Bridging the IT and OT Cybersecurity Divide

Experts from both domains can bolster business resiliency no matter what the cyber-threats target

By Peter Vescuso, dragos.com

Industrial organizations and modern enterprises are grappling with a two-sided cybersecurity problem. They must learn to take a mature security posture in both their information technology (IT) and operational technology (OT) environments at a time when both are coming under increasing attacks—and as the line between the two realms blurs together more and more by the day.

The challenge is that while OT shares some similar operating systems, network connections, digital architectures, and cybersecurity risks as IT, there is definitely not a one-to-one relationship between the two worlds. There remain many unique constraints to securing the operational world of industrial control systems (ICSs), which means that organizations cannot simply copy and paste IT cybersecurity strategy for OT cybersecurity.

Nevertheless, IT and OT networks are increasingly interconnected to support digital transformation efforts and initiatives that drive Industry 4.0, which means accountability and priorities need to be unified. Plus, organizations can still learn a lot from the long evolution of IT cybersecurity threats and defense. Applying those lessons to OT and tailoring that knowledge to the operational environment can help create an OT cybersecurity strategy that meets the threats and circumstances of ICS security both today and in the future.

However, that can only be done if organizations open the lines of communication between IT and OT. Experts from both domains must start to work cohesively to bolster the resiliency of the business no matter which side of the house the cyberthreats target.

Why OT cybersecurity matters

Digital transformation. Enterprises are spending trillions on digital transformation today, and industrial applications are at the spear tip of these investments. When industrial concerns use cloud-connected software to better automate plants, bolster predictive maintenance, or connect industrial devices at the edge to business intelligence platforms, they are by definition more tightly coupling OT with IT systems. The business benefits are tremendous, but the process of digitally transforming industry also greatly expands the cyberrisk to the OT environment.

The world is industrial. Although the field of industrial systems has never been just about power plants and manufacturing facilities, even the perception of that no longer exists. Whether it is OT systems that track shipping operations, smart heating and lighting systems that run office complexes, smart robots that stock store shelves, or automation systems that streamline warehouses, operational technology is everywhere in the enterprise today.

These are the systems that make up the fabric of our real-life business worlds—ones that would put business continuity or people's safety at risk if they were compromised. And yet they are often forgotten from a cybersecurity perspective.

Attackers are already here. One of the biggest problems enterprises face in bridging the IT to OT cybersecurity divide is complacency. There is a perception that because the industry has not yet witnessed evidence of cyberattacks in the OT environment, it must not need OT cybersecurity monitoring. The common mantra is "There's no way our OT is a target—we have not seen any attacks."

The thing is that many attackers operate stealthily, and enterprises just do not have the mechanisms in place to see them within their OT systems. This breeds a scenario where organizations lack cyber-visibility. Because they do not monitor OT, to them the adversaries do not exist. However, time and again, Dragos runs assessments for new customers that uncover adversaries who have been present in the OT environment all along.

The OT cyberthreats of today and tomorrow

OT cyberthreats are both worse than you realize and not as bad as you want to imagine.

Without a doubt, enterprises must take ICS and OT security seriously, because the compromises are quietly accelerating. Publicized examples of successful attacks against OT systems remain remarkably rare, because most in the OT cybersecurity community understand that it is better for the ICS world and public safety to keep successful attacks under the radar. Within individual organizations, many stakeholders may be unaware of a problem, because when accidents or maintenance events with cybercomponents strike, they are often undiagnosed as cybersecurity incidents.

But these incidents and the perpetrators who carry them out are growing more prevalent. In this regard, the OT threat environment mirrors its IT threat cousins. Over the decades, IT threats have grown more prolific and more sophisticated. A similar evolution is slowly unfolding within OT. Whereas a few years ago we would see maybe only one or two global adversary teams capable of carrying out attacks against ICS systems, Dragos now tracks 11 groups that are persistently targeting OT assets around the world. And there are more threat actors and capabilities brewing.

At the same time, the larger cybersecurity community and the early advocates for OT cybersecurity must slow down the hysteria. The claims that phishing emails will take down power grids are overwrought and hurting the cause. First of all, the ICS community on the whole has built out a very resilient physical infrastructure. The beauty of those global efforts by engineering and operations professionals to advance industrial safety is that this focus has already led to a natural level of security within so many OT systems.

