The Shortcomings of Traditional Security and Digital OT

Table of Contents

Executive Summary

Organizations across all industries are embracing new digital tools and services to accelerate and grow their businesses. The rapid adoption of these technologies has caused internet-connected information technology (IT) networks to increasingly intersect with previously isolated (and often difficult to update with patches) operations technology (OT) networks. This overlap also means that the ever-expanding IT attack surface now exposes OT systems to previously unknown threats within these environments. The result is that traditional security approaches are insufficient to protect connected OT environments.

45% of OT companies increased spending to manage processes related to IT-OT network convergence and to support remote work.[1]

When OT Met IT; A Network Convergence Story

Securing OT systems has become a crucial concern in industrial and critical infrastructure environments such as energy, utilities, manufacturing, communications, transportation, and defense. OT includes industrial control systems (ICS) that run equipment or machinery as well as the supervisory control and data acquisition (SCADA) subset systems that provide a graphical user interface for ICS.

The value of OT assets can range into the billions of dollars and their safe operation is often critical to public safety or national/global economic health. A system crash on a manufacturing floor can stall production for hours and potentially ruin millions of dollars in materials. Having to reset a 10,000-gallon boiler processing caustic chemicals can have far more devastating consequences than any IT network outage. In other circumstances, a SCADA or ICS breach within critical infrastructure (such as a hydroelectric dam or nuclear power plant controls) could endanger the lives of workers and surrounding citizens. This puts network operations analysts under tremendous pressure to simultaneously maintain security, operational uptime, and safety.

Until recently, the best way to do this was to keep IT and OT completely separate from one another—a process known as “air gapping.” It is very common to find OT systems that have been running for more than 20 years with legacy operating systems that have no available security patches. Isolation of vulnerable and delicate OT technologies protected them from almost all outside disturbances.

But increasingly, IT and OT are being integrated for greater business efficiency, increased innovation, and competitive advantage. The benefits of convergence include more effective and efficient monitoring of processes, the ability to leverage data from Internet-of-Things (IoT) devices to inform decision-making, and significant cost savings in power consumption, reduced raw materials waste, and employee efficiency. Convergence is the clear trend, but the process brings with it a number of security challenges because it eliminates the de facto security of the air gap against common internet-borne attacks.[2]

96%

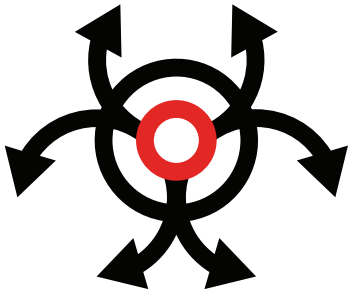
of organizations foresee challenges as they move toward OT-IT convergence.[3]

The Attack Surface Expands

IT and OT convergence means that the ever-expanding range of threats that target IT networks now have pathways to attack OT as well—which vastly expands an organization's potential attack surface. To complicate matters even further, the delicate nature of OT systems means that traditional security approaches are insufficient to protect these environments.

When it comes to cybersecurity, existing OT defenses are much less evolved than their analogous security counterparts in the IT realm due to prior lack of investment and knowledge. So, OT decision-makers must modernize their security controls. And as the attack surface continues to grow and evolve with greater IT-OT connectivity, improving the OT security posture is also constrained by the need to keep up with rapid change and a lack of staff resources. OT leaders continue to struggle to keep pace with change and the lack of skilled labor.

All of these factors contribute to a heightened sense of awareness of OT across the enterprise, with the awareness making OT security a top priority.



9 out of 10 OT organizations experienced at least one intrusion in the past year and 63% had 3 or more intrusions. The most common intrusions were malware at 57% and phishing at 58%.[4]

Security Incidents Are on the Rise

Where there is opportunity, there is exploitation. Threats targeting OT systems are on the rise. The current lack of effective OT security contributes to these risks. Two high-profile examples are:

- **SolarWinds:** This U.S. information technology firm was the victim of a cyberattack that spread to 33,000 of their customers and went undetected for months. When SolarWinds sent out software updates to its customers, it included hacked code that created a backdoor to the customer's information technology systems, which the attackers used to install more malware, so they could spy on companies and organizations.[5]
- **Colonial Pipeline:** One of the largest oil pipelines in the U.S. was the victim of a ransomware attack in May 2021 that infected some of the company's digital systems. Colonial Pipeline shut down more than 5,500 miles of pipeline for several days to prevent the ransomware from spreading.[6]

Politically motivated cyberattacks against critical infrastructure have the potential to do more than just grab headlines. They can be weaponized to cripple civil defenses, shut down production of vital resources, and even cause widespread harm to human lives. The current lack of effective OT security contributes to these risks.

