REPORT

Cybersecurity in the Oil and Gas Industry: Securing the OT Environment

Executive Summary

In spring 2023, Automation.com collaborated with Fortinet to assess the cybersecurity efforts, priorities, and overall preparedness of companies in the petrochemical industry. Automation and information technology (IT) professionals working for and with upstream, midstream, and downstream oil and gas operations were encouraged to share their views on protecting operational technology (OT) systems and their companies' cybersecurity activities in specific areas.

Surveys were sent to active names on lists from Automation.com, the ISA Chemical and Petroleum Industries Division (ChemPID), and ISA oil and gas regionally focused sections. We received 207 responses and a survey completion rate of 67%. Respondents who were not in the oil and gas industry or did not have knowledge of their company's cybersecurity activities were filtered out, leaving 62 highly qualified respondents.

The results show an industry roughly split. About half of companies are well on their way to what might be called a mature cybersecurity stance. They have completed most of the steps and subtasks associated with protecting their OT environments and have systems in place to monitor progress and continuously make adjustments. The other half of respondents seem to be just getting started, having a range of plans and good intentions but few concrete implementations of protective tools and procedures.

Both groups can benefit from the results of this survey by comparing where they are relative to their peers and seeing what they may need to focus on next.

Relevant Trends: OT Cybersecurity in Today's Oil and Gas Industry

Convergence between industrial OT systems and IT-based technologies and networks offers many potential business benefits. IT/OT network convergence can help reduce space requirements, eliminate physical hardware, shorten deployment times, improve cost savings, boost performance, and reduce siloed IT and OT department resources.[2] But these interconnections also puncture the OT air gap that traditionally kept critical infrastructure safe from many common forms of cyberattacks. As a result, three-fourths of OT-based organizations reported at least one intrusion in the last year; malware (56%) and phishing (49%) were the most common attacks, and nearly one-third of respondents reported being ransomware victims.[3]

As critical national infrastructure, oil and gas companies are key targets for cybercriminals. Cyberattacks on oil and gas companies promise maximum disruption and extortion opportunities.[1]

Oil and gas companies that maintain cybersecurity as a central tenet of their digital strategy stand to gain the most—however, companies failing to sufficiently invest in cybersecurity face financial and reputational harm.[4]

The oil and gas industry, in particular, presents an attractive target for attacks worldwide. In an opportunistic response to the Russian-Ukraine conflict, ransomware gangs have hit major organizations across Europe over the last year, resulting in widespread disruption to energy supplies.[5]

In the United States, the Government Accountability Office found that the Department of the Interior has taken insufficient steps to address cybersecurity risks to over 1,600 offshore facilities, producing a significant portion of U.S. domestic oil and gas.[6] A cyberattack on this infrastructure could cause physical, environmental, and economic harm and broad disruptions to oil and gas supplies and markets.

This survey report drills down into how industry leaders view the current state of OT-based cybersecurity risks and the subsequent preparedness of their organizations to maintain resiliency.

Important Activities for Securing the OT Environment

To begin the survey, we asked respondents to identify the most important activities for securing the OT environment. Ninety-one percent (91%) identified vulnerability assessment (which includes management scanning and early detection of attacks) as the most important, followed closely by incident response planning (90%). Security analysis, monitoring, and assessment tools are also very important (87%). Even the activities ranked as least important—visualization of security events and central management of security policies—were still highly valued by 72% of respondents.

