WHITE PAPER

2021 State of Operational Technology Security in Transportation and Logistics

Table of Contents

Research for this white paper was conducted by Virtual Intelligence Briefing (VIB). VIB is an interactive online community of more than 2.2M IT practitioners and decision-makers who share their experiences and opinions by engaging in vendor-neutral surveys across virtually all IT/OT domains. The survey methodology adheres to industry research best practices including respondent targeting and screening, bias-neutral question construction, respondent usability testing, and post-survey analysis.

Key Findings

Fortinet's research report 2021 State of Operational Technology (OT) Security in Transportation and Logistics (T&L) finds that security leaders in T&L companies generally feel supported by senior leadership for their efforts. However, most also remain worried that their OT infrastructure could be targeted by malware, exploited by phishing attacks, or contain existing or known vulnerabilities

- Only 14% of transportation and logistics organizations feel less than moderately supported by their board of directors when it comes to OT security
- Despite this, 56% of transportation and logistics organizations are more concerned about an OT cybersecurity breach than they were 12 months ago
- Meanwhile, in the last year, 43% of T&L organizations have experienced four or more OT cybersecurity breaches
- Eight of 10 T&L organizations feel malicious, negligent, or inadvertent insiders represent their most concerning OT security adversary
- Vulnerability management is the top OT security investment most T&L organizations are pursuing

Executive Summary

Overall, OT security leaders across medium- to large-sized T&L companies remain well-supported by senior leadership and their board of directors. However, those in charge of OT security in these organizations are growing more concerned that they will experience an OT cybersecurity breach in the coming year.

The harsh truth is that while 46% of T&L organizations have not discovered an OT cybersecurity breach in the last year, a nearly equal amount (43%) have experienced four or more breaches — indicating plenty of room for improvement when it comes to OT security.

While OT security technologies employed across T&L organizations are myriad, the top two areas of security investment are vulnerability management and network segmentation. This is a wise approach since a majority of T&L operational technology is now highly integrated into IT networks — meaning previously "air-gapped" OT systems are now internet-connected and vulnerable to exploitation.

As noted in Fortinet's 2021 State of Operational Technology and Cybersecurity Report, the responsibility for OT security is shifting from network operations directors to the CISO or CIO.[1] This shift is being echoed in transportation and logistics organizations, with only 7% of organizations declaring the security of OT remains the responsibility of the head of operational technology. This means OT may gain inclusion in larger security initiatives in T&L organizations but could also lose the specific and essential focus on unique OT security challenges.

Introduction

Operational technology dependence is on the rise, with solid growth projected through 2027.[2] This should come as no surprise to leaders in T&L enterprises because OT uses hardware and software to monitor and control physical processes, devices, and infrastructure — all critical to the efficient movement of freight, cargo, and people across cities, regions, nations, and continents.

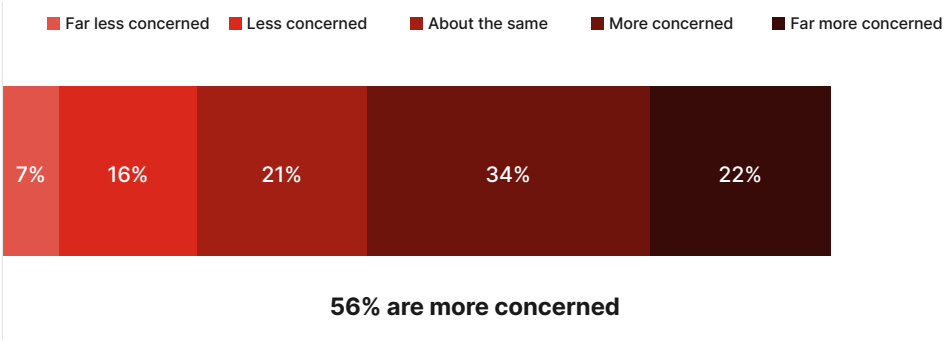
To boost operational efficiency and profitability, many T&L businesses have been digitally connecting OT infrastructure such as supervisory control and data acquisition (SCADA) systems with IT networks. We noted in our 2021 State of Operational Technology and Cybersecurity Report that competitive pressures are driving the need to reduce costs and increase efficiencies in a variety of ways, such as:

