tripwire

Industrial Cybersecurity Tips for CISOs

Advice, Trends and Insights from Six Experts

Expert Industrial Cybersecurity Tips for CISOs

Digital attacks are a growing concern for industrial control system (ICS) security professionals. In a 2019 survey conducted by Dimensional Research[1], 88 percent of respondents told Tripwire that they were concerned about the threat of a digital attack. An even greater percentage (93 percent) attributed their concerns to the possibility of an attack producing a shutdown or downtime. Other survey respondents expressed their worry over the quality of production and data exfiltration at 86 percent and 81 percent, respectively.

Clearly, many ICS personnel are worried about the security of their operational technology (OT). That's especially the case for organizations that are welcoming OT environments into their folds for the first time. In those organizations, the pressure is on for the CISO to extend the organization's digital security strategy across all of its new industrial assets.

But how does the CISO provide this type of leadership in the face of securing these increasingly complex environments? How can they keep track of their security responsibilities as they expand beyond the enterprise and into industrial environments?

1 tripwire.com/state-of-security/ics-security/survey-digital-attacks-affect-industrial-operations/

Expert Industrial Cybersecurity Tips for CISOs

TIP 1

Divij Agarwal

Senior Product Manager, Belden

For industrial networks and end devices, availability is far more important than protection from hackers and malware. A lot of industrial equipment has multiple layers of redundancy built in that prevent rebooting or restarting for years. Traditional OT equipment should be carefully scheduled for maintenance windows for patching and upgrades, keeping in mind its legacy software base and configuration program.

TIP 2

Lane Thames

Senior Security Researcher, Tripwire

CISOs will either need to build out cybersecurity teams that have deep knowledge of IT and OT systems, or have this expertise provided by a service provider. Regardless, the other aspect of the "people" component is that of collaboration. CISOs must ensure that their IT and OT departments are working closely together, potentially cross-training each other where appropriate.

TIP 3

Kristen Poulos

General Manager of Industrial Cybersecurity

Take a day to walk the plant floor if you have to. In the process, you'll likely learn a few new things and gain a sense of comradery before you jointly have to tackle critical security projects. You can even take the opportunity to give them some insight into your priorities and then discuss what makes the most sense for an OT environment.

Expert Industrial Cybersecurity Tips for CISOs

TIP 4

Robert Landavazo

ICS Engineer

Having spent parts of my career in the trenches of OT networks, I recall several explicit instances in which I would have loved to pass on my thoughts to the CISO at the time. First, I'm specifically reminded by an occasion that I had the privilege of presenting to the board of directors and was present for a report-out on the state of the organization's cybersecurity posture. It became apparent to me that the glowingly positive review of the patch status, incidents, and other metrics were applicable to IT environments only. The modern CISO should be confident that metrics being reported to the board accurately reflect all segments of the business, especially OT environments. Second, I'd encourage the CISO to help foster cooperation between seasoned IT security practitioners and their OT counterparts; the approach for securing OT networks today may differ (for good reason at the moment), but it's likely that the in the future we will be more willing and able to adopt the more mature security focused network and system hygiene best practices from IT that have matured at a much faster rate than in industrial networks.

TIP 5

Greg Hale

Founding Editor at Industrial Safety and Security Source

A true leader would be able to understand the needs of the OT environment and not walk in dictating and demanding. As it is with every leader, the ability to sincerely listen and clearly communicate with no hidden agendas will help everyone successfully navigate through a very complex OT ecosystem.

Expert Industrial Cybersecurity Tips for CISOs

TIP 6

Nick Shaw

Senior System Engineer

As more organizations go after tackling OT environment risk, modern CISOs need to recognize there are different risk appetites and security requirements when it comes to the plant floor. With that said, there needs to be a single governance structure to support both domains and balance requirements. Engineering and operations need to have a voice back to IT to provide consulting in developing solutions to support their requirements. Historically these relationships have been combative between IT and OT, but a trusted partner that has expertise in both domains can help facilitate the conversation and guide both sides on what is important. With the partner, come up with a multi-year plan to address OT risk, as there usually is a lot to bite off at one time.

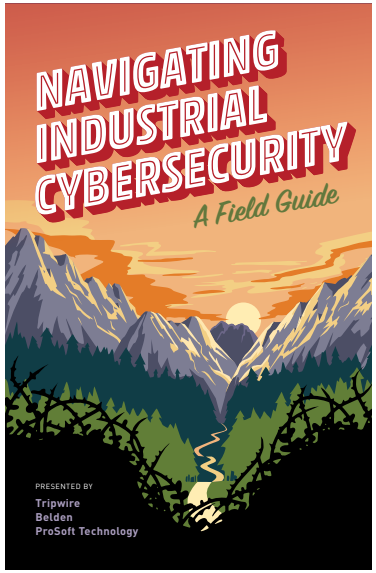
Learn More

Navigating Industrial Cybersecurity

By and large, commercial and critical infrastructure industrial organizations are underprepared for the digital convergence occurring in their IT and OT environments. ICS operators need to get a robust cybersecurity program in place—and fast.

Tripwire's free eBook covers how to do just that, with clear instructions on implementing industrial frameworks and foundational security controls, aligning IT/OT, gaining executive buy-in and selecting the right tools for the job.

Click to download ***Navigating Industrial Cybersecurity.***



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **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

 BRICTISO1b 2203