

OT Cybersecurity Technology Report 2024

(CS)²AI™

Radiflow



* Introduction

- 2 ◆ Chairman's Foreword
- 3 ◆ Editor's Foreword
- 4 ◆ Executive Summary & Recommendations
- 6 ◆ Sponsor Acknowledgments
- 8 ◆ About the Survey

9 Utilization

- 10 ◆ About the Report
- 11 ◆ Asset Management: Inventory & Platform
- 12 ◆ Operating Systems: Legacy & Updated
- 14 ◆ Wireless Functions in ICS/OT Environments
- 16 ◆ Remote Monitoring & Control
- 18 ◆ Authentication Methods
- 19 ◆ Technology Use
- 20 ◆ Procedure Use
- 21 ◆ Network Segmentation
- 22 ◆ Standards & Regulations
- 24 ◆ Security Assessments
- 25 ◆ Visibility & Legacy Systems
- 26 ◆ Network Blind Spots

27 Implementation

- 28 ◆ Level of Effort
- 29 ◆ Implementation Costs

31 Direct Feedback

- 32 ◆ What End Users Wish Cybersecurity Technology Providers Knew
- 34 ◆ Cybersecurity Technology Providers Should Stop Doing
- 36 ◆ What Cybersecurity Technology Providers Do Well

37 Demographics

- 38 ◆ Gender, Age, Education Level
- 40 ◆ Industry & Sector
- 42 ◆ Domain Authority
- 43 ◆ Geographic



Derek R. Harp

**Founder & Chairman
Control System Cyber Security
Association, International**



A Welcome from Our Chairman & Founder

Dear Industry Colleagues,

As our organization continues to steadily grow in membership and activity we continue to expand our projects. While most know us for our ongoing series of educational seminars and symposiums, our research is very near and dear to our hearts (and core mission). So I am both proud and pleased to bring this newest report to you.

The report findings come from a survey we designed hand-in-hand with our sponsors to answer key questions regarding the technologies available to and in use by ICS/OT cybersecurity professionals around the world, whether new or legacy. Each of us knows what we see and experience in this field, but it is only through these research projects that we can get the larger picture and find the commonalities and trends.

Our analysts found a number of concerning patterns in the responses from our participants. The prevalence of legacy devices, often unsupported and even un-supportable, some still in use since acquired before ICS/OT cybersecurity was a vendor design concern, ...

Similarly, the very significant percentage of invisible ICS/OT devices (i.e.. without telemetry from host or network tools) connected to networks our respondents support drew our attention.

The variety of technologies in use by our respondents illustrates the complexity of working in our field, with unique environments and configurations in every site. One leading SME told me recently that this is why he decided to work in control system cybersecurity because it required constant learning to keep up with the array of devices, equipment, software, and practices in use and their continual evolution.

It is the shared goal of both (CS)²AI and our project sponsors that readers of this report find information directly useable in their own work, that our data and analysis enable all of us to better understand and address the challenges we face every day in this field, to inform their decisions and clarify their priorities. Our team remains committed to advancing, strengthening and growing this community which serves to keep the lights on, the water flowing, and the planes in the air.

Editor's Foreword

Operational technology environments, once isolated and insulated from traditional IT threats, now face unprecedented challenges as they become increasingly connected and integrated into broader digital ecosystems. I have witnessed firsthand the accelerating pace of change in our industry. The complexities of securing these environments demand not only advanced technological solutions but also a deep understanding of the unique risks and constraints inherent to industrial systems.

This report, which I am proud to have sponsored and contributed to, represents a critical examination of the current state of cybersecurity within OT environments. It delves into the strategies, tools, and practices that organizations across various sectors are employing to protect their most vital assets. Our findings highlight both the progress we have made and the significant challenges that remain, particularly in areas like legacy system security, network visibility, and the integration of modern cybersecurity technologies.

It is my hope that this report serves as a valuable resource for industry professionals, providing actionable insights that can be directly applied to enhance the security posture of their organizations. The data and analysis contained herein reflect the collective experiences and expertise of a diverse group of OT cybersecurity professionals. As we continue to navigate this complex and evolving landscape, collaboration and knowledge-sharing will be key to our success.

I extend my deepest gratitude to all those who contributed to this report, as well as to the sponsors who made it possible. Together, we are working towards a safer, more secure future for the critical infrastructure that underpins our modern world.

Patrick C. Miller
President & CEO
Ampyx Cyber



Strategic Recommendations

1. Enhance Legacy System Security

Develop strategies and technologies that can integrate with and secure legacy OT systems.

2. Improve Network Visibility

Implement a comprehensive detection in depth strategy: Deploy sensors in depth to improve network visibility, create detection and response frameworks for both IT and OT, and align your SOC strategy.

3. Foster Provider-Client Partnerships

Encourage cybersecurity providers to engage more deeply with clients, focusing on education, adaptability, and collaborative problem-solving.

4. Comply with Regulations

Continue to prioritize and improve compliance with relevant industry standards and regulations to strengthen cybersecurity postures.