Additionally, the saving grace for the cybersecurity of OT systems today is that most of them are still very custom and very heterogenous. True, many OT systems run Windows like their IT cousins. But in OT there still exist many customized processes, customized hardware, customized embedded systems. Just by this very design it takes attackers a lot more effort, a lot more reconnaissance, and a lot more data collection to figure out how to build malicious software to achieve their attack goals. Most importantly, it blocks attackers from scaling attacks, because they cannot easily port techniques from one facility or organization to another.

The point is: Do not panic—but be aware that the mitigating factors for OT cybersecurity will start to deteriorate in the coming years. As digital transformation accelerates, industrial control systems will grow more homogenous, more connected, and more converged with IT. For example, cloud convergence has many organizations moving toward cloud-direct connections to historians and sensors. This opens up the kind of back doors into the OT environment that no one is properly planning for or thinking through.

As OT infrastructure changes through digital transformation, the threat actors will adapt to that with greater sophistication. Thus, it becomes crucial to add a higher level of cybersecurity competency and controls to the mix of safety measures already present in the industrial environment.

What we can learn from IT cybersecurity

As OT cybersecurity threats begin to advance, organizations can certainly learn to defend against them by looking at how IT attacks and defensive philosophies have evolved over the years. In the past decade, the IT networks have been increasingly deluged with automated attacks on all sides, perpetrated by adversaries with numerous and complex motivations. In an era of rampant ransomware attacks, financially motivated attackers are carrying out cyberespionage, theft, disruption, and destruction of IT assets.

The best practitioners in IT cybersecurity have recognized that this constant and persistent attack pressure means that it is inevitable that the bad guys will eventually manage to break into the network—somewhere, somehow. But the best cyberdefenders came to the dual realization that this does not have to translate to adversary success in achieving their attack objectives.

IT security veterans know that the goal is not to keep threat actors from ever exploiting vulnerabilities in any given system. It is to keep them from stealing valuable intellectual property, committing fraud, encrypting machines for ransom, and so on.

The fundamental truth in IT cybersecurity today is that the most resilient cyberdefenses are those that slow down adversary progress in the network and that speed up incident response to the initial break-in. It has become survival of the fastest, and veterans in IT cybersecurity have found that digital resilience boils down to three important metrics: time to detect, time to investigate, and time to remediate.

These metrics are in direct opposition to a concept and attack measurement the IT industry calls “breakout time.” Breakout time is the length of time it takes for an adversary to use an initial foothold on the network to break out of that first system and start attacking other systems in the network.

To counter that, the best in IT cybersecurity strive for the 1-10-60 benchmark. That benchmark dictates that if you can detect attacks in one minute, investigate in 10, and remediate in 60 minutes, you can generally thwart adversaries from ever getting close to their attack objectives.

Now, even in IT cybersecurity, that response speed is a reach goal at best. Most detection, investigation, and remediation response times are measured in hours and days rather than minutes. However, the closer organizations move their metrics toward the benchmark, the more they move the needle on cyberresilience.

The differences between IT and OT cybersecurity

Let’s be realistic. OT cybersecurity is nowhere close to achieving the detection, investigation, and remediation times of the IT world. And that is OK for now.

We should bring the fundamental truth about IT cybersecurity to bear on OT while keeping in mind that OT is very different. In the most simplistic way, you can think of it this way:

OT = IT + PHYSICS

Physics in this equation stands in for the physical processes that OT systems control—whether it is machines and robots in manufacturing facilities, pumps and valves at water stations, or electrical grid equipment run by the power plant.

The physics piece is the hardest part for attackers to influence. It takes quite a bit of planning and design for them to execute manipulations against physical processes and make

an impact on facilities and equipment. Take for example the public attack in Saudi Arabia in 2017 using a piece of OT-focused malware called TRISIS. In that example, the adversary had compromised environments for three years before carrying out an attack against an oil and gas facility. This was the first publicly disclosed OT cyberattack clearly designed to injure or kill someone. Fortunately, in this case, the attack failed to hurt anyone due to an error in the malicious code.

However, it does offer a good lens into the problem—namely that there is a magic window for cyberresponse, and it is likely to shrink due to digital transformation and convergence.

