DARKReading RESEARCH

DECEMBER 2022

The (Precarious) State of OT/ICS Security

As threats and regulatory demands continue to rise, enterprises find themselves struggling to cover the basics of securing operational technology (OT) and industrial control systems (ICS).

XONA

Executive Summary

Attacks on operational technologies and industrial control systems are on the rise. A quick look at a handful of megatrends that affect these environments tells us why: operational technologies and industrial control systems are becoming increasingly digital and networked, traditional enterprise IT and OT/ICS converging, all-the-while nation-state-backed or aligned attackers have grown increasingly emboldened, and the tools and techniques used to attack these systems are growing more common. Compounding these challenges, critical infrastructure is often shipped with exploitable vulnerabilities.

During a hearing with the U.S. Senate Committee on the Judiciary, then director of the Cybersecurity and Infrastructure Security Agency within the U.S. Department of Homeland Security, Christopher Krebs testified that cyber threats remain one of the most significant strategic risks for the U.S. and that such risks are "threatening our national security, economic prosperity, and public health and safety." He continued: "Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy."

"The OT/ICS environment is quickly evolving," says Bill Moore, Xona Systems CEO, and founder. "With more intelligent devices and more computing systems at the edge, we will see increased threats target these converged and increasingly connected systems," he adds.

One doesn't have to look far to find examples of global attacks crippling business operations, energy distribution, and water supplies. Recently, Italy's National Cyber Security Agency warned that the volume of attacks targeting the nation's energy industry is expanding. The announcement followed a pair of attacks against the nation's energy industry, including oil and gas giant Eni SpA. "Eni confirms that the internal protection systems have detected unauthorized access to the company network in recent days," a company representative told Bloomberg News.

Earlier this year, the intelligence community from the U.S., Canada, U.K., Australia, and New Zealand, issued a joint advisory warning that critical infrastructure operators are under increased attack from nation-state-backed threat actors. While OT/ICS systems were not attacked directly in the 2021 attack against Colonial Pipeline, the subsequent shutdown exposed the dangers to the nation's critical infrastructure and the interdependency between operational and IT systems. A few months later, a Presidential executive order requiring power systems to bolster their cybersecurity defenses and readiness, was issued.

This report, based on an exclusive survey conducted by Dark Reading, finds that organizations actively securing operational technologies are fully aware of these threats and are struggling with the security basics. We investigate the current state of OT/ICS systems and examine the approaches OT/ICS security managers are taking to secure these systems and the challenges they face while doing so.

Top Level Findings

- Firewalls continue to play a significant role in OT environments. A little over half of the organizations rely on firewalls to provide remote access to OT and ICS devices, and 31% of respondents say they segment OT/ICS network traffic using network firewalls. Another 35% rely on virtual LANs to segment network traffic.
- While the majority of organizations have not experienced a significant security incident in their OT and ICS networks in the past year, they are concerned about potential ransomware attacks.
- A zero trust approach is important, but adoption is uneven. About 40% of respondents say they rely on zero trust to secure OT systems and ICS in their organizations, but only 24% use it to handle authentication for remote users.

The Top Threats to Operational Technology

As OT/ICS technologies grow more computerized and networked (TCP/IP), they will face the same risks and threats as traditional computing systems. Threats include human attackers relying on targeted exploits, denial-of-service attacks, and widespread malware, such as viruses, worms, and ransomware, to carry out their operations.

Our survey found the OT/ICS security managers are most concerned about ransomware attacks. When asked to rank the threats they are the most concerned about, respondents list ransomware as their top threat, followed by phishing, malware/viruses, denial of service, stolen data, and attacks on third parties from their own systems **(Figure 1)**. There was a noticeable gap between the top two rankings — ransomware and phishing — suggesting that respondents were significantly more concerned about ransomware in their OT/ICS environments than they were about phishing.

A cursory look at alerts from the National Vulnerability Database and CISA reveals an endless stream of vulnerabilities affecting operational and industrial hardware, system software, and components. "As more components are deployed that support TCP/IP, and organizations seek the convenience of remote access and monitoring, the attack surface and the associated vulnerabilities are going to continue to expand and grow in number," says Xona Systems' Moore.