- Utilizing digital twins to reduce risks supporting asset performance management (APM)
- Increasing overall equipment effectiveness (OEE) to drive increased manufacturing yield
- Shifting from calendar-based to condition-based maintenance to minimize lost production from service outages
- Increasing asset availability and reliability
- Digitization of paper recordkeeping and service reports for service and maintenance activities

While the previous findings were across all industries managing OT, most of these initiatives apply to T&L businesses and organizations as well. However, the improved agility and efficiency derived from IT/OT network convergence also comes with increased risks. The diminishing presence of the "air gap" between OT networks and IT systems means the OT infrastructure is subject to the threats that IT systems have traditionally faced. Worse, the attack surface for an OT system can comprise industrial internet of things (IIoT) devices that control critical systems — resulting in potentially dire health and safety consequences if breached.[3]

We think the rise of IT/OT integration is why 56% of T&L operational technology security experts feel more concerned about an OT cybersecurity breach happening in the next 12 months than they were in the year prior.

OT-related cybersecurity breach concern in next 12 months



56% are more concerned

Our latest study of OT security in transportation and logistics has generated several key insights, along with some best practices that all T&L businesses should implement to increase their OT security.

Methodology

This study was conducted in November 2021 with members of 73 organizations (ranging in staff sizes from 1,000 to 10,000 employees) that specialize in logistics and/or transportation (public, rail, air, or maritime). The majority of people surveyed came from larger logistics companies with most (74%) individuals being managers or directors of IT and/or OT.

Top 3 OT Insights for Transportation and Logistics

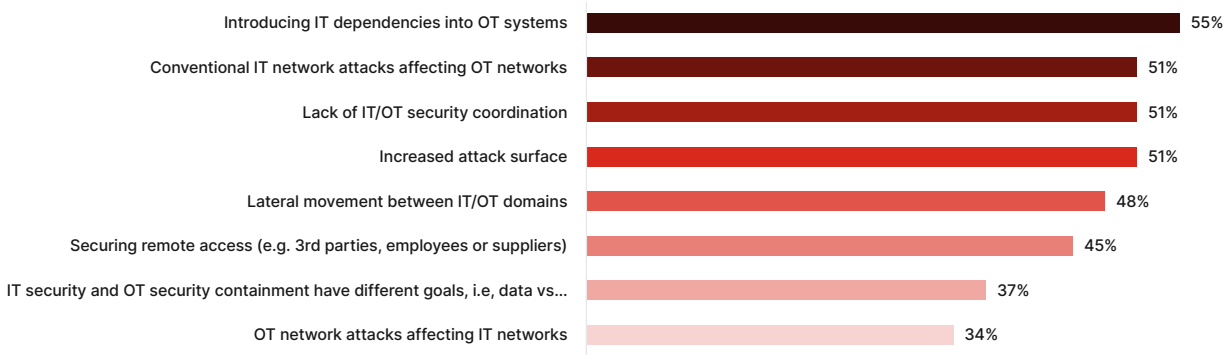
As noted from our 2021 State of Operational Technology and Cybersecurity Report, OT leaders continued to struggle with changes related to IT/OT convergence, and transportation and logistics echoes many of these.[3] T&L organizations have very advanced maturity in their OT, but still face challenges related to security measurements and analysis — with some organizations experiencing a significant number of intrusions in the past year.

Insight 1: While business objectives are driving OT maturity in T&L organizations to advanced levels, cybersecurity concerns about specific threats and threat actors are on the rise.

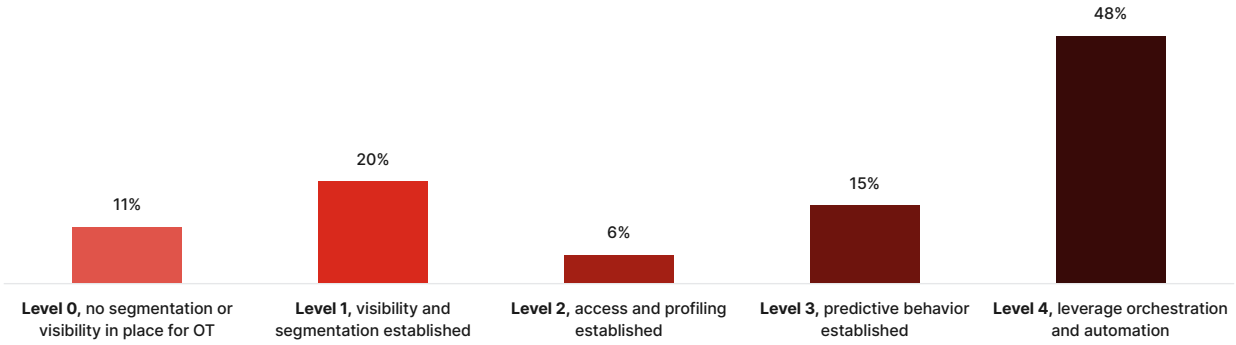
Within T&L, the need to innovate and transform is driving the integration of IT and OT. Similar to the IT experience over the last decade, cloud is a major force, with 58% of respondents indicating access to cloud applications was driving their IT/OT integration.

