable breach of access, rather than securing your cybersecurity and cyber resilience outright.

## Relying on Traditional Approaches is no longer enough

Cyber attackers are more intelligent and relentless when it comes to modern-day phishing techniques. Returning access control, segmentation and security to the organisational side ensures that employees no longer need to create, see, or type passwords. Using a safe path from receiving, storing to using encrypted credentials, means they don't have to worry about leaking them accidentally to cyber actors.

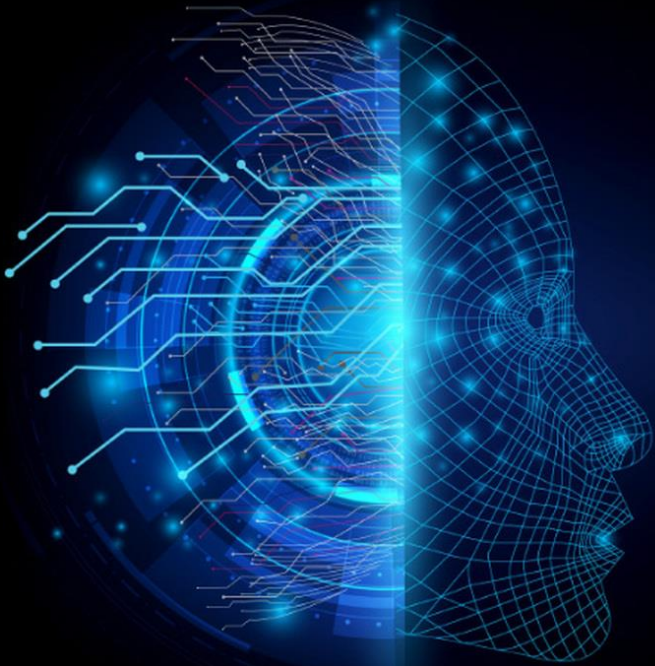
By segmenting access across their entire digital infrastructure, and distributing unique encrypted passwords directly to their employees, businesses remove the potential for unauthorised password sharing, theft or phishing. Any breach can be contained to one system, meaning that in the event of another BitB attack, the rest of your network remains safe from harm. Through this, organisations can stay one step ahead of ransomware threats.

### About the Author

Julia O'Toole, founder and CEO of MyCena Security Solutions, a breakthrough solution to manage, distribute and secure digital access. An inventor and author of several patents, Julia uses maths, neuroscience and technology to research and design simple yet innovative solutions for complex problems. Julia's areas of research and expertise include cybersecurity, collaboration and search. Julia founded MyCena in 2016, which has since become a market leader in segmented access management and safe password distribution. With its ground-breaking patented security system, MyCena protects companies from the risks of password error, fraud and phishing, loss of command and control, ransomware, and supply chain cyberattacks.



Julia can be reached online at [julia@mycena.co](mailto:julia@mycena.co) or [linkedin.com/in/juliaotoole](https://www.linkedin.com/in/juliaotoole) and at our company website <http://www.mycena.co>



# Cyber Threat **INTELLIGENCE**

## Threat Intelligence: Cyber and Electromagnetic Activities (CEMA) with Software-Defined Radio (SDR)

By Brendon McHugh, FAE & Technical Writer, Per Vices

Under the umbrella term Cyber and Electromagnetic Activities (CEMA), a number of military operations must be synchronized and coordinated. This includes cyberspace offensive and defensive operations, electronic warfare (EW) attacks, EW protection, and EW support, as well as spectrum monitoring and management operation. To maintain strategic advantages and ensure mission success, multi-operational domains in space, air, land, and maritime all need to be coordinated. Adversaries continue to seek new opportunities to exploit the domains of the cyber and the electromagnetic spectrum and the associated infrastructure, particularly as there is a proliferation of embedded electronics on the battlefield.

In this article, we first discuss CEMA and explain the inner workings of the organization's various operations and objectives, as well as challenges often encountered. Following this, we discuss how software-defined radio (SDR) is paramount to the present and future CEMA operations, as they are able to assist with various cyberspace, EW, and spectrum monitoring capabilities and solve many of the challenges outlined.

### Fundamentals of Cyber and Electromagnetic Activities (CEMA)

Broadly speaking, CEMA consists of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO), as shown in *Figure 1* below. CEMA operations are used by military forces to seize, preserve, and exploit dominance over hostile adversaries in both cyberspace and the electromagnetic spectrum (EMS). Along with this, CEMA is used for denying and degrading adversary use of their own CEMA capabilities and thereby protecting the CEMA organization and related systems.

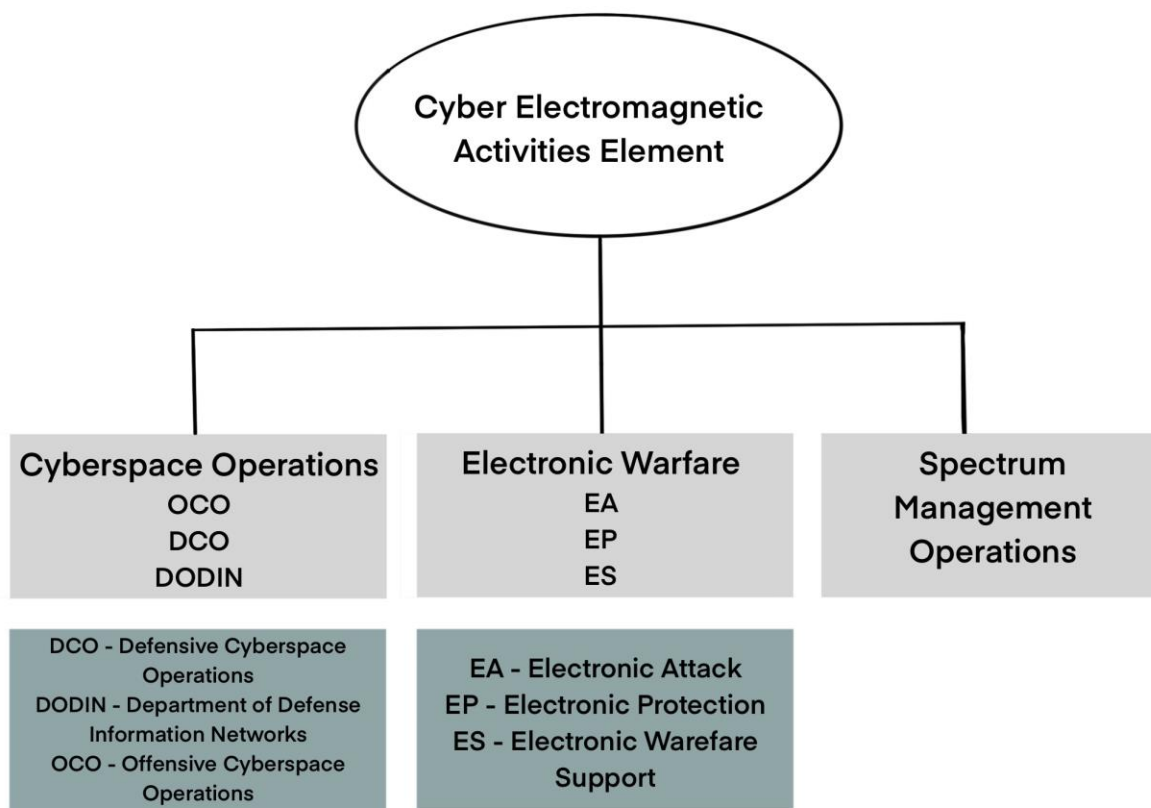


Figure 1: CEMA operations (adopted from <https://irp.fas.org/doddir/army/fm3-38.pdf>)

The key to the entire CEMA operation is integration and synchronization. Integration is the arrangement of various military forces and their respective capabilities in order to create a force that operates by engaging as a whole— that is integration of space, maritime, land, and air forces. Just as important is synchronization. This consists of the arrangement of military actions in time, space, and purpose to produce maximum combat capability and power at a decisive place and time.

The purpose of CEMA is to provide military forces with capabilities to increase spectrum awareness, situational awareness, and overall survivability. Examples of enhanced capabilities by EW include the use of expendables such as flares (i.e. redirecting heat-seeking missiles), electronic countermeasures against radio-controlled improvised explosive devices (IEDs), and jamming to disable an enemy’s equipment or capability. On the other hand, SMO can be used for mitigating electromagnetic interference in systems from the friendly use of EW. Lastly, CO ensures the secure and uninterrupted flow of data and information that allows military forces to respond rapidly to a changing battlefield and synchronize with other joint capabilities.

---

## Cyberspace Operations and Challenges

Cyberspace is a worldwide information environment consisting of interdependent networks of information technology (IT) infrastructures and local data/traffic users, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers—both wireless and wired. High-performance software-defined radios (SDR) also fall into this category, which is essentially a device that incorporates all the preceding technologies in one box.

Within CEMA, cyberspace operations (CO) consist of three functions: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defence (DoD) information network operations (DODIN). Important for OCO operations is conducting cyberspace attacks. These consist of actions that create various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial of service that is hidden or that manifests in the physical domain of a network.

Unique to cyberspace is how interrelated it is to the space domain, primarily because of how satellites play a critical role in military telecommunications and networks, particularly for the vast number of PNT (position, navigation, and timing) requirements. Moreover, the relationship between cyberspace and the space domain (i.e. military-band satellite communications) activities within the electronic magnetic spectrum (EMS) greatly expands and complicates the operational framework, recasting a concentrated physical battlefield into a global battlefield. For example, computer viruses or malware executed in cyberspace may reach their intended target, but also blindly strike and wreak havoc on subsystems relied upon by other allied forces around the world. These interrelationships are important considerations when planning for CEMA on a global scale.

Numerous challenges within the cyberspace domain exist, particularly when it comes to exploiting network protocol stacks. Often communications are based on the Open System Interconnection (OSI) model, where often the internet protocol (IP) is combined with Transmission Control Protocol (TCP) to form TCP/IP. This system is designed for packet exchange of critical data/information between CEMA operations but is one of the causes of flooding and other attacks.

## Electronic Warfare and Challenges

EW is an activity that is integrated into operations through CEMA and consists primarily of three functions: electronic attack (EA), electronic protection (EP), and electronic warfare support (EWS). *Figure 2* shows the general functions of EW. These EW functions are carried out and applied from the air, land, sea, space, and cyberspace by manned (i.e. surveillance aircraft) and unmanned (i.e. drones), or unattended systems (i.e. autonomous UAVs/sensors).

EW capabilities are now becoming important for how a battle is fought and won, as these capabilities are becoming increasingly important for how commanders shape operational environments to their advantage. For example, commanders may order that EW be used to establish favorable conditions for



---

cyberspace operations (CO) by stimulating adversary networked sensors, denying wireless networks, or other related actions.

Other examples of offensive EA include jamming enemy radar or electronic command and control (C2) systems. Using electronic deception to confuse enemy intelligence, surveillance, and reconnaissance systems. Using directed-energy weapons to disable an enemy's equipment or capability.

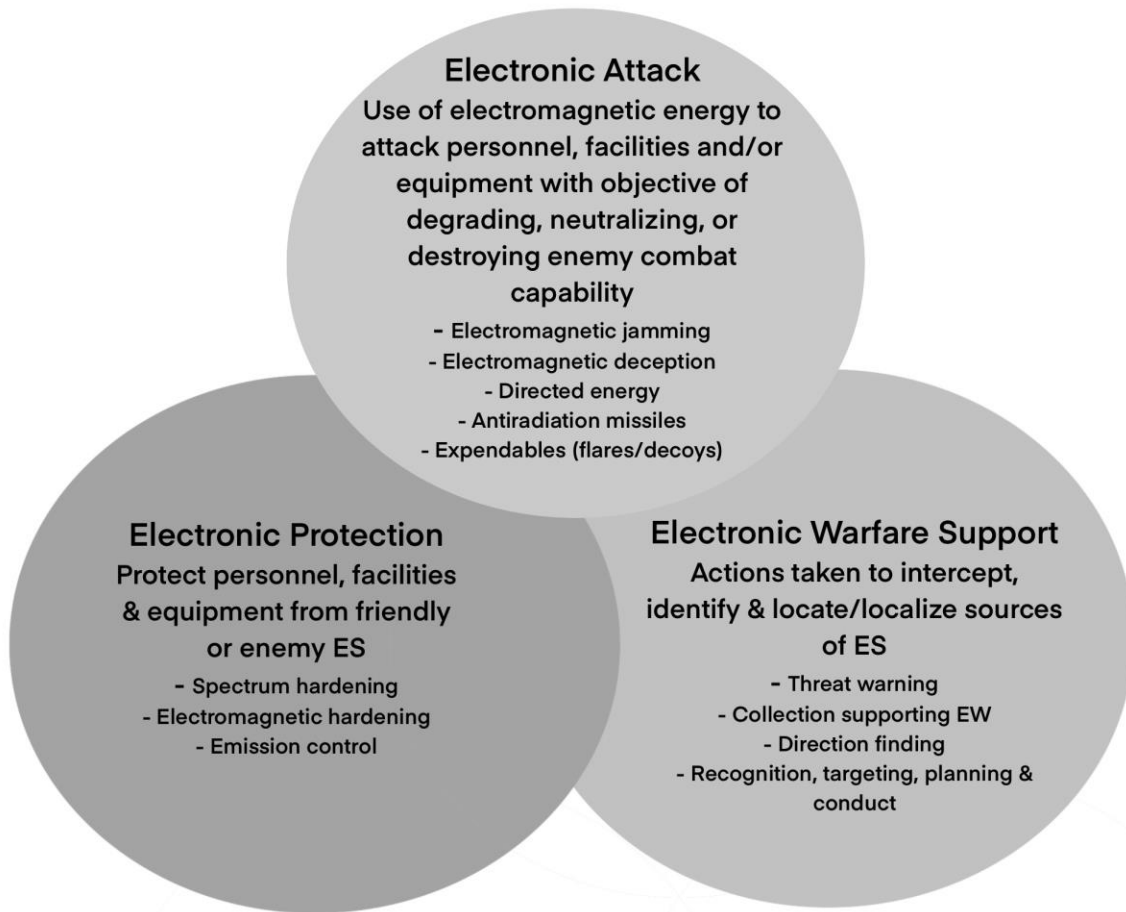


Figure 2: EW functionality (Adopted from <https://irp.fas.org/doddir/army/fm3-38.pdf>)

Spectrum management is often classified as part of electronic protection as well. Swift coordination is required for such tasks as deconfliction of spectrum resources allocated to different aspects of military forces. For instance, spectrum managers are often involved directly in planning EW operations to ensure that there's no electromagnetic interference during an EW attack mission.

Finally, the US Department of the Army<sup>1</sup> states that “electronic warfare support (EWS) is a division of electronic warfare involving actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated

---

electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.” In other words, this involves the geolocation of RF emitter sources and establishing a plan of attack.

With the advance in computing and RF technologies, has come a number of challenges with detecting adversary emitter sources. This includes the ability of fast frequency hopping techniques to avoid detection of enemy transmission, various beam focusing/steering technologies, as well as the design of hard-to-detect waveforms that last in very short durations.