In an alert published in September, the CISA warned that OT/ICS assets would continue to be an attractive target for malicious cyber actors. These threat actors will target these systems for political gains, economic advantages, or destructive effects. "Because OT/ICS systems manage physical, operational processes, cyber actors' operations could result in physical consequences, including loss of life, property damage, and disruption of national critical functions," the agency warned.

"OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, many tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks," according to the alert.

Figure 1.

Most Concerning OT/ICS Attacks

Please rank the following types of attacks on OT/ICS in the order your organization is most concerned from highest to lowest.

	OVERALL RANK
Ransomware/extortion	1
Phishing	2
Malware/viruses	3
Denial of service/availability	4
Stolen data/data exfiltration	5
Attacks on third parties from your systems	6

Note: Rank is based on a weighted score. Answers are weighted, and scores are a sum of all weighted counts.
Data: Dark Reading survey of 75 IT and cybersecurity professionals, July 2022.

How do respondents believe such attacks are most likely to manifest in their organizations? When ranking the attack vectors on OT systems and ICS, respondents are most concerned about vulnerabilities in software and systems **(Figure 2)**. That was followed in order by concerns about financially motivated cybercriminals, insider threats, contractors/consultants, nation-state attackers, attacks from third parties, and terrorism. "As more threat actors gain skills in OT/ICS systems and the tools they use become more commonplace, we're going to see the number of attackers that target these systems grow," says Moore.

The following section examines how attacks on these systems impact operations.

Figure 2.

Attack Vectors on OT/ICS

Please rank the following vectors of attack on OT/ICS in the order your organization is most concerned from highest to lowest..

	OVERALL RANK
Software/system vulnerability	1
Financially motivated cybercriminals	2
Insider threat	3
Consultants/contractors	4
Nation state attackers	5
Attack from third-party	6
Terrorism	7

Note: Rank is based on a weighted score. Answers are weighted, and scores are a sum of all weighted counts.
Data: Dark Reading survey of 75 IT and cybersecurity professionals, July 2022

How Attacks on OT/ICS Systems Impact Operations

Cybersecurity attacks, once squarely in the domain of the digital world, are increasingly reaching the physical domain, primarily through OT/ICS systems. While the vast majority of respondents didn't endure a significant breach in the past year, a startling one-in-five respondents reported suffering a significant security incident during that time frame — and these attacks are impacting real-world operations. Affected assets include business systems and operational technologies.

Of the one-fifth of respondents who suffered a breach on their OT/ICS assets, 64% say office/business PCs were affected. The remaining identified impacts included their Windows servers (50%), operator devices (29%), Linux/Unix servers (29%), OT/ICS systems (29%), mobile devices (21%), and security technology (21%) such as their firewall or VPN.

Organizations with operational technology can expect more disruption. An analysis published in The Washington Post recently highlighted how with the digital conflict between Israel and Iran heating up, attackers targeted three Iranian steel plants, with production allegedly even being halted. "In late June, Iran's state-owned Khuzestan Steel Co. and two other steel companies were forced to halt production after suffering a cyberattack. A hacking group claimed responsibility on social media, saying it targeted Iran's three biggest steel companies in response to the "aggression of the Islamic Republic."

A few years prior, attackers tried to compromise the ICS command and control that managed Israel's water pumping and sewer systems. Those attacks ultimately failed.

Consider IBM's recent Cost of a Data Breach Report 2022. This report found that ransomware and destructive attacks were responsible for 28% of breaches, with ransomware attacks accounting for 12% of critical infrastructure breaches and destructive attacks accounting for 16% of critical infrastructure breaches. According to the report, another 17% of breaches in these industries were supply chain attacks where a third-party business partner was the attack vector.

APT and nation-state attacks on OT/ICS systems aren't going to let up any time soon; in fact, attacks against operational technologies within manufacturing, energy, industrial, and health care organizations are only going to increase, and so will the strain on OT/ICS systems.

