CISOs TALKING SHOP AND TRADING WAR STORIES

# InfoSecurity PROFESSIONAL

JULY/AUGUST 2022

Practical Advice. Actionable Insights.

RETOOL USING MITRE ATT&CK

ASSESSING CRITICAL INFRASTRUCTURE

MINIMIZING HUMAN ERRORS

# IT/OT CONVERGENCE

Benefits. Disruptions. Consequences. Implications.

(ISC)²®

# Rock-solid cyber defense.

**At BlueVoyant, we recognize that effective cybersecurity requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem.**

Ebook

Digital Risk Protection

From Reactive to Proactive Security Posture

BlueVoyant
Sky: DRP

BlueVoyant

**Digital Risk Protection Platform**
BlueVoyant provides organizations with real-time visibility of digital threats by continuously monitoring domains and websites, social media, apps in official and unofficial stores, deep & dark web, instant messaging and open-source – allowing for quick and effective breach mitigation.

BlueVoyant's extensive global coverage, data science, and analyst expertise, enables identification of malicious "look-alike" attacks, live phishing pages, and more. A competitive differentiator, we have an unmatched ability to take action on your behalf to eliminate threats to your brand, employees, and customers.

**BlueVoyant's new eBook, "Digital Risk Protection: From Reactive to Proactive Security Posture" addresses the following:**

- Common cyberattacks used by today's threat actors
- Recent changes to the threat landscape based on the increasing popularity of hybrid work models
- The advantage of leveraging a Digital Risk Protection (DRP) solution to establish visibility and establish a proactive approach to security

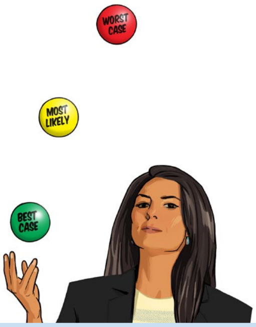
Learn more at www.bluevoyant.com
Download the DRP eBook:
https://www.bluevoyant.com/resources/digital-risk-protection-ebook/

CONTENTS ▪ JULY/AUGUST 2022 ▪ VOLUME 15 - ISSUE 4

Are we accurately assessing threats to critical infrastructure?

PAGE 27

## FEATURES



*Cover photograph by John Kuczala*

*Photograph (above) by Getty Images*

*Page 33 illustration (right) by Frank Stockton*

## DEPARTMENTS

# EDITOR'S NOTE

**ANNE SAITA** **EDITOR-IN-CHIEF**

## Are We Teaching Emerging Professionals the Right Lessons?

**ONE OF MY FAVORITE** columns is Office Hours, written by two, alternating cybersecurity leaders who speak from experience on a range of topics. While Mike Hanna and Spencer Wilcox, both CISSPs, usually focus on professional development, sometimes they veer in a different direction. Such is the case with this issue in which Spencer discusses how vulnerable industrial control systems (ICS) remain. It is a nice complement to our cover story on IT/OT convergence by CISSP Julien Legrand in Hong Kong.

Spencer recalls two disasters that caused large-scale loss of life and what has been done since to reduce human errors. One approach has been to modernize the infrastructure surrounding ICS along with supervisory control and data acquisition (SCADA) systems known for long-term use of lagging tech. And yet, in doing so, once an IT asset is virtualized and networked, it also is more suspectable to cyberattacks. Russia's assault on Ukraine this year is a reminder that we all must devote ample resources to preventing critical systems from being compromised.

Spencer's piece, however, homes in on the non-technical aspects of systems protections. Humans still account for the bulk of breaches, whether from misconfigurations or malware. It made him wonder if formal programs to groom future cyber professionals miss the mark with curricula that emphasizes how to break in, rather than hold off threat actors. He cites Capture the Flag competitions in high schools and colleges, which reward those who penetrate networks and databases with dopamine-like accolades.

Understanding adversarial behavior is certainly an important skill. And Spencer himself says Capture the Flag contests serve a purpose in someone's cybersecurity education. This seems to be recognized in the number of organizations that now conduct purple teaming, a hybrid of the more familiar red team/blue team pen testing. Purple teaming is built on a more collaborative model in which teams work alongside—rather than against—each other to test existing controls against pre-determined attack methods.

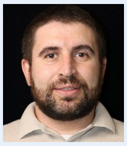
This approach to understanding adversarial behavior is gaining traction at a good time, especially for manufacturers and industrials beginning or continuing to virtualize aging IT components. With every digitization comes a new set of risks and an expanding attack surface. Finding the right tools and training to protect an expanding IT/OT threat landscape is important. And not just to those whose livelihoods are on the line. ●

Photograph by Louise Roup

**Anne Saita** lives and works in San Diego. She can be reached at asaita@isc2.org.

## CONTRIBUTORS

**Julien Legrand**, CISSP, fell in love with Asian culture while traveling a few years ago and decided to move to Hong Kong, where he still lives and works and wrote our cover story on IT/OT convergence. He looks forward to resuming his travels, including to (ISC)² events.



**Éder de Mattos**, CISSP-ISSAP, ISSMP, CISSP, CCSP, has spent the past 15 of his 21 years in security/cloud/networking/IT working for telecom service providers, most recently as a Brazil-based professional services senior cloud security consultant at a large cloud provider. He shares what he's learned in our feature on protecting critical infrastructure, starting with telecommunications.

Our third writer this issue is **Charlene Deaver-Vazquez**, CISSP, CISA, who shares how to pivot and stay agile using the MITRE ATT&CK framework. No stranger to challenges, in the 1990s she was dropped in a remote region of the Alaska Range to hike solo for a week among golden eagles, dall sheep, caribou, wolves, grizzlies, and what she fondly refers to as Alaska's unofficial state bird—the mosquito.

Some may think it would have been best to digitally colorize the ropes used on our cover story images, but expert photo manipulator **John Kuczala** chose to hand-dye the fibers for greater authenticity and impact. Mission accomplished.

Early on, **Frank Stockton** was influenced by Jackie Chan and Star Wars films, and Italian Renaissance painting. Frank later earned an MFA from UCLA. He teaches college-level illustration. Nominated for a comic-industry Eisner Award, his work has been featured in *Wired*, *The Atlantic*, *Rolling Stone*, *Forbes*, *Inc.*, *Money* and many more.

CONTENTS

(ISC)²

# SECURITY CONGRESS

## In-Person and Virtual

OCT 10 -12 LAS VEGAS CAESARS PALACE

Join thousands of your professional peers at (ISC)² Security Congress, cybersecurity's ideas-and-education global conference. Don't miss this unparalleled meeting of the minds, driven by the mission to advance the interests of industry professionals around the world at every stage of their careers. This fall, we're back in person!

### 12th annual Security Congress Features

- Star Keynotes
- 120+ Sessions
- Career Guidance and Resources
- CPE Credit Opportunities
- Industry-leading Exhibitors and Sponsors
- Pre-Conference Training Courses
- Exclusive Networking
- Group Pricing – Bring Your Team!

Register Now

Congress.isc2.org | #ISC2Congress

InfoSecurity
PROFESSIONAL
Practical Advice. Actionable Insights.

(ISC)²® INSPIRING A SAFE AND SECURE CYBER WORLD

isc2.org community.isc2.org

READ. QUIZ. EARN.

## Earn Two CPE Credits for Reading This Issue and Taking the Online Quiz

In order to earn the two CPE credits, you must pass the issue quiz. Please provide your name and (ISC)² member number so that we can award the two CPE credits to your account. This typically takes up to 15 business days to be added to your account.

https://www.isc2.org/InfoSecurity-Professional

Learn about more opportunities to earn CPE credits at https://www.isc2.org/Membership/CPE-Opportunities

## ADVERTISER INDEX

For information about advertising in this publication, please contact Vendor Sponsorship: Lisa Pettograsso, lpettograsso@isc2.org.

| | |
|---|---|
| BlueVoyant | 2 |
| (ISC)² Enterprise Training Solutions | 4 |
| (ISC)² Security Congress | 6 |
| (ISC)² Secure Summits | 9 |
| Identity Defined Security Alliance | 13 |
| (ISC)² Cyberthreat Defense Report | 14 |
| SimSpace | 16 |
| (ISC)² CISSP+CCSP: The Power of DUO | 17 |
| (ISC)² 2022 Cloud Security Report | 19 |
| (ISC)² CCSP: The Next Big Thing | 26 |
| SEM | 36 |
| (ISC)² Secure Webinars | 37 |
| (ISC)² Commit to CCSP | 39 |

*InfoSecurity Professional* is produced by Twirling Tiger® Media. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email lpettograsso@isc2.org.

**(ISC)² MANAGEMENT TEAM**

EXECUTIVE PUBLISHER
Chris Green
+44-203-960-7812
cgreen@isc2.org

DIRECTOR, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129
jlefebvre@isc2.org

MANAGER, MEMBER COMMUNICATIONS
Kaity Pursino
727-683-0146
kpursino@isc2.org

SR. CORPORATE COMMUNICATIONS SPECIALIST
Andrea Moore
727-270-9613
amoore@isc2.org

**SALES**

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

**TWIRLING TIGER MEDIA MAGAZINE TEAM**

EDITOR-IN-CHIEF
Anne Saita
asaita@isc2.org

ART & PRODUCTION DIRECTOR
Maureen Joyce
mjoyce@isc2.org

Twirling Tiger Media is a women-owned small business. This partnership reflects (ISC)²'s commitment to supplier diversity.

CONTENTS

# CISOs Talking Shop and Trading War Stories

BY JON FRANCE, CISSP, CISO, (ISC)²

**It might surprise you to learn that I am the first** chief information security officer (CISO) at (ISC)². The organization that has helped the careers of many CISOs now has one of its own, somewhat in part recognizing the importance of having a CISO report into the CEO, ensuring that the expanding digital footprint of (ISC)² is protected, along with playing a part in the organization's focus on closing the skills gap.

I'm also located in the United Kingdom, which is the second largest membership location globally, rather than the United States like most other (ISC)² executives. Again, (ISC)² is firmly committed to a diversified workforce, including hiring executives around the globe.

I spent my early career in the media sector, building online products as well as all the related infrastructure and network—back in the days of on-premises server rooms, racks and tin! I then moved into the mobile telecoms sector, looking after the mobile industry association's global infrastructure and cybersecurity before moving into a pure security role representing the interests of the industry until landing here at (ISC)² in January.

