Industrial Cybersecurity Experts Share 14 of Their Biggest Tips and Predictions

Are You Prepared for the Future of ICS Cybersecurity?

Introduction

The task of building and running an effective cybersecurity program is a major challenge for any complex organization, but those in charge of industrial control systems (ICS) have their own set of hurdles to overcome that are entirely different than those of their strictly-IT counterparts.

How can industrial organizations address the cybersecurity skills gap? What about the increasingly-difficult endeavor of bringing the IT and OT sides of the organization together under one unified cybersecurity mission?

In addition to these concerns, there's the reality that ICS security is evolving quickly. Whatever challenges there are today won't be the challenges of tomorrow. That raises the question: what will have the greatest impact on ICS security in the next 5–10 years?

We asked a number of security experts how they think these questions should be addressed.

Question #1: How Can Industrial Organizations Strengthen Their Security Posture Amidst the Ongoing Skills Gap?

Galina Antova
Co-founder, Claroty

Automated technology is a very key part of that answer since organizations require integrated cybersecurity posture across IT and OT networks, consolidated processes and teams. Therefore, new technologies that could provide the traditional cyber defense mechanisms but do so in the context of OT networks (which have different uptime/availability requirements) will help a lot with this growing gap.

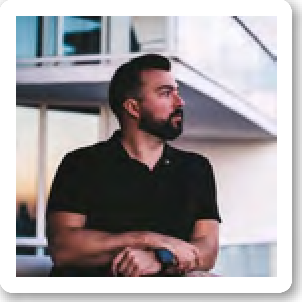
Kristen Poulos
GM of Industrial, Tripwire

First and foremost, organizations can (and should) be constantly talking about cybersecurity. Industry role models have already formed internal committees that regularly meet to discuss how they as an organization can become more cyber-secure and how the threat landscape is evolving. It's those discussions where other skills-gap closing topics come to light, such as treating cybersecurity like a program (not a project) and considering external resources like managed service providers to further close the gap.

Question #1: How Can Industrial Organizations Strengthen Their Security Posture Amidst the Ongoing Skills Gap?

Patrick Miller
Managing Partner of Archer Energy Solutions

I think there is a gap between existing HR/management hiring expectations and the thriving talent pool that is out there. If you have a job posting that asks for a college degree, five years of experience, multiple programming languages, professional certificates and security clearance for a salary of $75k, you won't get anyone. Some engineers are interested in security and IT. Some IT people are interested in engineering and process control. Many entry-level people are brilliant and thirsty for more knowledge and just need to be paired with a senior to rocket their way up three levels in a year. Throw out the old hiring models, and the blinders will be lifted.



Nick Shaw
Senior System Engineer, Tripwire

Either way, regulated or not, industrial organizations have two ways they could go about solving the skills gap: 1) hire talent and strategically develop a cybersecurity strategy/policy that aligns with best practices or 2) hire a reputable third party to augment their staff capabilities and provide managed services. Industrial organizations will need to identify and strategically align with good partners that have proven experience in the cybersecurity landscape. The right partner will go a long way to develop a comprehensive plan that builds up cybersecurity posture over time.

Tripwire Tip

To help industrial organizations close the cybersecurity skills gap, Tripwire offers a range of managed security services. Learn more here.

Question #2: How IT and OT Can Collaborate in the Name of ICS Security?

Susan Peterson
Digital Leader Of Energy Industries, ABB

Over the past 10 years, I've been privileged to help bridge the gap between operations and IT teams. For operations teams, focusing on finding ways to automate routine security maintenance tasks and showing how security monitoring technologies can help solve operations related challenges are great ways to build a bridge. For IT teams, helping them understand the importance of engaging OT suppliers and the maintenance cycles of OT assets is key.

Paco Garcia
Director of Cybersecurity and Networking Digital Plant Line of Business, Schneider Electric

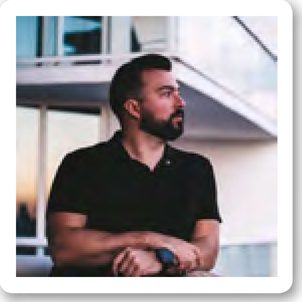
This convergence is mandatory for those people/companies who want to adapt to new technologies and paradigm changes that come with Industry 4.0 and IIoT. As the owner of budget resources for deploying cybersecurity programs, IT must establish a clear framework and enlist OT personnel to help secure the plant. The scope of IT and the OT involvement must be defined explicitly at the outset of every project. Both roles should be complementary and should not involve competition between them. In that sense, defining the owner for each task helps to avoid conflicts. Lastly, from a top-down approach, each company must promote and enforce the creation of workgroups made up of IT and OT people with the objective of promoting the company's digitalization and strengthening the organization's internal cybersecurity culture.

Gary Difazio
Strategic Marketing Director, Tripwire

The one word for this is: collaborate. At the end of the day, we all want to do the right thing for our organizations. Do what is best through collaboration. Understand the unique needs and direction of the shop floor so that cybersecurity solutions can be implemented to support availability, safety, productivity and quality of the operation.

Remember that cybersecurity is a journey that never ends. Automation systems continue to evolve, and the threat landscape is always changing. Slow and steady will win the race. We must all be on this journey through collaboration and teamwork.

Question #2: How IT and OT Can Collaborate in the Name of ICS Security?



Larry Vandenaweele
Industrial Security Professional

Reducing cybersecurity risks and getting better visibilities across the IT and OT network environments require involvement and participation of IT, OT, security and management stakeholder groups. Learning from each other by means of practical awareness workshops is a first step of educating each other.

The folks on the IT side of your organization should educate their business operation tasks, and illustrate the risks and challenges they face and how they link to the OT environment. For example, installation of patches is a recurring activity in IT environments while in contrast OT environments are seldom patched due to operational challenges, maintenance windows, etc.