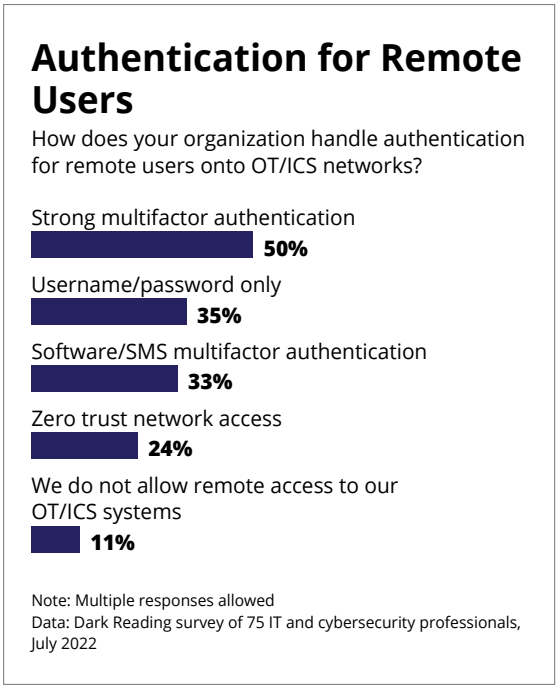
Regarding securing and managing operational technology, the ability to remotely access these systems is growing more critical. In the next section, we detail why organizations facing this requirement see it as one of the most difficult challenges.

Top Operational Technology Secure Remote Access Challenges

The survey found that many organizations are turning to stronger authentication and a zero-trust approach to enable remote access, while many others remain reliant on more precarious mechanisms such as VPNs, usernames/passwords, and air gaps.

Regarding zero-trust architectures, which have garnered a lot of attention within the market, zero trust is only listed as in use by about a quarter of respondents **(Figure 3)**. That figure closely mirrors IBM's Cost of a Data Breach survey, which found that 79% of its respondents haven't adopted a zero-trust architecture. Slow adoption likely stems from the reality that most organizations still struggle deploying security basics, with most finding it moderately to significantly challenging to secure their OT/ICS systems. Most respondents plan on increasing their budget in the year ahead.

Figure 3.



Consider that 77% of respondents describe the maintenance of system security as either moderately or significantly challenging, while 67% say the challenge is in keeping remote access traffic secure. Additionally, respondents found nearly every aspect of securing remote access at least moderately challenging, including maintaining availability, monitoring remote access, segmenting open ports and protocols from trusted networks, identity and access management, and password management.

Identity and access management also remain a significant hurdle. Regarding remote access to OT/ICS systems, the vast

majority of respondents (57%) say they manage remote users' access permissions as part of their standing IT identity and access management program. Only 36% have a dedicated OT/ICS identity governance program, and either the device/system owner (26%) or business unit owner (19%) manages access directly.

The same is true for authentication, with 50% using strong authentication such as hardware tokens or biometrics to authenticate to OT/ICS. While 35% of organizations are still using usernames/passwords to authenticate, 33% are using software-based authenticators or SMS authentication, and 24% are using zero trust.

Surprisingly, 13% of respondents don't allow remote access.

The way enterprises protect their OT/ICS systems looks like how they protect their traditional business-technology systems. The only technology that most — three out of five — respondents have in use are firewalls **(Figure 4)**. Every other security control listed, from access control through vulnerability management to anti-malware, is in use at less than half of organizations. The three most common methods for remote access management and security are firewalls (54%), VPNs (45%), and secure shell (34%) **(Figure 5)**. The other options are far less common, such as JumpServers, leased lines, and satellite links. This creates an unacceptably high level of risk as OT/ICS assets, and the systems that manage them, increasingly look like traditional computing devices. Simply bolting on legacy security technologies won't protect these mission-critical systems to the level necessary.

If organizations are segmenting their operational technology network traffic, they are doing so primarily with virtual LANs and network firewalls. And with one-fifth experiencing attacks and attacks on OT/ICS, the ability to detect attacks on these networks remains crucial. Respondents say the most common technology used to track security-related events on OT/ICS systems are security information and event management systems, intrusion detection/prevention systems, log analysis tools, and open source/custom monitoring tools **(Figure 6)**. Only 19% of respondents have integrated operational technology data into their IT security operations.

Figure 4.