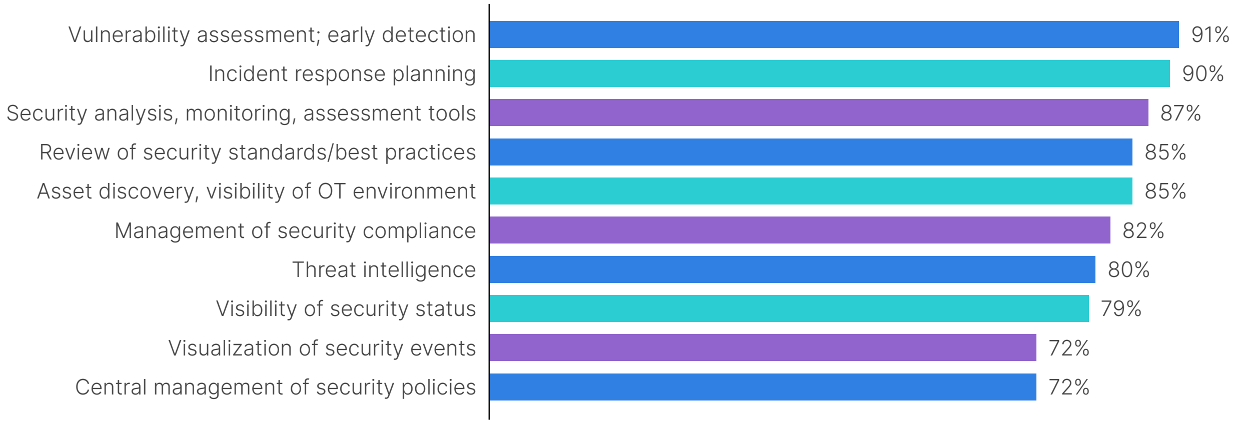

Figure 1: Most important for securing OT environments

Perceived Effectiveness Performing Specific OT Cybersecurity Activities

The survey asked respondents to rate their company's general effectiveness in performing specific activities related to securing the OT environment. More than half of respondents think their company is above average when it comes to knowledge of cybersecurity standards and best practices or performing vulnerability assessments. But self-assessment is often better than reality, so the extent of "above average" responses here is not surprising. When it comes to areas related to cybersecurity governance, however, overconfidence presents a serious risk to the resiliency of systems and business continuity.

What's more interesting is where respondents think their company is performing below average. More than a quarter of respondents (26%) believe their company is below average when it comes to threat intelligence, incidence response planning, or visualization of security events, for example. There is also a governance consideration here.