Interestingly, the convergence of security for the two disciplines is listed as the second and third driving forces for integration in most T&L organizations. This integration to consolidate and bolster security represents both beneficial opportunities as well as potential exposure vectors for OT systems that have typically been air-gapped and non-accessible to potential threat actors.

Key concerns with IT/OT network integration

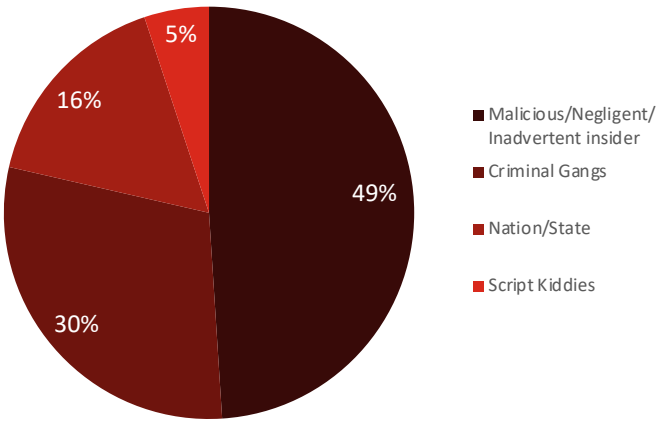


Because T&L organizations have depended on OT for quite some time, it is no surprise that nearly two-thirds are very mature when it comes to their OT implementations and reliance on a legacy security strategy. However, just over 10% of T&L organizations have no network segmentation or visibility in place to detect and deter potential threat actors — representing significant risk to their business.

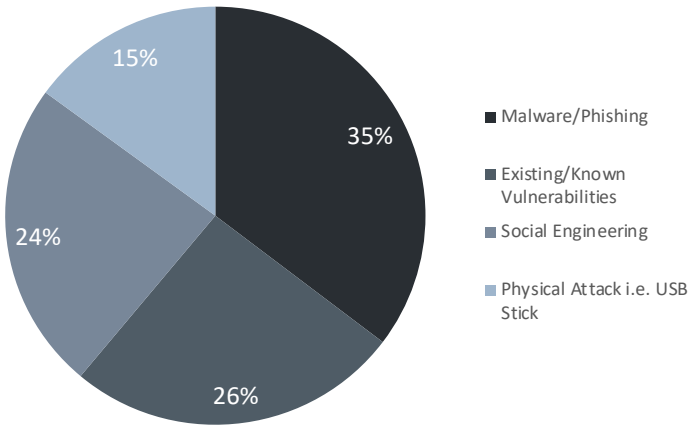


The areas of greatest concern to OT security leaders within the T&L industries are either unwitting, unaware, or malicious insider threats or criminal organizations engaging in successful malware/phishing attacks or exploiting existing or known vulnerabilities.