## Spectrum Management and Challenges

The importance of the electromagnetic spectrum (EMS) and its relationship to the operational capabilities of the military is the focus of the electromagnetic spectrum operations (EMSO). Generally, the EMSO overlaps largely with electronic warfare (EW) and signals intelligence (SIGINT) operations. Within the EMSO organization are the interrelated functions of spectrum management, frequency band assignment, host-nation coordination, and various policies enabling planning, management, and execution of operations within the electromagnetic operational environment for all phases of a mission. Ultimately, the EMSO and its spectrum managers are responsible for coordinating EMS access among civil, joint, and multinational partners throughout the operational environment.

As discussed, the spectrum manager plays an integral part in all EW planning, who are able to inform commanders of spectrum conflicts initiated by friendly systems for personnel protection, enemy exploitation, or enemy denial. The advent of common user “jammers” has made this awareness and planning critical for the spectrum manager. Moreover, the spectrum manager coordinates with satellite managers to maintain awareness of frequency channels being used by satellite communications systems during uplink/downlinking. Thus, it is largely in the hands of the satellite manager to generate and process satellite access requests for all very high frequency (VHF), ultra-high frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF) satellite systems which are important for military communications.

As mentioned, there is a lot of overlap between EW and EMSO. For instance, when the EMSO detects an adversary signal of interest, such as a radar jammer, EW can proceed to geolocate the enemy emission source. Then a plan of EA can occur, where EMSO processes an access request to use anti-radiation missiles to suppress the enemy radar jammer (these weapons use radiated energy emitted from a target as the mechanism for guidance onto the target).

Challenges in the management of the spectrum are often down to it being extremely contested and congested on the battlefield. This includes adversaries who aggressively launch electronic attacks and cyber technologies that erode the ability to use the spectrum for military operations, combined with the global wireless broadband and commercial satellite industry continuously attempting to reallocate spectrum from defense and satisfy consumer demands for greater mobility and data connectivity. Thus

---

the challenges faced by all RF technologies used in military missions— from radar to satellite to tactical radios— will be to ensure efficiency, adaptability, and flexibility in using spectrum resources.

## Putting it all together: Software Defined Radio (SDR) for CEMA

High-performance software-defined radio (SDR) is a technology that is at the heart of CEMA operations. This device generally consists of a radio front-end (RFE) and digital back end. The RFE is responsible for the actual tuning of RF frequencies used in transmit (Tx) and receive (Rx) functionalities. The RFE terminates at SMA connectors which can be connected to various antenna systems for communications between satellites, maritime vessels, aircraft, drone/UAV control systems, radar, and various other CEMA operations. On the other end, the digital back end, often with an embedded field-programmable array (FPGA) consists of a means to conduct various DSP as well as packetize RF data into transportable Ethernet packets over networks in cyberspace.

Size, weight, and power (SWaP) are also important characteristics of SDRs used in various applications in CEMA. Fortunately, these SDR devices can be tailored to suit the requirements of various operations. For instance, an SDR used in a satellite payload has very different requirements than an SDR used in a radar system.

The software part of an SDR stems from its ability to be reconfigured for tuning to center frequencies, analyzing different bandwidths, modulating/demodulating signals and data, and generating and transmitting new waveforms. These features help to solve challenges related to EW and EMSO, whereby the contested and congested spectrum can be navigated using the flexibility and adaptability inherent to SDR.

SDRs are also able to solve many of the issues encountered in cyberspace operations. For starters, issues related to cyberspace attacks, such as flooding or replay attacks, can be mitigated with various security features embedded into the SDRs FPGA used for de-framing packets. This can include multi-factor authentication algorithms, cryptographic schemes and a means to alert of various attacks.

Mitigation of spectrum management challenges is also possible with SDR. This includes evaluating and mitigating electromagnetic environmental effects, managing frequency records, and databases, deconflicting frequencies, frequency interference resolution, allotting frequencies, and EW coordination to ensure EM-dependent systems operate as intended. SDRs are often combined with storage solutions on a battlefield in order to be part of the CEMA network or cloud infrastructure.

Particularly important for processing signal data to determine timing, location (i.e. direction finding), or other RF emitter source information. Through an SDR's high-performance radio front end (RFE), these systems are able to detect weak signals in a crowded spectrum (by having high instantaneous bandwidth, exceptional noise figures, and excellent dynamic range in the receiver chains). Moreover, elusive enemy

signals using frequency hopping spread spectrum (FHSS) can be detected when using the highest instantaneous bandwidth SDRs, such as Per Vices Cyan, as shown in *Figure 3*. Swept mode operation or having a high instantaneous bandwidth ensures that enemy emitters will not fall out of band when using FHSS.

SDRs also provide timestamped data that make it possible for algorithms used in direction finding, particularly those related to time-difference of arrival (TDOA). As well, when using other direction-finding techniques, such as phase difference or interferometric measurements, high-performance SDRs have highly phase-coherent channels to ensure these measurements are possible.



*Figure 3: Cyan SDR with the highest instantaneous bandwidth*

## Conclusion

CEMA is a continuously evolving means to integrate and synchronize the various operations in cyberspace, EW as well as spectrum management. SDR is fast becoming an integral part of these operations, due to its ability to combat a number of challenges related to CEMA.

Per Vices has extensive experience in developing, building, and integrating SDR for CEMA operations. To find out how we can help you on your next project, contact [solutions@pervices.com](mailto:solutions@pervices.com).

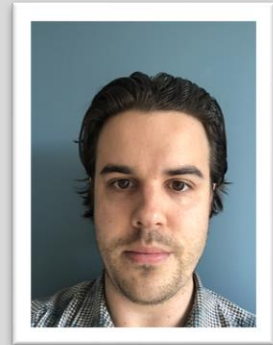
## References:

1. Cyber Electromagnetic Activities, Department of the Army Headquarters (2014). <https://irp.fas.org/doddir/army/fm3-38.pdf>

---

### About the Author

Brendon McHugh is the Field Application Engineer and Technical Writer at Per Vices Corporation. Per Vices has extensive experience in developing, building, and integrating software defined radios for CEMA operations. Brendon is responsible for assisting current and prospective clients in configuring the right SDR solutions for their unique needs, and possesses a degree in Theoretical and Mathematical Physics from the University of Toronto.



Brendon can be reached online at [solutions@pervices.com](mailto:solutions@pervices.com) and at our company website <https://www.pervices.com/>



# Cyber Security and Cloud Computing in the New Era of Remote Working

Emerging trends and their security implications

By Enrique Gomez - COO GAT Labs

In my experience there have been, perhaps, three major trends with significant security implications for corporate data in the last decade.

The first is the increased practice of corporations moving their data to the cloud. This is particularly the case with enterprises offloading their office environments to cloud-based solutions. The second is the involvement of more and more state actors in the business of hacking enterprises. This brings an increased level of sophistication and boldness to the perpetrators, who in most cases act with a sense of impunity within their own State. The third trend has yet to fully play out, but it's fair to say that COVID-19 has forever changed the workplace landscape, and far more knowledge workers are likely to work from home, off the local area network (LAN), in future.

If we look at the movement of the office environment to the cloud, we can see the many advantages it offers enterprises. Perhaps most notably is its cost (reduced capital spend and labor) and increased

---

security. Few, if any, enterprises would have security teams with either the size or requisite skills needed. However, what remote work offers in terms of increased data security, it takes away in terms of user oversight (user audit and observation).

The [US Bureau of Labor Statistics](#) estimates that the enhanced need for security measures for remote workers will contribute to the projected employment of information security analysts, which is expected to rise by one third between 2020 and 2030.

### User oversight in the LAN vs the Cloud

In the now “old” model, where all users were on the LAN (or required to backhaul through it) and all traffic was forced to flow to local servers or through local firewalls, the levels of user audit, observation and accountability could be very high.

However, the cloud’s ‘login from anywhere on any device’ model means such oversight has been lost for enterprises. The challenge in the modern era is to give these enterprises the same level of security and oversight they had when users were on the LAN, but in the Cloud.

Whether on the LAN or in the Cloud, I believe the user has always been the weak point in any attack. That’s why an enterprise’s ability to monitor and protect the user was, and always will be, key to protecting corporate data.

### How to effectively protect Users in the Cloud

According to [Statista](#), 60% of all corporate data is stored in the cloud. This figure has doubled since 2015. With this in mind, protecting your corporate data has never been more important.

Furthermore, a January 2022 [Insight Report](#) by the World Economic Forum found that 39% of organizations have been affected by a third-party cyber incident in the past two years.

Today’s main cloud providers typically offer rich application programming interface (API) sets that allow third parties to build auditing and reporting tools to boost the cloud reporting capabilities of enterprises. These tools provide a first line of security defense and allow system administrators to understand issues such as file sharing and email flows more effectively. Some tools even offer remedial actions such as revoking external file shares or bulk deleting spam email.

---

These solutions work well for primary data stores. However, as companies use more cloud services, rich corporate data becomes more dispersed across different platforms and cloud service providers. Since each platform has its own unique reporting APIs, where enterprises utilize a mix of different platforms, messaging, customer relationship management (CRM) and financial systems, I believe using a third-party cloud security tool is no longer sufficient.

I have come to the conclusion that no third-party tool has APIs for all the cloud platforms available. In fact, it is probably not even possible to develop such a tool in a practical sense. Even if there were only one could, it would be a foolhardy task as the frequency of API changes alone can be challenging for even one or two platforms.

### **Get the Same Level of User Oversight you had on the LAN via the Browser**

Nearly every current cloud platform shares one thing in common: they're accessed through the browser. While they may sit in thousands of locations and have tens of thousands of APIs, access to data happens through the browser for the vast majority of enterprise users. The key is to make the browser environment act like it was permanently on the 'LAN'.

As a starting point, let us take a closer look at the advantages the browser offers as a tool for accessing data. Browsers significantly reduce the attack surface and tend to be more secure than PC applications in general. PCs present multiple opportunities to access local data and to network to other nodes, once compromised. The browser, on the other hand, presents some kind of a wall that needs to be jumped to get to the cloud data, particularly when access is protected with 2FA (Two Factor Authentication). Keyboard scraping is easy, so passwords are practically redundant as a means of protection.

To give enterprises the same level of LAN protection and oversight in the cloud, the approach we take at GAT Labs, for instance, is to protect the USER in the browser environment. In effect, we get the browser to act as if it were on the enterprise's private LAN.

Developing for the browser has many advantages. Apart from the reduced number of platforms you have to develop for 'real time', protection can be achieved, something even APIs don't offer.

Monitoring what happens in the active tab allows us to alert on or block important data like company credit card or bank account numbers in real time, except on allowed sites. This, in turn, improves your enterprise's data loss prevention (DLP) in the cloud. It has the added advantage of being able to account for all your users time in the browser. This greatly improves capacity planning and productivity reporting.



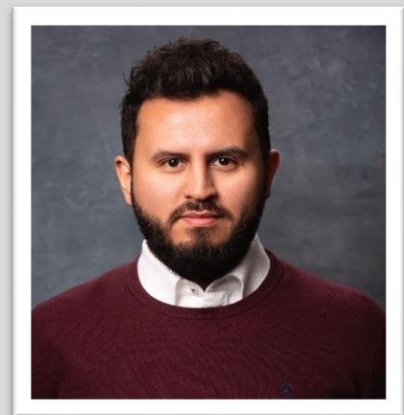
---

In the case of our own tools, we can even tell, using AI, if the user typing on the keyboard is not the user whose account is logged in, thus enabling an on-going 3-factor authentication shield in the browser. Phishing detection is also available.

These and many more security features greatly help enterprises increase the protection of the end user, who in my opinion will continue to remain the weakest security link.

### About the Author

Enrique Gomez is the Chief Operating Officer (COO) at [GAT Labs](#), an Irish-headquartered specialized general audit tool developer. Enrique has an MBA in International Marketing from ULA, Mexico. He joined GAT Labs in 2014, where he is responsible for the implementation of operational processes and ensuring employee alignment towards the organization's goals and key targets. When Enrique joined GAT Labs, there was a noticeable gap in the market for innovation within the cloud security and auditing industry. Google Workspace was quickly identified as the platform on which GAT should develop and test technologies and products. A new company process structure was subsequently implemented, with technological software introduced to better manage human resources. Outside the office, Enrique is an avid traveler. In the past, he has snowboarded in the Andes and slept under the stars of the Sahara Desert. He attributes his ability to travel to his penchant for hard work and his curious nature – characteristics he carries over into his role at GAT Labs.



Enrique can be reached online at [enrique@generalaudittool.com](mailto:enrique@generalaudittool.com) and at our company website, [gatlabs.com](http://gatlabs.com)



## Control the Uncontrollable, The Path to Supply Chain Security

By Ed Chandler, AE and Cybersecurity Lead, TÜV SÜD America

When I was initially asked to write this article, I didn't hesitate as to what the article should be about. My mind immediately jumped to supply chain security. For any organization, it is hard enough to protect information that is within their own walls, but can you protect your organization in your Supplier's walls? Throughout this article, I will cover the history of cyber security compliance, security obligations, new methods of security, and adding secure products to your final solution.

When I think about the history of cyber security, I immediately think about how computers have made a difference in everyone's lives, both at home and work. The invention of the computer is probably the most profound change in our lives, and throughout my life I have seen organizations with a minimal number of computers all the way through to multiple computers per employee, whether they are in the office or on an assembly line. Additionally, even mobile employees are utilizing computers in more ways every day. There is no question of the Return on Investment or "ROI" of adding technology, but there is also risk associated with it, and people have not historically protected this information. Due to the constant push for ROI, IT organizations look for ways to justify securing budget from within their organization. And it can be a struggle for CISOs to obtain additional budget to protect the company, even with the constant expansion of their threat landscapes.

In the past year our supply chain has been on high alert, and we have learned how brittle it is. Now, while most of the disruption is directly or indirectly related to COVID-19, there are many other disruptions that can impact the supply chain and the final products that we use in our everyday lives. However, the

---

question is how do you protect yourself against threats outside of your organization's walls? There are solutions available, and the good news is that these are not new concepts, but some industries have yet to adopt them. Let's look at how some industries have minimized their risk traditionally and presently.

Organizations that accepted credit cards at high volumes were amongst the first targets of cyber-attacks. This was due to the ease of monetizing a credit card number and selling it on the Darknet. The initial response by the card brands was to create their own cyber security standards. The challenge to a program like this was that it became difficult for merchants to meet the requirements of, in some cases, four different card brands. In some circumstances it meant that even if they met the requirements for one it would automatically make them non-compliant with another. The confusion prompted the creation of the PCI-SSC (Payment Card Information Security Standards Council), which led to the establishment of PCI-DSS (Payment Card Information Data Security Standard). This produced concise and clear requirements for those who choose to accept credit cards as payment. The initial versions of this standard were snapshots in time, but due to an evolving threat base over time the assessments evolved into an ongoing management of security. Additionally, the card brands' increased ability to locate fraud faster made it more difficult for stolen cards to be used. And as it became increasingly more difficult to obtain cards, values dropped, and as cards were being quickly shutdown, these once highly sought-after targets became less lucrative. Many of you are probably thinking, this isn't really about the supply chain, however, it is a fantastic case study of how organizations were able to secure partners outside of their walls.

Supplier's trust, or lack thereof, can be one of the most damaging aspects to any organization. An example of this is Target. Target had a good cyber security program but opened their firewall for a HVAC vendor who did not have them same kind of security controls in place. This led to one of the largest cyber breaches in history. However, the good that came out of this was the emphasis on securing your vendors.