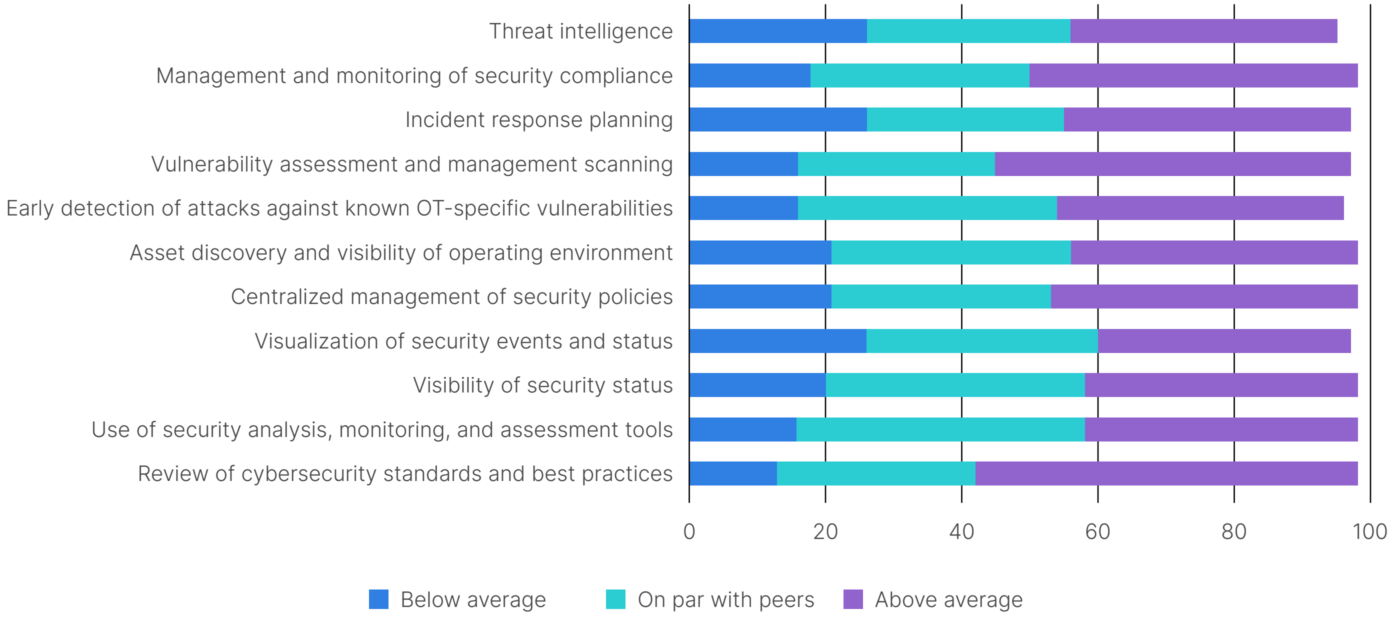

Figure 2: Effectiveness of OT cybersecurity activities

Six Aspects of Cybersecurity Maturity

The Fortinet *2023 State of Operational Technology and Cybersecurity Report* showed that the number of OT security leaders who consider their organization's security posture as "highly mature" fell from 21% to 13% year-over-year.[7] This suggests that there's a growing general awareness among OT professionals and more effective tools for self-assessing cybersecurity capabilities.

Effective OT cybersecurity involves multiple assessment and implementation steps that, when combined, reflect a company's level of cybersecurity maturity. Respondents were asked what their companies had accomplished in six different areas. Broadly speaking, results fell into two main groups—many organizations are well on their way to a mature OT cybersecurity program, while many others are just getting started.

1. Prioritizing assets and risks

With regard to prioritization of assets and risks, 52% of the respondents say that their company has completed more than half of the tasks related to prioritizing assets and assessing risks, such as identifying a cybersecurity strategy or roadmap, performing asset or risk prioritization, and identifying risk appetite and thresholds.

About another half of respondents remain in the early stages. Just 6% say their companies have not begun, and 8% say their companies have plans in place but have not completed any tasks. Only 29% say their company has identified and completed some asset priority and risk assessment tasks. However, as seen in the answers for the other five aspects of OT cybersecurity maturity, just because a company hasn't done assessments doesn't mean it hasn't implemented protections.

2. Enlisting frontline personnel

An important area of OT cybersecurity preparedness involves enlisting frontline personnel. This can include ensuring adequate awareness and training around cybersecurity risks, identifying the organization's risk culture, ensuring adequate awareness and training of contractors and non-OT employees, and recruiting and developing cybersecurity talent. Nearly half (45%) of survey respondents have either not begun this work, only have plans in place, or have only made some progress toward maximizing the protective potential of their current staff resources.

While hiring more skilled OT security experts to compensate is one approach, like every other business sector worldwide, the oil and gas industry faces a persistent global shortage of experienced and knowledgeable security staff.[8] Leaders should focus on identifying those who could benefit the company with access to additional training. Upskilling and reskilling offer an alternate strategy for filling the cyber skills gap and keeping OT environments safe.[9]

3. Integrated operational resilience

Integrating operational resilience is essential to mature OT cybersecurity preparedness. It involves making sure processes are resilient at all levels. This includes risk reporting and metrics, product security, vendor management, and resilience within the organizational structure and security roles. A full 16% of respondents have plans in place, and another 32% have completed some tasks in this area. 48% have completed more than half of the tasks involved.

4. Integrated incident response

Interestingly, 58% of respondents report that their companies have completed the majority of tasks related to integrated incident response. This aspect of OT cybersecurity maturity involves having a security incident response plan, conducting simulations and testing, and having business continuity, disaster recovery, and system resilience plans.

5. Integrated security technology

More than half (58%) of respondents say their companies have integrated security technology into their OT environments. This includes asset management, software patch management, cloud and edge security, secure architecture, endpoint and mobile security, physical security, and secure system development.

6. Active defenses and layers of protection

The part of OT cybersecurity that seems to have gotten through to the majority of companies is the need for active defenses and layers of protection for their most important assets. An impressive 63% of respondents say that most tasks have been completed, while another 23% report some tasks completed. These tasks include implementing cybersecurity policies, standards, and assessments; implementing diagnostic, compliance, and audit procedures; deploying active defenses like cyber intelligence, vulnerability awareness, and asset monitoring; and applying analytics.

OT-Specific Cybersecurity Maturity

Because many of the previous cybersecurity activities may be seen as the responsibility of the IT department, we wanted to ask similar questions about OT-specific systems security.

Industrial control systems (ICS)

Regarding protecting the broader superset of ICS technologies deployed across their organization, about two-thirds (68%) of respondents report that their company had most tasks completed; 18% had some tasks completed, and 10% have plans to protect these systems.