Most concerning adversary



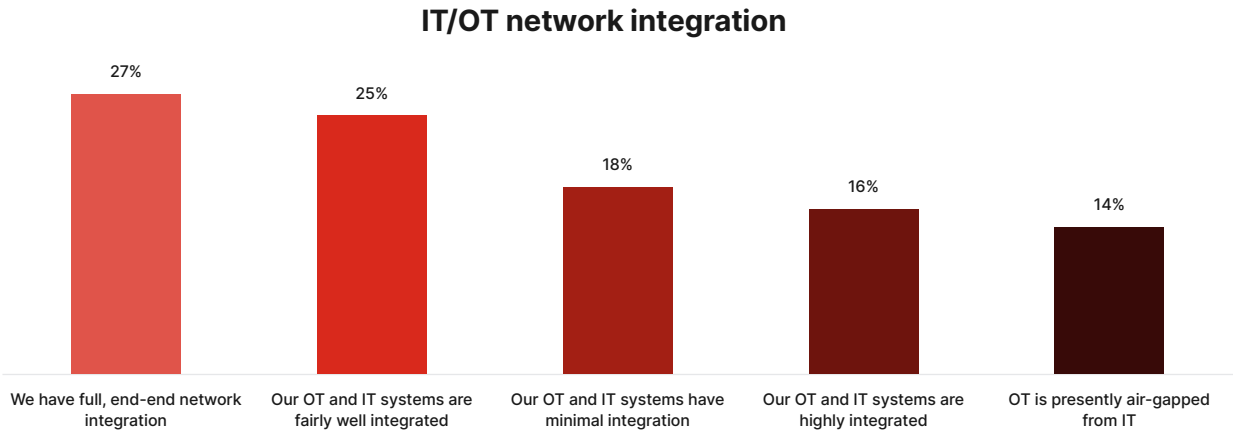
Attacks of most concern in OT environment



Insight 2: For most of T&L, the historical OT "air gap" that both assisted and hindered security has essentially disappeared, leading to increased concerns that must be addressed.

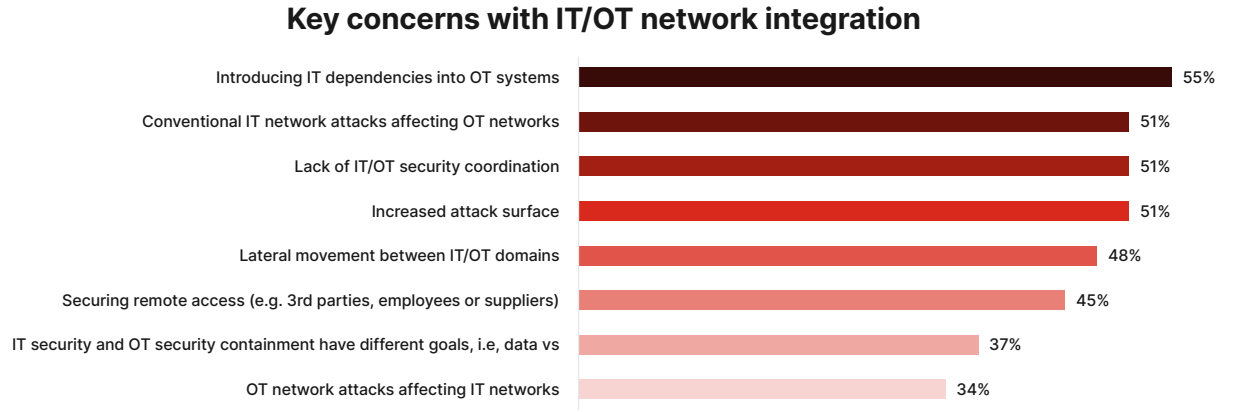
Traditionally, OT cybersecurity was less necessary since OT systems were not connected to the internet. As such, they were not exposed to outside threats. However, this historical air gap resulted in just as many security problems as it resolved. Because IT and OT networks were kept separate, there was often duplication of security efforts and little transparency between teams. This made it difficult to identify the boundaries of the attack surface as these disparate teams lacked shared network asset situational awareness.

Nearly two-thirds of T&L organizations enjoy well-integrated IT and OT networks, leaving nearly a third dealing with the security challenges of minimally integrated networks. The air gap may protect to some extent, but as we observed earlier, the desire for better and more integrated security across all networks is driving IT/OT network integration in most T&L organizations.