As the organization's CISO, I'm tasked with three main strategic objectives:

- Protect the organization from cyber threats
- Advocate on behalf of the membership
- Help close the global workforce gap

Only one of these falls under the traditional CISO role, but the other two are equally important to our organization and industry at large. Quite frankly, the world needs more (ISC)² members to swell the ranks of cybersecurity professionals at all levels, ultimately resulting in qualified, globally benchmarked and certified cybersecurity professionals to properly protect our data, systems and networks.

**Jon France** is the (ISC)² CISO. He can be reached at jfrance@isc2.org.

## CISO Roundtables

We also need to support cybersecurity leaders in both the public and private sectors, which is why I'm excited by the thought leadership events happening this year that include CISOs as part of a broader Executive Roundtable program. These peer-to-peer sessions with global leaders are focused on thought leadership; that is, these are high-level, vendor-neutral or -agnostic discussions that focus on current and emerging issues and how they might impact organizations in the near future. How do we position resources to combat current and emerging threats? Where are attackers now succeeding—or failing? And how do we harden assets and infrastructure in a digital business and IT environment?

My role is to seed interest in topics at each of these regional gatherings—topics I know are of interest and importance to CISOs … like me. Each participant should walk away with a better understanding of their own organization's strengths and weaknesses and where to devote more resources going forward. In turn, (ISC)² will learn from these sessions and incorporate the insight into our work for the benefit of all members.

We all need to support each other and continue filling talent pipelines with people who are good technologists as well as critical thinkers who can solve problems quickly. That's what makes this such an interesting time to be in our industry and respective fields. As they say, "It's a target-rich environment." ●

CONTENTS

(ISC)²®

# SECURE SUMMITS

**Make plans now to attend this exciting new event series in 2022.**

Register today and join your peers for a collaborative deep dive into the most current cybersecurity issues impacting organizations in your local and regional markets. You'll come back inspired with new ideas and solutions from a diversity of perspectives.

**Each SECURE Summit features:**

- Expert Presentations
- Exclusive Networking
- 7 CPE Credits Available
- Exhibit Hall

**IN-PERSON SUMMITS:**

- SECURE Singapore
  Thursday, July 14
  Shangri-La Singapore
- SECURE Washington, D.C.
  Friday, December 9, 2022
  Renaissance Washington,
  DC Downtown Hotel

**LIVE VIRTUAL SUMMITS:**

- SECURE Asia-Pacific
  Thursday, November 10
- SECURE U.K. & Europe
  Thursday, December 8

LEARN MORE
AND REGISTER AT
www.isc2.org/events

**INTERESTED IN SPONSORING?** EMAIL US FOR MORE INFORMATION.

# Balancing Security and Business Requirements

*The best security professionals understand the end game is more than protection; it's staying profitable*

BY SANDIP DHOLAKIA, CISSP

**THOUGH STAYING** secure is a cybersecurity professional's priority, it isn't the only one. Staying in business is just as important, no matter your title.

To be the best cybersecurity practitioner, you must embrace both the IT and business sides of an organization. More than your career depends on it.

## At your service

While some functions may differ, security architect is almost an umbrella term for someone who provides the cybersecurity blueprint within an organization. To drive a security strategy, they must thoroughly understand end-to-end business processes as well as information security.

Sometimes the goals of security come into conflict with other service lines, particularly product development. Leadership typically wants to quickly produce functional, feature-rich products with minimal friction. Unfortunately, these teams too often see cybersecurity recommendations (or even requirements) as adding time and costs to production schedules. Business requirements take priority over the security ones—after all, security is still too often labeled only as a supporting function/cost center while product is seen as making money for the organization.

## Here to help, not hinder

Such an attitude can make it difficult to get buy-in from a product team, including its leadership, to implement security measures, even now when cyber threats are rising—as is public awareness.

In my experience, the easiest way to incorporate security requirements in the design stage is first to find out the type of data an application will process and store. The data classification decides the amount and type of cyber protections needed for the application—and prevents us from over- or under-protecting products in development.

Implementing the right level of security controls before and during the deployment stage—threat modeling, dynamic code scans, pen testing, etc.—translates into direct savings if they prevent expensive exploits and breaches. That needs to be made clear to stakeholders inclined to balk at our involvement.

Sandip Dholakia

Implementing the right level of security controls before and during the deployment stage—threat modeling, dynamic code scans, pen testing, etc.—translates into direct savings if they prevent expensive exploits and breaches.

The challenges continue in the operations phase, where a product team always wants to log everything possible. This can add to storage costs and analysis time. Security architects can instead guide teams to select logs based on security and regulatory requirements. In the retirement phase, product teams typically want to dispose of data and media without careful consideration of the proper method of disposing data based on its classification. Security architects should provide them with a process and criteria to ensure retired product is securely destroyed.

## Don't forget the importance of training

Over the years, I have noticed that most developers resist security testing because they fear a security scan will break the application. Or they'll discover something that will take time to fix and delay the release of the product. Here's where a security architect can provide security training, so developers see these measures as proactive protections, not productivity stoppers.

In conclusion, let's remember: An army needs air cover to advance in the battlefield. So too do security teams need support from upper management—employees will take us seriously only if management does. Let's give them a reason to root for us by showing we understand them and want to help everyone achieve their goals. ●

A version of this appears in the June *Insights* enewsletter.

CONTENTS

# We Stand with All of You

*Earlier this year (ISC)² issued an organizational statement in opposition to anti-DEI legislation. The statement is being published here in case you missed it on the (ISC)² blog.*

**AS THE WORLD'S FOREMOST** cybersecurity professional organization, (ISC)² is leading the charge to ensure our profession reflects the diversity of the world we serve. Diversity, equity and inclusion are strategic priorities for the individuals and organizations (ISC)² represents, and we believe that inspiring a safe and secure cyber world means ensuring a diverse, equitable and inclusive cybersecurity profession.

Today, our profession does not reflect the world we live in, and at the same time, the current Cybersecurity Workforce Gap as tracked by the (ISC)² Cybersecurity Workforce Study reports unfilled demand for more than 2.7 million professionals. Building a more diverse and inclusive profession is key to addressing the workforce shortage.

As an association that is actively driving change to ensure a more diverse, equitable and inclusive workforce and workplaces, we are troubled by any legislative measures that not only limit, but in some instances, outlaw, discussions about and considerations of diversity in schools and the workplace. These laws stand in direct opposition to our core values, and they could hinder the ability of organizations to directly address diversity, equity and inclusion in the workplace, which is vital for success in a globally interconnected world.

Only through frank and honest discussion can we break down barriers, establish common ground and affirm, for all, that DEI is about inclusion for everyone, not exclusion for anyone. We stand with other professional organizations like the American Society of Association Executives (ASAE) in opposing such laws as they undermine the development of a diverse and inclusive cybersecurity workforce.

**Only through frank and honest discussion can we break down barriers, establish common ground and affirm, for all, that DEI is about inclusion for everyone, not exclusion for anyone.**

(ISC)² represents almost 170,000 certified members in 175 countries worldwide. Our DEI Strategic Plan outlines the steps our organization is taking to ensure diverse, equitable and inclusive practices, and our DEI Resource Center provides dozens of guides that serves as a roadmap for other organizations and individuals seeking to establish similar programs. We will continue this important work and speak out against actions that curtail the progress we are making to inspire a safe and secure cyber world.

We support all our members globally, including members who may be directly affected by laws of limitation, and we will work to preserve their rights and expand our DEI practices. ●

Getty Images

# (ISC)² Giving 100k Career Pursuers Free Entry Into New Cert

**(ISC)² HAS ANNOUNCED THAT** it will help expand the United Kingdom's cybersecurity workforce by offering free certification and education for 100,000 cybersecurity career pursuers through its new entry-level cybersecurity certification.

The U.K. is one of the largest cybersecurity career markets in Europe, with more than 300,000 active cybersecurity practitioners. However, U.K. government figures indicate at least 17,500 new people need to enter the industry annually just to maintain the status quo. ●

CONTENTS

# Notes from (ISC)$^2$ SECURE London

*The first in a series of 2022 regional events considers global events' impact on current cyber resources*

**(ISC)$^2$'S FIRST IN-PERSON EVENT** since the start of the pandemic touched on several global issues: from the pandemic disruptions and unprecedented digital transformations to geopolitical strife at the doorstep of Europe generating fears of global cyberattacks.

## A tale of two tracks

Dual tracks allowed attendees to explore a variety of themes, from how to plan and deliver a successful security awareness program, told from the perspective of Data Protection Officer (DPO) Laurie-Anne Bourdain, CISSP, from Isabel Group. Meanwhile, Paul Schwarzenberger, CISSP, a cloud security specialist from Celidor, took attendees on a security deep dive into the three prevailing cloud platforms to determine which came out on top. Schwarzenberger looked at everyday use cases and live demonstrations to compare the security architectures and features across AWS, GCP and Azure.

Prevention of internal security issues was examined in detail by Dave Cartwright, CISSP, who explained how regardless of the investment in training, education, policy and more, organizations will still face human-induced cyber risk, simply because eventually someone will do something they shouldn't—be it intentionally or accidentally. Determining how to react—and when—is key to minimizing repeat incidents, as is defining whether a documented policy can apply to all instances. Going zero-tolerance can be counter-productive, he warned, while going zero-blame can also result in a lack of remedy from repeat offenders if there is no motivation to improve.

Current geopolitical and health issues have put the importance of robust supply chain cybersecurity in stark focus. (ISC)$^2$ CISO Jon France explored the latest developments and impacts on supply chains and critical infrastructure, discussing how supply chain cybersecurity practices have had to change and adapt in the face of COVID-19, digital attacks, and an increasingly interconnected world of infrastructure.

Diversity, equity and inclusion (DEI) is at the forefront of industry efforts to expand both the workforce and the talent pool, as well as make cybersecurity a more welcoming and accessible career path for more people. A panel bringing together Andrew Elliot, deputy director of cyber security innovation and skills at DCMS; Richard Yorke, managing director of Cyber Cheltenham; Catherine Burn, associate director at cybersecurity recruiter LT Harper; and Dr. Sanjana Mehta, advocacy director at (ISC)$^2$, explored with the audience what a diverse ecosystem means, who must be involved to deliver a successful diversity and inclusion effort, and debated why a more inclusive cyber profession will ultimately ensure the delivery of a safer cyber world for individuals and organizations alike.