Supervisory control and data acquisition (SCADA)

As for the protection of deployed SCADA systems that monitor and control equipment for improved operating efficiencies, 68% of respondents report that half or more of the necessary tasks have been completed. Another 10% have some tasks completed, and 8% have plans to protect their SCADA systems but have not implemented specific measures.

Distributed control systems (DCS)

DCS technologies help control operations and automate safety processes. Like ICS and SCADA, current DCS cybersecurity is robust among survey respondents; 68% report that half or more of their planned cybersecurity tasks have been completed. Another 17% have some tasks completed, and 8% have plans in place but have not implemented specific measures.

Edge and cloud computing systems

OT environments are increasingly connecting with IT networks for new strategic benefits, such as utilizing cloud-native capabilities and improving frontline decisions using IT and OT systems data.[10] IT environments are commonly used to configure and manage OT devices; they are also where key data must be collected, normalized, processed, and reported on so organizations can effectively manage their OT systems.

As more IT assets migrate to cloud-based environments, OT assets become exposed to cybersecurity challenges that previously did not exist.[11] While edge and cloud computing devices are often considered the responsibility of IT, their increasing application to OT systems means that certain associated cybersecurity responsibilities may fall within the OT realm. Perhaps not surprisingly, 14% of respondents are unsure if these systems are protected. Another 14% say their company has not addressed cybersecurity for these systems.

Remote workers and mobile devices

Oil and gas companies increasingly use remote workers and wireless mobile devices. While these practices can bring greater efficiency to organizations, they can sharply elevate cyber risks at the same time. Sixty-six percent (66%) of respondents say their company has completed most of the necessary tasks to protect these devices and the systems they are connected to. Eleven percent (11%) have completed some protective tasks, and 10% have plans in place. Eight percent (8%) are unsure of the status, while 5% say protective steps have not been implemented.

Software change control and patch management

Awareness is growing around the importance of software change control and patch management as another layer of protection against cyber threats. Sixty-one percent (61%) of respondents report that these protective measures are being implemented for OT system software most of the time, and another 15% say they're being applied some of the time. Sixteen percent (16%) have plans in place to implement software change control and patch management.

Top Drivers for Pursuing OT Cybersecurity Now

We wanted to know what motivates automation professionals in oil and gas companies to pursue improved cybersecurity for their OT systems now. Perhaps not surprisingly, cyberattacks in the news topped the list. One respondent said, "The new fast-growing threats to the OT industry" were an important driving factor.

In July 2023 alone, newspapers reported that the Norwegian recycling and mining corporation TOMRA suffered an "extensive cyberattack,"[12] Japan's Port of Nagoya resumed operations two days after a ransomware attack,[13] and a contractor who worked at the water treatment facility in the Town of Discovery Bay, California, faced charges for a January attack that intentionally uninstalled the main operational and monitoring system and then shut down the servers running those systems.[14]

In addition, Israel's largest oil refinery, BAZAN Group, was attacked by hacktivists in July, taking its website offline and releasing screenshots of their SCADA systems as well as diagrams of various systems and code for the refinery's programmable logic controllers.[15]

The second most cited reason for pursuing OT cybersecurity is increased regulatory pressure. This speaks to the general awareness of cybersecurity as a business enabler and the importance of cybersecurity governance ensuring uninterrupted critical infrastructure operations. One respondent said, "We started when TSA issued the security directive post-Colonial Pipeline incident." The U.S. Transportation Security Administration (TSA) recently updated its security directive to reinforce cybersecurity preparedness and resilience for the nation's critical pipelines following the initial directive announced in July 2021 and renewed in July 2022.[16]

President Biden's National Cybersecurity Strategy Implementation Plan was also recently released, setting up the potential for more regulation.[17] The strategy calls for two fundamental shifts in how the U.S. allocates roles, responsibilities, and resources in cyberspace and details 69 high-impact federal initiatives, each assigned to a responsible agency and given a timeline for completion. Eighteen agencies are leading initiatives.