The question is how did we get to where we are today in the manufacturing industry? A lot of it has to do with the historical relationship between suppliers and customers. Our customers consistently expect you to build efficiencies repeatedly to minimize cost, while improving quality and security over time. This includes on-time delivery, concepts such as "Just in Time Manufacturing", and automation. All of these are great concepts and can create the efficiencies your customers are looking for to minimize costs. However, until about three years ago, cyber security was not even a thought for most of the manufacturing industry. The most common objection within the sector was, "we don't have information that is valuable". While it is true many in this industry do not have Personal Information, Health Information, or even Credit Card Data, criminals have learned organizations are willing to rather than cause interruptions to their customers. Companies are beginning to realize that breaches not only affect themselves, but also their customers upstream which can be Millions of Dollars a minute and result in contractual fines and/or a loss of future business.

How do these organizations ensure that their supply chain is secure today? There are a few ways in which companies push requirements to their suppliers. The most common being questionnaires, where we ask our suppliers to complete these to measure and minimize risk. These questionnaires can be great ways to communicate the minimum-security requirements, however they are not the best at enforcement. Many times, organizations will just have their sales teams fill out the questionnaires, and

---

the chances of an organization checking “No” to these are slim to none. Thus, leading to potential operational issues, and distrust with your suppliers.

Another common way organizations secure their supply chain is through conducting supplier audits. This will ensure that their suppliers are meeting the minimum requirements to continue conducting business together. While this enforces trust between you and your supplier, the problem is that either the cost is high, not only to you, but also to your supplier leading to push back and ultimately you are only touching a subset of your suppliers. Additionally, it is important not to overload your suppliers as this can have a negative impact.

The above two scenarios are the same problem that the Card Brands ran into when trying to implement cybersecurity measures to their merchant network. So, learning from history we can look at what other sectors are doing to build the foundation of a framework.

ISO 27001 is the most widely used Information Security Framework in the world, and for good reason. It allows organizations to demonstrate they have the basic pillars and buy-in from upper management to maintain information integrity. This can be used in place of multiple supplier audits minimizing the overhead of your supplier. Not only that, but it also allows you to share a globally accepted accredited certificate to your customers rather than a report. Finally, this is a language many within the manufacturing industry already speak. Such as:

- Internal Audit
- Management Review
- Corrective Action

These are all things that our industry is used to speaking about, and part of their everyday life, through their ISO 9001 certification. As cybersecurity professionals, we consistently strive to find ways to tie security into other parts of the organization, and by doing so will provide the coverage we dream about. By utilizing a framework like ISO 27001 it allows security teams to collaborate with teams such as quality, operations, management as well as create efficiencies through integration of internal audits, and building consistent corrective actions as a team to gain buy-in from the entire organization. Additionally, with this framework you can add in additional compliance requirements, and it can be easily cross-walked to other common frameworks such as NIST 800-171, and COBIT. Those are widely used successful frameworks, however unlike ISO 27001 they cannot provide a trusted accredited certificate.

As the market develops, TÜV SÜD is starting to see requests for standards around Supply Chain (ISO 28000) and Business Continuity (ISO 22301). This is to ensure that organizations can continuously run even in the chance of disruption, and we anticipate that these standards will continue to grow as we find more flaws in the supply chain.

As each industry is unique so are their desires for supplier security, this has led to industry specific standards across the Supply Chain. These are based upon the two major markets, and I anticipate this will continue to be replicated by other industries throughout their supply chains.

---

Automotive is probably the most forward thinking of all manufacturing segments. The industry is notorious for strict supplier guidelines with very heavy penalties for delayed product, and non-compliance. Unlike others, they have implemented requirements both for enterprise security as well as the security of the products being supplied themselves. This has led to many manufacturers looking at how they handle data and securely code new products.

The idea of product security is new for many. There are standards coming out daily, such as NIST 8259 for IoT, and IEC 62443 for Industrial Control Systems. However, automotive continues to impress me with their forward thinking around security. Recently, ISO 21434 has come out to ensure that suppliers are creating a secure lifecycle for their products. This has forced the industry to look for outside help, provide security training internally, and plan how they will provide the minimum level of security to their customers products. This has truly revolutionized the concept of supply chain security as it added a new dimension.

While not the entire automotive industry has adopted third-party audits, the German OEMs worked to build TISAX (Trusted Information Security Assessment Exchange) through their partner Verband Der Automobileindustrie (VDA). This requirement is being pushed through their entire supply chain and is actually a subset of the ISO 27001 requirements. The main purpose of this standard is to ensure information, data, and prototype security. This was initially adopted by European base suppliers, and it has started to gain momentum in the Americas and Asia. The impact of the requirement is that someone who wants to conduct business with one of the German OEMs will not be able to provide a bid for the work until they receive their TISAX Labels.

One area we continuously overlook is the importance of planning for a worst-case scenario. An incident response plan is critical for any organization. This is amplified with the current state of ransomware attacks, which can create mass disruption if not properly mitigated. Ransomware can be easily avoided, but continuously is not taken seriously. However, we consistently create budgets to pay attackers rather than invest in our business to prevent or minimize the damage of these attacks. If you think about it, by paying the attacker, we only promote the attacks. Additionally, we train for worst case scenarios our entire lives starting in kindergarten with fire drills, tornado drills, and even dangerous person exercises. However, many organizations have never considered running a tabletop exercise to test their incident response program. Leading to the first time they test it is during a live scenario, setting anyone up for failure.

As professionals, we should always have our customer's best interest at heart, and we should provide them the same security that we expect ourselves. Although we continue to look for a silver bullet usually in the technology space, the reality is that there is none and only a multi-pronged approach will minimize your risk. The smartest CISOs I have spoken with are of the assumption that it isn't an if, but a when it will happen.

---

## Conclusion

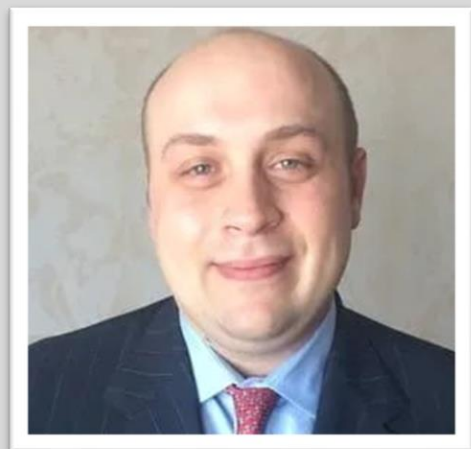
- To adopt a framework that will allow you to cross borders in creation of policies for both you and your suppliers,
- History repeats itself so look at others prior outcomes when putting your solution together and use what has already been learned,
- Implement and test your incident response program.

### About the Author

Ed Chandler, AE and Cybersecurity Lead, TÜV SÜD America.

Ed Chandler has worked in the technology field since 2010, and Cybersecurity since 2011. During this time, he has had great success working for organizations such as Trustwave, Great Bay Software, and Virtual Forge. In Cybersecurity he has had the opportunity to work with organizations in sectors such as: Financial Services, Education, Government, Healthcare, and Manufacturing.

Ed can be reached online at [Edward.Chandler@tuvsud.com](mailto:Edward.Chandler@tuvsud.com) and at our company website <http://www.tuvsud.com/en-us/contact-us>





## Defend Your Castle with Zero Trust

**Protecting yourself, your company and your data from the vulnerabilities of connectivity is no longer an option, but an imperative.**

**By Peter Oggel, Chief Technology Officer, Irdeto**

In medieval times, rulers would dig a deep moat around their castle walls. At night, the drawbridge would be raised, and anyone inside the castle walls would be protected effectively from intruders. Perimeter security on your company's systems and connected devices is a bit like those moats. It's not going to protect you from modern hackers who can sneak into your system undetected, or can disguise themselves as your employees. That's why a Zero Trust Architecture is the only way to protect anything that is connected to the internet – whether your existing internal systems or your new connected devices.

Protecting yourself, your company and your data from the vulnerabilities of connectivity is no longer an option, but an imperative. The ever-growing number and intensity of cyberattacks makes it mandatory for organizations to take a hard stance: every person, every application and every device must require constant verification and authorization to enter. Start to finish, at every step of the process.

---

## Trust no one and nothing

The increasing sophistication of cyberattacks compels companies to take a much deeper look at who's in their systems, and what they're doing there. This starts with multi-factor authentication and levels of authorization that determine what information the person can access, once identified (segregation of duty). Before any type of connected communication is permitted within your system, you must be able to identify who the user is, what they're allowed to access, and how they're allowed to access it.

Next, you must enforce strict controls to manage breaches when they occur. Perhaps most importantly, only constant and automated monitoring and adjustment of your security posture will help you stay ahead of the rapidly adapting hacker behavior. As hackers evolve their attack techniques, your security systems must adapt alongside them in a fully automated fashion.

## Protect every device, everywhere

How big is the scope? Pretty big. Basically, any device that has an IP address needs to be protected with Zero Trust Architectures. For example, non-connected cars can safely and effectively use IT technologies to enable communication between the driver, the controls and the engine. The computer 'knows' that all the signals are coming from inside the car. But in connected cars, a remote hacker could be in control of the gas pedal and the brake. The difference is connectivity – and it can be both a blessing and a curse.

The more connected we become, the more complex the situation gets. Today, anything that can be accessed remotely is vulnerable to attacks. From medical devices and smart thermostats to data centers and movie production studios. And the bigger the value of the target, the more motivated a hacker is to crack it.

## Your weakest link, your biggest asset

When it comes to security, the majority of companies struggle with the same dilemma: people are often the weakest link in the security chain. Sometimes, that email link or 'special offer' is just too enticing to resist. Even though their gut may be telling them it sounds too good to be true, they simply can't help themselves: they have to click and see for themselves.

But that intrinsically human 'gut feeling' can also be your company's biggest asset. If you constantly train and remind your people of your Zero Trust policies, they will be even more vigilant and suspicious of anything that even looks slightly out of the ordinary. Pure intuition can help stop attacks and sound the alarm, simply because they are constantly reminded that Zero Trust is part of your company culture.

Irdeeto is certainly not immune to attacks. After all, countless hackers around the world would do it simply for the bragging rights: "I took down the cybersecurity experts." In just the past year, one employee's human intuition protected us from unthinkable invasion. And another employee's human error nearly enabled another. But because of the multiple levels of protection and multi-factor authentication protocols of Zero Trust, our systems remained protected. Still, we never stop monitoring and improving. And we never stop reminding our colleagues of the importance of vigilance.



---

## Make it all easier

The great news is, as multi-factor authentication matures, it gets easier to use and less intrusive. And the easier and less intrusive identification becomes, the more layers of verification we can add to security systems, and thereby protect systems with millions of invisible moats.

Soon, there will be no need for passwords at all. Systems will use ‘voice or behavior DNA’ to authenticate a user’s identity. The system will be able to distinguish between the actual person’s voice and a deep fake. Biometric identification, like fingerprints, will become more prolific. And mobile technology’s motion sensors and gyroscopes will be able to identify you from your patterns of movement, your walking cadence and the way you hold your phone. So, if you happen to lose your unlocked phone, the system will know someone else has picked it up. The same multi-DRM systems that protect video entertainment can also protect connected cars. A policy-based management system and multi-factor authentication will ensure that no one drives the car unless they are authorized to do so. It can even enable user-specific controls.

## Start yesterday

Need to be convinced that there’s no time to wait to work on your Zero Trust Architecture? Just look around. Every single day, all over the world, we find cases of invasion that Zero Trust may have prevented. And the price of ‘waiting and seeing’ if it happens to you is simply too high. So, start going through your business from top to bottom and review every connection point, every potential target, and every possible threat. Prioritize your list based on the impact of a breach, and get to work. Called attack modelling and a cybersecurity risk register, this prioritized list should guide your immediate and ongoing action for cybersecurity. And it should be constantly updated. After all, something that’s only a mild threat today, could very easily be a major threat tomorrow.

The register will also enable you to invest in the right security at the right time, and evolve your security structures over time. And remember: AI and ML are enabling automated cyberattacks. Be sure to use the same technology to create automated protection. Otherwise, you’re just bringing a knife to a gunfight.

## The newer, the better

There are certainly plenty of opportunities to ensure that any new devices or systems you build have the best protection possible. This starts with Security by Design: every new product should be built with the necessary security elements and ability to upgrade them. After all: you must plan to keep your devices fully secure for their entire lifetime, from the cradle to the grave. And given the rapid pace at which attacks are developing, you can safely assume that the security measures you put in place in the initial design of your device will already require an update by the time your product is ready for launch. Hackers never sleep, and neither should you.

---

## Five tips for Zero Trust

When designing your Zero Trust Architecture, there are a few general principles you should always keep in mind.

1. Pirates and hackers are fairly lazy. The more difficult you make it for them to crack your system, the sooner they'll give up. That's why multiple layers of protection, and extra protection for your most valuable assets, are essential.
2. You should never assume anything. Establish and verify trust for every person, every interaction, every device and every connection. The only secure solution is one in which no one is trusted until they're verified.
3. The less noticeable your multi-factor authentication is, the better. Use the latest technology to make passwords obsolete and give authorized users the feeling they have seamless access. If authentication is too difficult or cumbersome, it will only increase the likelihood that your employees will take shortcuts that leave your system vulnerable.
4. Make your people alert, and keep them alert. Security training should never be a one-off event. Everyone in your organization should have a clear and frequent reminder of your security protocols and the reasons for them.
5. Think in layers. Your employees are human, and humans make mistakes. It's just a fact. Layers of protection and authentication points can be your best friend. That way, if someone accidentally leaves the front door open, your precious valuables are still locked safely away in the company vault.

### About the Author

**Peter Oggel, Chief Technology Officer, Irdeto.** Peter joined Irdeto in May 2009 and is currently Chief Technology Officer at Irdeto. He is a seasoned ICT and telecommunications industry executive with over 20 years of international experience and a consistent track record. Prior to joining Irdeto, Peter founded and served as the Managing Director of Smile Telecom, a start-up that pioneered WiMAX technology while launching an operational mobile service provider (MVNO) and fixed line service provider (VOIP) in the Netherlands.



Before he founded Smile Telecom, Peter was a Vice President at LogicaCMG where he held management positions in Strategic Sales, General Management, Operations and R&D, and was instrumental to the success of LogicaCMG's mobile messaging and data solutions. Prior to joining LogicaCMG, Peter worked at different positions in Fintel S.A. and Digital Equipment Corporation in Switzerland and France. Peter holds a Bachelor of Science degree in Technical Physics from the Technological University in Eindhoven (the Netherlands).

Peter Oggel can be reached online at [peter.oggel@irdeto.com](mailto:peter.oggel@irdeto.com) and at our company website [www.irdeto.com](http://www.irdeto.com)



## Transparency And Collaboration Between Vendors and Customers Are Key to Reducing Third-Party Security Incidents

By Nick Sorensen, CEO of Whistic, Inc.

It's no secret the number of third-party security incidents continues to rise annually. Last year started with the SolarWinds breach, ended with Log4j, and virtually every day in between was marked with news of one breach or another.