## The power of the crowd

One of the most popular sessions focused on crowdsourced security, led by Alex Haynes, CISSP, the CISO at software provider CDL, and Joseph Carson, CISSP, chief security scientist and advisory CISO at access management provider Delinea. For the last decade, crowdsourced security has had a fundamental impact on pen testing, but it's not without risks. As well as discussing the pros and cons, Haynes provided attendees with insight into how the approach has been weaponized in the Ukraine conflict and has impacted innocent bystanders. Carson wrapped up the technical sessions with an extensive look at ransomware incidents and a step-by-step demonstration of an attack and how to effectively respond to it.

The day concluded with an interactive (ISC)² Insights session. Attendees posed questions to a panel composed of (ISC)² CEO Clar Rosso; CISO Jon France, CISSP; and board member Yiannis Pavlosoglou, CISSP. Panelists were asked about the forthcoming Entry-Level Cybersecurity Certification, the U.K. and global skills gap, the potential for government regulation of cybersecurity professional development and the role of a no-blame culture in cybersecurity response and remediation.

For (ISC)², SECURE London also represented an important milestone, the first purely in-person event staged by the organization since the COVID-19 pandemic took hold. Safely bringing together representatives from across our industry to meet, network and debate has been something we've looked forward to doing for a long time, with the results well worth the wait. ●

This was excerpted from a blog post on the (ISC)² website.

### Upcoming SECURE Events

- November 10 – SECURE Asia-Pacific (virtual)
- December 8 – SECURE U.K. & Europe (virtual)
- December 9 – SECURE Washington, D.C. (in person)

CONTENTS

(ISC)²

# Benchmark Your Organization's SECURITY POSTURE and BEST PRACTICES

How do your perceptions and security posture stack up against those of your peers? Find out in **CyberEdge Group's 2022 Cyberthreat Defense Report**, sponsored by (ISC)².

CYBEREDGE GROUP
2022 Cyberthreat Defense Report
North America | Europe | Asia Pacific | Latin America
Middle East | Africa
<< Research Sponsors >>
PLATINUM
GOLD
SILVER

Among a long list of key findings in the report, results reveal cybersecurity teams faced these challenges:

- A record 71% of organizations were compromised by ransomware last year; 63% of those victims paid ransoms
- Malware, account takeover attacks and ransomware are the most-feared threats
- 85% of organizations suffered from a successful cyberattack last year

Download the report and use the 2022 findings to benchmark where you organization stands.

Get the Report

# From NOCs to SOCs: How Did We Grow So Far Apart?

BY ÓSCAR MONGE ESPAÑA, CISSP, CCSP

**Technology constantly changes, requiring people** and processes within an organization to adapt to maximize benefits of these investments. Yet to move forward, we need to continually revisit what's changed to make sure it still makes sense.

More than 20 years ago, we, as an industry, began to define organizational monitoring models and establish what would be called Network Operations Centers (NOCs) to "take the temperature" of an organization's telecommunications health and maintain network uptime. Information security became a fundamental part of those initiatives and how we came to create Security Operations Centers (SOCs). Before long, the two merged at many companies into Network and Security Centers (NSCs).

These two entities worked side-by-side to make sure the monitoring of infrastructure and systems were used according to the internal acceptable use policy. The NOC focused on performance and telecom enablement while the SOC dealt with network threats like viruses and worms, primarily around endpoints.

As technology evolved, we saw the roles of the two teams diverge and each operations center's work isolated from the other. The NOC maintained the network backbone and access control lists, DMZs and ports left open for systems to communicate. The SOC enabled SIEM, endpoint, anti-malware and DLP solutions, among others.

Isolation is one of those common problems that exist within an organization and might lead to duplication of efforts or slower delivery of services because of the lack of communication and coordination.

Information security became cybersecurity and as corporate assets were digitized and cloud platforms emerged, defense perimeters no longer existed, attack vectors multiplied, and applications no longer ran on servers. We turned to containerization, infrastructure-as-code, cloud technologies, IoT, OT, and so on. In the process, we changed the concept of trust completely—as in we are no longer trusting any identity or device.

The separation of the NOC and SOC is no longer viable. The Wide Area Network (WAN) connectivity is no longer seen as connecting remote sites to a central location via MPLS; rather, software-defined WAN or SD-WAN technologies maximize resource utilization.

Because today's networking devices have more security capabilities, configurations need to be done differently so that mistakes are less likely and business requirements are considered. We need to move to what I call the Next Generation Network and Security Center (Next-Gen NSC) while still maintaining the fundamental concept of separation of duties.

Basically, this "cyberfusion" of two traditionally isolated teams removes silos while respecting each team's different mandates and methods of working. A Next-Gen NSC will be ready to adapt seamlessly to trends like Zero Trust, which relies heavily on endpoint activity, network configuration, identity management, application flow visibility and control, while stitching all together in a data lake (or alike) and maintaining continuous monitoring in a SIEM solution for continuous validation of access to the desired asset; the team would be able to operate, respond and configure the technology from a central location (virtually speaking).

**Óscar Monge España**, CISSP, CCSP, is a Zero Trust architect at Palo Alto Networks.

CONTENTS

Further along, as more organizations move to the cloud, maintaining and monitoring a multi-cloud strategy, having control of the applications, infrastructure and maintaining a good secure posture would be achieved in a faster and consistent manner.

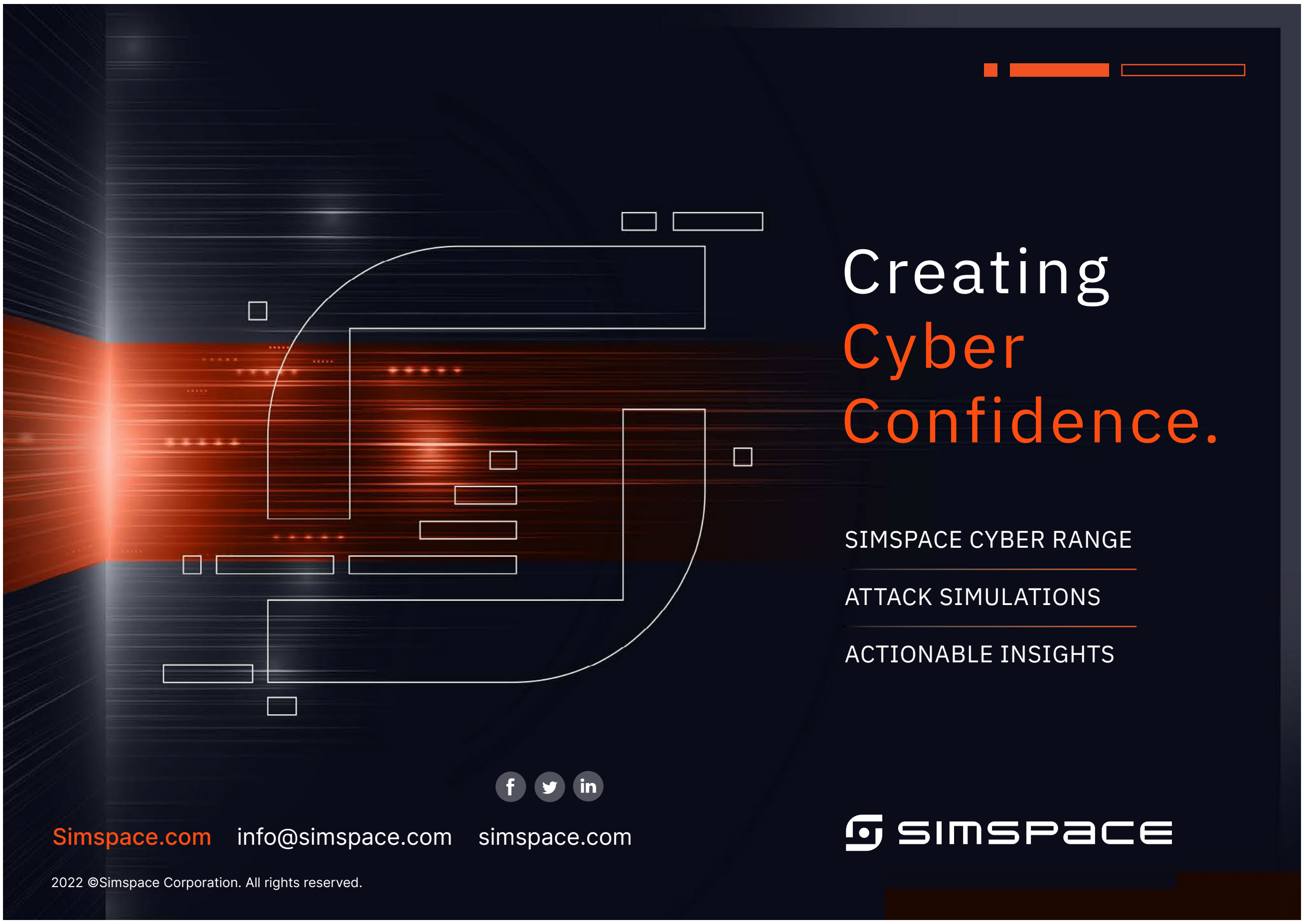
Fusing these two teams will require a high degree of change management. Members from both sides will be introduced to new technologies and concepts.

Here are some indicators to assess if a cyberfusion is necessary within your organization:

- Is the organization going through a refresh cycle of network solutions which greatly increase the security capabilities on them?
- Do changes in networking infrastructure affect negatively or positively your security operations team?
- Is there a perception that communication does not flow as expected between the networking and security teams?
- Are security or network solutions being chosen or implemented by a team without assessing the impact on the other parties involved?
- Does your security roadmap require regular changes to network infrastructure or configuration settings?

Technology, as previously stated, will continue to evolve. How we as organizations align and adapt our processes and keep our people engaged in this ubiquitous change is our responsibility, and eventually leveraging more automation would enable the organization to adapt to changes easily and faster. This fusion may be the first step toward other fusions within IT, like the SOC and the vulnerability management teams, for example.

How can we achieve that? Senior management would need to be closer to the enablers of the business. Also, a continuous industry scan would be preferable on a regular basis, aligning the business risk appetite for adoption; it would help define the strategy for mid-long term and identify the outliers for changes in people and processes. ●



# Protect Trade Secrets with Nondisclosure Agreements

BY DEBORAH JOHNSON

**Your company has developed successful proprietary** software and a strong base of clients. A nondisclosure agreement (NDA), also known as a confidentiality agreement, is one way to guard information such as business processes, designs, formulas, software code, and vendor and customer lists.

But NDAs are not a cure-all, and they come with their own set of problems, especially if they are too broad.