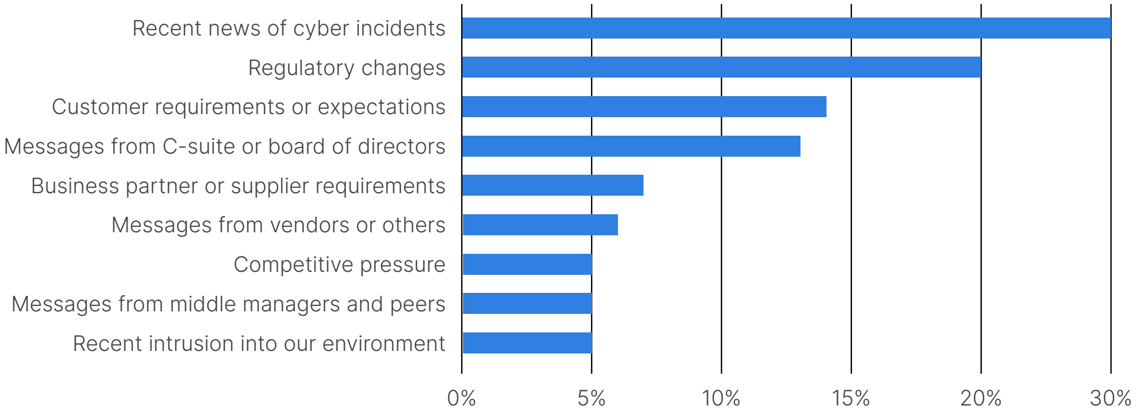

Figure 3: Top drivers for pursuing OT cybersecurity

How OT Cybersecurity Will Change in the Next 12 to 24 Months

We asked respondents whether they agreed with a series of statements describing how OT might change over the next 12 to 24 months.

The vast majority (86%) believe that cyberattacks targeting their company's OT environment will increase in sophistication over the next one to two years. Similarly, 86% of respondents said their organization will implement new solutions to address cyber risks to OT. And 84% of those surveyed agree that organizations will increase their effectiveness at mitigating OT security risks over time (with 47% strongly agreeing).

Their confidence in the future showed less enthusiasm regarding cybersecurity talent. While a majority agreed that their company will have the right talent in place to address OT cyber risks, only 27% strongly agreed, and a significant 13% disagreed (either strongly or somewhat).

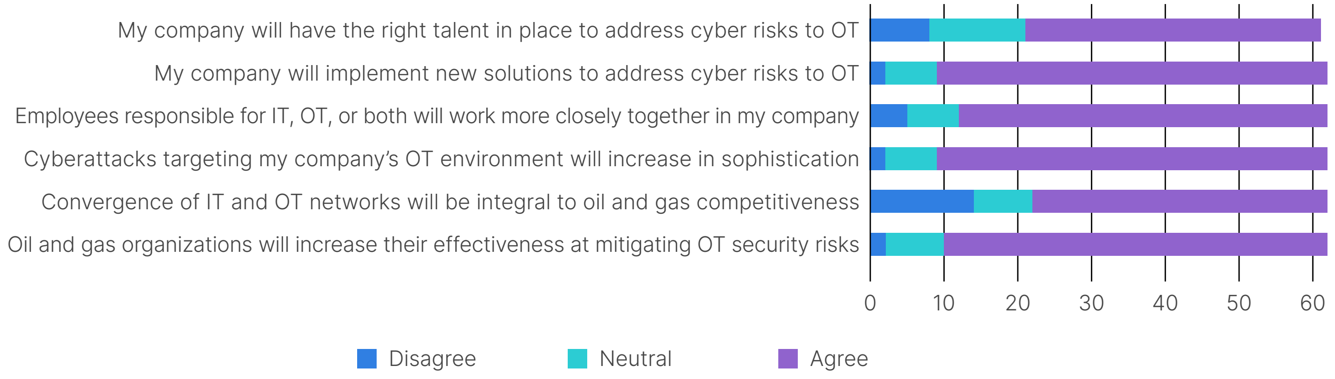

Figure 4: How will OT security change in 12 to 24 months?

OT Cybersecurity Risks Compared to Other Business Risks

Compared to other business risks for oil and gas companies, OT cybersecurity is by no means perceived as the main risk, but it is in the top five for more than half (61%) of respondents.