Recent research by Whistic found that nearly half of all businesses surveyed experienced a data breach in the last three years with more than 80% of those being caused by third-party vendors. Cleaning up after a breach can be costly and not just from a financial perspective ([\\$4.24M/incident according to IBM](#)), but also the damage it does to your brand and customer trust is often insurmountable.

With that potential threat ever present, cybersecurity leaders now require most vendors to pass a security review before being brought into their environment. Despite that knowledge, most teams often put the security review off until the very end of the sales cycle, which can cause deals to push to the next quarter or in some instances causes them to lose the deal outright because they didn't respond quickly enough.

---

In fact, according to the [State of Vendor Security report](#), 90% of sales reps said they have at least one deal push per quarter because they can't respond to security reviews in time.

In the past, this was because of how difficult the vendor assessment process was for both vendors and customers. Up until recently, the primary tools for managing vendor assessments were spreadsheets and emails, which made it difficult to keep track of where vendors were in the process and ensuring each assessment got completed, especially considering the volume of vendors assessed each month.

As a result, customer/vendor relationships were often adversarial instead of collaborative. It was almost like pulling teeth for customers to track down all of the information needed to initiate the assessment and it would only get worse once they started engaging directly with the vendor.

However, as technology has advanced in recent years those relationships are starting to improve and clients are beginning to look at their vendors as partners when it comes to security, which is the way it should have always been.

It is in this environment that Whistic joined together with other top technology vendors, including Okta, Airbnb, Zendesk, Asana, Atlassian, Snap, Notion, TripActions, and G2, to form the Security First Initiative with the goal of making transparency between vendors and customers the expectation instead of the exception. The reason being that transparency leads to trust, which ultimately leads to better protection against third-party incidents for everyone involved.

In a nutshell, the vision of the initiative is this: The future of vendor security must be built on a foundation of collaboration...[It's] the only way to meet the needs of both buyers and sellers in the ecosystem. It's also the most efficient way to make transparency the expectation in vendor security, and when that happens, everybody wins.

Making it easy for vendors to consolidate all of their security documentation, standard questionnaire responses, certifications, and audits into an easy to share security profile, ensures that companies have no excuse not to share their security information as early as possible in the sales cycle. Taking the extra time to build out a profile before your customers ask can save countless hours that infosec and cybersecurity teams once spent reacting and responding to one off requests.

An added benefit for vendors is that a transparent security posture can also be a differentiating factor between you and your competition that ultimately leads you to close more business. According to the [2021 State of Trust and Transparency](#), 90% of respondents indicated that when a company publishes their security and compliance information publicly it increases their trust in that business. Additionally, 96% of respondents said they would be more likely to purchase from a vendor that is transparent about security posture.

If you would like to join the Security First Initiative or would like more information, you can read more about the initiative [here](#).

---

### About the Author

Nick Sorensen is CEO of Whistic, Inc., the network for assessing, publishing, and sharing vendor security information. The Whistic Vendor Security Network accelerates the vendor assessment process by enabling businesses to access and evaluate a vendor's Whistic Profile and create trusted connections that last well beyond the initial assessment.





## Responding To High-Level Cyberattacks on A Mid-Level Budget

By Jesper Zerlang, CEO, LogPoint

Protecting your business against threat actors is no small task. Not only has the number of cyberattacks increased dramatically during the last year, but attacks are also becoming increasingly complex.

Organizations' attack surface is expanding due to the quick advancement of digital transformation. The COVID-19 pandemic has significantly increased remote work, and businesses are using a growing number of SaaS solutions and applications, conducting more and more business online.

Simultaneously, cybercriminals are developing their techniques. For example, next-generation supply chain attacks have increased by [650 percent in 2021](#), and the number of victims to double extortion has risen an [astonishing 935 percent](#) in 2021. We also saw one of the most critical vulnerabilities of our time, [Log4Shell](#), discovered in December, putting all organizations at risk for many years to come.

For a long time, people – especially management level – have assumed that the larger the organization is, the bigger the cybersecurity threat. Media tend to cover the cyberattacks hitting large companies, critical infrastructure, or governmental institutions, fueling the belief even today. It is time to revisit and disprove the assumption once and for all and address cybersecurity management in the mid-market.

---

## Detecting and responding to threats in the mid-market

In today's threat landscape, no company is safe from cybercrime. [Verizon's 2021 Data Breach Investigations Report reveals that small organizations are closing in on large ones regarding data breaches](#), with 307 in large and 263 in small. The genuine threat poses a massive dilemma for the mid-market: Who handles cybersecurity and how? My experience tells me that many middle-sized businesses place security administration with the IT department. Either they don't have dedicated cybersecurity professionals to detect and address the inevitable security incidents at all, or they have very few.

Meanwhile enterprise-level companies typically have 30, 50, or 100 security analysts to monitor and respond to indicators of compromise in a dedicated security operations center (SOC). Leaving security operations in the hands of the general IT department is the same as asking a neurologist to diagnose and treat heart disease. Although competent, the neurologist might overlook something critical or choose a sub-par course of action to handle an identified problem because the skill level is unsuitable. The risk becomes that a small problem turns into a big one.

## Cybercriminals slipping through the cracks

Although general IT professionals are highly competent at IT operations, they do not typically understand the threat landscape in-depth or know how to detect and respond to threats appropriately. Even if a business invests in sophisticated and complex platforms to protect against cyberattacks, the lack of expertise prevents it from leveraging the features. Many cybersecurity vendors only build security operations platforms to optimize enterprise-level SOC's, a solution far above a middle-sized organization's budget and skill level.

The lack of expertise puts the organization behind the curve, decreasing chances of overcoming a security breach without financial or reputational damage. Cybercriminals only need one opportunity to slip through the cracks and breach your system, e.g., exploiting unpatched software or getting an employee to click a malicious link.

## Winning a seemingly losing battle with AI

There are ways for organizations in the mid-market to circumvent the issue of lacking the expertise to ensure a strong cyber defense. Some organizations turn to managed security service providers (MSSP), providing security services 24/7 in a SOC with the necessary capabilities to detect and respond to cyber incidents. Others turn to automation technologies to automate the SOC and eliminating human intervention as much as possible.

No matter which direction mid-level organizations take to bolster their defenses, there is a need for a consolidated and holistic approach to cybersecurity. Businesses need to stop running after best-in-class tools, and leverage AI and automation maturity to simplify security operations and ensure effectivity. An AI-driven system allows you to detect threats and execute a response automatically, either in-house or through an MSSP.

---

## About the Author

Jesper Zerlang, CEO, LogPoint. Jesper Zerlang is a passionate proponent of increased cybersecurity awareness at the Executive and Board level, and champion of the integration of cybersecurity as a core component of any business strategy. Jesper has been the CEO of LogPoint since 2009 and has led the company to become one of the dominant Cybersecurity vendors in Europe, now expanding throughout the world. He has more than 25 years' experience in the IT industry and has held executive management positions at Telia Company, Dell Computer and Compaq. His strong customer and partner focus, passion for his employees and strong entrepreneurial spirit sparks innovation and growth at LogPoint. He has supplemented his leadership skills with executive management programs at Harvard Business School. He can be reached at [LogPointPR@matternow.com](mailto:LogPointPR@matternow.com) and at our company website <https://www.logpoint.com/en/>.







## Security Gotcha of Consumer and Industrial IoT Devices

By Smit Kadakia, Chief Data Scientist, Seceon Inc.

Internet of Things (IoT) and Industrial IoT (IIoT) are not just buzzwords any more. The broad use of these devices and their impact on our society and modern businesses is changing our everyday life in a way that was unimaginable even a decade ago. Always-on visibility of intruders to your home, precise control of your energy use and the remote control of your garage and car doors are some examples of consumer use of the IoT's technological advances. Such broad adoption of IoT and IIoT also increases the cybersecurity attack surface exposure for the society and the businesses. Most of the non-technical people and businesses are unaware of the risk that this poses and are likely to be caught off-guard, potentially resulting in substantial damage to them. So, what are these risks and how do you manage them?

### IoT and IIoT Security Risks and Challenges

Security exposure for any IoT and IIoT device is a multi-dimensional problem referred to in the industry as the attack surface. These attack surfaces are directly proportional to the age of the IoT device, for the most part, the older the device generally means the bigger the attack surface. Sometimes a recently manufactured device with a dated design can mislead the buyer about the built-in security of the device. Beyond the common-sense view of better security offered by contemporary devices, one needs to think about inherent security risks of these devices as well.

---

## Device hardening

Many of these devices operate in an environment of a customized special purpose hardware and software platform. The platform's operating system is typically a stripped-down popular OS such as Windows or Linux. The underlying assumption is that such devices, corresponding platform, and the application will operate in a closed environment and do not need to be hardened for full security, as offered by a non-stripped standard OS. Lack of hardening is a risk that the modern-day attackers understand well and have figured out how to leverage.

The other dimension to the security risk is the outdated OS such as Windows 95, NT, Windows 7, XP or similar older versions of Linux. The lack of upgrade to these OS from the OEM and lack of connectivity from these devices to the OEM adds to the hardening risk.

The third dimension to the security risk is the arcane but field proven utilities. Based on their age and the design parameters for security, the risk should be assessed. Some of the obvious insecure utilities use unencrypted data such as ftp and sh instead of sftp and ssh.

## IoT management

Information Technology (IT) is traditionally known as the technology that deals with information to make decisions to operate and protect its own infrastructure. In the world of IoTs the Operational Technology (OT) is employed and architected along with IT.

OT is used to monitor and control the IoT/IIoT devices through a good understanding of the device which generates events and takes appropriate actions based on the generated event. OT operations on its own with no other outside connection is generally quite safe. However, IT and OT are inherently interconnected making it easier to pass inherent risks and benefits of each architecture to the combined infrastructure. OT acts as a bridge that increases the security risk to the IoT/IIoT infrastructure through expanded connectivity to the attackers. IT is traditionally more agile and less rigorous, requiring much more sophisticated security risk management. OT is inherently different on both fronts, the agility and rigor adding significant security risk while facilitating easier operations.

To get a sense of heightened security risks, a Kaspersky analysis of its telemetry from honeypots in the 1st half of 2021, more than 1.5 billion IoT attacks were detected during the period. These were up from 639 million during the previous half. The rate of growth of attacks on the IoT/IIoT devices and the infrastructure has more than doubled causing increased attention to the security.

## Dated data management

Information Technology is considered data centric whereas Operations Technology is considered management oriented. This is a good functional description and de-emphasizes the importance of data in Operations Technology. Most cyber security attacks are centered around the data and lack of emphasis on data in Operation Technology is fundamentally a risk.

---

Common risk metrics for these can be viewed from a couple of perspectives. One is how is the data accessed or is the data in transit encrypted? This is critical to ensure that even if someone accessed the data, can they do anything with it to take a detrimental action such as create operational disruptions, impose physical harm, or raise financial liability to name a few? The other aspect revolves around the data protection in the case a breach really occurs. This is referred to as data encryption at rest. This is generally not thought through during the system design of an IoT devices-based infrastructure such as control systems.

There are many other risks that exist and we can probably go over them in the next installment of this article. To provide a glimpse of those risks, some of the standard proactive threat prevention methods can help us enumerate them and plan accordingly to mitigate them. These methods include authentication services, device manufacturer parameters such as default and maintenance access communication among collaborating devices and systems, operator errors or lack of security knowledge to name a few.

Additionally, there is a class of industry specific risks. For example, fraud in financial IoTs is a commonplace occurrence. Similarly, the utility/energy companies have risks of service disruptions in the middle of the critical consumption period, overloading the inputs to permanently damage the entire infrastructure and literally stealing the outputs such as electricity, gas or water to cause huge financial damage.

## Risk Management

Now that we know about the risks and challenges, let's review the key components of risk mitigation and management. The saying "Intellectuals solve problems, geniuses prevent them" conveys the best approach from the design perspective, while the saying "An ounce of prevention is worth a pound of cure" describes the financial savvy of an organization.

## Security Hygiene

Similar to the concept of healthy eating habits will prevent sickness while enhancing the longevity, security hygiene will help significantly in thwarting the attacks and hence provides one of the most effective mitigations. Some of this security hygiene include employing firewalls and Intrusion prevention systems to access Operations Technology Infrastructure and for Operation technology infrastructure to access physical devices infrastructure. This can also be augmented with modern authentication systems with safeguards such as multi-factor authentication to prevent unauthorized accesses. There are many other dimensions to security hygiene such as allowing encrypted traffic and reducing access levels down to need-to-know basis. The important aspect is to pay special attention to Security Hygiene as an important foundation for the security architecture and sharpening the focus on proactive security controls.

---

## Policy Management

One of the key aspects of security management in the IT industry is to not keep key access information static. This is accomplished by reducing the lifespan of such information as short as possible without making it operationally difficult. Common example is to employ forced periodic change of important credentials and employing multi-factor authentication as a requirement. The security education of employees is a key aspect that many organizations ignore due to lack of staffing and the perception of education. The recent pandemic has accentuated this difficulty and has required organizations to hire reduced skilled staff and spending education bandwidth on imparting productivity related skills at the expense of important security awareness. Management buy-in of the security aspect is extremely important, this foresight shows a forward looking and business sustainability driven management style to external stakeholders.

## Pen Testing

Simulating any of the emergency scenarios such as fire drills are considered very important, and laws are enforced in many communities to make sure they take place and are regularly tested. The Importance of security breach testing should be like a fire drill, simulating security attacks through penetration testing plays an important role in the overall security posture of an organization. Pen Testing will surely provide a good assessment on how well your current security measures are protecting you. However, it can also be designed to assess the organizational readiness in case of real attack. The assumption that we all will be attacked at some point and the question is when? helps organizations prepare for the actual attack or breach and will tremendously improve the preparedness to react in such situations rapidly and effectively. Such readiness will be certainly appreciated by all internal and external stakeholders as well as clients. On the contrary, lack of readiness in the event of a real attack can potentially put the entire organization out of business and leave a bitter taste in the community and individuals associated with the business.

## Layered Security System

Modern security infrastructure has evolved to counter sophisticated threats and attackers. The overall approach should certainly provide a proactive defense against all known attacks and also offer a very good defense against unknown attacks. Layered security systems built on security hygiene with machine learning (ML) and artificial intelligence (AI) are needed. The security hygiene generally consists of silo solutions like perimeter firewalls, authentication systems such as Windows Active Directory and proxy services. The threat response should be proactive and in near real-time. Note that we are referring to response and not just the detection.

Given the lack of skilled security professionals availability, it is imperative that automation that minimizes or eliminates manual operations is needed. The industry has started to coin the term XDR (extended detection & response) to describe this, but one will find various vendors using different combinations of the products to promote their version of XDR. Let's look at XDR from the purpose driven approach.

---

The security system (XDR) should be unified and is expected to include Security Information and Event Management (SIEM), Machine Learning, Artificial Intelligence, User and Entity Behavior Anomaly (UEBA), Network Traffic Analytics (NTA), Security Orchestration and Automated Response (SOAR), Endpoint Detection and Response (EDR) and Vulnerability Assessment (VA). XDR in a single platform is essential for the practical and effective security posture for IoT and IIoT environments. Such a system has to provide flexibility and efficiency for the security operations center (SOC) to effectively mitigate any attack proactively and in minutes.