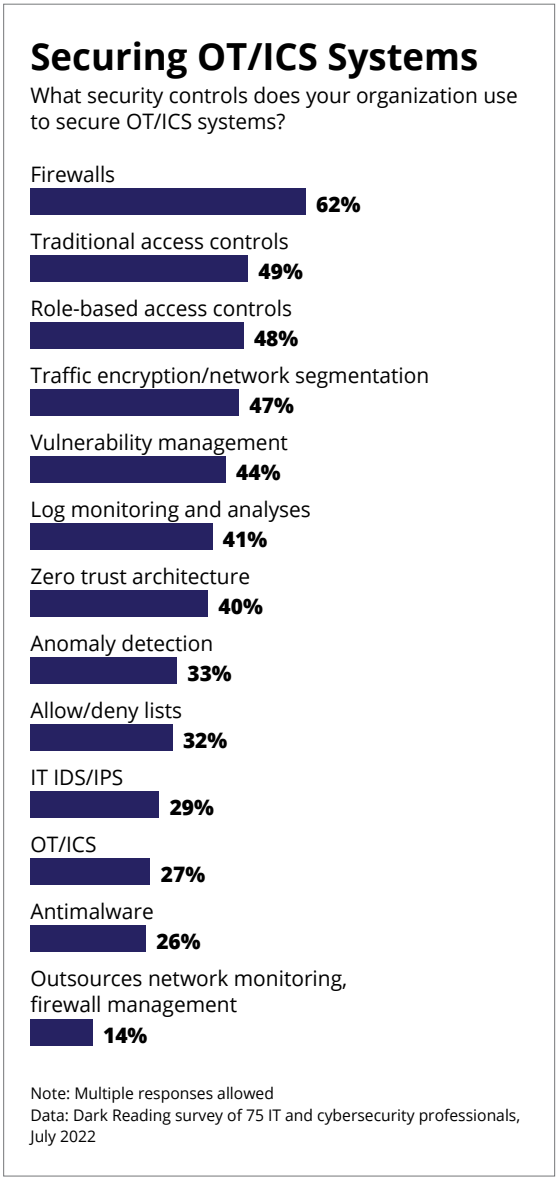


Figure 5.

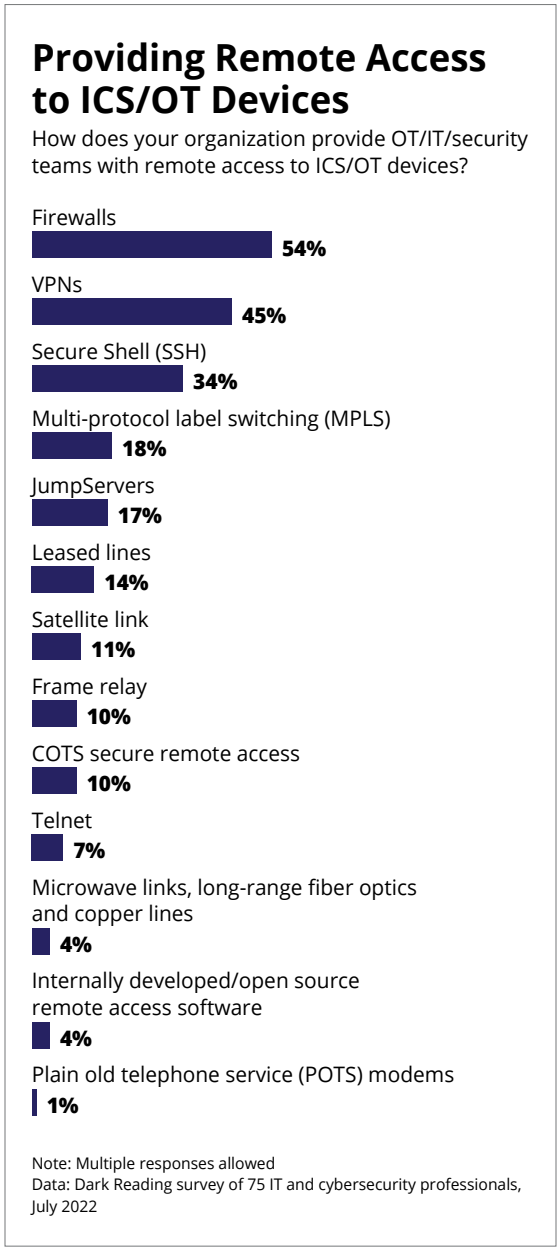
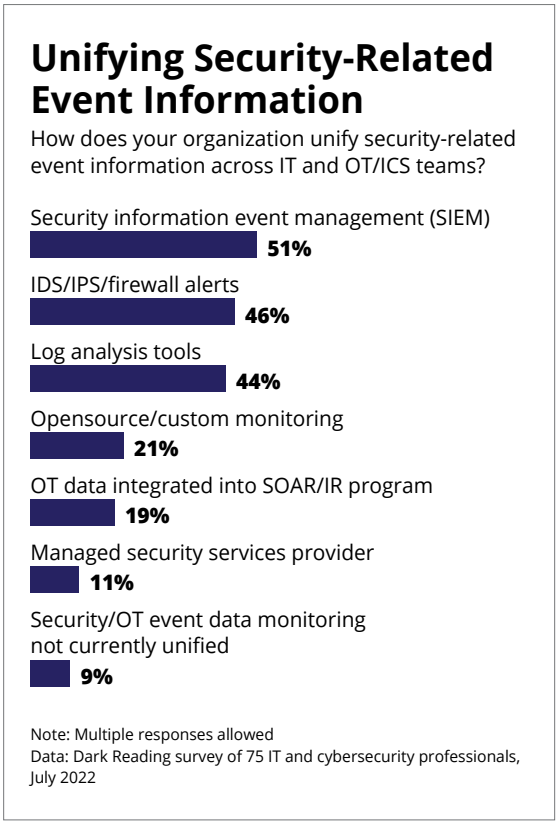