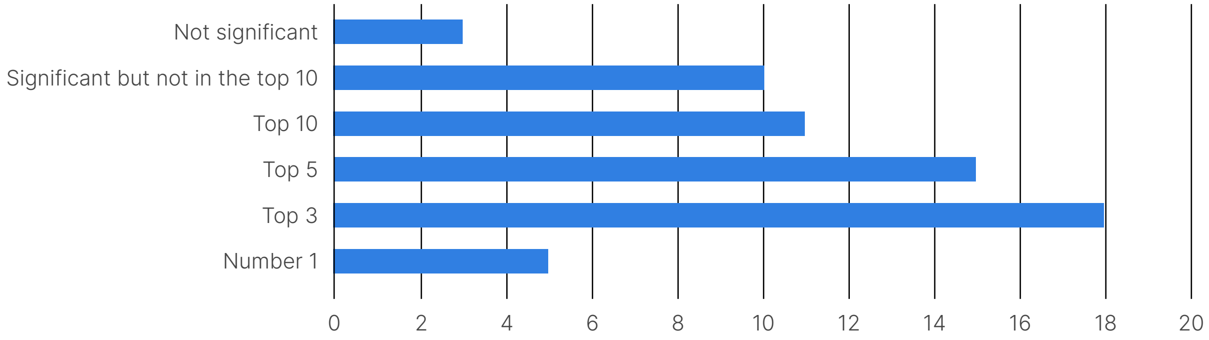

Figure 5: OT cybersecurity risks compared to other business risks

OT Cybersecurity Risk Reduction

We asked to what extent respondents thought their companies were taking proactive steps to reduce risks to their OT environment across various threat and vulnerability vectors. The highest majority agreed that focused attention was being placed on the areas of unauthorized access (89%), operational disruption (79%), and insider threats (78%).

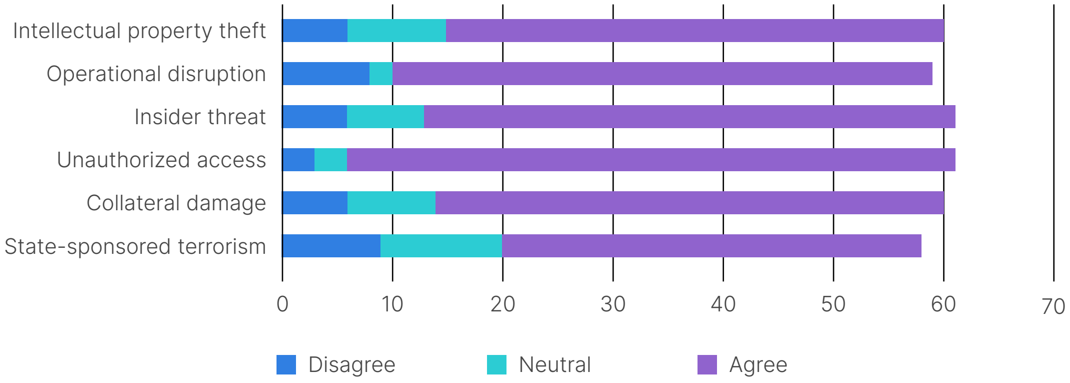

Figure 6: Proactive OT cybersecurity risk reduction

OT Cybersecurity Incident Detection

Most respondents said their companies could accurately detect when a cybersecurity incident occurs in their OT environment. The majority use either internal resources (32%) or a mix of internal and external (contracted) resources (38%). Only 14% could not detect these incidents or did not know if they were prepared to do so (11%).

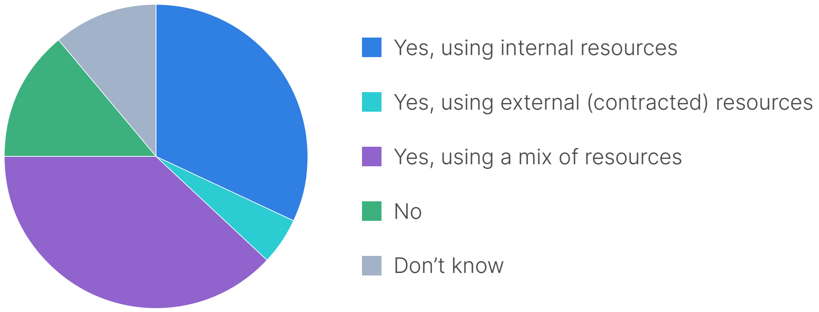

Figure 7: Detecting OT cybersecurity incidents

Most Common Cybersecurity Capabilities or Controls

The top five most common OT cybersecurity capabilities or controls applied by the oil and gas industry professionals who took our survey are internal network segmentation, internal security training and education, a hardened network (which means disabling or removing unnecessary services), role-based access control, and a dedicated SCADA/ICS security team. Additional security controls, in descending order of frequency, include multi-factor authentication, remote management of physical security, scheduled security compliance reviews, physical audits of SCADA/ICS, third-party security products, outsourced security consultants, encrypted SSH/TLS, cloud computing protection, “walling off” of machine data processes, zero-day protection, removal of proprietary network protocols and deception technology.