At the same time, it is crucial to remember that OT has a different mission, different systems, different threats, and different impact on organizations than IT. Safety, environmental impact, process availability, and intellectual property are key for OT.

Many of the basics of IT security simply do not apply. For example, vulnerability and patch management are fundamental to IT security, but much less important for OT, because many of the vulnerabilities in OT do not necessarily threaten the ultimate safety or mission of that OT system. A recent Dragos study found that some 64 percent of all industrial vulnerabilities do not actually introduce any risk, and a further 34 percent were inaccurate. This means that in the industrial world a patch-at-all-costs mindset does not make sense so much as one that has organizations smartly patching but prioritizing architecture and threat tactics instead.

The overarching lesson is that there are definitely lessons to learn from IT cybersecurity, but as organizations seek to improve OT cybersecurity capabilities it does not make sense to copy and paste your enterprise cybersecurity strategy into the ICS.

Where to get started

Applying lessons from IT cybersecurity and tailoring them to the OT environment is a years-long process toward maturation. But there are some important first steps that organizations can take to kick start their OT cybersecurity strategy and execution.

1. Engage operations

Cybersecurity professionals who want to help improve OT risk postures should start first by listening and learning the language of operations. This can be initiated with a gesture as simple as bringing a box of donuts to break the ice and start a friendly conversation with operators and engineers. Use that opening to ask them to teach you about what goes on in their side of the house. This should be done with no security ulterior motives: no checklists, no enforcement efforts, no vulnerability benchmarks. This opens up a conduit for future cooperation to create relevant cybersecurity policies and procedures that align with OT objectives.

2. Initiate knowledge transfer

The cybersecurity skills gap experienced in the IT world is magnified in OT. It is hard to get access to industrial environments for training purposes, and industrial cyberranges are often extremely costly with few virtualizations. Organizations should be seeking out ways to transfer knowledge and share it—to make more experts in-house and develop security champions among operators and engineers. A good way to initiate that knowledge transfer is to bring in external teams such as Dragos' professional services to do assessments of the environments. Do not just get a report from them—ride along during the assessment and ask lots of questions.

3. Read up and train

Beating the OT cybersecurity skills shortage and learning the language of OT cybersecurity will require all stakeholders to read up and train along the way. Fortunately, the resources are growing for OT cyberdefenders, many of them free. We list a few at the end of this article.

4. Make OT threats visible

The only way to understand the depth and breadth of your OT risk is to start adding better visibility to the OT environment. Use security monitoring to put the right information at the fingertips of defenders, operators, and engineers. But learn from the flubs of IT security in the past—do not overload defenders with every piece of possible information. Be sure systems offer up vetted, relevant, and actionable OT security information so that teams are not drowned out. Bubble up visibility—put information at their fingertips but vet information and make it relevant and actionable—without drowning small teams out.

5. Go on a hunt

Once you have observed, learned the language of OT, grown to love your operations, and learned more about your environment, go on an OT threat hunt. Be proactive in your own environment, and you will start to figure out what you have and what you do not have in terms of information collection and defenses. It is a great way to learn more about the environment and continually improve your risk posture.

RESOURCES

Robert M. Lee's reading list
https://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity

Dragos platform
https://dragos.com/platform

Industry news
https://dragos.com/blog/industry-news/a-dragos-industrial-control-system-security-reading-list

SANS ICS courses
https://ics.sans.org/training/courses

Dragos five-day course
https://dragos.com/training

ABOUT THE AUTHOR

Peter Vescuso leads the marketing team at Dragos, which specializes in helping to defend industrial organizations that provide running water, functioning electricity, and safe industrial working environments. This article is a distillation of a recent webinar titled "IT and OT: A bridge too far? Crowdstrike and Dragos don't think so." Vescuso is a seasoned B2B marketing and enterprise software veteran who has spent more than two decades leading marketing for high-growth software businesses. Prior to joining Dragos, he was division vice president at PTC, a $1.5B global software company where he was responsible for marketing digital transformation solutions to the manufacturing industry, including the market-leading industrial IoT platform ThingWorx. Vescuso holds a bachelor's degree in mechanical engineering from New York Institute of Technology and a master's degree in operations research and management from the Thayer School at Dartmouth College.