Figure 6.

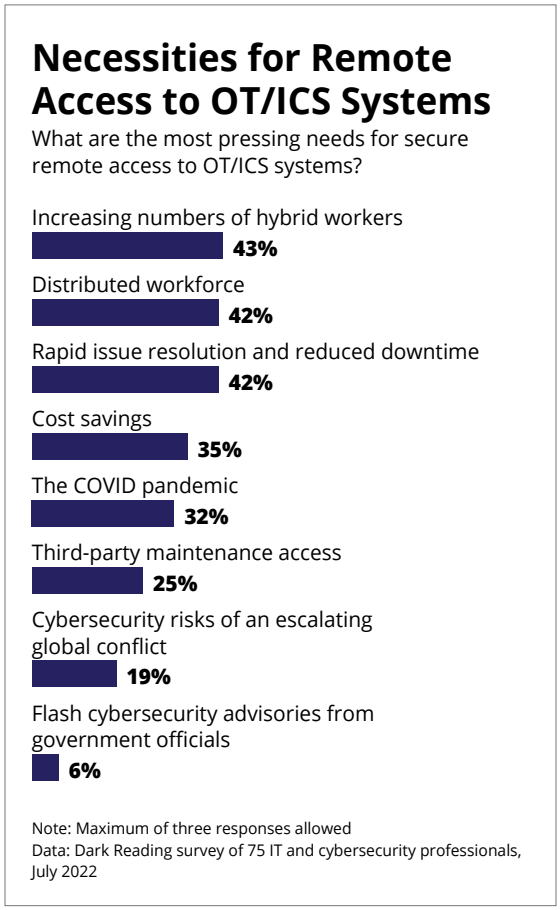


The megatrends causing stress to traditional IT security teams are also stressing OT/ICS teams out. When asked to name the three most pressing needs for secure remote access to their OT systems and ICS, respondents listed providing secure access to their increasing hybrid workers (43%), supporting a distributed workforce (42%), and the ability to resolve cyberattacks and reduce downtime quickly (42%) **(Figure 7)**.

Other needs included trying to reduce costs (35%) and giving access for third-party maintenance (25%).

The survey shows most respondents underestimate the risk of nation-state-backed APTs and third-party risks. Breaches on third parties have been increasing in recent years. Despite most attacks generally originating from third parties, survey respondents vary in how they vet their third-party vendor security. Forty-nine percent of respondents say that they issue a third-party security questionnaire based on established standards, such as from NIST or ISO27001, conduct independent application security assessments (48%), third-party reviews or certifications (43%), customized security questionnaires (37%). Surprisingly, 16% of respondents have yet to start a third-party cybersecurity review.

