Machine Design®

DAVID MELTZER, chief technology officer at Tripwire, and
JEFF LUND, senior director of product line management, Industrial IT, Belden Inc.

Outmaneuvering the Security Threats of Tomorrow

What should you do to guard against cyberattacks as products and systems become more connected, and where do you get more information on this escalating problem?

Since 2015, U.S. manufacturers have become targets of an increasing wave of cyberattacks. The attackers—more sophisticated and better funded than ever before—seem to concentrate their efforts on mission-critical industrial environments that are often vital for economic stability, such as plants that create automobile and aviation parts. In these applications, time sensitivity, or "just-in-time manufacturing," means the target is at a serious disadvantage when subjected to a cyber event, such as a malware infection or ransomware. One mishap can cause the whole production line to fall through.

The quick turnaround times inherent to this sector give most manufacturers no more than a day and a half to supply stock at any given time. This means any attack, from a small threat, such as an unauthorized login, to the entire takeover of a network or critical infrastructure, will leave a manufacturer unable to deliver parts needed by customers to create their end-products. Considering these companies already operate on paper-thin margins, such a scenario can be devastating. If a network is down or held captive, companies lose valuable production time, significant profit, and suffer hefty downtime costs.

Take the example of a transmission plant in North Carolina. Last summer, the company's entire computer network was attacked when malware entered the control system via an email, distributing a virus. The attacker threatened to shut down the production line until a ransom was paid. In this case, the company was set to lose over a quarter of a million dollars for every hour that production was stopped. Luckily, the company identified the culprit before the event took place, but this example highlights the risks faced by every mission-critical environment.

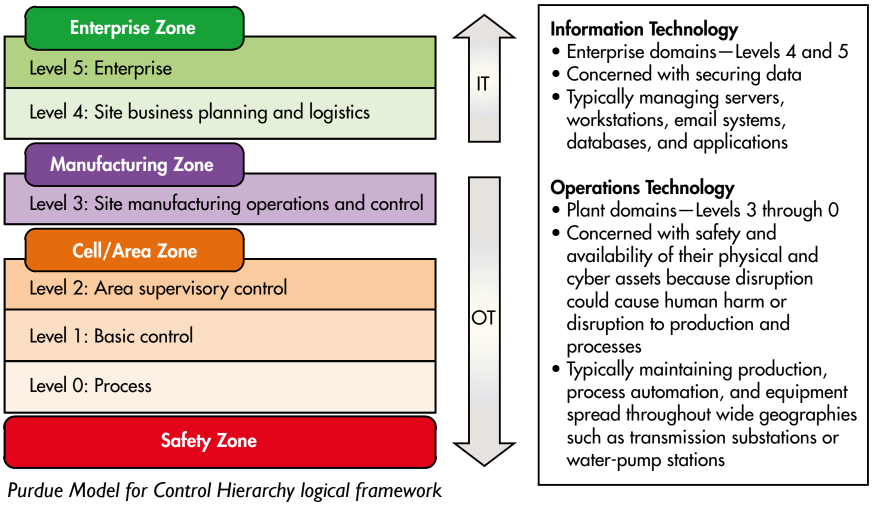
HOW TO PROTECT YOUR INFRASTRUCTURE FROM A CYBERATTACK

To ensure the safety of an industrial control system (ICS), preventive cybersecurity measures are imperative. These measures can take many forms, such as extensive background knowledge, preemptive strategies, and more. Considering real-world industrial incidents, as well as understanding how cyberattacks happen and their impact on critical infrastructures, will shape the importance of which security strategy is best for specific organizations.

Study Up on the Cyber Landscape

The technology we were using 20, or even 10 years ago, differs greatly from the technology we use today, and from what we will likely use 15 years from now. In the past, organizations didn't have the internet we use nowadays, which means older control networks were not designed for the evolving communications technologies and security challenges of today's industrial infrastructures.

To get a grip on their network's security—no matter how current—the ICS teams must first understand the landscape of current control systems and their vulnerabilities. Staying abreast of the most relevant and threatening attacks will help teams create mitigation plans for the types of threats that may target and infect their network.