## Conclusion/Summary

Operation Technology and Information Technology (OT and IT) used in a reasonable size Industrial environment for monitoring and control must be augmented by an XDR that builds upon basic security hygiene and includes SIEM, ML, AI, UEBA, NTA, VA and SOAR. Proactive security planning, readiness in case of attack, business continuity plan and security awareness are critical ingredients for the modern organization to sustain themselves in the dangerous world that we all operate in.

### About the Author

Smit Kadakia is the Chief Data Scientist of the Seceon Inc. He has been an executive leader overseeing business growth and technology differentiation in the Cybersecurity Industry at Seceon for over 7 years. He heads Seceon's Data Science and Machine learning team in creation of the state-of-the-art aiXDR solution. Prior to Seceon, he was an executive member at the Tradepoint Systems which was later acquired by Kewill Systems. At Kewill, Smit helped grow the business multi-fold by addressing broader global markets while shortening the revenue cycle. Technologically he helped transform the legacy supply chain products to modern, competitive and cost-effective SaaS platform. Prior to that, Smit was the Engineering Director at Upspring Software, which was later acquired by MKS. Smit holds a B.S from Victoria Jubilee Technical Institute (VJTI), Mumbai, an MS in Computer Science from Indian Statistical Institute (ISI) and an MBA from Southern New Hampshire University (SNHU).



Smit can be reached online at [LinkedIn](#) and at our company website <https://www.seceon.com/>



# Operational Security

## Operational Security: How to Get Rid of Digital Footprints On The Internet?

By **Viktoria Sokurenko**, CMO of Ukrainian start-up X-ray

OPSEC (Operational Security) is a term used by US intelligence to describe the analytical process of preventing enemy access to information threatening the secrecy and security of the mission.

The private sector also uses OPSEC as a safeguard against collecting confidential information by competitors and attackers.

In this article, we will talk about the basic measures for personal data protection:

- How to find and delete compromising information about yourself.
- Whether you can remove yourself from the Internet.
- How to prevent credential hack and data theft.

### Identification of sensitive data

The first step is to identify sensitive information, precisely how and where it is stored. Put yourself in the place of a competitor or attacker and, using OSINT methods, look for information about yourself or your company.

---

### Types of private personal data:

- full name
- date of birth
- e-mail
- personal and corporate phone numbers
- address
- profiles on social networks
- passwords

### Types of private company data:

- intellectual property
- business research
- financial information
- information about employees (family, habits, lifestyle, working environment)
- customer information
- passwords to access resources
- IP, MAC addresses of workstations

## Search engines

Start checking for a person or company on the web by using Google, Bing, Yahoo, or DuckDuckGo. Use advanced search operators for advanced keyword search:

inurl:

- username - searches all pages with the username URL.
- [your name] intext: [personal information, such as phone number, ID card, or address] - shows pages that contain personal information about a person.
- site: docs.google.com "companyname" - finds publicly available Google Docs documents that include a company name.

- 
- "companyname.com" - provides resources that link to the company's page, such as sites with reviews of employers, job search sites, and media portals.
  - password filetype: docx site: companyname.com – shows docx files on the company's website that contain the word "password". In some cases, such a set of operators will find a file with users' passwords due to the administrator's negligence.

## Image search

Reverse image search services use a face recognition system and determine which sites have photos of the searcher. Among them are:

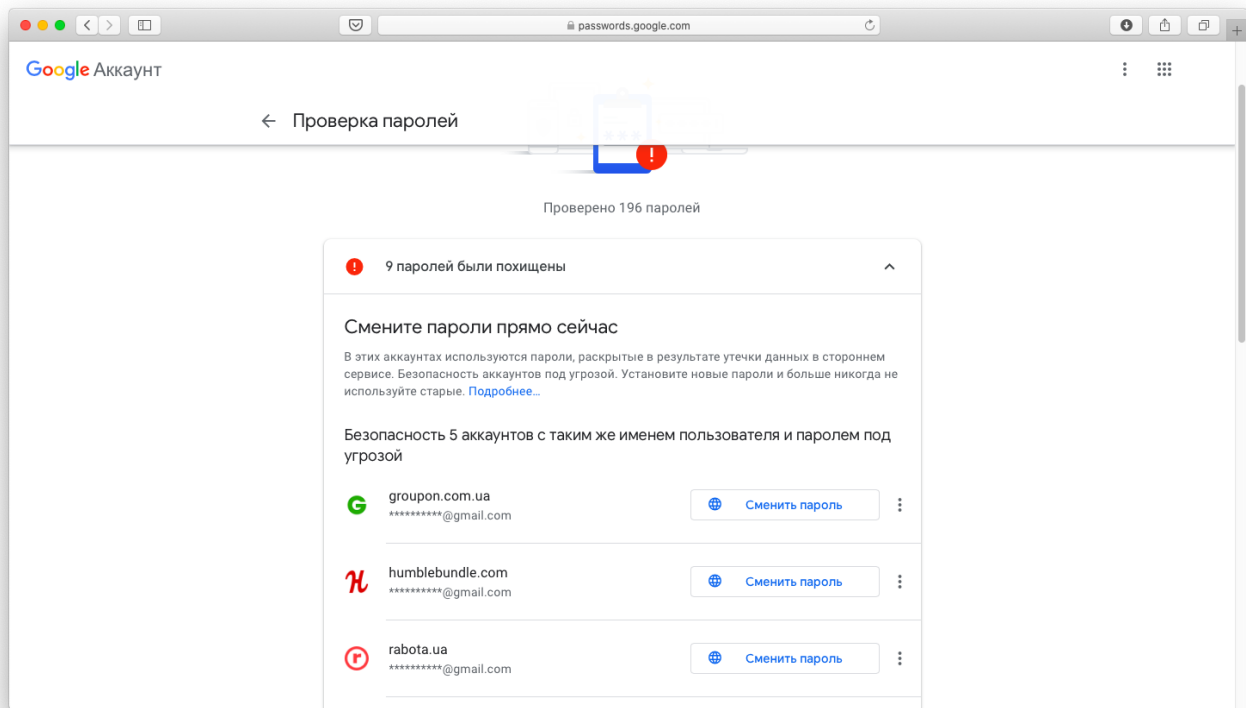
- [Google Images](#)
- [Bing Images](#)
- [Tineye](#)

## Search for email accounts and passwords in leaks databases

In the case of hacking online services, users' data gets to "leaks databases". Attackers use databases to understand the logic of password creation and determine if they recur. The goal is to steal identity or gain unauthorized access to computer systems and online services. The following services can be used to verify accounts and passwords in leaks databases:

- [Haveibeenpwned](#)
- [Google Passwords](#) (check for password leaks stored in your Google Account)
- [Spy Cloud](#)
- [Ghost Project](#)
- [pwndb2am4tzkvold.onion](#) (log in with Tor-browser).





Google Passwords Check checks not only the password for the e-mail account but also the passwords for other services stored in Google

## Vulnerability analysis and risk assessment

Make a spreadsheet or chart with known accounts, usernames, and names. Write down telephone numbers and e-mail addresses provided during registration or as contact information.

Identify the vulnerabilities used to gain access to private data and assess the risk level associated with each of them. Factors to evaluate the level of risk include:

- probability of an attack
- degree of damage
- the amount of work and time required for recovery

The more likely and dangerous the attack, the higher the priority of eliminating the vulnerability. The analysis determines which information to keep public and which to hide or delete. Remember that once you enter mail or mobile phone in the contacts section, they are compromised forever.

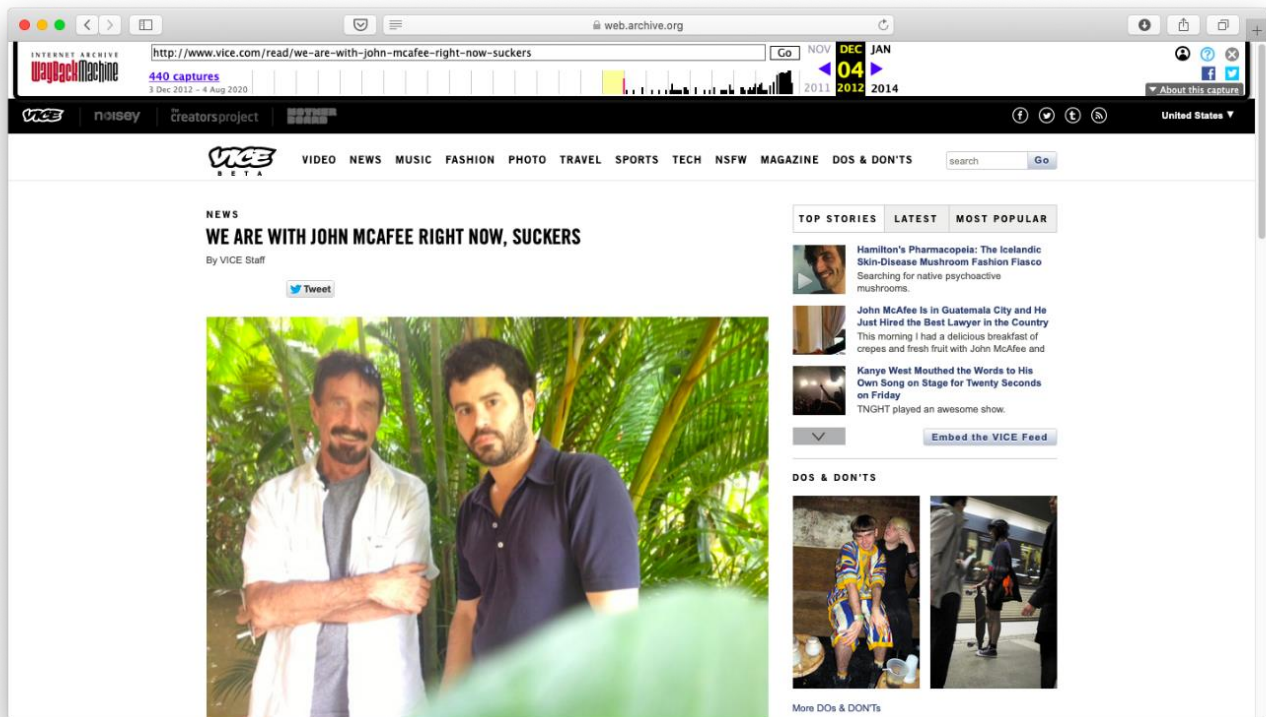
---

## Application of measures

Depending on the degree of risk, data protection methods include creating strong passwords or passphrases, hiding geolocation, filling the account with false information and fictional stories, or deleting data completely. However, control is an illusion. Everything that got on the Internet stays there forever. Even if you follow the main rule of safety and silence, the result is not guaranteed. The following rules will protect against basic information gathering, but if someone is seriously interested in you, they find everything.

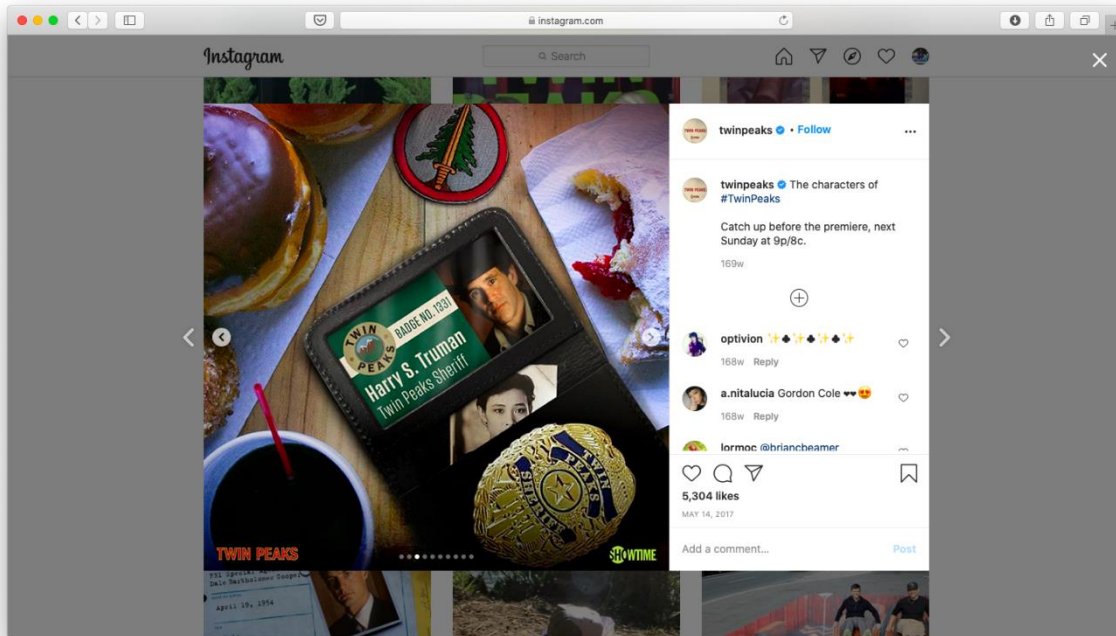
## Basic rules of operational security

- Divide accounts. Come up with random e-mail account names for personal use. Create separate accounts for financial transactions, social media registrations, and general purposes.
- Don't repeat passwords. Use the password manager to generate different passwords for each online service. For additional protection, set up two-factor authentication.
- Delete metadata and hide geolocation. In 2012, programmer and businessman John McAfee was wanted on suspicion of murder. Hiding from Belize police, McAfee ran an escape blog with Vice Magazine, a journalist of Vice Magazine. McAfee's location in Guatemala revealed a photo in the post as it had been taken on an iPhone and contained EXIF metadata, including geolocation.



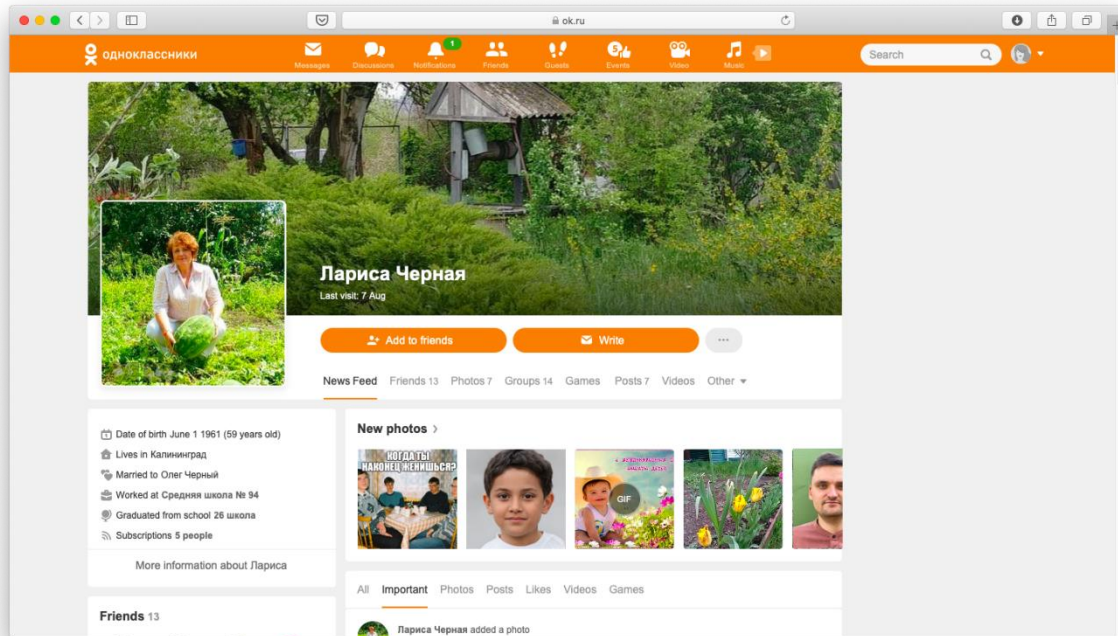
EXIF metadata includes camera model, shooting date and time, and geographic coordinates. Just delete metadata before publishing content to protect your privacy. Better yet, disable geolocation and use VPNs in depersonalized browsers like Tor.