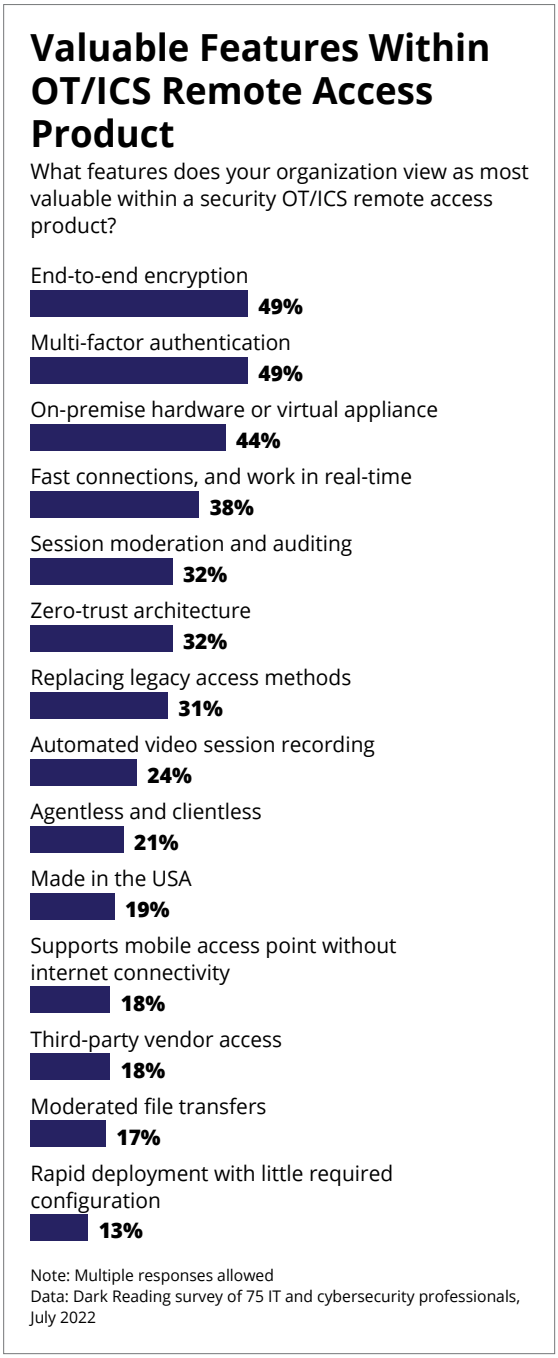
Figure 7.



One of the most promising ways to improve remote access and the general security of OT/ICS environments is zero-trust access control. With a zero-trust approach, authentication and authorization are unequivocally and regularly verified, with users and devices being granted only the least privileges necessary to perform whatever roles they need. This way, zero trust makes it more difficult for attackers to breach an organization successfully. If they find a foothold in an environment, they find it extremely difficult to move laterally and cause damage or steal more data.

The survey asked which feature was the most valuable within a security OT/ICS remote access product. End-to-end encryption tied with multifactor authentication as the most valuable, with 49% of respondents **(Figure 8)**. Zero-trust architecture was not too far behind, with 32% of respondents saying it was the most valuable. The focus on both multifactor authentication and zero-trust architecture shows respondents are beginning to recognize the role of zero trust in OT and ICS environments.

Figure 8.



However, while zero trust is difficult to implement in traditional business-technology environments, it's especially so in OT/ICS environments because these systems have no room for disruption. If a user or device needs access to a system, the transaction must go through or risk disruption to critical services. This is so whether it's mass transit, manufacturing, or energy. Cybersecurity approaches within operational technology must be not only effective but also be able to meet this level of performance demand.

The following section provides some guiding practices to help organizations do that.

Best Practices for Securing OT Systems Today and in Future

While operational technology may look like traditional security of business-technology systems — understanding assets, identifying and mitigating vulnerabilities, monitoring systems for indications of compromise — operational security is quite different.

The first is that the cyberattack risks involved are much higher as it's not just information confidentiality, integrity, availability, online transactions, and data at risk. That's all serious enough. But when it comes to operational technology, all of that is at risk, in addition to delivering healthcare, electricity, manufacturing lines, and more. Additionally, the protected devices are quite different from traditional computing systems and are much easier to disrupt inadvertently through scans or changes in configurations. Finally, incident response requires specialized skills to conduct response effectively and without disrupting availability.