2/3 are highly integrated, while 1/3 minimally to no integration

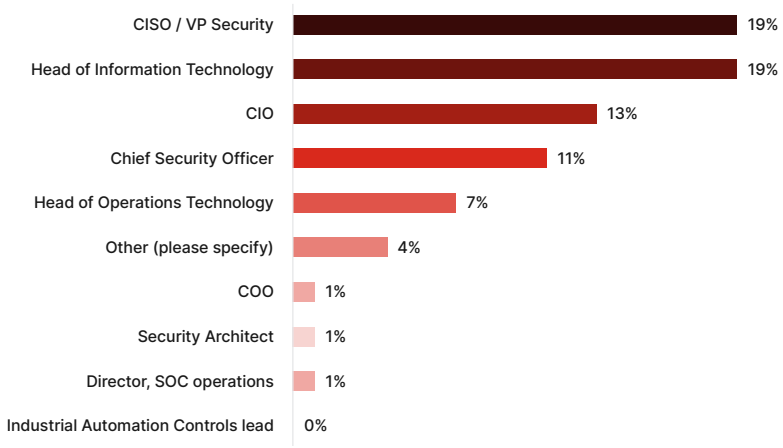
The proliferation of network integration in T&L industries does represent significant risk to traditional OT though — and T&L organizations have some key concerns. These concerns are justified, given that many organizations have bolted-on point solutions to address specific issues. These patchwork approaches to OT security result in a complex network where solutions do not share vital intelligence or provide full visibility.



Insight 3: T&L organizations are on the right track when it comes to security, but too many remain vulnerable and are experiencing breaches with significant impacts to their businesses.

As of 2020, 70% of all OT organizations plan to roll OT security under the CISO in the next year (only 9% of CISOs oversee it currently), and 62% of OT security budgets are being increased. T&L organizations appear to have made progress on the first goal of consolidating OT security under the CISO or VP of IT security.