5. Enhance the Digital Work Force

Conduct tabletops and training to identify skill and labor gaps against your protection strategy, enhance skills through modern digital training and cyber ranges, leverage a broader and more diverse talent pool for new hires - enriching the talent and perspectives. Implement initiatives aimed at increasing diversity within the cybersecurity field, enriching the pool of talent and perspectives available to tackle security challenges.

Executive Summary

Professionals in the field navigate a complex landscape marked by various technological challenges and trends. The following executive summary focuses on these elements, providing insights into how organizations are adapting to and implementing cybersecurity technologies within operational technology (OT) environments.

Technological Adoption and Implementation: The survey data indicates a robust adoption of foundational cybersecurity technologies such as firewalls, antivirus solutions, and secure remote access across various sectors. More advanced technologies, including SIEM systems and passive network anomaly detection, are also gaining traction, though they present higher complexity and integration challenges. The broad implementation of these technologies underscores the critical need for effective cybersecurity solutions to protect OT environments from evolving threats.

Challenges in Legacy Systems and Integration: A significant portion of OT environments comprises legacy systems, which respondents noted as outdated or end-of-life. These systems pose substantial security risks due to extreme vulnerability and compatibility issues with modern cybersecurity solutions. The findings highlight the necessity for cybersecurity strategies that can handle tomorrow's threats to the latest technology while effectively integrating with and securing these older systems without compromising operational functionality.

Network Visibility and Monitoring: Visibility within OT networks remains a considerable challenge, with an average of nearly 39% of network components reported as not visible through existing monitoring tools. This lack of visibility can hinder effective threat detection and response, emphasizing the need for improved monitoring solutions that can provide comprehensive insights into all network activities.

Cybersecurity Practices and Provider Relationships: Respondents value cybersecurity providers that demonstrate a deep understanding of OT-specific requirements. Effective providers are those who engage in active listening, offer simplified and adaptable solutions, and foster strategic partnerships with their clients. There is a strong call for providers to move away from fear-based marketing and towards more supportive, educative, and collaborative engagements.

Regulatory Compliance and Industry Standards: Compliance with industry-specific regulations and standards is a high priority for OT cybersecurity professionals. Most organizations target compliance with frameworks such as NIST and IEC 62443, reflecting their relevance in enhancing cybersecurity measures and practices within OT environments.

Professional Demographics and Workforce Dynamics: The survey reflects a highly educated and predominantly male demographic, with a significant representation from senior and specialized roles in cybersecurity. This demographic profile highlights the need for ongoing efforts to understand labor and skill gaps while being much more open-minded in identifying and recruiting candidates with fresh perspectives.

This report underscores the intricate interplay between technological adoption, integration challenges, and strategic practices in enhancing OT cybersecurity. As technology evolves and threats become more sophisticated, the insights derived from this report will be critical in guiding future strategies and implementations in the field of OT cybersecurity.



Patrick C. Miller
Editor in Chief
President & CEO
Ampyx Cyber

Contributing Analysts



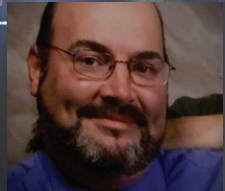
Andrew Ginter
Contributor
VP Industrial Security
Waterfall Security Solutions



Brent Huston
Contributor
Security Evangelist & CEO
MicroSolved, Inc.



Bryan Singer
Contributor
Principal Director, Global OT
Incident Response Lead
Accenture



Bengt Gregory-Brown
Contributor
President & Co-Founder
(CS)² AI

Thanks to Our Sponsors

We are proud to bring together a cohort of industry leading contributors for this inaugural OT Cybersecurity Technology Report. It is a significant undertaking to design and deliver such a technical and sensitive survey to a global audience of OT security professionals. We're proud to have the support of these sponsors, without whom this report would not be possible.

Title Sponsor

Radiflow

Manager Sponsor



Advocate Sponsor



Supporting Sponsors



About The Title Sponsor

Radiflow

Radiflow is a leading, global provider of OT Security and Risk Management solutions and services for critical infrastructure and industrial automation organizations. The company enables operators to continuously safeguard their operations while they manage risk, optimize their security budget, and comply with standards, regulations, and industry best practices.

Scalable and flexible, Radiflow solutions can be deployed in a wide variety of configurations and industrial conditions to perfectly match customer requirements and configurations. Locally or centrally deployed, Radiflow solutions integrate with leading technology and partner platforms as well as other enterprise systems and applications.

The Radiflow threat-detection solution, iSID, provides visibility of devices, protocols, and sessions, asset inventory management, detection of threats and attacks, policy monitoring and validation of operational parameters, and networked device management. Upon initial deployment, iSID automatically learns the network, devices, and communications, and establishes a baseline of normal behavior. Continuously monitoring network traffic, iSID determines deviations from proper behavior, detecting anomalies which may be indicators of compromise. It handles known threats to the network, including changes to PLCs, RTUs, and industrial protocols, based on up-to-date threat intelligence gathered from across the cybersecurity research community. iSID classifies assets in the operational environment, eliminating alert noise, and helping security practitioners respond effectively and efficiently. It smoothly integrates with a wide range of SIEM, Firewalls and Secure Remote Access gateways and other solutions.