"If you're using generic terms like 'all financial information' or 'all business-related information' … that runs the risk of being blunted in its usefulness because it's not specific enough for purposes of enforceability," cautioned Karina Sterman, a partner with Greenberg, Glusker in Los Angeles. "Find out why you have the NDA, what it should actually contain and who should actually be signing it. And potentially have different NDAs based on the tiers of information that you're trying to protect."

Intellectual property attorney Stephen Murray agreed. "Make sure that it's narrowly tailored to information that's likely to come about in whatever your actions are going to result in."

A partner with Philadelphia-based Panitch, Schwarze, Belisario & Nadel, Murray argued that you must be specific. "If you're in a venture with another company on a particular project, you're going to want to have the NDA directed mainly to the information related to that project."

## When secrets are spilled

What do you do if you find that someone breached their NDA?

"Sometimes you can build into these NDAs some kind of alternative dispute clauses, like arbitration or mediation," Murray said. "If you suspect a breach, instead of going to court, you say, 'Okay we're going to arbitrate,' which tends to be much less expensive."

If it's a serious breach, consider decisive steps, including locking out the suspected employee while the incident is being investigated, advised Sterman. "[Deciding if it's] intentional or negligent will determine next steps, whether it's a pure disciplinary issue or you have to do some serious damage control. Because it's not going to be enough at that point to just fire the person."

## New hires with previous NDAs

There are risks to hiring team members under an NDA from a former employer, Sterman highlighted. "It depends on the position you're hiring them for. If they will be working in the same type of job with access to exactly the same client, that is a red flag. It's likely that the new employer and former employee will become a target of a lot of vigilance."

Murray suggested that new employees "sign an agreement to the effect of, 'We're not asking you disclose any of the confidential information that is the subject of the NDA with your prior employer, and you agree not to disclose, as part of your employment, any such information.' That way, you're kind of protecting yourself."

However, the bottom line may be that hiring that potentially valuable employee is too big a risk. "Sometimes it means that you can't hire that person because it's not possible for them do their job without it sending off all kinds of red flags," warned Sterman. ●

Photograph by Louise Roup

**Deborah Johnson** lives and works in San Diego. She can be reached at djohnson@twirlingtigermedia.com.

(ISC)² | Cybersecurity INSIDERS

*Discover the Latest*

# CLOUD SECURITY
# TRENDS & CHALLENGES

As organizations continue to migrate workloads to the cloud, utilizing new technologies to benefit from increased efficiency, better scalability, and faster deployments, they remain concerned about the security of data, systems, and services in the cloud.

The 2022 Cloud Security Report, sponsored by (ISC)², explores:

- Current cloud security trends and challenges
- How organizations are responding to security threats in the cloud
- Tools and best practices organizations are considering in their move to the cloud

Get the Report

CERTIFICATION MAGAZINE
2022 TOP CERT
CCSP
(ISC)²
THE NEXT BIG THING

"CCSP was just named
"The Next Big Thing"
by Certification Magazine!"

CCSP®

Certified Cloud Security Professional
An (ISC)² Certification

# IT/OT CONVERGENCE

**Disruptions and a dire prediction should have all of us carefully considering the cybersecurity implications of an IT/OT convergence**

**BY JULIEN LEGRAND, CISSP**

PHOTOGRAPHS BY JOHN KUCZALA

LAST YEAR GARTNER PREDICTED THAT BY 2025, operational technology (OT) environments would be hijacked by bad actors to harm or kill humans.

"In operational environments, security and risk management leaders should be more concerned about real-world hazards to humans and the environment, rather than information theft," Gartner senior research director Wam Voster told a New Zealand news outlet. By then, cyber attackers had launched ransomware to disrupt food and fuel supplies. Everyone wondered: What's next?

One answer has been the continued melding of information and operational technologies that applies virtual controls to physical processes within industrial control systems (ICS) surrounding manufacturing, energy, and other industries that comprise critical infrastructure. The rise of the internet of things (IoT) and edge computing is shifting more resources from physical to cyber security, what we commonly refer to as an IT/OT convergence.

## WHAT IS IT/OT CONVERGENCE, ACTUALLY?

IT/OT convergence describes the integration of information technology (IT) deployments and operational technology (OT) infrastructure. Whereas organizations use the former for data-centric functions like computing, enterprises use the latter to monitor and maintain industrial operations, devices and processes and adjust them accordingly.

Also, IT and OT play separate and distinct roles in running modern organizations. For example, OT systems represent a traditional and physical world where organizations rely on machines, manufacturing equipment, electromagnetic devices and many industrial systems to manage critical infrastructure. On the other hand, companies rely on IT infrastructure, representing a more digital world where companies leverage networking, storage solutions, servers and digital devices, to process data and manage enterprise applications.

Today, organizations are integrating IT and OT as they digitally transform to remain competitive. In a 2020 IDC survey, factors like increased demand for new services, products and experiences, technological advancements and volatile market conditions have accelerated changes to various operations.

In that survey, Jonathan Lang, the research manager for IDC Worldwide IT/OT Convergence Strategies, stated that "2020 and beyond are all about getting back to basics for industrial enterprises—focusing in areas like data governance for operational data, unifying infrastructure across industrial and enterprise networks, and rationalizing the overall operational technology portfolio."

## UNDERSTANDING THE HISTORY OF IT/OT CONVERGENCE

The idea of converging IT and OT has existed a long time. IT/OT convergence enables businesses to interoperate and integrate multiple technologies as a single system, resulting in enhanced efficiency, minimized operational costs, higher competitive advantage and reduced or eliminated errors.

IT and OT infrastructures have coexisted in enterprise processes with minimal integration, crossover and cooperation for many years. Historically, organizations have used OT to run mission-critical, proprietary systems to ensure uptime and availability of critical infrastructure, while IT-managed systems run enterprise-wide networks, computers and applications.

However, with businesses looking to achieve high scalability at reduced costs, there have been plans to develop an open architecture encompassing both technologies since the 1980s. Also, the emergence of the IoT, Industrial Internet of Things (IIoT), and associated technologies have impacted organizational IT and OT significantly. Networked digital technologies capable of collecting, processing, analyzing and transmitting industrial information promises numerous advantages—such as better automation and orchestration to keep up with threats.

Organizations have leveraged IT and OT functionalities for several decades in distinct spheres. For instance, OT has existed as a separate realm from organization-wide IT networks responsible for supervising and controlling critical infrastructures and mission-critical operations. Also, OT communications have been in restricted networks that utilize proprietary protocols.

By contrast, organization-wide IT developments have focused on convergence efforts, bringing together data centers to support seamless interoperation. For instance, IT developments bred converged IT infrastructure, paving the way for hyper-converged infrastructure that merges different management tools, servers, networking and storage into a cohesive, centrally managed IT infrastructure.

## AN ACCELERATED MERGE OF PHYSICAL AND DIGITAL

As such, IT/OT convergence seeks to integrate physical OT equipment into a digital IT world. Factors like machine-to-machine (M2M) communications, the development of advanced IoT actuators and sensors, and IIoT systems that can fit into OT physical infrastructure have accelerated IT/OT convergence.

In addition, new protocols, gateways and intelligent sensors are permitting enterprise OT to access, use and share data across a broader organization-wide network spectrum. For instance, a company like Fairbanks Energy deploys temperature monitoring sensors to help clients reduce data center cooling costs. Another example is Matrix Booking, which integrates intelligent sensors into software to offer an end-to-end workspace management solution. Emerging protocols, gateways and intelligent IoT sensors are also increasingly used in other areas, like pollution and climate control. For example, the Department of Environment and Conservation (DEC), an agency responsible for protecting and conserving the environment nature of Western Australia, uses the technologies to identify polluters and mounting cases for legal prosecution to prevent pollution.

Experts predict that 45% of operation-intensive organizations require digitizing OT assets by 2023 to sustain a strong competitive positioning. That isn't long from now, so cybersecurity professionals need to align resources now to protect these assets and critical systems.

## MAIN CYBERSECURITY RISKS FOR OT SYSTEMS

Based on research in the past year, organizations aren't ready for such a convergence. Not by a longshot.

Skybox Security researchers in 2021 found that at least 83% of organizations using operational technologies to manage critical infrastructures suffered a security breach in the last 36 months. Researchers also revealed that 73% of CISOs and CIOs underestimate the security risks facing OT systems by being overly confident that their enterprises can't suffer OT cyberattacks. The most common cyber risks facing OT infrastructures: supply chain attacks, OT network complexities, limited cyber risk mitigation options and functional silos.

Then came Gartner's troubling predictions that malevolent cyber actors will weaponize OT environments by 2025 to cause grave harm to humans, as well as $50 billion in financial damages. Attacks targeting OT software and hardware used to control and monitor critical equipment, processes and assets continue increasing. Moreover, they have evolved from attacks that aim to shut down an energy or water plant to hacks that compromise industrial environments to cause harm. In a news release, Gartner's Wam Voster warned OT security leaders should be more concerned about real-world hazards to humans and the environment, rather than information theft.

**In a news release, Gartner's Wam Voster warned OT security leaders should be more concerned about real-world hazards to humans and the environment, rather than information theft.**

OT environments are, by their very nature, vulnerable to hazards and threats as more industrial organizations move from Industry 3.0 to Industry 4.0. We've seen an exponential rise in assaults on OT in recent years, including Stuxnet, Dark Energy, and others. The attackers are taking advantage of known flaws and a lack of knowledge about the threats.

First, it's essential to recognize that ICS vulnerabilities are poorly understood, even compared to the amount of research devoted to IT security vulnerabilities. They can be found in the context of the following:

### Functional Silos

Plant managers, CISOs, CIOs, engineers and architects all agree that functional silos are the biggest challenges to protecting OT systems from attacks. Functional silos in OT are systems and infrastructure that operate independently to serve individual business units.

Recent research found that more than one-third of participants lacked centralized oversight that inhibited implementing and enhancing security programs, exposing OT to multiple attacks.

### Supply Chain Threats and Attacks

Third-party risks and attacks are common challenges preventing the enterprise from securing its operational technologies. Hackers may introduce malware deep in the supply chain or infiltrate an organization through third parties lacking adequate cybersecurity safeguards to compromise entire

OT deployments. In fact, recent research found that 40% of organizations' supply chains and third parties pose the highest security risk to operational technologies.

### Phishing, Insiders and Malware

A 2021 State of Operational Technology and Cybersecurity Report revealed that phishing attacks targeting organizations running OT increased significantly, with 58% of organizations reporting them. The increased attacks result from accelerated working strategies adopted due to the COVID-19 pandemic. While organizations required employees to work remotely, attackers targeted operational technologies to compromise security weaknesses.