- Hide hints. Do you like to take selfies on Instagram or photo reports about corporate events on Facebook? Social networks have taken care of privacy and automatically removed EXIF before publication. However, there are tips in the photo: silhouettes of buildings, advertising signs, reflections in the mirror, the type of outlet, and documents on the desktop. Such details make it easier to identify a person, find the location of the office or home address, as well as give an idea of the target's lifestyle.



Photos with badges will be useful to attackers during social engineering attacks

- Learn to be silent. Posting content online is a threat to privacy. Social networks feed on emotions, encouraging to share feelings. Before posting comments or photos, think if it gives the attacker information to create a dossier on a person or company. Additionally, teach your loved ones not to post pictures on Facebook, or in the case of Russia, in "Classmates". In this way, the employer or partner cannot find details of family gatherings, children's illnesses, and travel.



Russian mothers happily leak photos of their children in "Classmates" after family events.

### Filling an account with false info

If you want to protect the information, make sure that the digital trail does not retaliate for clues. Distortion of data will confuse the enemy and will not allow them to make a connection between accounts. In this way, three goals can be achieved simultaneously: you preserve your friendly and credible image, veil your actual goals, and send competitors in the wrong direction.

- Don't use the actual date of birth, but enter it randomly when registering accounts.
- Don't enter a full name or use different names for each account.
- Use random profile images for non-public accounts. For example, portraits generated by AI. Make sure photos are unique to each site to prevent finding connections between them by reverse image search.

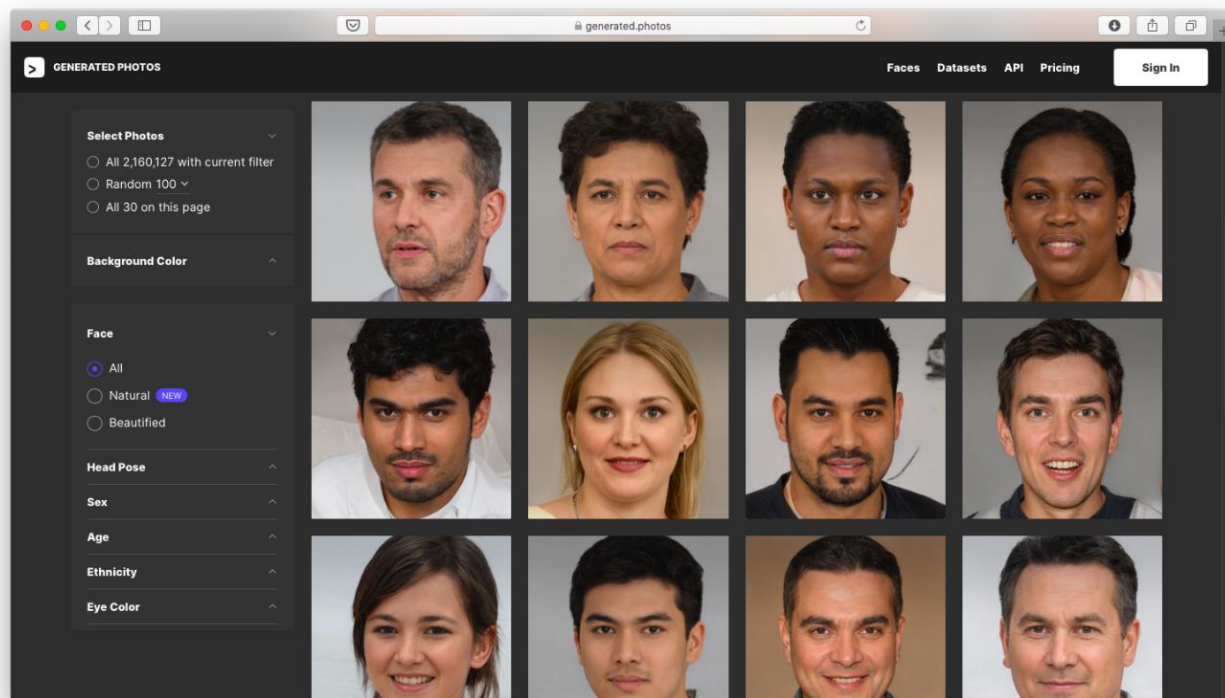
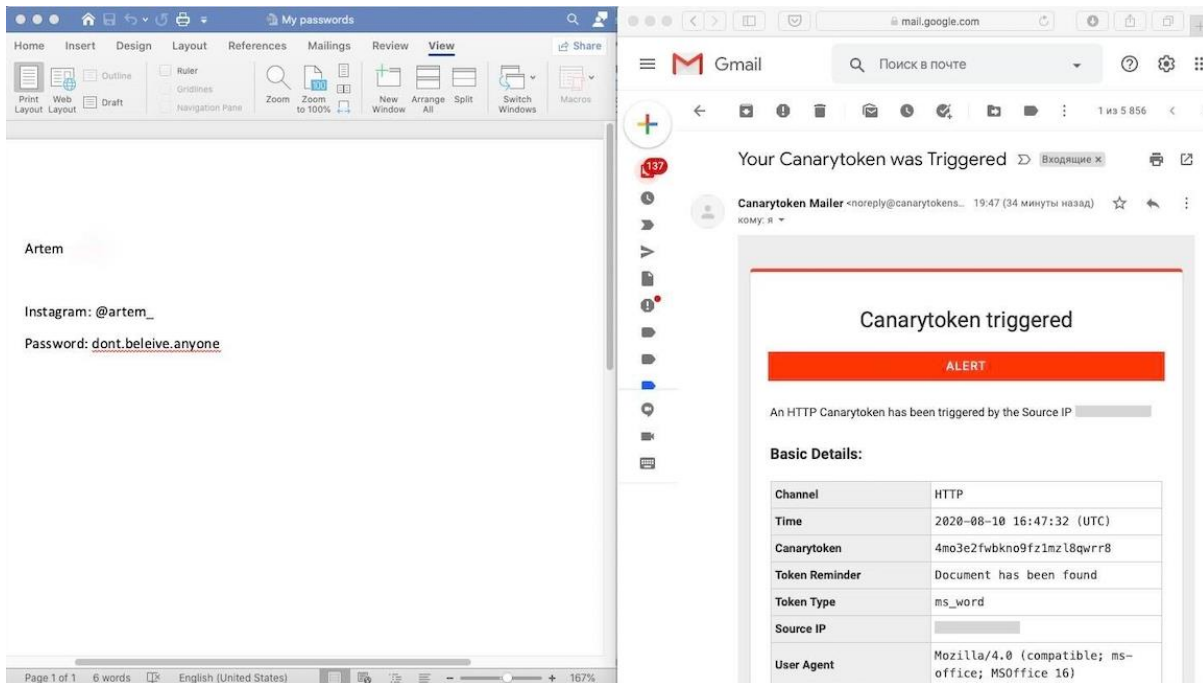


Image caption: Generated Photos uses AI to create portraits of non-existent people

- Create trap files that contain fake credentials or financial statements. Use the [Canary Tokens](#) service to receive notifications when opening files and track the IP address of an attacker's DNS server. [IP Logger](#) generates links to place traps or discredited communication channels inside files and tracks the hacker's IP address and location.



It looks like a regular document (left), but the metadata contains code. The Canary Tokens service sends a message (right) each time you open a Microsoft Word file.

## Data deletion

It is impossible to remove yourself from the Internet altogether. Open state registers contain information about vehicles, real estate, and lawsuits, and this data cannot be deleted. Web archives store historical photos of sites. Realistically, you can only delete unused accounts, exclude yourself from brokers' databases, and send a request to delete publications on social networks and other sites.

1. Delete unused accounts. Go to the [directory](#) of direct links to delete unused accounts. Remember that it is better to delete an account than to block or deactivate it. When deactivated, the account technically remains online and searchable.
2. Exception from brokers' databases. People search sites or "data brokers" (Pipl, Acxiom, WhitePages) collect and sell personal information from open registries and social networks. To exclude a profile from databases, email owners, or administrators. If there are no contacts on the site, go to the [WHOIS catalog](#) and find out the owner's contacts. In some services, deleting a profile is available through an online form. For a list of links and instructions, see [Vice](#).
3. Delete publications in search results, social networks, and other sites. If you do not want personal data to appear in search results, contact the site owner where it is published. Once the information is deleted, Google will not be able to find and add search results. If the site owner refuses to comply with the request, Google will [block](#) certain types of personal information. Such requests remain public because if you withdraw a compromising article by contacting Google, the request for removal and the article itself will appear in the [Lumen Database](#).

---

The same scheme works on social networks: ask a person to delete a post or uncheck a photo. If they refuse, report the violation to the administration and disable the option to tag people on a photo in the settings. There are complaint instructions for:

- [Facebook](#)
- [Instagram](#)
- [LinkedIn](#)
- [YouTube](#)

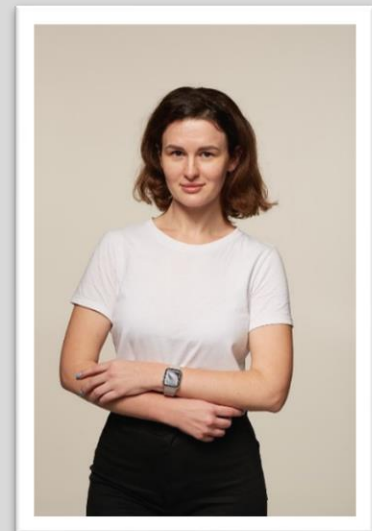
Analyzing activities from a competitor or attacker's perspective is the first step in protecting private data. Use OPSEC methods to neutralize intruders' attempts to steal identity, prevent competitors from gathering information, hide mistakes of your past from a prospective employer, or avoid law enforcement issues. If you do not have time to study OPSEC techniques, contact specialized agencies that perform a full vulnerability test for you.

### About the Author

Viktoria Sokurenko, CMO of Ukrainian start-up [X-ray](#), a platform for finding interconnected information about a person.

Any human interactions with each other can lead to large-scale search results. Victoria started her career in business communications. She works closely with field intelligence teams specializing in OSINT and HUMINT in various niches in the markets of Europe and US. After 2+ years in marketing and PR of competitive intelligence, she led the marketing and PR department.

Viktoria can be reached online at <http://www.linkedin.com/in/viktoria-sokurenko> or [vs@x-ray.to](mailto:vs@x-ray.to) and at company's website <https://x-ray.to/>







## How the Cloud Upended Security – and How Encryption Helps Restore It

By Tilo Weigandt, co-founder, Vaultree

Data is everywhere and anywhere, and as a result, data management is out of control. Once a user or customer has signed up for a service or purchased a product, they usually have no idea about where their data is being stored, with whom it is shared or how it is secured. The adoption of cloud services – while very beneficial in many ways – have made it nearly impossible for companies to have 100% control and knowledge about what is happening to data, where and at what time. The situation is even fuzzier in places where data is being stored and processed in several countries.

Data protection regulations like GDPR apply to companies based in the European Union – or companies doing business in these countries – but ambiguity persists. Companies need to take back control of data, and encryption can play a role in this.

### Data privacy, security, and the cloud

While enterprises have financial incentives to scale their businesses using distributed tools like cloud computing services, they are also required to comply with industry standards and federal regulations.

---

These regulations require restricting access to sensitive data to authorized users only; otherwise, companies face severe penalties if audits fail. Customer service level agreements (SLAs) frequently include provisions for data security, as well.

Two of the most frequently mentioned challenges in cloud computing are data security and data privacy. There's concern that Cloud Service Providers (CSPs) may collect and exploit customer data for their own gain (including the sharing of customer data with third parties). Data encryption can allay these anxieties, but the way most CSPs are using it falls short of providing complete data protection.

## How encryption fits in

Encryption ensures the security of both data-in-transit and at-rest when employed in its traditional form; nevertheless, it must be decrypted before any type of processing can be conducted on it. CSPs need access to the accompanying decryption keys to retain the ability to process encrypted data with acceptable performance levels. These keys can be kept on the CSP's premises or forwarded to the CSP whenever the customer needs to access their data. While this solution addresses some of the concerns about cloud data security and privacy, it can't be considered totally safe because it requires clients to reveal their decryption keys and therefore, data.

What typically happens is that companies wind up blindly trusting their cloud providers and leave the decryption keys with them. And what happens? Leaks and hacks continue to increase. Advanced encryption schemes, on the other hand – providing fully encrypted cloud environments without the need to decrypt data to process it – are gaining traction and for good reason. There's simply no other way to get out of this mess.

Advanced encryption is an enabler – not just a security enabler but a technology and business enabler. It brings many monetary, brand and efficiency benefits with it that some executives underestimate. Encryption is the basis for all other security measures; without it, all the rest is pointless. There can be as many vulnerability trackers and endpoint security measures in place as a company wants. But if an attacker breaches the network and the data is in plaintext, it's lost. It's the equivalent of setting up a security camera facing your front door yet leaving it wide open for burglars to enter.

## Evaluating encryption solutions

There are several best practices you can put in place when deploying encryption. First and foremost, educate yourself about advanced encryption. Encryption must be viewed as a business enabler and revenue driver; it's an opportunity to show prospective customers that you take security seriously.

As you vet solutions, don't overlook startups and newer companies as part of that evaluation. There are some innovative approaches happening in this field that haven't yet hit the big time. You want to look for a solution that securely manages encryption keys across all on-prem and cloud environments. Again, there are good solutions available today that avoid having to disclose your keys and that bypass the traditional way of managing encryption. And what's more is that encryption no longer needs to be seen

---

as something that's time consuming to implement – there are newer solutions available that offer a more “plug and play” approach.

At the end of the day, you want a solution that lets you encrypt and process all of your data with near plain text performance in the safest environment.

## Keep calm and encrypt on

With the mass adoption of the cloud, the concept of traditional perimeter security has flown out the window. Hacks and leaks continue, but help has arrived. Organizations need to have a new approach to security that meets the same standard of quality, regardless of location – and that enables high performance and scalability. Encryption is critical to data security and privacy but disclosing decryption keys poses dangers of its own. Advanced encryption eliminates those dangers and provides solid security for all your data in all circumstances. Use the best practices above to find the solution that works best for your organization.

### About the Author

Tilo is a program manager, business developer and marketer with a “nothing is impossible” attitude and more than a decade of experience in starting things from scratch. He has been developing highly scalable tech products, business segments and brands in several industries and markets, including data protection, where he found his passion. Applying his broad skill set at Vaultree, Tilo's big goal is to bring cybersecurity closer to the public and accessible to everyone. can be reached via [LinkedIn](#) and at our company website <https://www.vaultree.com>





## Public Sector Must Remain Diligent as Cloud and Ransomware Intersect

By Rick Vanover, Senior Director of Product Strategy at Veeam

Often, when a citizen interacts with a government agency, a piece of personal information is provided and stored. This means ransomware attacks threaten the exposure of both internal government data as well as citizen information.