Most Common Security Capabilities or Controls

1. Internal network segmentation (76%)
2. Internal security training and education (73%)
3. Hardened network (71%)
4. Role-based access control (68%)
5. SCADA/ICS security team (65%)

Well-Done OT Cybersecurity Protection Activities

We asked the survey respondents to brag about their companies, especially regarding what they had done particularly well or approaches that had been most successful in protecting OT systems. The most common response was network segmentation. Others referenced adopting relevant industry standards or programs to improve security governance and awareness. Deployment of network access controls and earning buy-in from the various teams in support of security objectives were also recorded responses.

What Has Your Company Done Particularly Well?

1. Network segmentation
2. The adoption of the Purdue reference model and ISA/IEC 62443 ZCRs
3. Governance, monitoring, and awareness
4. Controlled access to OT areas using network media access controls
5. Engagement of security, IT, and OT operations teams to architect and deploy the most secure network and systems

Not-So-Well-Done OT Cybersecurity Protection Activities

Network segmentation comes up again in a final question about lessons learned. We asked respondents what important OT cybersecurity task(s) their company had ignored, not done well, or had not gotten to fast enough. These six items are things to remember when tackling future OT cybersecurity plans and implementations.

What Has Your Company Not Done Well?

1. Segmentation of the OT environment and not allowing access from corporate
2. Removing obsolescence from the OT environment
3. Moving process data users to a DMZ and away from the process control network
4. Asset inventory, life-cycle management, and visibility into OT networks
5. Asset management and event logging
6. Earning buy-in from the shop floor

From Maintaining to Maturing Your OT Cybersecurity Program

The oil and gas industry faces escalating cyber risks and expanding legal requirements, such as new incident reporting obligations and required vulnerability assessments. As targeted attacks against OT systems in critical infrastructure continue to rise, security leaders in the industry need to continue their efforts to develop a mature and resilient program for OT cybersecurity.

The results of this survey should help organizations compare their current program's status with industry peers and guide them toward critical areas for improving the protection of their OT infrastructure going forward.

[1] "Leading oil and gas companies in the cybersecurity theme," Offshore Technology, May 22, 2023.

[2] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 2023.

[3] Ibid.

[4] "Leading oil and gas companies in the cybersecurity theme," Offshore Technology, May 22, 2023.

[5] "2022 Oil and Gas Sectors Threat Landscape," Deloitte, October 13, 2022.

[6] "Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure," U.S. Government Accountability Office, November 17, 2022.

[7] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 2023.

[8] "Distribution of companies experiencing a shortfall of skilled IT security personnel worldwide from 2018 to 2023," Statista, May 11, 2023.

[9] "Effectively upskilling cybersecurity professionals to help close the skills gap," CSO, August 14, 2023.

[10] "Converge IT and OT to turbocharge business operations' scaling power," McKinsey & Company, June 28, 2022.

[11] "IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems," Carnegie Mellon University, July 18, 2022.

[12] "Norwegian Giant Tomra Suffers "Extensive" Attack," Infosecurity Magazine, July 19, 2023.

[13] "Japan's Nagoya port resumes operations after ransomware attack," CSO, July 6, 2023.

[14] "Former water contractor employee tampers with water treatment systems, posing public health and safety threat," Industrial Cyber, July 10, 2023.

[15] "Website of Israeli Oil Refinery Taken Offline by Pro-Iranian Attackers," Dark Reading, July 31, 2023.

[16] "TSA updates, renews cybersecurity requirements for pipeline owners, operators," U.S. Transportation Security Administration, July 26, 2023.

[17] "National Cybersecurity Strategy Implementation Plan, U.S. White House, July 2023.

FORTINET

www.fortinet.com

October 10, 2023 1:44 PM

2310526-0-0-EN