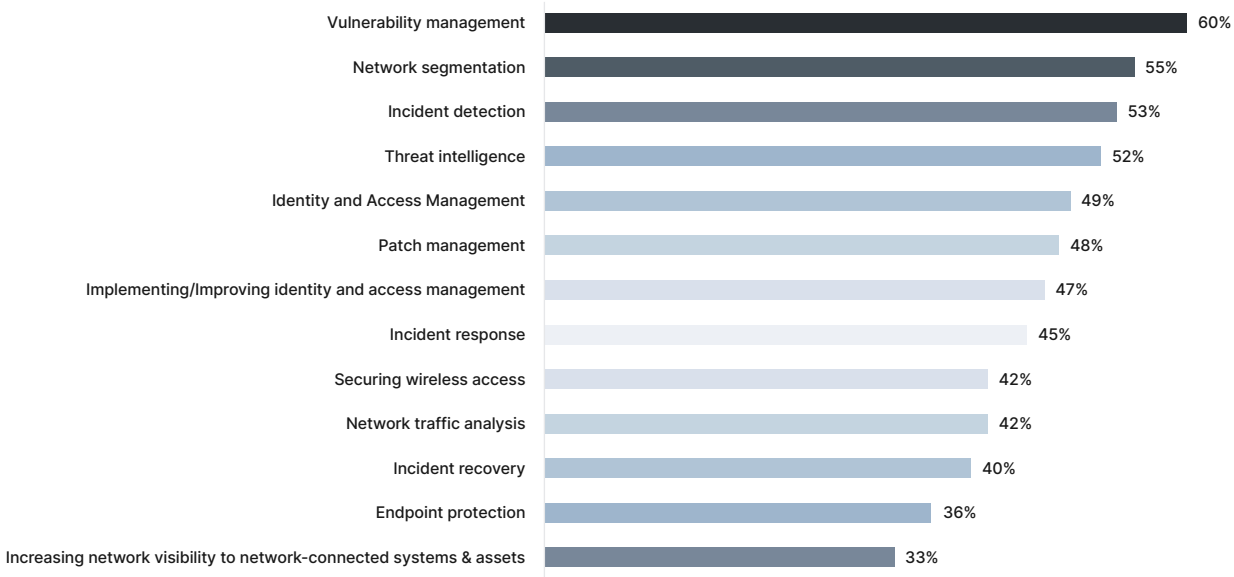
Overall responsibility for OT



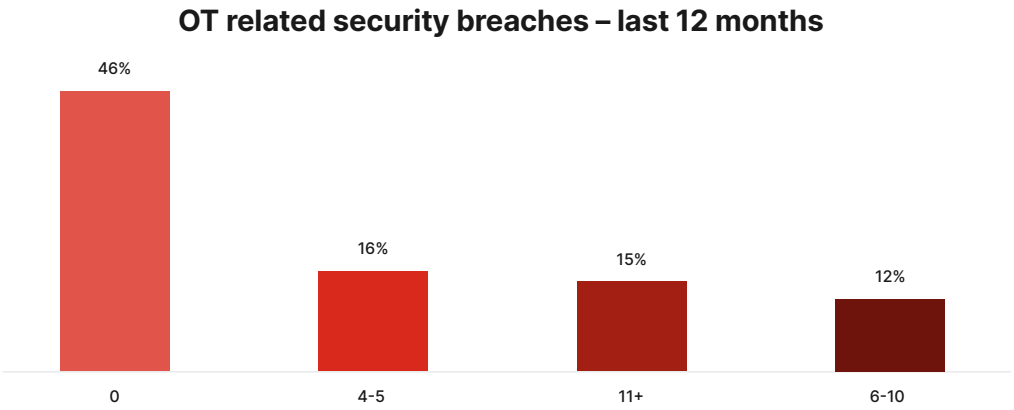
Predominantly VP, C-level

And it appears T&L organizations are aggressively pursuing OT security and plan to invest in this area soon, possibly indicating increased security budgets as well.

OT security investment in 12-18 months

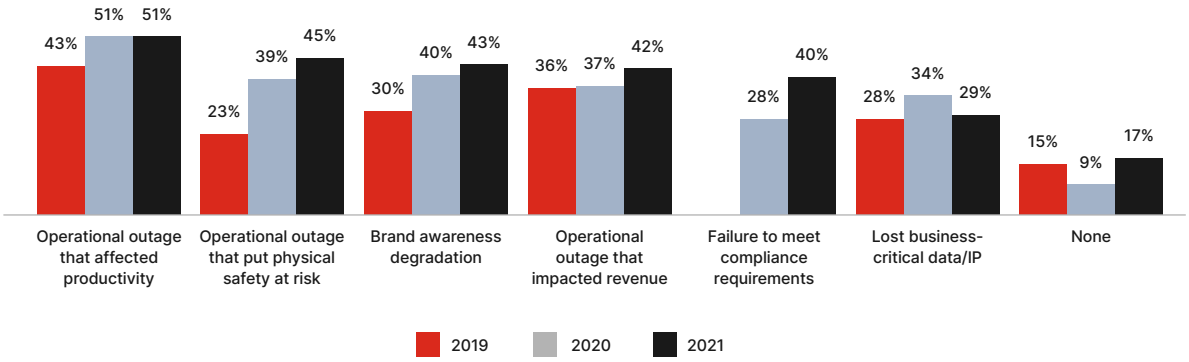


The desire to invest in OT security near-term is wise. As of 2021, there are nearly as many T&L organizations experiencing four or more security breaches per year on their OT systems as there are detecting none. This relatively high “no breach in the last year” result for T&L may indicate that many have implemented successful security measures. Given how many T&L organizations are fairly mature (Level 4), this is not surprising.



However, this also means a nearly equal percentage (43%) of more immature T&L organizations remain vulnerable and are experiencing elevated numbers of breaches. A successful breach can have severe consequences for a T&L business — from impacted services and risk of physical harm to loss of reputation and revenue.

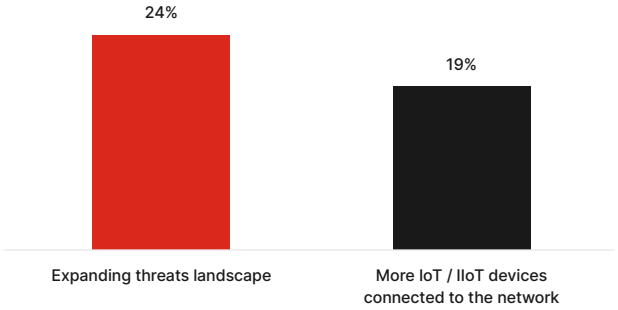
Based on research from the Fortinet 2021 State of Operational Technology and Cybersecurity Report across all industries, it is logical to assume that those T&L organizations that experienced an OT security breach had similar impacts as a result.



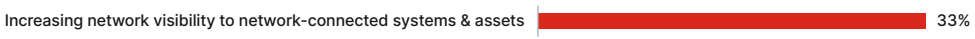
As noted, it is important to ensure integration and compatibility across combined IT/OT security teams and technologies to avoid exploitable gaps and inefficiencies in response.