Being the proprietor of citizen data – from motor vehicle records to photo identification documents – puts government agencies in a more precarious position than private companies.

According to a recent Maximus research brief, [91% of the responding federal employees](#) indicated that “they have all, most, or some systems and solutions in the cloud.” The current work from home environment the pandemic helped cultivate caused cloud capabilities and by extension, SaaS, to become a necessity for government and private industries alike.

It is estimated that the federal government spent over six billion dollars on cloud computing in 2020, a figure that is expected to increase in the future.

As we evolve how and where we store personal data, our adversaries too evolve the means in which they target it. And, because of this increase in personal information being stored on the cloud, bad actors are more frequently targeting cloud capabilities.

---

With the [Office of Personnel Management's recently released telework guidance](#), the recommendation to increase telework access means continued reliance on cloud and SaaS, and the accompanying potential for cloud-targeted ransomware attacks.

It is projected that by 2025, [75% of IT organizations](#) will be hit with at least one ransomware attack, it's more important than ever that agencies using SaaS and cloud programs back up their data.

## A Three Step Process for Government Agency Resiliency

Cloud and SaaS capabilities will continue to be staples for federal agencies so, how can the government make sure they protect and backup data to prevent ransomware attacks?

For government agencies to effectively protect cloud-hosted data and the associated web-based software, they need to know their opposition, implement a strong backup infrastructure, and deploy processes to deal with the aftermath of an attack.

Ransomware attacks tend to go after remote access methods that are not built in a secure manner), utilize phishing attacks or capitalize on system vulnerabilities. By implementing secure remote access, training employees about phishing and ensuring systems and software are always up-to-date, agencies can take a preventative stance against ransomware.

Because ransomware agents seek to block system access in exchange for payment, the best defense against these attacks is a strong backup infrastructure and data protection system.

Implementing multi-factor authentication for SaaS applications can strengthen data protection because it strengthens accessibility requirements. And, while it goes without saying that data should always be backed up, it's especially important that cloud-based data backups are stored on devices that aren't connected to a network. According to [Veeam's 2021 Cloud Trends Report](#), more than half of SaaS admins agree that data should be backed up to protect an agency against a cyber event.

And, while many government agencies already utilize data encryption, they should take that practice a step further by encrypting backups for an added layer of protection.

Unfortunately, no matter how well agencies are prepared, ransomware attacks are still likely to occur in the coming years. Therefore, it's imperative that government is prepared to handle a successful attack and has the necessary processes in place.

To start, government agencies should have an emergency contact list prepared that identifies who and how to contact the necessary IT teams, employees and external resources in security, incident response and identity management.

Prompt response can ensure necessary data is more effectively recovered as well as aid in minimizing the risks related to the data that has been lost. If the data loss impacts citizens and their personally identifiable information, cross-agency collaboration is likely to ensure the appropriate measures are put in place to protect those affected.

---

## After a Ransomware Attack, Rebuild and Start Again

Ideally government agencies won't see an increase in ransomware attacks on cloud capabilities even as systems more frequently leverage them because of the uptick in remote work. To remain vigilant, they should know their potential enemies, implement a strong backup infrastructure, and deploy processes to deal with the aftermath of an attack.

### About the Author

Rick Vanover is a Senior Director of Product Strategy at Veeam. Rick is an expert in intelligent data management and backup. In his role at Veeam, Rick sits at the crossroads of many types of storage. Whether it is storage systems, critical application data, data in the cloud or data anywhere in between; Rick has experience in the data management practice as IT practices change with new technologies. Follow Rick on Twitter [@RickVanover](https://twitter.com/RickVanover) and he can be reached online at [www.veeam.com](http://www.veeam.com)





# EVENTS



# CYBER DEFENSE CONFERENCES

**SOLUTIONS**



**SHOWCASE**

**CISO CONFERENCE**

TOP 100 CISO  
2022  
CyberDefenseCon



**CYBER INVESTOR  
WHALE TANK™**

## ***THREE EVENTS IN ONE***

**Orlando, Florida, USA | October 27-28, 2022**

***One of the most exclusive, fun and educational CISO conferences of the year!***

***Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world renowned expert - meets 100 top cyber defense companies in an intimate, high value two day summit***

**[www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com)**





# **RSA**<sup>®</sup>Conference

---

## **San Francisco**

---

**Moscone Center & Digital | June. 06 - 09, 2022**



**REGISTER NOW**



# Why Attend?



GES-2022



## Renowned Speakers, Unparalleled Content

Global EmergeTech Summit - is an ideal platform for networking with industry players; senior managers, decision - makers, and practitioners operating in the transformation space and making the most of emerging technologies like AI, Data, and Cloud. The Summit will host leaders and experts from across the region representing, varied industry verticals.



## Gain an Edge, with Latest Perspective

Global Industry Experts, who will delve into the latest cutting-edge tools and frameworks - shaping the business - will also share case studies and success stories that help acquire a competent viewpoint in achieving your set goals



## Network with industry leaders face-to-face

Meet subject experts who are leading the transformation agenda, discuss and deliberate on various issues. Leverage this opportunity to meet your idols and click a selfie with leading luminaries



## Learn, Learn Learn!

Expand your knowledge and find relevant solutions to pressing concerns, learn from thought-leaders, share your ideas and gain insights on the best and next practices prevalent in your industry



# GES-2022

## Global EmergeTech Summit

### Impactful Innovations Influencing Digital Transformation

May 10<sup>th</sup>, 2022

Venue : The Address Dubai Mall, UAE

Through the Global Emergetech Summit, we aim to explore how key technologies at the frontier, such as cloud and AI, to those that form the bridge to tomorrow, such as Big Data, IoT and Blockchain, are impacting businesses. The Summit will look into the current adoption of these technologies in the Middle East, along with the benefits they have to offer and discuss best and next practices that leaders & experts are following to foster a successful transformation.

## Our Speakers



Lama Arabiat  
Head Of AI Ministry of digital economy and entrepreneurship, Government of Jordan



Dr. Jassim Hajji  
President Artificial Intelligence Society / President International Group of Artificial Intelligence



Latifa Saleh Aishchhi  
Head of Data Management, Road and Transport Authority



Kate Barker  
Chief HR Futurist & strategic advisor, Neom

## Our Sponsors

**NUTANIX**

## HYBRID – Attend in-person in Dubai or the virtual stream online

CONTACT US AT

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

+44 20 3808 8625



SCAN TO KNOW MORE



Conceptualized and Organized By



In Association With

# DACHsec

SECURING THE REGION FROM CYBER THREATS

10th - 11th May 2022

Munich, Germany

[dach.cyberseries.io](https://dach.cyberseries.io)

Join Us at the DACHsec IT Security Summit in Munich on 10th-11th May!

The 4th annual **DACHsec IT Security Summit** brings together **120+ IT security leaders** from across the **Banking & Finance, Retail, Government, Healthcare, Oil & Gas, Energy and Transportation industries** for 2-days of insight building and expert knowledge exchange in **Munich, Germany** on **10th - 11th May**. Join us to hone your skills in areas including:

- Reducing Insecurities in the Cloud for Better Security Strategies
- Cyber Regulation: How to Ensure Compliance
- Is the CISO Responsible for Your Cyber Security?
- Cloud Security: How to Build a Safe, Mature Cloud Security Strategy
- Cyber Risk in the Financial Sector



Speakers include CISOs, VPs, Heads of IT Security at: **Bucher Industries, Vontobel, Fresenius, Texas Instruments** and more...



Stefan Wenigmann  
Group CISO





Oliver Wyler  
CISO





Stefan Romberg  
Group CISO





David Watrin  
CTO & CISO





Andreas Prass  
CISO/DPO





Rouzbeh Barzegar  
Cyber Culture & Training  
Manager





Linda Strick  
Director CSA EMEA





Hans-Wilhelm Dünn  
President





Ali Baccouche  
Regional Information  
Security & Data Privacy  
Officer



This is a one-of-a-kind opportunity for cyber security leaders across DACH, to come together and safeguard their networks. View the agenda & **secure your place for FREE** using the discount code: **CDMVIP** at: [dach.cyberseries.io](https://dach.cyberseries.io) - T&Cs apply.

# CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

## We're Back!

### Live & In-Person, 11-12 May 2022, Santa Clara Convention Centre, CA

The **Cyber Security & Cloud Expo** will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

 <b>8</b> Conference Tracks	 <b>250+</b> Speakers	 <b>150+</b> Exhibitors	 <b>6</b> Co-Located Events	 <b>6,000+</b> Attendees
---	---	---	---	--

## Speakers include:



**Roland Cloutier**  
Global CSO,  
*TikTok*



**Kavitha Venkataswamy**  
Senior Manager -  
Product Security,  
*Capital One*



**Sri Esha Subbiah**  
Director of Engineering  
*American Express*



**Bruce Kaalund**  
Lead Cyber Security  
Analyst  
*Visa*

## Register now for free tickets!

> [www.cybersecuritycloudexpo.com/northamerica](http://www.cybersecuritycloudexpo.com/northamerica)  
> [enquiries@techexevent.com](mailto:enquiries@techexevent.com)



**TECHEX**  
NORTH AMERICA

**Contact:**  
[www.techexevent.com](http://www.techexevent.com)  
[enquiries@techexevent.com](mailto:enquiries@techexevent.com)

**CYBER SECURITY & CLOUD CONGRESS**  
NORTH AMERICA

**IOT TECH EXPO**  
NORTH AMERICA

**AI & BIG DATA EXPO**  
NORTH AMERICA

**BLOCKCHAIN EXPO**  
NORTH AMERICA

**EDGE COMPUTING EXPO**  
NORTH AMERICA

**DIGITAL TRANSFORMATION WEEK**



# PRIVACY-ENHANCING TECHNOLOGY SUMMIT NORTH AMERICA

**BOSTON, USA**

**MAY 18 & 19**

**ENABLING INNOVATION, IMPROVING  
INFORMATION SECURITY &  
FACILITATING COMPLIANCE**

**BOOK NOW TO SAVE!**

## 25+ SPEAKERS



Erwin Gianchandani  
Senior Advisor for  
Translation, Innovation,  
and Partnerships  
National Science  
Foundation



Alex Taylor  
Global Head of Emerging  
Technology  
QBE Ventures  
QBE Insurance Group  
Limited



Shahidul Mannan  
Head of Data  
Engineering  
& Innovation  
Mass General Brigham  
(Partners Healthcare)



Hitesh Yuvraj  
Director - Product  
Management &  
Strategy  
Mastercard

**DOWNLOAD OUR AGENDA FOR MORE INFORMATION!**

[Follow Us On LinkedIn](#)

[Follow Us On Twitter](#)

[Visit Our Website](#)

# ePAY SUMMIT

E-payments & online banking

EUROPE

HYBRID

19 MAY 2022 • LONDON

**DIGITAL PAYMENTS IS  
NO LONGER AN OPTION  
IT IS A NECESSITY.  
GET STRAIGHT TO  
THE HEART OF THE  
EPAY AGENDA.**

**REGISTER TODAY**

[www.epaysummit.com/eu](http://www.epaysummit.com/eu)



SUPPORTED BY

سلطنة عُمان  
وزارة النقل والاتصالات وتقنية المعلومات  
Sultanate of Oman  
Ministry of Transport, Communications and  
Information Technology

böwö  
العاصمة العربية الرقمية  
Muscat Arab Digital Capital  
2022

PARTNERS

oits  
الجمعية العمومية للمعلومات  
Oman Information Technology Society

الجمعية العمومية للخدمات النفطية  
Oman Society for Petroleum Services

31<sup>st</sup>  
EDITION

COMEX  
Technology Show معرض كومكس للتكنولوجيا

23 - 25 MAY, 2022  
Face 2 Face at OCEC Muscat &  
on Virtual Platform

EMBRACING

FUTURE

TECHNOLOGIES

#COMEXOMAN

KEY INDUSTRIES

MANUFACTURING

HEALTH CARE

TOURISM

RETAIL

TRANSPORT & LOGISTICS

EDUCATION

OIL & GAS

BANKING & FINANCE

ICT INVESTMENTS

COMEX  
eGOVT PAVILION  
Ministries | Authorities | Government Companies

COMEX  
BUSINESS ARENA

COMEX AI  
CONFERENCE

COMEX  
EXCELLENCE  
IN TECHNOLOGY  
AWARDS

COMEX  
BANKING  
AND FINTECH  
ZONE

COMEX  
كومكس للمشاريع التقنية  
TECH VENTURES



CONSUMER TECH &  
SMART SHOPPERS



COMEX  
EXPERIENTIAL



SCHOOL'S X



SCHOOL  
STEM



WORKSHOPS



COMEX  
TECH CLUB

MAIN SPONSOR

DELL Technologies

DIGITAL TRANSFORMATION PARTNER

Microsoft

YOUR DATA CENTRE & ICT PARTNER

MDS  
MIDDLE EAST DATA SYSTEMS - OMAN

ORGANISER

Arabian  
Research  
Bureau

OITE

DIAMOND SPONSORS

المركز الوطني  
للإحصاء  
والمعلومات  
سلطنة عُمان  
NATIONAL CENTRE  
FOR STATISTICS  
& INFORMATION  
Enhancing Knowledge  
SULTANATE OF OMAN

TREND  
MICRO

نפטعمان  
omanoil

FORTINET

عنصر للتكنولوجيا  
Onsor Technologies

PLATINUM SPONSOR  
GLOBCOM  
Bringing IT Together

SILVER SPONSORS

AMW  
GAS

OFFICIAL TRAVEL PARTNER

السلام  
SalamAir

VISITOR BAG SPONSOR

مدائن  
madayn

MEDIA PARTNERS

TELECOM Review  
thebusinessyear

Dossier

arabnet

thebusinessyear

CYBER DEFENSE  
MAGAZINE

For more info, visit: [www.comex.om](http://www.comex.om)

+968 95098034

# ItaliaSec

## SECURING ITALY FROM CYBER THREATS

24th - 25th May 2022

Milan, Italy

Join Free with Code: CDM-VIP

Join Us at the ItaliaSec Summit on 24th - 25th May!

The 6th annual **ItaliaSec Summit** brings together **150+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **24th - 25th May**. Join us in **Milan, Italy** to hone your skills in areas including:

- *Cyber resilience for the digital age*
- *Reacting to the growing attack surface*
- *Emerging trends and risk factors in modern cloud security frameworks*
- *Risk-based security to aid business agility*
- *Developing and updating incident response plans*
- *Strategies for mitigating insider threats*
- *And, more!*



Speakers include CISOs, VPs, Heads of IT Security at: **Leroy Merlin, Illimity, Volksbank, Intrum**, and more...



Alessio Setaro  
CISO



Gianluca Manzini  
Head of IT



Simone Pezzoli  
CISO



Loredana Mancini  
Vice Chair



Uberto Vittorio Favero  
Cyber Security Expert



Paola Rocco  
ISO



Franco Cerutti  
IT Director



Matteo Corsi  
Global IT Security  
Manager



Petra Chiste  
Head of IT Security



Massimo Ravenna  
Head of Cyber  
Security



This is a one-of-a-kind opportunity for cyber security leaders across Italy to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: [italy.cyberseries.io/register](https://italy.cyberseries.io/register)/T&Cs apply.