**While organizations required employees to work remotely, attackers targeted operational technologies to compromise security weaknesses.**

Similarly, malicious adversaries exploited the confusion resulting from the sudden changes in working routines to ramp up malware attacks since 57% of enterprises reported malware attacks targeting their operational technologies.

Lastly, insider threats increased due to organizations' inability to manage remote employees, with 42% of companies reporting insider threat attacks targeting their operational technologies.

### Management

Lack of enterprise risk management (ERM) practices can lead to several problems for organizations.

First, it can make it challenging to identify and assess risks. This can lead to decision-makers being unaware of potential threats to the organization and thus not taking appropriate actions to mitigate them.

Second, the lack of ERM can also impede effective communication between different departments and levels of management. This can lead to a siloed approach to risk management, where each department or unit is focused on its risks without considering the impacts on other areas of the business.

Finally, there is no centralized repository for risk information without ERM in place. This makes it difficult to track and monitor risks over time and makes it more likely that risks will fall through the cracks.

In short, ERM is essential for any organization looking to manage its risks effectively.

### Operations

According to a recent study, most organizations believe that a lack of network segregation between IT and industrial control system networks is the main cybersecurity risk for their organization. Other risks include weak remote access procedures, incident detection and response, and reporting procedures.

The study found that most organizations have implemented some form of network segregation, but many do not have comprehensive policies and procedures in place.

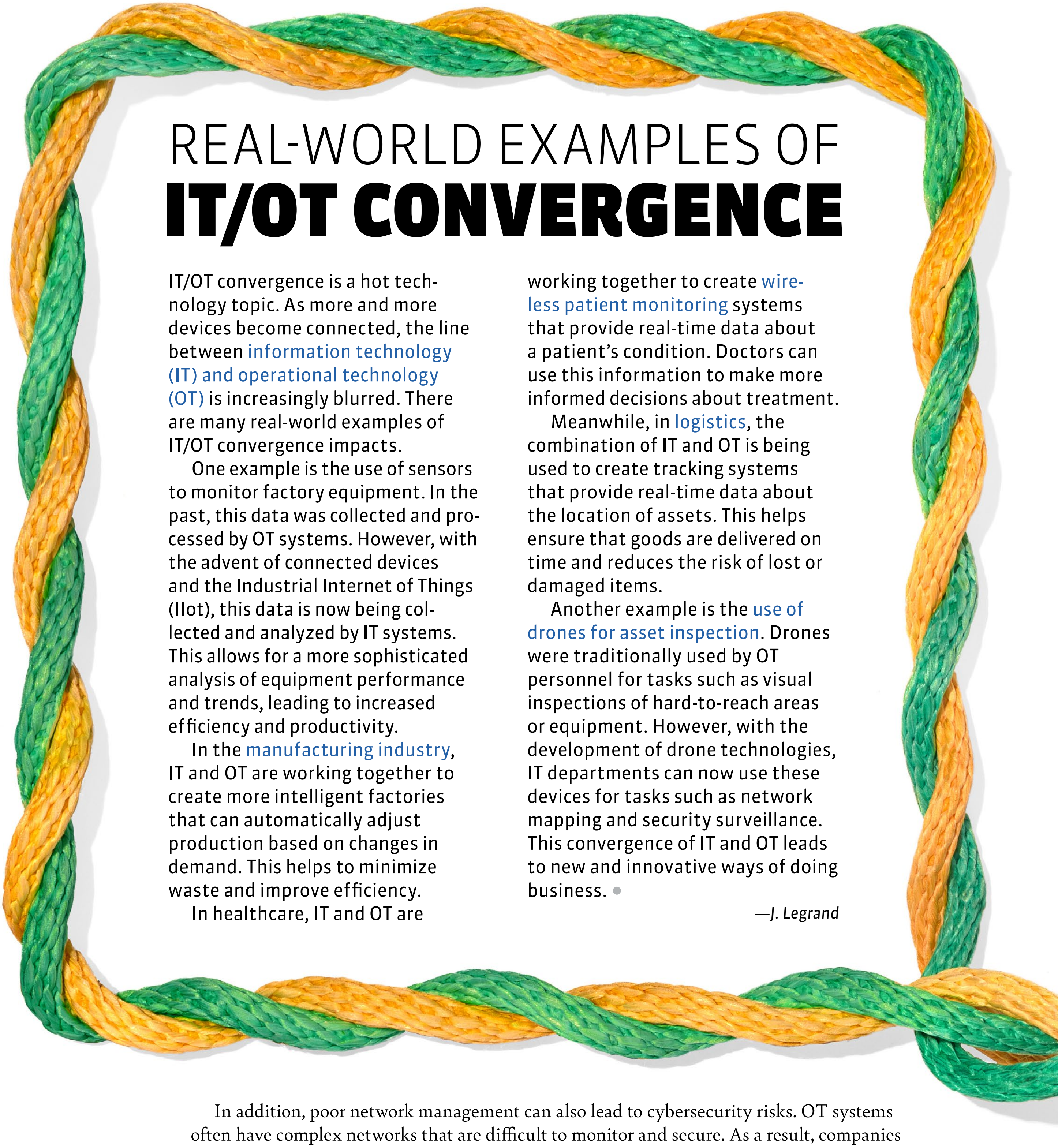
Additionally, most organizations do not have dedicated staff or budget for cybersecurity specifically for their OT systems. As a result, these systems are often not as well protected as they should be. With the increasing reliance on OT systems in critical infrastructure, organizations must take steps to improve the security of these systems.

### Technique

As the world becomes increasingly reliant on technology, the potential for cyberattacks grows.

While many people associate cybersecurity risks with personal information and data, industrial systems are also at risk. In particular, OT systems are vulnerable to attacks that can cause severe damage.

One of the main risks comes from the outdated technique. As hardware and software evolve, older versions can become obsolete. This makes it difficult to patch security holes and leaves systems open to attack.



## REAL-WORLD EXAMPLES OF IT/OT CONVERGENCE

IT/OT convergence is a hot technology topic. As more and more devices become connected, the line between information technology (IT) and operational technology (OT) is increasingly blurred. There are many real-world examples of IT/OT convergence impacts.

One example is the use of sensors to monitor factory equipment. In the past, this data was collected and processed by OT systems. However, with the advent of connected devices and the Industrial Internet of Things (IIot), this data is now being collected and analyzed by IT systems. This allows for a more sophisticated analysis of equipment performance and trends, leading to increased efficiency and productivity.

In the manufacturing industry, IT and OT are working together to create more intelligent factories that can automatically adjust production based on changes in demand. This helps to minimize waste and improve efficiency.

In healthcare, IT and OT are working together to create wireless patient monitoring systems that provide real-time data about a patient's condition. Doctors can use this information to make more informed decisions about treatment.

Meanwhile, in logistics, the combination of IT and OT is being used to create tracking systems that provide real-time data about the location of assets. This helps ensure that goods are delivered on time and reduces the risk of lost or damaged items.

Another example is the use of drones for asset inspection. Drones were traditionally used by OT personnel for tasks such as visual inspections of hard-to-reach areas or equipment. However, with the development of drone technologies, IT departments can now use these devices for tasks such as network mapping and security surveillance. This convergence of IT and OT leads to new and innovative ways of doing business. ●

*—J. Legrand*

In addition, poor network management can also lead to cybersecurity risks. OT systems often have complex networks that are difficult to monitor and secure. As a result, companies must be diligent in protecting these systems from cyberattacks.

### THE ROLE REGULATIONS IN IT/OT SECURITY CONTROLS

As more and more industries adopt digital technologies, the line between IT and OT is increasingly blurred. This convergence brings several benefits, such as increased efficiency and flexibility. However, it also creates new security risks, as malicious actors now have potential access to a broader range of sensitive information.

CONTENTS

To mitigate these risks, proper security controls must be put in place. Regulations can play a crucial role in facilitating this process by setting standards for collecting, storing and securing data. Furthermore, by requiring organizations to adhere to these standards, regulations can help ensure that proper security controls are in place, helping to protect against the ever-evolving threat landscape.

## OTHER FACTORS THAT MAKE ICS SO VULNERABLE

ICS is a critical part of any economy and society; they are also notoriously vulnerable to cyberattacks. One thing that makes ICS so vulnerable is that, at least in Western nations, they operate like a public utility but are privately owned. This limits governments' role in forcing better cybersecurity.

Also, many ICS were not originally designed with security in mind, and as a result, they often lack basic security features. Besides, ICS are often interconnected with other systems, providing attackers with additional entry points into the system.

Moreover, outdated software often manages ICS that the manufacturer no longer supports. These factors combine to create a perfect storm of vulnerabilities that malicious actors could exploit.

To protect ICS from attack, it is essential to understand these vulnerabilities and take steps to mitigate them. As a result, many ICS are woefully unprepared for the increasingly sophisticated cyber threats they face.

**By converging IT and OT systems, businesses can understand how their operations are performing. This data can then be used to optimize processes and identify areas for improvement.**

## BENEFITS OF IT/OT CONVERGENCE

Many business leaders now recognize the benefits of converging their IT and OT systems. By integrating these two systems, businesses can enjoy greater efficiency, cost savings, and improved safety.

One of the key benefits of IT/OT convergence is enabling businesses to collect and analyze data more effectively. In the past, data was often siloed within individual departments, making it difficult to get a holistic view of operations. By converging IT and OT systems, businesses can understand how their operations are performing. This data can then be used to optimize processes and identify areas for improvement.

Additionally, IT/OT convergence can help businesses reduce costs by enabling them to share resources and consolidate infrastructure. By bringing these two systems together, businesses can realize significant cost savings while improving their operational effectiveness.

## WHERE TO GO FROM HERE

Disruptions are a fact of life. There's always something that can happen to throw a wrench in our plans.

However, we usually think of disruptions as isolated incidents that don't have lasting effects. But what if there was a disruption that not only had lasting effects but also had the potential to wreak havoc on our lives? That's the kind of disruption that an IT/OT convergence can cause.

When IT and OT systems converge, the potential for disruptions increases exponentially. And those disruptions can have serious consequences, including loss of life. That's why it's so essential for us to consider the cybersecurity implications of an IT/OT convergence.

Only by doing so can we hope to mitigate the risks associated with this type of disruption. ●

**Julien Legrand,** CISSP, is a cybersecurity architect at Thales. He lives and works in Hong Kong and wrote about how to handle ransomware demands in the September/October 2021 issue.

