Cybersecurity

antaira®

making connectivity simple...

Information Technology networks have traditionally been a favorite target of would-be attackers and malicious actors. By taking advantage of vulnerabilities, weak security policies, and various other attack methods, "bad guys" have infiltrated business networks, causing havoc and disarray for administrators.

On the other hand, Operation Technology or control networks have been immune to these types of attacks. Due mainly to the physical separation between IT and OT networks known as "air gaps." These air gaps allowed control engineers to operate their OT networks in a separated Ethernet space, creating a virtually impenetrable barrier with free rein and no concern about cyber-attacks outside the plant.

However, with the introduction of Industry 4.0 or the Industrial Internet of Things (IIoT), technologies that all changed.

The State of Industrial Cybersecurity

The introduction of new IP-based technologies inside isolated OT networks has been a double-edged sword. While IIoT devices have given administrators and control engineers insight into real-time data, this has led to improved operations and an overall increase in performance. These new technologies have also created a door to existential security threats that didn't exist before.

Driven by the need for access and data, administrators have converged the once separated networks, essentially creating a pathway between existing IT and OT networks. This convergence expanded the attack surface, creating optimal conditions for major security breaches that we are witnessing today.

- Fully 50 percent of manufacturing firms said they experienced a network breach in 2019 — with 11 percent facing "major" breaches — and in 2021 one in five firms found themselves targeted by cyberattacks.

The recent Colonial Pipeline attack offers an example of this problem in practice. When attackers from cybercriminal group DarkSide infected IT-side operations with ransomware on May 7, 2021, the company chose to suspend all functions — IT and OT — until the problem was solved. This decision wasn't made lightly; Colonial transports more than 100 million gallons of fuel along the East Coast every day, meaning even short-term disruptions could have massive long-term impacts.

Our Protective Perspective

Simply put, OT cybersecurity has now become even more critical than IT defense. Here's why: OT breaches of utility, supply, or manufacturing firms can mean more than just operation disruption — they can cause substantive economic harm or even death.

Consider an energy company that supplies power to thousands of homes. While a breach of their HR or financial databases is problematic for cybersecurity experts and could cause the loss of employee or customer utility data, it does not affect the available power supply. However, suppose attackers deliberately targeted supervisory systems that controlled generators, values and tampered with monitoring tools. In that case, an attacker could force a company to shut down power grids or take complete control of power distribution, leaving customers without electricity. If this were to occur during frigid winter months or in blazing heatwaves, the result could be a loss of human life. This potentially devastating impact means that even if attacks aren't directly targeting OT systems, companies can't afford the risk of exposing operational systems to security breaches.

The Colonial Pipeline attack offers a real-life example. Although the IT network was the starting point for the breach, the OT network was immediately shut down, even though there was no evidence of compromise. Why? Because operational disruptions were more concerning than their information counterparts.

While taking operations offline for a day to ensure IT issues were resolved, it also meant temporarily curtailing production capacity.

If a would-be attacker had taken control of OT network, the result could have been devastating. Damages could have taking days or weeks to correct, suspended fuel production could have cost millions of dollars in lost revenue and the possibility of cause loss of life.

Critical Challenges in Industrial Cybersecurity

Despite a growing recognition that industrial cybersecurity is at least on par with its IT counterpart, critical challenges remain. These are a few of those challenges.

Creating Robust Network Segregation

Many companies continue to leverage "flat" network structures that don't effectively segment the different pieces of their IT and OT networks. As a result, operational controls may not be securely separated from other aspects of network operations, making it easier for attackers to compromise key systems.

In practice, these attacks often start when criminals exploit vulnerabilities on connected, third-party devices or services and then move laterally through networks to access more critical

functions. Unsegmented networks make this easier for attackers since the level of security is the same across the board.

Controlling Network Access

Restricted network access is also challenging for many companies. While administrators and control engineers may need complete access to OT operations and underlying frameworks, most staff should only have access to the functions required for their current job or project. Here, robust role-based access control (RBAC) is essential to ensure the right people have the right access to the right data — but companies are often unsure where to start.