When it comes to effective operational security, research firm Gartner recommends the following ten operational technology security controls:

- **Define roles and responsibilities.** Establish someone responsible for security within the organization and have them assign roles and duties to anyone who gains access.
- **Security awareness training.** All staff within the organization must be trained to identify and understand security risks and how to respond to security-related incidents.
- **Incident response.** Create an OT-specific incident response program so that the organization is prepared for such incidents, can detect anomalies and attacks, contain and remove the threat, and recover to normal operations.
- **Backup and restore.** Continuously backup systems so that, in the event of a digital attack or physical disruption, systems can be restored back to their functioning state.
- **Manage portable media.** Gartner recommends organizations create a policy that all portable media is scanned for malware before being permitted to connect to any OT systems.
- **Asset inventory.** As part of ongoing operations, the OT security manager should maintain a continuously updated inventory of OT assets.
- **Network segregation.** Operational technology networks must be segregated from both external and internal networks, with all network traffic between the OT network and other networks being thoroughly monitored.

- **Log collection and anomaly detection.** By collecting logs and searching for potential indicators of compromise, organizations can more readily mitigate their risk and damage from attacks.
- **Secure configuration.** Systems could be configured and deployed with secured settings, and continuously monitored for misconfigurations that can creep into systems over time.
- **Formal Patching.** Assets should be scanned and kept up to date.

Moore explained that some organizations remain fearful of allowing any remote connections when it comes to operational security. "They are still reluctant to access these OT systems remotely because they're concerned about the security aspects and the resulting safety issues. But some platforms provide security that can be trusted," he says.

Regarding operational technology, creating security that can be trusted means logically isolating the OT network and requiring appropriate levels of authentication as systems are discretely accessed.

"To get to the level of security needed for today's OT systems, you need to compartmentalize each asset and provide role-based and condition-based access to those assets. You also have site-level controls, such as assigning somebody to be responsible for permitting or denying remote access and who can also monitor what is exactly going on with that access," Moore says. In addition, Moore suggests maintaining a full forensic recording of network traffic. "If there are any cyber incidents, you could go back and play a movie file and see exactly what the user did on that system."

One way to compartmentalize each asset is through Protocol Isolation. Protocol Isolation confines the use of certain protocols (e.g., RDP, SSH, VNC) to a specific network location, and isolates it from the rest of the network. Such locations could be segmented networks, so the control network is separate from the data network; or a virtual machine. This approach makes it very challenging for attackers to move laterally through environments and escalate privileges. It also mitigates the impact of malware.

That's a level of security that would provide organizations the operational availability they demand while providing a level of protection most organizations don't have today.

Conclusion

Organizations with operational technology must do something different to secure these systems adequately. The threats these systems face — from profit-seeking ransomware operators to nation-state-aligned APTs — will only continue to grow. The number of OT/ICS systems becoming networked is rising every year, and they're proving vulnerable. While this survey found organizations are making security investments and plan to increase their security investments, many are investing heavily in bolt-on security technologies, such as legacy VPNs, usernames/passwords, and anti-malware. Modern operational technologies demand more.

Survey Methodology

Dark Reading conducted a survey in July 2022 on behalf of Xona Systems, exploring OT/IT environments and how security teams approach modern access control and remote access for operational technology and industrial networks. The final data set used for this report is made up of 75 cybersecurity, IT, and OT/I&C/control systems professionals. The margin of error for this base (n=75) is +/- 11 percentage points.

Nearly 20% of respondents are IT director level, 12% are CSO/CISOs, and 10% are CIO/CTOs. Other titles include security management, IT management, IT/security staff, OT/I&C/control systems, and OT security architecture. Respondents work at more than 35 industries concentrated mostly in North America, among them water treatment, architecture, engineering, electricity, oil, gas, cable & satellite, electronics, industrial machinery, hospitals, and R&D, to name a few.

Thirty-six percent of respondents work at organizations with 5,000 or more employees, 16% at organizations with 1,000 to 4,999 employees, 26% are companies with 100 to 999 employees, and 22% under 100 employees.

The survey was conducted online. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

About XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

To learn more, please visit xonasystems.com.