CCSP. Certified Cloud Security Professional

An (ISC)² Certification

# Build on Your CISSP Expertise and MASTER CLOUD SECURITY

You've proven your expertise in cybersecurity…now prove yourself as the authority in cloud security for your organization.

The Certified Cloud Security Professional (CCSP) credential was designed to build on your deep technical and managerial CISSP knowledge and position you at the highest level of mastery for cloud security.

- **Grow with (ISC)²** – Validate your specialized skills and invest further into your membership with no additional fees. CISSPs already meet the experience requirements and your CPE credits are transferrable.
- **Cutting-Edge Credibility** – CCSP positions you as an authority in cloud security, highly adept in staying on top of the latest technologies, developments, and threats.
- **Broad Agility** – CCSP's vendor-neutral and multivendor qualifications may be applied across a range of cloud platforms, making your individual skillset more marketable.
- **Soaring Demand and Earning Power** – The demand for cloud security skills is projected to grow 115% over the next 5 years and command the highest premium at US $15,025.

CERTIFICATION MAGAZINE 2022 TOP CERT CCSP (ISC)² THE NEXT BIG THING

Make Your Move

# ASSESSING Critical Infrastructure

BY ÉDER DE MATTOS, CISSP-ISSAP, ISSMP, CISSP, CCSP

**CRITICAL INFRASTRUCTURE** (CI) is paramount to a nation's well-being and worldwide political stability. Everyone in and outside of cybersecurity knows this; yet, until recently we've resisted a more forceful approach to combatting threats posed by cyberterrorism that could have catastrophic impacts around the world.

Recent ransomware attacks against fuel, water and food industries brought the need for greater protections to our attention. The Russian war in Ukraine also reminds us of the dangers posed by nation-states to disrupt critical operations and supplies using cyberattacks.

Never phone it in when it comes to making telecommunications systems more resilient to attacks

Getty Images

In Q1 2022, we experienced three major cyber events tied to telecom infrastructure.

**Viasat:** According to the satellite company's website, Viasat on Feb. 24 (the official day of Russia's invasion into Ukraine) suffered "a multifaceted and deliberate cyberattack against Viasat's KA-SAT network, resulting in a partial interruption of KA-SAT's consumer-oriented satellite broadband service. While most users were unaffected by the incident, the cyberattack did impact several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe."

**Vodafone:** The news agency Reuters reported on Feb. 8 that Vodafone's Portugal unit suffered an overnight cyberattack that disrupted services, leaving thousands of customers unable to make phone calls or access the internet. During service restoration, 4G networks remained unavailable, forcing everyone to again rely on 3G.

**Starlink:** News organizations reported U.S.-based SpaceX in March stymied a Russian effort to jam its Starlink satellite broadband service, which was keeping Ukraine connected to the internet. SpaceX founder Elon Musk steered thousands of Starlink terminals to Ukraine after an official sent him a tweet asking for help keeping the besieged country online.

It's difficult to focus on how to secure all CI sectors. But by taking a closer look at one—telecommunications—we can make headway on the others. That's because telecommunications systems connect people and systems; therefore, their availability impacts the other CI sectors. Establishing sound procedures to assess CI resilience is vital for increasing ecosystem maturity; reviewing processes, architectures and tools; avoiding fraud; and producing a very strong shield of protection against directed and destructive attacks.

It's difficult to focus on how to secure all CI sectors. But by taking a closer look at one—telecommunications—we can make headway on the others.

## WHEN ONE SECTOR FAILS, THEY ALL ARE IMPACTED

To begin better protecting CI assets, we must understand threat actors and what motivates them. We all are aware that cybercrime syndicates and lone wolves sometimes operate at the behest of a nation-state, which employs cyber specialists to create malware used to spy, steal and extort. Sometimes it's as easy as masquerading as an employee to gain credentials or sensitive data; sometimes it takes more effort to evade existing network and data protections.

Whether attacks are against energy, finance, defense, telecommunications or the other 12 sectors, when one CI sector is compromised, damages can be severe—from the loss of confidential data to loss of money and lives.

That includes a telecom, which is paramount in connecting people and institutions and the exchange of data and information. When a telecommunication system is compromised, thousands or millions of citizens and companies, including other CI providers, can suffer serious consequences.

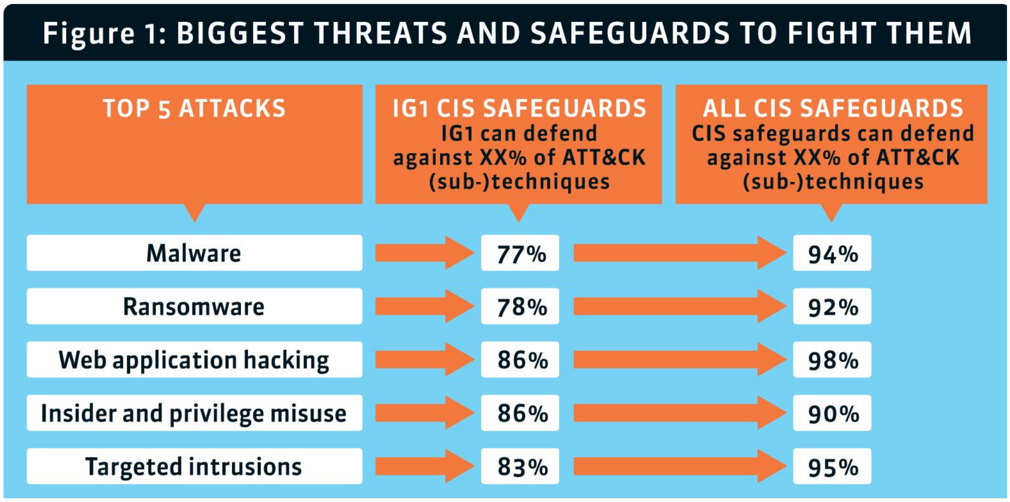
## IMPROVING TELECOM SECURITY PROVISIONS

Once we gain a broad understanding of a sector's vulnerabilities, we need to assess both the critical infrastructure and security posture of the agencies or private enterprises that operate them. This involves governance, maturity and threat modeling.

**Governance** is foundational in any security assessment. It creates an organized process, communication and hierarchy of decision-making and responsibilities—strategic, tactical and operational—to guarantee that each activity will happen at the correct time and improve conditions that produce better results from mapping and treating known or new risks.

**Maturity** of security controls must be determined, typically using a framework such as the one from the Center for Internet Security (www.cisecurity.org). For instance, the CIS controls in version 8 of the framework hold a total of 153 safeguards, divided into 18 controls and three implementation groups. Each group complements the others without overlapping.

**Figure 1: BIGGEST THREATS AND SAFEGUARDS TO FIGHT THEM**

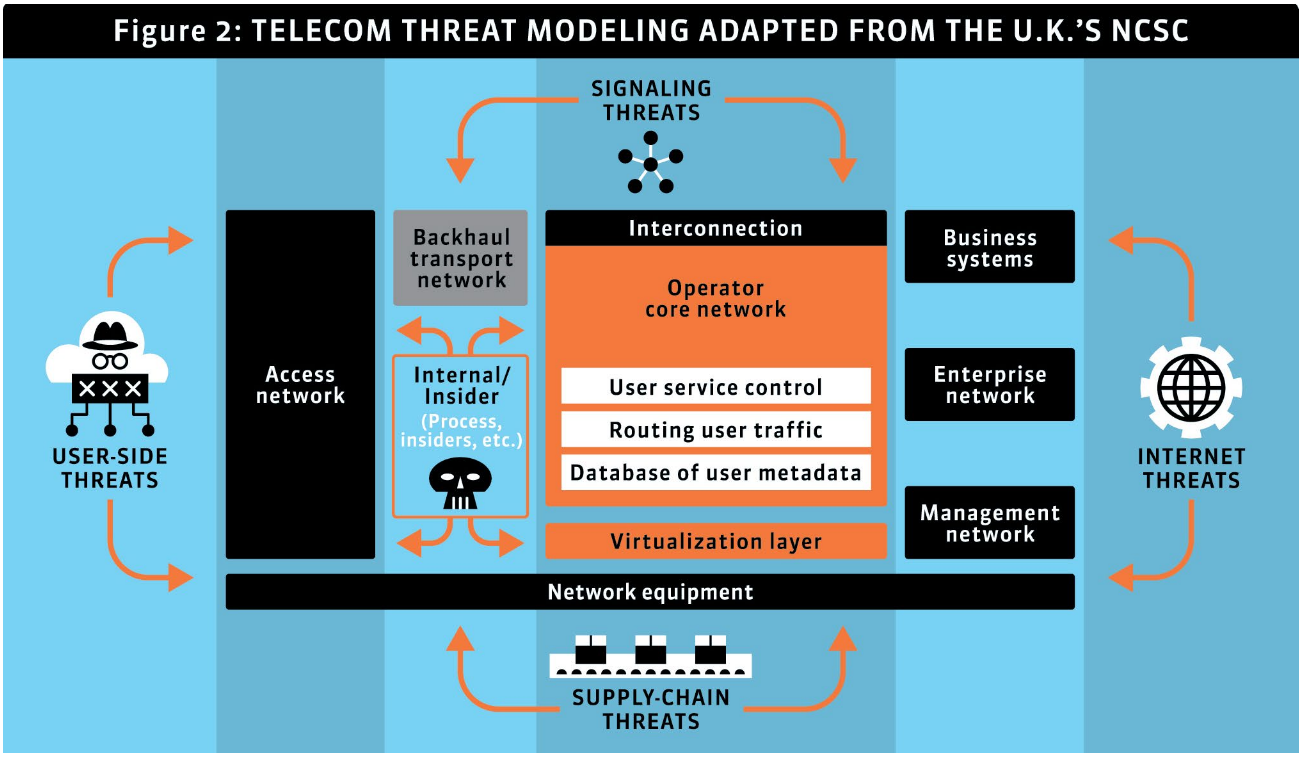


| TOP 5 ATTACKS | IG1 CIS SAFEGUARDS<br>IG1 can defend against XX% of ATT&CK (sub-)techniques | ALL CIS SAFEGUARDS<br>CIS safeguards can defend against XX% of ATT&CK (sub-)techniques |
|---|---|---|
| Malware | 77% | 94% |
| Ransomware | 78% | 92% |
| Web application hacking | 86% | 98% |
| Insider and privilege misuse | 86% | 90% |
| Targeted intrusions | 83% | 95% |

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

Source: Center for Internet Security

**Figure 2: TELECOM THREAT MODELING ADAPTED FROM THE U.K.'S NCSC**



Source. Infographics by Robert Pizzo

When a company implements all 153 CIS safeguards, the five biggest attacks (malware, ransomware, web app hacking, insider and privilege misuse, and targeted intrusions) can be defeated against at least 90% of cases, according to CIS literature. *(See Figure 1, above.)*

Successfully implementing all 153 safeguards isn't always easy, especially if you're a telecom company using both legacy and cutting-edge technologies within an enormous ecosystem. For instance, that environment may support 3G (or older) wireless protocols as well as 5G to keep customers happy.