The folks on the OT side of the organization deal with challenges that can be directly related to operational and regulatory requirements, making a simple task such as patching not as simple.

Tripwire Tip

In order to bring the IT and OT sides of your organization together under one cybersecurity program, Tripwire's portfolio extends key security controls such as vulnerability management and change monitoring into the industrial environment. Learn more here.

Question #3: What Will Have the Greatest Impact on ICS Security in the Next 5–10 Years?

Justin Sherman
Cybersecurity Policy Fellow, New America

In the next 5–10 years, industrial systems are going to become increasingly connected to the internet as the Internet of Things becomes more and more essential to industrial operations and as those systems are also hooked into 5G cellular networks, which are promising much lower communication delays between devices. Internet of Things device security is usually terribly weak right out of the box, so this will be a serious challenge for industrial systems to manage when IoT devices are deployed at scale.

Add to this the fact that increased connectivity means more actors can attempt to break into systems—and that more sophisticated actors can have potential visibility into systems—and the cybersecurity challenges from this growing connectivity are exacerbated even further. It'll also impact not just those managing and securing industrial systems but also those on the public policy side of things as well given that many industrial systems, if manipulated in a certain way, could have physical impacts on human life.

Kristen Poulos
GM of Industrial, Tripwire

It's such a fast-moving industry, even knowing what's going to happen in the next 5–10 months can sometimes be challenging! But in all seriousness, the themes of IT/OT convergence and automation will continue to substantiate the need for organizations to have a top-to-bottom cybersecurity plan. This means budget consolidation (likely to IT teams) and vendor consolidation. Certainly, a significant industry cyber event could turn any prediction upside down, but our mission as a security community is to provide the solutions to prevent that from happening.

Question #3: What Will Have the Greatest Impact on ICS Security in the Next 5–10 Years?

Patrick Miller
Managing Partner, Archer Energy Solutions

In the next 5–10 years, the biggest impact on industrial cybersecurity will be the unintended consequences of digital transformation. This change is good and necessary, but it comes with risk. As we introduce more and more digital endpoints, these will become data streams. There will be so many data streams that we won't be able to hold or efficiently analyze all of that data on-premise. Further, we will use that data to drive decisions about the process—or even the process itself. Eventually, probably through AI/ML, we will begin to allow the analytical data-products to become inputs back into the process.

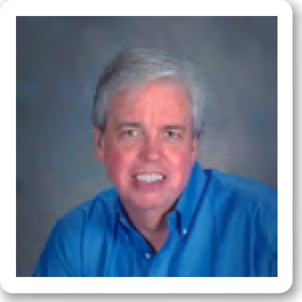
In other words, process generates data, that data leaves the process network and goes anywhere/everywhere (e.g. cloud, fog, lake, on-premise, off-premise), gets analyzed, repurposed and fed back into the process. All of this introduces new risks to the process data and associated systems outside the control/process networks in ways we are just now beginning to consider.

Galina Antova
Co-Founder, Claroty

The main topic of conversation 5–10 years ago was as follows: "Are industrial networks really air-gapped?" I think we all know by now that this is not the case. Moreover, the increased connectivity (needed for productivity) is making this challenge even greater. As companies aggressively undertake their digital transformations, portions of the industrial process have already migrated to the cloud, and in the next 5–10 years, we can reasonably expect that most of the non-critical applications will be hosted in a cloud environment.

If this transition is done with the right security measures in place, then it could have huge positive impact on productivity. However, for entities that don't invest enough time/resources into the cybersecurity angle, this cloud migration could become significant exposure.

Question #3: What Will Have the Greatest Impact on ICS Security in the Next 5–10 Years?



Greg Hale
Editor/Founder, Isssource

A quick and easy answer to what will have the biggest impact on cybersecurity in the coming decade is two-fold: artificial intelligence and big data analytics. Given the fact that these developments will have a major impact in the coming years, I am convinced a secure environment in 5-10 years will come down to how AI and analytics all play into a resilient and holistic security plan that encompasses the entirety of security, which includes cyber and physical.

With the Industrial Internet of Things (IIoT) becoming more pervasive in the manufacturing enterprise moving forward, security experts must have a plan that understands and knows what all the networks should look like and how they should behave. At the same time, all security plans need to be resilient enough to withstand any kind of assault coming its way.

Gary Difazio
Strategic Marketing Director, Tripwire

I think that there will continue to be events impacting many different kinds of industrial environments no matter what the vertical. These incidents will consist of either collateral damage from IT-based malware or ransomware, or will be specifically targeted against industrial control systems. These events will negatively affect productivity and quality and also have the potential for physical damage.

While malware is a risk, nation-state cyber warfare activities will also be more prevalent. This will be the new battlefield. Automation vendors will be pressured to create automation systems that are secure by design, and as plant or line upgrades happen over time, the next-generation systems will be more cybersecurity aware to thwart malicious behavior. Cybersecurity capabilities will become part of control systems' DNA.

Tripwire Tip

Did you know Tripwire has the broadest library of built-in templates covering the standards, security policies and regulatory requirements for ICS? Learn more here.

You Can Trust Tripwire With ICS Security

Tripwire turns raw ICS data into actionable information. Our holistic tools span the IT/OT landscape, and our large ecosystem of technology integrations and vendor-agnostic solutions give ICS operators plenty of freedom of choice in the selection of automation systems that are best for their business.

Tripwire provides deep visibility through a comprehensive suite of highly-integrated products to detect ICS cyber threats and breaches, prevent future incidents by discovering and prioritizing risks, and continuous monitoring to help keep your security program on track.

Learn More

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

***The State of Security*: News, trends and insights at** tripwire.com/blog **Connect with us on** LinkedIn, Twitter **and** Facebook