Enterprise Zone
Level 5: Enterprise
Level 4: Site business planning and logistics
Manufacturing Zone
Level 3: Site manufacturing operations and control
Cell/Area Zone
Level 2: Area supervisory control
Level 1: Basic control
Level 0: Process
Safety Zone
IT
OT

Information Technology

- Enterprise domains—Levels 4 and 5
- Concerned with securing data
- Typically managing servers, workstations, email systems, databases, and applications

Operations Technology

- Plant domains—Levels 3 through 0
- Concerned with safety and availability of their physical and cyber assets because disruption could cause human harm or disruption to production and processes
- Typically maintaining production, process automation, and equipment spread throughout wide geographies such as transmission substations or water-pump stations

Purdue Model for Control Hierarchy logical framework

Know What's at Stake

Develop a solid understanding of the types of cyber threats the network may be prone to, and thoughtfully consider why an attacker might target an individual company. What do they hope to gain access to? Is there anything of value they may be after? Different types of malware allow attackers to access certain types of information and override specific system controls. Knowing what a company might be risking by not implementing different high-level security measures will help frame their counter-threat strategy.

It is important to remember that in control systems, most "attacks" are actually accidental or unintentional intrusions caused by human error or device failure. The interior of a system also needs protection, not just the borders. The extra security will enhance system reliability and availability as well as improve a network's cyber posture.

Recognize that Two is Always Better than One

Information-technology (IT) organizations tend to focus on guarding specific types of data, like financial and customer information, intellectual property (IP), and corporate materials. Information of interest to attackers could be housed on any number of company systems, which is why it is important to add safety measures to all servers, workstations, emails, applications, and databases. A siloed approach to risk management doesn't work to protect the business in the long-run.

For integrated computer systems, it is generally not the data produced by the system that we're trying to protect, but rather the safe operation and integrity of the system itself. As IT and operational-technology (OT) systems come together, it is critical to keep these differences in mind.

Holistic Security Approaches to Consider

Preemptive safeguarding alone isn't enough to deter pesky hackers, or protect you from human error or device failures. It is highly recommended that companies develop a layered, defensive strategy for their networks. Defense-in-depth, originally a military tactic now applied to security controls, uses different layers and identifiers to target and impede individual threats. These extra layers of precaution help protect the business. When one layer is breached, it doesn't mean that a full-blown attack will ensue and a failure in one part of the network won't propagate to other parts. The attacker must get through another layer or two of defense before they've won the battle.

Another approach that can be combined with defense-in-depth is the Center for Internet Security's five Critical Security Controls (CSC). The controls are a set of internationally recognized measures developed, refined, and validated by leading security experts from around the world. The top five include:

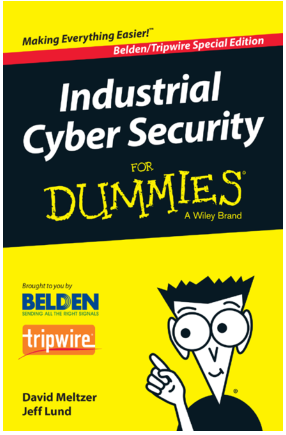
1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
4. Continuous vulnerability assessment and remediation
5. Controlled use of administrative privileges

There are 20 controls in total, but the top five are vital security elements to any industrial environment. Incorporating the most critical controls can reduce a network's risk of attack by 85% to 95%. We like those odds!

ALWAYS ON DEFENSE

Half the battle is altering your mindset. Although gaining control of cybersecurity threats may seem overwhelming at times, the key to successfully defending against attack is preparation and constant vigilance. This requires teams to be thoroughly knowledgeable about their company's critical infrastructures and to continually innovate their approach to outmaneuver a potential threat.

To learn more about developing a complete and tailored security strategy for your network you can download "Industrial Cyber Security for Dummies."


Making Everything Easier!
Belden/Tripwire Special Edition
Industrial Cyber Security
FOR
DUMMIES
A Wiley Brand
Brought to you by
BELDEN
tripwire
David Meltzer
Jeff Lund