CONTENTS

Then there's threat modeling, in which telecoms commonly face five threat vectors/agents. *(See Figure 2, p. 29).*

- **Internal/insider** – Disgruntled users, users who are victims of extortion or bribery.
- **Internet** – Attacks originating from any part of the internet.
- **Signaling** – Attacks originating in the telecom signaling (SS7/diameter) or specific networks (routing/management/virtualization).
- **Supply chain** – Attacks using VPNs or other links between the supply chain vendor and telecom company, exploiting trust relationships.
- **Users** – Attacks that exploit a telecom's customers' poorly protected devices and/or permissive telecom perimeter control.

## HANDS-ON ASSESSMENT-RELATED ACTIVITIES

To adequately map activities related to the assessment, consider which group or individual vectors will be used to evaluate communication points' current security. Some suggested hands-on security assessment activities for all threat vectors include:

- **Discovery:** A big-picture activity that will gather information about the whole company, technologies, people and processes. In this phase, the telecom should join efforts to discover everything—old or new systems, all equipment and inventory (we can't protect what we don't know).
- **Attack Surface (including dev/QA and labs):** Having executed a discovery, delineate the surface and the points most sensitive or residing in more critical corporate elements (e.g., core routers, servers) or systems (e.g., orchestration, controllers, signaling, online charging), normally known as the crown jewels.
- **Architecture Evaluation and Hardening:** Organize a review of all reference, test or production architectures (networks, systems integration and communication, flows) and include a review of the hardening process.
- **Penetration Testing:** With the knowledge about surface and architectures, it's time to penetration test both models: internal and external. In blind/double-blind external valuation, it's useful to find breaches in the perimeter or internet-accessible services. The internal test will discover problems that could easily be exploited by disgruntled users. Again, in telecoms, there are lots of new and old technologies working at the same time, including obsolete, end-of-life software or equipment more easily exploited.
- **Maturity, Controls, Process and SDLC (Systems Development Life Cycle):** You'll also want to conduct a comprehensive review of maturation levels on all existing controls and processes, in accordance with CIS. An SDLC revision will guarantee new projects are done in accordance with legacy or unused technologies that can be decommissioned.
- **Vulnerability Management and Compromised Elements:** With all previous activities completed, it's time to establish or review a vulnerability management process. Keep a close eye on systems controls and possibly evaluating elements previously compromised (i.e., Is there anything/anybody that shouldn't to be here?).
- **Data Protection:** A complete review about information protections, lifecycle, classification, tagging and other best practices.
- **Systems Evaluation:** Specific to telecoms, many systems (legacy or new) have had integration difficulties and should always support all telecom working. Legacy protocols like telnet are common and susceptible to packet sniffing or other simple attacks.

In blind/double-blind external evaluation, it's useful to find breaches in the perimeter or internet-accessible services.

# WHAT TO EXPECT

## ONCE YOU'VE COMPLETED AN ASSESSMENT

Once a hands-on assessment is completed, an organization should have a wealth of data and documents to build a stronger security posture that can ward off known and emerging threats. They include:

- Samples of best practices in project management, process, and communication used during assessment and could be incorporated in telecom practices
- Independent evaluations done by a security team, without bias
- Risk analyses
- Mitigation plans for critical problems
- Action plans to correct other issues in accordance with a telecom's risk appetite
- Recommendations and prioritizations
- Manuals, baselines and policy reviews
- Organizational and human resource reviews (including training gaps) and improvement plan
- Decommissioning all obsolete or unnecessary systems
- Incorporating newer industry best practices
- Budget management to help in decision-making on future investments
- Improved documentation and evidence

### OUTCOMES

At the end of the assessment, an organization should be equipped to provide the following:

- Updated inventory and a reviewed BC/DR strategy
- Governance-leading activities
- Risk management system
- Process management within a product's lifecycle
- Security seen as a value to the business
- Greater protection against destructive and directed attacks
- Maturity and continuous monitoring following CIS controls
- Better, more insightful documentation
- Improved intra-corporate communication
- New key performance indicators
- Improved products and services delivered to internal and external clients

*—Éder de Mattos*

For internet and customer-origin vectors:

- **Perimeter:** A specific and dedicated test to check the perimeter's robustness. An important layer of protection in telecom is the perimeter.
- **Customer Premises Equipment/Devices (CPEs), Volume/Amplification:** Equipment is evaluated, tested and certified to operate within the telecom parameters and rules. This step also involves hardening best practices, device lifecycles and vulnerability/penetration test checks. A compromised group of CPEs can be a source for botnets and large DDoS attacks. Another important point: Weak or poorly controlled CPEs are susceptible to spoofed attacks and should be disabled and removed.

For the insider vector:

- **Review:** Read through all user processes, including for desktops, tools (allow only those necessary) and privilege creeping.
- **Single Sign-On/Federation/MFA (Multi-Factor Authentication):** Apply appropriate levels of authentication for all users and all systems. This condition enforces security levels and reduces the possibility of abuse.

For supply chain vectors:

- **IN->OUT and OUT->IN:** Consider revising all access and network flows from or to vendors and restrict to only those necessary (like a Zero Trust architecture).

A compromised group of CPEs can be a source for botnets and large DDoS attacks.

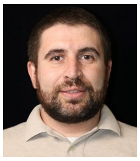
For the signaling vectors:

- **Control/Management/Virtual Plane:** Requires a comprehensive revision of all systems, protocols, tools, access, etc., responsible for keeping networks and equipment working. These are the most sensible and critical to the company. In recent telecom network construction, adoption of software-defined networks improves controls but also can disrupt networks if compromised. Virtual planes do as well. Cloud adoption in telecom is happening quickly, and there currently is a gap of knowledge in this emerging space.
- **Voice:** Revise all protocols (the flow traffic is in plain text) to filter unnecessary information or flow, with special attention to SMS, roaming and SIP flows, using newer and secure protocol versions whenever possible.

For all perspectives:

- **Compliance:** Once done with all previous activities, review all applicable regulations and laws for compliance. Malicious hackers or adversaries would love to intercept telecom flows, while regulators want to enforce privacy and confidentiality rules.
- **Documentation:** Preserve all documentation generated during the assessment and make it available to key users and future assessors or complementary activities. It's part of a company's due care and due diligence.

All of this may seem onerous, but many of these activities are already happening at companies operating critical infrastructure, including telecommunications. A security assessment is a way to improve the conditions for a company, so everyone knows the best path forward to deal with the challenges faced daily. ●



**Éder de Mattos**, CISSP-ISSAP, ISSMP, CISSP, CCSP, has worked for telecom service providers for 15 years. He is currently a Brazil-based professional services senior cloud security consultant at a large cloud provider, where he helps Latin American customers with security assessments, architecture review and complex projects.

# LEARNING TO PIVOT AND RAPIDLY RETOOL USING MITRE ATT&CK

Cyberattacks are increasing exponentially in number and complexity. Organizations need to be equally agile.

BY CHARLENE DEAVER-VAZQUEZ, CISSP, CISA

**MOST CYBERSECURITY PROFESSIONALS** are overwhelmed just trying to stay on top of current patches, compliance requirements and user support. As long as our focus is at this level, we'll never get ahead of the game.

Forecasting cyberattacks requires a shift in focus, giving us valuable time to develop new strategies and mitigations. It begins by quantifying the risk and expressing the likelihood of an event as a range of probability.

ILLUSTRATION BY FRANK STOCKTON

How can we forecast cyberattacks? We start by modeling the "what if" attack scenario to identify vulnerabilities and gaps in our protections. To this we can add basic mathematical models designed to forecast the number of events and outcomes. There are even new advanced models being developed that will forecast event behaviors. But for our purposes, let's focus on basic models' ability to predict a cyberattack.

I use two frameworks. The first is MITRE ATT&CK, which I prefer because it groups techniques and tactics around the attack life cycle. The second tool I use is the Probabilistic Risk Model for Cyber (P-RMOD4Cyber), which is a spreadsheet-based set of mathematical models designed to forecast likelihood of events, number of events and more. It's used in forecasting risk in supply chain and compliance, procedures, cyberattacks and more. It's available at fismacs.com.

## A LOOK AT CYBER TRENDS TO GATHER 'WHAT IF' QUESTIONS

In late 2021, the European Union Cybersecurity Agency ENISA reported that supply chain attacks were set to increase four-fold in 2021. Not only were attacks increasing, but they also found that older frameworks used to defend against such attacks were inadequate.

Around the same time, IoT World Today reported that IoT attacks more than doubled during the first half of 2021.

In its 2021 Cyberthreat Defense Report, CyberEdge Group reported the largest annual increase in successful attacks within the last six years with four in 10 organizations experiencing six incidents or more cyberattacks.

In the 2022 Threat Predictions, McAfee Enterprise and FireEye fellow and chief scientist Raj Samani issued this joint statement: "Over this past year, we have seen cybercriminals get smarter and quicker at retooling their tactics to follow new bad actor schemes from ransomware to nation-states and we don't anticipate that changing in 2022. With the evolving threat landscape and continued impact of the global pandemic, it is crucial that enterprises stay aware of the cybersecurity trends so that they can be proactive and actionable in protecting their information."

It's not just that there are more cyberattacks; there has been a major shift in threat actor capabilities.

There is a convergence between nation-state and criminal organizations in a thriving underground market. As TEHTRIS explains, criminal cyber gangs are forming their own cartels with agreements between groups for joint action. They recruit on the dark web, fund activities and sell tools. In a cartel, each group performs a specific tactic like DDoS, phishing and ransomware.

Alternatively, one group subcontracts to another group or an individual purchases services on a per-attack basis. This gives unprecedented ability to rapidly retool and pivot attacks between tactics and platforms.

## USING MITRE ATT&CK TO PREDICT WHERE WE'RE MOST VULNERABLE

Given such threat actor capabilities and attack trends, how do we as cybersecurity professionals factor in risk quantifications and forecast with "what if" scenarios.