Successful intrusions resulted in the following damages at OT companies:

- **Productivity, 51%**
- **Revenue, 42%**
- **Brand Reputation, 43%**
- **Business-critical Data, 29%**
- **Physical Safety, 45%[7]**

Key Problem Areas in OT Security

For network operations analysts, there are a few problem areas of interest that must be understood to approach a comprehensive solution for OT network security.

1. **Adding IT-based innovations brings IT-based vulnerabilities.** Automation and improved operational efficiency are driving forces behind OT and IT convergence. New digital technologies in OT require internet interconnections—and with the good comes the bad.

2. **Traditional security approaches are no longer effective.** The increasingly distributed nature of any modern network (IT or OT) has made traditional perimeter-only defenses an ineffective strategy. Many organizations allow a substantial number of wireless and IoT or Industrial IoT technologies (such as smart environmental controls) to connect to their OT networks for greater efficiency. Most of these technologies are thought to be contained in a closed OT environment without their owners realizing that these devices are connected and therefore adding to the OT attack surface. IoT devices deployed within OT environments can provide backdoors for internet-based threats to reach vulnerable systems like SCADA and ICS. And because IoT devices themselves are typically headless—lacking the ability to support their own sophisticated, built-in defenses—they require holistic security from an outside source.

3. **OT systems can be hypersensitive.** Legacy OT systems can operate for 30 to 40 years and may depend on dated configurations that remain unpatched. Because updating devices can require shutting down entire systems, many operations managers follow the "if it isn't broken, don't fix it" rule. As a result, many older OT systems are notoriously vulnerable to malware and other threats that IT networks are naturally protected against. Complicating the problem even further, devices and systems installed in an OT network can be notoriously fragile when it comes to how they are secured. Even processes as benign as active device scanning can cause them to fail. This can become a case of both the disease and the cure potentially causing serious harm.

In light of this somewhat unique set of problems, OT network security must be fully reconsidered at a foundational level. And lacking many of the basic controls that IT networks have already adopted in recent years to address digital evolution and sophisticated threat exposure, OT security may seem a daunting task to take on.

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

-Sean McGurk, Former Director, NCCIC, the Department of Homeland Security[8]

The Path Toward Comprehensive Network Protection

To be successful, security must become seamlessly integrated into OT environments without disrupting the often-sensitive nature of the systems in use. With an expanding attack surface, new threat exposures on multiple fronts, and a dearth of advanced threat protection solutions in place, network operations managers need to ask questions such as the following to determine their level of OT risk:

- ☐ How integrated are our IT networks and OT systems and what risks does this pose for the organization?
- ☐ Do we have transparent visibility across our OT environments or do SCADA/ICS reside in silos?
- ☐ Is the security for our OT and IT environments integrated and do we have single-pane-of-glass visibility and unified controls?
- ☐ How many headless OT devices and systems exist and what risk do these present to our broader OT and IT environments?
- ☐ Which OT devices and systems cannot be updated regularly and present a threat risk (and what does that risk look like)?
- ☐ How long does it take for us to respond to a threat detection across the entirety of our OT and IT environments?

There certainly are other questions that network operations analysts can ask, but this list is a good starting point.

[1] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[2] "Independent Study Finds That Security Risks Are Slowing IT-OT Convergence," Fortinet, May 23, 2021.

[3] Ibid.

[4] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[5] Isabella Jibilian and Katie Canales, "SolarWinds Hack Explained," Business Insider, April 15, 2021.

[6] Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know," TechTarget, July 7, 2021.

[7] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[8] Sanjay Chhillar, "Common ICS Cybersecurity Myth #1: The Air Gap," Global Cybersecurity Alliance, July 6, 2021.

FORTINET®

www.fortinet.com

October 25, 2021 9:51 PM

360405-A-0-EN