RegTech Africa  
Conference

# REGTECH AFRICA

# CONFERENCE 2022

Theme: Regulatory innovation:  
Bolstering Africa's role in the  
global economy

Date

25th & 26th, May 2022

To Register

[www.regtech.africa/register](http://www.regtech.africa/register)

For information on sponsorship opportunities please contact us on:

Tel: +2348034225060 or Email: [info@regtech.africa](mailto:info@regtech.africa)

For more information visit: [www.regtech.africa](http://www.regtech.africa)



# EUROPEAN CONGRESS

TOULOUSE  
30 May - 1 June 2022

Smart and Sustainable  
Mobility for all.



**Toulouse**

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

# Registrations are open! Book today!

ORGANISED BY:



HOSTED BY:



2<sup>ND</sup> EDITION OF  
**CYSEC GLOBAL**  
SERIES



# **CYSEC** **QATAR**

**21 JUNE 2022**

JOIN US IN-PERSON IN DOHA, QATAR

**BY-INVITATION ONLY EVENT**

Securing the Digital Qatar's  
Economy in the Smart  
Connected World

ORGANIZED BY

**MAK**

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

**SCAN ME**  
FOR MORE DETAILS





# BACK TOGETHER, STRONGER TOGETHER

This 21 - 23 June, at ExCeL London, the Infosec community will be back together in force. Be there to meet the most influential cybersecurity solution providers, hear the world's leading thought leaders and network with your peers.

[Register Now](#)

Visit us at [infosecurityeurope.com/cyberdefense](https://infosecurityeurope.com/cyberdefense)

**info**security

EUROPE

ExCeL London

21 - 23 June, 2022

# NFT



EXPOVERSE

**THE LARGEST MASS  
ADOPTION BLOCKCHAIN  
EVENT OF THE YEAR**

*This July*

FRI  
**29**

SAT  
**30**

SUN  
**31**

**Los Angeles, CA**  
LA Convention Center



**SCAN HERE!**

Use code **CDEFENSEMAG** for **10% OFF** tickets!

[nftexpoverse.com/get-tickets](https://nftexpoverse.com/get-tickets)



Media Partners  
**100+**



Attendees  
**15,000+**



Speakers  
**150+**



Vendors  
**400+**

# Future Tech Event

UNDER THE PATRONAGE

سلطنة عُمان  
وزارة النقل والاتصالات وتقنية المعلومات  
Sultanate of Oman  
Ministry of Transport, Communications and  
Information Technology

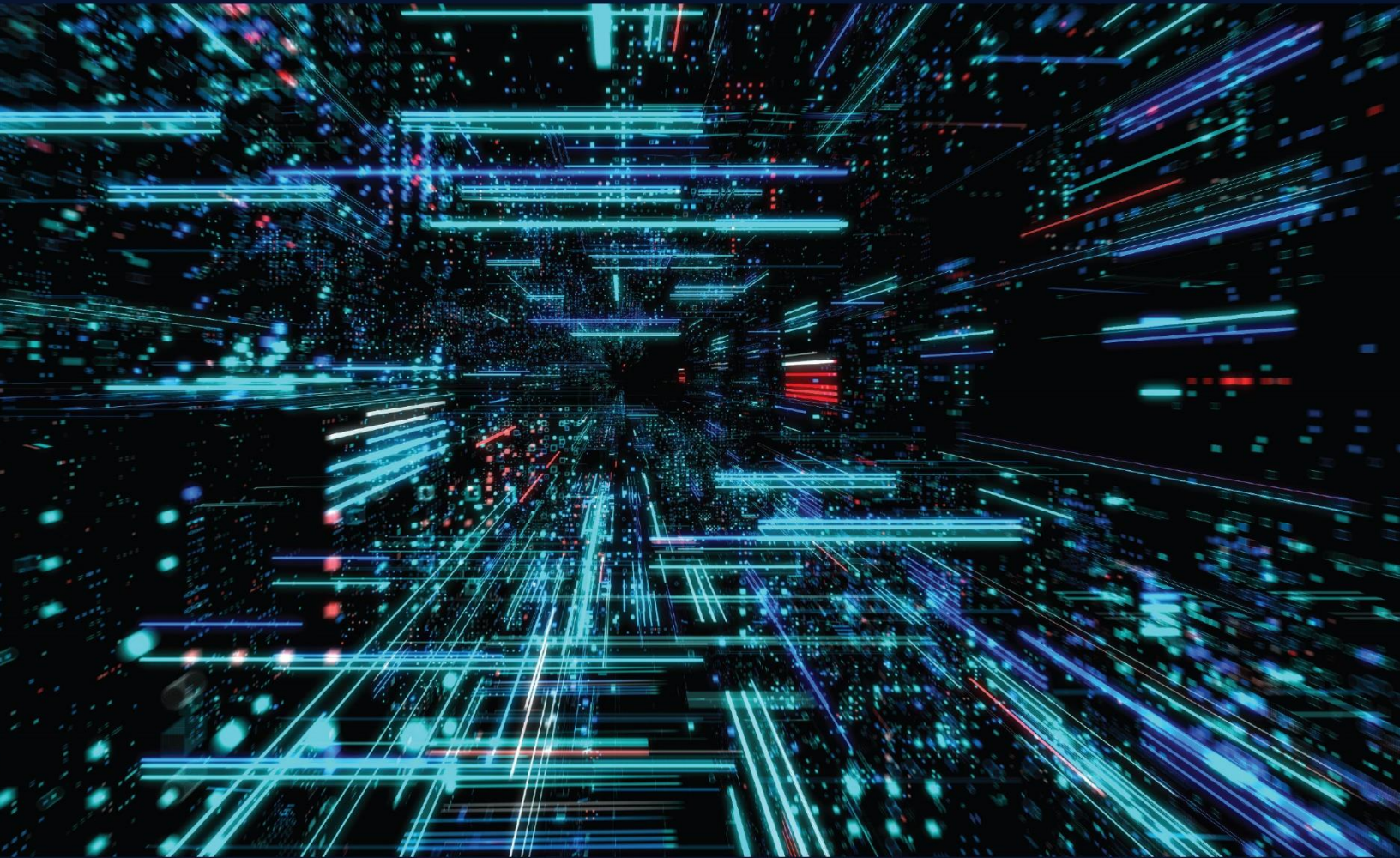


## ENABLING OMAN'S VISION 2040

12 - 13 September 2022 | Oman Convention and Exhibition Centre | 9 am - 4 pm

**HYBRID+** (In-Person and Online)

Future Tech is Sultanate of Oman's foremost B2B and B2G  
bespoke Technology Expo and Summit.



For Exhibiting Enquiries and Sponsorship Opportunities please contact:

Navneeth K, Director - Business Development

+968 9123 7892 | [bdm@wpsummits.com](mailto:bdm@wpsummits.com)

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

ORGANISED BY



مسقط إكسبو  
MUSCAT EXPO

**WPS**

WHITE PAPER  
SUMMITS

# CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

## We're Back!

Live & In-Person, 5-6 October 2022,  
Santa Clara Convention Centre, CA

The **Cyber Security & Cloud Expo** will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.



**8**  
Conference  
Tracks



**250+**  
Speakers



**150+**  
Exhibitors



**6**  
Co-Located  
Events



**6,000+**  
Attendees

## Speakers include:



TikTok

**Roland Cloutier**  
Global CSO,  
TikTok



Capital One

**Kavitha Venkataswamy**  
Senior Manager -  
Product Security,  
Capital One



AMERICAN EXPRESS

**Sri Esha Subbiah**  
Director of Engineering,  
American Express



headspace

**Elizabeth Cartier**  
Director - Information  
Security,  
Headspace Inc.

## Register now for free tickets!

> [www.cybersecuritycloudexpo.com/northamerica](http://www.cybersecuritycloudexpo.com/northamerica)  
> [enquiries@techexevent.com](mailto:enquiries@techexevent.com)



# TECHEX

NORTH AMERICA

Contact:  
[www.techexevent.com](http://www.techexevent.com)  
[enquiries@techexevent.com](mailto:enquiries@techexevent.com)

**CYBER SECURITY & CLOUD CONGRESS**  
NORTH AMERICA

**IOT TECH EXPO**  
NORTH AMERICA

**AI & BIG DATA EXPO**  
NORTH AMERICA

**BLOCKCHAIN EXPO**  
NORTH AMERICA

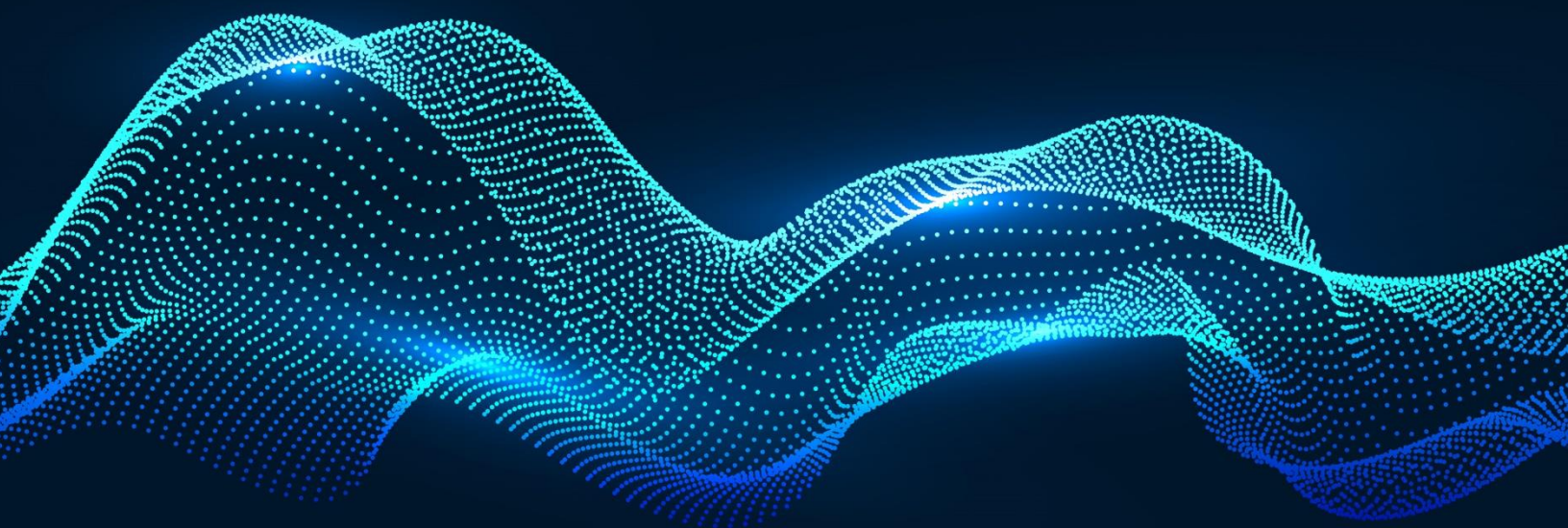
**EDGE COMPUTING EXPO**  
NORTH AMERICA

**DIGITAL TRANSFORMATION WEEK**

# LEVELLING UP UK CYBER SECURITY

We believe there is a knowledge gap between the expertise of the cyber community and UK business leaders.

We want to close that gap.



Contribute to the programme by visiting [www.ukcyberweek.co.uk/call-for-papers](http://www.ukcyberweek.co.uk/call-for-papers).

## OUR PARTNERS



3 >> 4 NOVEMBER 2022

Business Design Centre | London





# CYBER DEFENSE TV

## INFOSEC KNOWLEDGE IS POWER

[CyberDefense.TV](https://www.cyberdefense.tv) now has 200 hotseat interviews and growing...

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

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

### The Interviews

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

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. [www.cyberdefense.tv](http://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) 2022, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com, and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

All rights reserved worldwide. Copyright © 2022, 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.

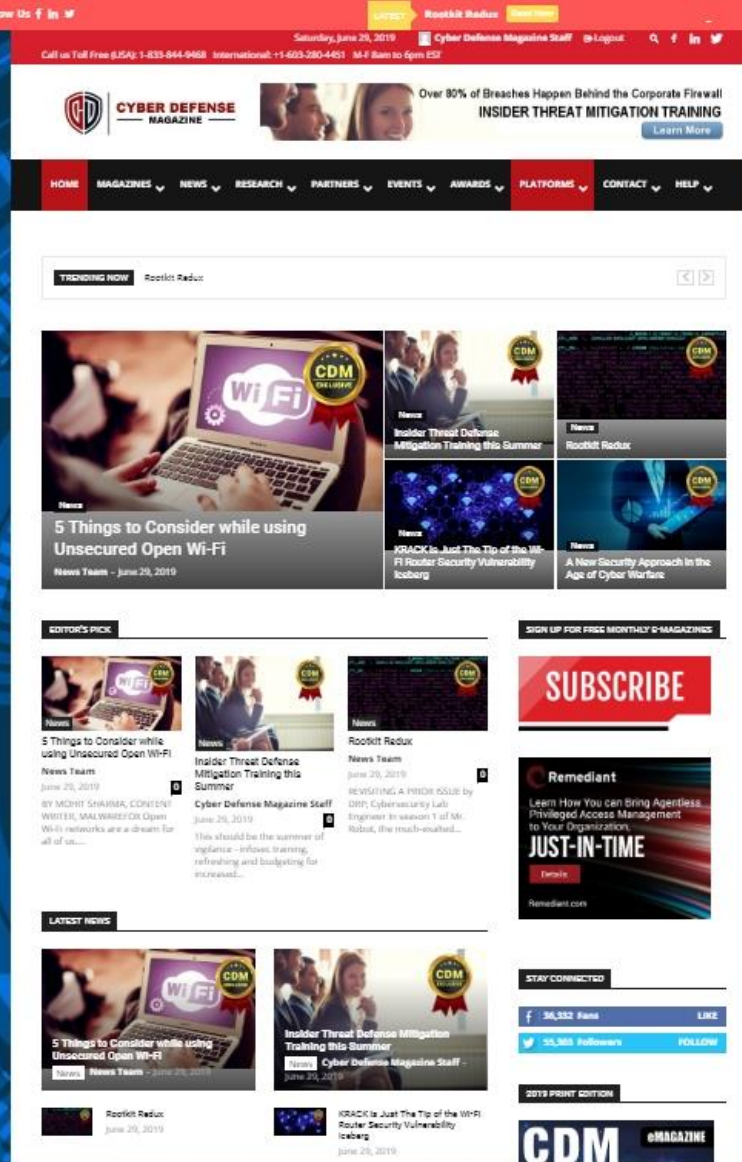
All rights reserved worldwide.

[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: 05/02/2022



Books by our Publisher: <https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPN59NH> (with others coming soon...)

*10 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 past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and [CyberDefenseMagazine.com](http://CyberDefenseMagazine.com) up and running as an array of live mirror sites and our new B2C consumer magazine [CyberSecurityMagazine.com](http://CyberSecurityMagazine.com). *Millions of monthly readers and new platforms coming...starting with [www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com) this month...*

# CyberDefenseCon 2022

# 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**

# Preventing Tomorrow's Malware Today.



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



# CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER



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

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

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

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

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



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