The process begins with MITRE ATT&CK and selecting our "what if" scenario. I like to start by picking a threat agent that gives me access to a typical set of techniques. You could, of course, select any set of techniques. As an example, let's look at the Sandworm Team attributed with the NotPetya attack of 2017, which was a precursor to SolarWinds, one of the worst breaches in history. NotPetya used a malicious software update (Technique T1195). It also used several other techniques like phishing, network sniffing for credentials, account manipulation, enumerating system connection, and more. This gives us a profile of sorts we can use to evaluate our security, vulnerabilities and protections.

Next, we can expand our "what if" to include additional techniques. This reflects what we know of current threat agent capabilities. Groups can purchase services and tools rapidly expanding current known techniques. As we develop our "what if" scenario, consider options for techniques not currently within a group's capabilities list but currently used by groups that might work together where there are shared political interests—or shared target communities.

For each technique, or group of related techniques, we look to our own vulnerability data and knowledge of our network architecture and configurations. The outcome of this part of the process is to develop our estimates of weakness. Express each as a percentage of systems or attack surface. Within our model, we can consider several factors as we develop our estimates.

Weaknesses can be determined by grouping factors together where applicable and aggregated. The total weakness for any grouping cannot exceed 100%. For example, we may find that 10% of systems are missing patches related to authentication and 20% of systems have a configuration weakness also related to authentication. When we eliminate the overlap, we may document this as a 25% authentication weakness.

## USING MATHEMATICAL MODELS TO DETERMINE PROBABILITY

Our mathematical models use probabilistic methods such as Bayesian joint probability and Monte Carlo simulations which can run a thousand scenarios at once. These methods are well established and used in a wide variety of applications in finance, epidemiology, seismology, and in space and nuclear safety analysis. They provide standard, repeatable and defensible approaches to describing uncertainty.

For instance, we can use a Bayesian joint probability formula for risk. The formula in Figure 1 *(below)* reflects the probability of the union of A and B to equal the probability of A given what we know of B times the probability of B.

It's easy to think of this as a Venn diagram. We designate threat as B and likelihood as A in the diagram. The overlap of threat and likelihood is risk. Therefore, the Bayesian formula for the joint probability can be simplified to *risk = threat x likelihood*.

## FROM WORST- TO BEST-CASE SCENARIOS USING MONTE CARLO SIMULATIONS

To illustrate another model, we'll develop three likelihood estimates: worst-case, most likely and best-case. This gives us the full range of uncertainty. If our scenario includes use of a zero-day, we might estimate the worst-case is very high, or 80%. We might agree that our most likely estimate is 50% and our best-case is 25%.

The model will auto-calculate for us, but we can do the math here as (.80 x .25 = .20, .50 x .25 = 12.5, .25 x .25 = .0625) or a range of 20% to 6.25% with the most likely being 12.5%. Now we can input these values into a Monte Carlo simulation as our worst-case, most likely and best-case values, and it will chart 1,000 probabilities of risk.

In the Risk Range chart *(see Figure 2, p. 36)*, we see that from our best-case estimate of 6.5% risk increases to a high of 11.7% with some risk distributed to the right of the chart all the way to our worst-case 20%. This grouping is because our most likely value is 12.5%, so the chart is slightly skewed to the left, with a larger portion of risk on the righthand side. The average risk is 13%.

We can also use another probabilistic method called a Poisson, which calculates the number of expected events based on the risk range we provided. In the Number of Expected Events chart *(see Figure 3, p. 36)*, we can see that

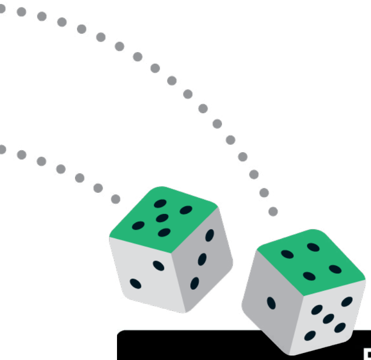
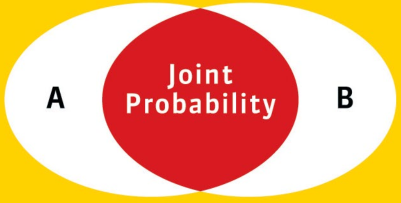


Figure 1:
BAYESIAN JOINT PROBABILITY FORMULA FOR RISK



$Pr(A \cap B) = Pr(A|B)*Pr(B)$

Risk = Threat x Likelihood

Infographic by Robert Pizzo

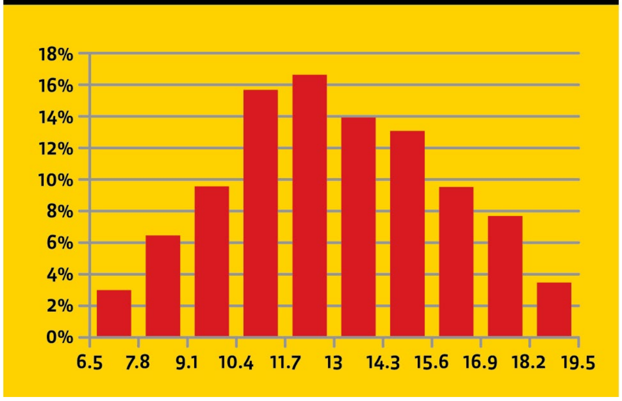


**Figure 2:**
**RISK RANGE**

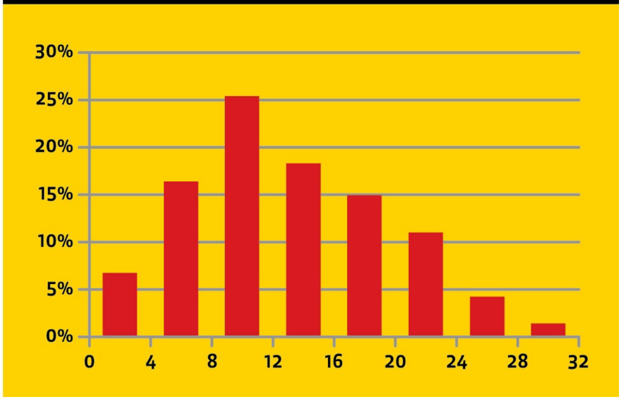


**Figure 3:**
**NUMBER OF EXPECTED EVENTS**

Infographics by Robert Pizzo

we could expect between zero to 32 events, with the average being 14. We can see that probability is between eight to 12 events with much lower probability of experiencing 28 to 32 events.

To this we could add an estimate of the impact of these events. That would be a simple equation of *(threat x likelihood) *impact*. That is a rating of the risk and is useful for comparing scenarios with different impacts.

## THE BENEFIT OF FORECASTING CYBERATTACKS

> By quantifying the risk with "what if" scenarios we shift our focus from the never-ending cycle of patching to a strategic view of risk. We can move from being reactive to proactive and develop strategies and mitigations.

By quantifying the risk with "what if" scenarios we shift our focus from the never-ending cycle of patching to a strategic view of risk. We can move from being reactive to proactive and develop strategies and mitigations. The process allows us to identify contributing factors such as specific weaknesses which can help us prioritize remediation activities. By performing a before and after remediation analysis we can also measure the reduction of risk.

Now we have metrics and measures that are truly meaningful. Add to this an estimate of the impact, whether operational or financial, and you have the basis for more easily communicating risk and risk reduction to stakeholders.

Most importantly, by quantifying the risk, you have defined and differentiated one risk from another. This is the foundation of making risk-informed decisions. This is why tools like P-RMOD4Cyber are so important. They can help us fundamentally change how we measure, manage and communicate risk. ●

**Charlene Deaver-Vazquez**, CISSP, CISA, is the creator of the Probabilistic Risk Modeling for Cyber (P-RMOD4Cyber) framework and co-author of *Ensure Your Business Success with Risk Informed Decision: How to Easily Quantify Cyber Risk* available on Kindle.

CONTENTS

# IT/OT Convergence and Minimizing Human Errors

BY SPENCER WILCOX, CISSP

**A lot more attention is being paid to the convergence** of IT and OT following Russia's invasion of Ukraine this year, particularly in protecting industrial control system (ICS) assets. News of Russian forces attacking a nuclear power plant drew tremendous attention—and reminded us of what we already know is possible.

I was about 12 years old when 40 tons of toxic gas were released from a Bhopal, India, Union Carbide factory. It killed or maimed many thousands of people in the area. Then came the Chernobyl nuclear plant meltdown. Safety instrumented systems became a common feature in nearly every control system, as did the eventual computerization and networking of such systems to reduce the risks of the human failures that led to both the Bhopal and Chernobyl tragedies.

In cybersecurity, we regularly see human failure as the most common mode of ingress in a cyberattack. Phishing, vishing, social engineering, insider threats, espionage, and good old-fashioned "fumble fingers" continue to disrupt systems. We don't allow conventional weapons in our workplaces, but anyone can use a computer to click a phishing link or open an attachment, effectively weaponizing it.

Similarly, we train college students in "cybersecurity," with curricula emphasizing pen testing, reversing, vulnerability identification and password cracking to solve a problem. We incentivize them to find the flaws so we can fix them and be compensated by generous bug bounties. Let's be honest: breaking stuff is fun … and clearly profitable.

Our news and entertainment media continue to glorify breaking into a system instead of teaching them how cool it is to build a system, application, piece of hardware or engineering system that is resilient and reliable, even while the bad guys are wailing away at it.

**Maybe instead of Capture the Flag contests designed to give kids a thrill when they successfully exploit a network, they should be retooled to provide better rewards when no one can get through.**

Maybe instead of Capture the Flag contests designed to give kids a thrill when they successfully exploit a network, they should be retooled to provide better rewards when no one can get through. I'm not against Capture the Flag contests; they indeed serve a useful purpose. But why do we continue to glorify the act of destruction? Why don't we glorify resilience and reliability instead?

There will always be a case to build a warfighting apparatus to counter and destroy an adversary. But shouldn't we spend at least as much time training a cadre of defenders who are taught to identify, protect, detect, respond to and recover from all hazards, including those caused by human failure?

Ukraine has demonstrated an overall level of systemic resilience that surprised the world. Despite dealing with a first-tier nation-state cyber and physical threat, Ukrainians have managed to remain online far longer than expected. Their cyber resilience is impressive and a lesson to all of us. •

**Spencer Wilcox**, CISSP, is a CSO and Ph.D. candidate living and working in New Mexico.