Best Practices for OT Security in Transportation and Logistics

1. **Identify assets, classify, and prioritize value**
   Improving security posture starts with visibility. One cannot protect what one cannot see. Lacking visibility is a critical security gap within many organizations. Only 58% of organizations have a formal program to inventory OT assets, and 57% document connections that lead outside of OT (down from 62% in 2019).[4] Going forward, a significant number of T&L organizations expect an increase of devices, and an expanding threat landscape will impact their OT security plans.



   One-third of all T&L organizations plan to increase their network visibility in the next 12 to 18 months.



   T&L operational technology security teams need an up-to-date inventory of devices and applications running on the network. One challenge is that many OT networks can't be actively scanned with the methods used for an IT network. For example, many programmable logic controllers (PLC) devices are notoriously delicate, and even actively scanning these devices can cause them to fail.[5]

2. **Segment the network**
   Given the relative disappearance of the OT air gap in T&L organizations, network segmentation is one of the most effective architectural concepts for protecting OT environments.

   The concept is to divide the network into a series of functional segments or "zones" (which may include subzones or microsegments), and make each zone accessible only by authorized devices, applications, and users. A firewall defines and enforces the zones, and it also defines conduits, which are channels that enable essential data and applications to cross from one zone to another.

   In the next year and half, more than one out of every two T&L organizations plan to invest in network segmentation.

3. **Analyze traffic for threats and vulnerabilities**
   Once next-generation firewalls (NGFWs) divide a combined IT/OT network into segments and conduits, it is valuable to analyze network traffic for known and unknown threats. Security teams should seek to integrate a NGFW capable of inspecting encrypted application traffic. Additionally, the NGFW should be integrated with a live-feed service to provide updates on the most common OT protocols and OT application vulnerabilities.

   Of the T&L organizations surveyed, 42% have plans to invest and implement network traffic analysis in the near future.

4. Control identity and access management

Stolen credentials are an element of many OT cyberattacks, including three of the four previously profiled. Spear phishing deployed to steal credentials was a key part of those attacks.

Nearly half (49%) of the surveyed T&L organizations plan to increase their identity and access management (IAM) in 12 to 18 months to improve their OT security.

T&L security teams should seek an IAM solution that:

- Enforces role-based access for each user, limiting access through integration with the firewall to only appropriate resources and network microsegment
- Validates identity with multi-factor authentication, combining something the user knows (such as username and password) with something the user has (such as a phone, laptop certificate, or physical security key) or something the user is (such as a fingerprint or other biometric)
- Enables single sign-on (SSO), saving time by enforcing enterprise user identity-based security without requiring additional sign-on screens
- Authenticates devices attached to the network by observing their characteristics and behavior and noting the need for software updates to patch vulnerabilities
- Restricts access to only authenticated devices, locking down all other ports

5. Secure both wired and wireless access

In an OT environment, two attractive targets for cyberattacks are network switches and wireless access points (WAPs). Both should implement security by design, administered from one central interface, instead of relying on protection via point security solutions managed through multiple interfaces.

42% of the surveyed T&L organizations plan to invest in the security of their wireless access points in the next year and half.

Security management that is centralized not only reduces risk, but it also improves visibility and minimizes administration time for security and operations teams.

Conclusion

Cybersecurity risks continue to be high in companies that are charged with protecting OT environments, holding steady from last year.[6] Given that in most T&L organizations, OT networks are rarely air-gapped from IT networks and connections to the internet, OT systems are more vulnerable.

The good news is that most T&L businesses appear to be aware that they face increasing risks from IT-borne and internet-borne attacks and appear to be mature enough in their OT security stance; aware they must be vigilant and coordinated in their IT/OT security response; and wise enough to invest in needed OT security technologies to avoid breaches.

Resources:

1. "2021 State of Operational Technology and Cybersecurity Report," Fortinet, 2021.
2. "Global Operational Technology Market—Industry Trends and Forecast to 2027," Data Bridge Market Research, July 2020.
3. "2021 State of Operational Technology and Cybersecurity Report," Fortinet, 2021.
4. "A SANS 2021 Survey: OT/ICS Cybersecurity," SANS, August 2021.
5. "A Solution Guide to Operational Technology Cybersecurity," Fortinet, March 1, 2021.
6. "2021 State of Operational Technology and Cybersecurity Report," Fortinet, 2021.