Cultivating IT/OT Communication

IT and OT are effectively two sides of the same coin. Both deal with fundamental functions that impact line-of-business operations. But these two groups often find themselves in opposition. While IT teams have a deeper knowledge of the information-based processes that power key operations, OT engineers have the practical, hands-on experience required to make the best use of industrial technologies.

The result? Communication suffers as both sides claim ownership of key network assets, in turn opening up potential security holes for attackers to exploit.

Correcting for Legacy Concerns

Many enterprises are still leveraging legacy industrial control systems (ICS) or supervisory control and data acquisition (SCADA) solutions for OT functions. In many cases, these tools weren't designed to work with public-facing networks or services — while they can be retrofit or modified to make the jump, this can introduce security threats related to stock passwords, lacking visibility, and in many cases, lead to an inability to update the firmware or software contained on these devices.

Left unchecked, these legacy frameworks can create pockets of unprotected operation within larger and more advanced OT networks.

Common Myths Around Securing Industrial Networks

While existing challenges set the stage for OT struggles, common myths around securing industrial networks can exacerbate these issues. Although every firm is different, these are some of the most prevalent myths.

Industrial Networks are Behind the Curve

There's a common perception that industrial networks are behind the technology curve — that because of their roots in air-gapped, inward-facing legacy devices, they're not as advanced. In fact, many of today's most advanced technologies such as artificial intelligence (AI), and machine learning (ML) tools are increasingly geared toward OT networks as consistent operations become critical in line-of-business efforts. While it's true that many control engineers don't have the same system administration experience as their IT counterparts, the integration of IIoT and Industry 4.0 technologies is now closing the gap, setting the stage for fundamental shifts in the IT/OT balance.

Separate Equals Secure

Despite their evolution, many OT networks remain largely separate from their IT counterparts. It makes sense; there's no reason for most production line or shop floor processes to have direct external connections. But this can provide a false sense of security since these devices still require regular updates from centralized network controllers, which in turn exist across both IT and OT frameworks. The result is a partially separated system that often lacks robust monitoring for potential security threats because it's assumed that distance from outward-facing functions will provide natural protection.

In fact, this lack of oversight can open the door to substantive security risk. If attackers can compromise IT functions, move through networks to connected OT solutions and then shift into production environments, they can disrupt operations at scale, in turn causing partial or full function shutdowns.

OT Networks Don't Need the Same Level of Security

With data now fueling a revolution in analytics and operations, there's often a mistaken assumption that IT networks require more security than OT frameworks. In fact, the opposite is true — while the loss of data could be damaging to business reputations or cause compliance issues, loss of control over pipelines, powerplants, or production lines could have real-world impacts that range from supply shortages to property damage to physical harm.

How Antaira Can Help Streamline Security

Securing OT networks is a collaborative and continuous process. There's no single solution capable of completely removing risk and ensuring that teams are able to detect and defend against every attack. Instead, closing the security gap depends on a multi-layer approach that prioritizes security by design: The idea that each piece of the operational puzzle can actively contribute to better security. Industrial Ethernet switches, industrial media converters, and industrial wireless routers from Antaria can help streamline this process with robust, DoD-compliant layer 2 and layer 3 security that helps effectively manage network traffic at scale.

Our full suite of security controls effectively gives administrators the tools to build on existenting security policies and company standards. For example, our Authentication, Authorization, and Accounting mechanism can track users' activities while limiting essential controls to employees who require them. In addition, Access Control Lists (ACLs) can further filter accessibility, by limiting network traffic to only trusted sources, restrict management access to designated networks and allow user access on selected machines.

Mind the Gap

OT security is now more critical than its IT counterparts. Informed by IIoT expectations and driven by the potential for substantial service disruptions, companies need to close the gap with robust security strategies that connect controllers, sensors, routers, and switches — no matter where they reside in the network.
Curious about how we can help? Learn more about our Industrial Networking solutions. Ready to make the switch? See where you can purchase Antaria products worldwide.