The Radiflow iCEN solution simplifies management of real-time cybersecurity. Multi-site industrial operators and Managed Security Service Providers (MSSPs) require centralized monitoring and management of security posture at the enterprise level and at each region and site. From a single pane of glass, iCEN streamlines management of the activities of multiple instances of iSID installed at remote sites.

To manage today's cyber risk, a proactive, continuous, automated, and data-driven risk management approach is essential. Radiflow's risk management solution, CIARA, automatically discovers and learns key risk indicators, and accurately evaluates per-site and overall security posture and risk. It determines how best to direct the OT security budget to maximize the effectiveness of threat-mitigation controls based on cybersecurity regulations, standards, and frameworks like NIS2, IEC 62443, and NIST CSF. CIARA risk assessments are highly accurate and may be run as frequently as desired.

From vast experience, Radiflow recognizes that OT organizations might not want to take on all the responsibilities of cybersecurity and risk management in-house. For these customers, Radiflow via its service partners can provide all the necessary security functions from occasional security reporting to 24/7 security monitoring and response, from periodic risk assessments and reporting to a full, ongoing risk management and compliance program.

With the strong backing of Sabanci Holding and ST Engineering, Radiflow protects over 8,000 sites worldwide and continues to enhance its portfolio to meet the evolving security needs.



Ilan Barda
CEO, Radiflow



Michael Langer
Chief Products Officer, Radiflow



Efrat Schneider-Genzer
VP of Marketing, Radiflow

About the Survey

The OT Cyber Security Technology Survey provides a comprehensive analysis of current trends, challenges, and practices in the field of operational technology (OT) cybersecurity. By gathering insights from a diverse group of professionals across various sectors, this survey offers a unique vantage point into the technological landscape that underpins critical infrastructure security.

The analysis of the survey data reveals both the breadth of cybersecurity technologies employed and the depth of the integration challenges faced by those at the forefront of safeguarding OT environments. As we delve into the results, we aim to uncover not only the prevalent strategies and tools in use but also the industry's collective response to evolving threats, technological needs, and the critical interplay between legacy systems and cutting-edge security measures. The survey was intended to explore how OT professionals navigate the complex cybersecurity technology terrain, highlighting their preferences, approaches, and trends.

The survey was distributed globally to asset owners, ICS and OT practitioners, and cybersecurity technology solution providers. More than 400 people participated from late 2023 to early 2024. These participants were identified by specific segments (detailed on page 42 of this report), and shown portions of the survey, or the complete survey, depending on their category.





Utilization

About the Report

This report compiles data from the OT Cyber Security Technology Survey, implemented in late 2023/early 2024 by Control System Cyber Security Association, International. With expert analysis from OT cyber professionals, the commentary illustrates trends that are relevant in the selection, implementation, maintenance, and sunseting of various technological solutions. It also provides a benchmark to measure trends in the prioritization and utilization of various standards, practices, and technological solutions.

We intend this report to serve as a decision-support tool for administrators and cyber decision makers faced with increasing choices in a growing market of solutions. As you review this data, reflect on how and whether your organization mirrors the outliers, or finds itself more in the middle of the pack of respondents. What are the regional and global standards that you may be able to leap ahead in?

With data compiled in nearly equal measure from asset owners and security technology vendors, the aggregate data strikes a holistic balance from both perspectives. With support from our sponsors, we aim to continue to build on this data to measure trends and shifts, whether regional, or across entire sectors and industries, as they emerge.

Engineering-Out Cyber Threats

There is something new in the world. While this report looks at cybersecurity technology, adoption and implementation, Cyber-Informed Engineering (CIE) looks at all ways to address cyber threats to industrial systems, including cybersecurity. Yes, cybersecurity is part of CIE, but there is more.

For example – mechanical overpressure-relief valves prevent boilers from exploding, both when earthquakes block steam piping and when cyber attacks overheat boiler furnaces. The valves take boiler explosions away as possible consequences of both physical and cyber threats. But – where in ISO 27001, or the NIST CSF, or the IEC 62443 standard, are the overpressure valves? Where in these standards are manual operations as a fall-back, or network engineering at consequence boundaries? The valves are not cybersecurity. The valves are examples of engineering approaches that can subtly change the design of our physical and manual processes, our automation and systems even our cybersecurity systems like remote access. These

engineering design changes outright eliminate important consequences and attack vectors.

For two decades we have looked to cybersecurity “people, processes and technologies” to address cyber threats. With CIE we finally recognize that, yes we need cybersecurity, but we have more tools available than cybersecurity alone. As we go through this (important) report looking at the effectiveness of our cybersecurity postures, technologies and decisions, please consider the engineering tools and approaches that CIE highlights as well. While many of these tools have addressed physical threats for a long time, they have not been used widely to address cyber threats, and thus represent a new kind of opportunity to help address the most difficult of our cyber problems.

Andrew Ginter

VP Industrial Security
Waterfall Security Solutions
... and CIE awareness champion



Asset Management: Inventory & Platform

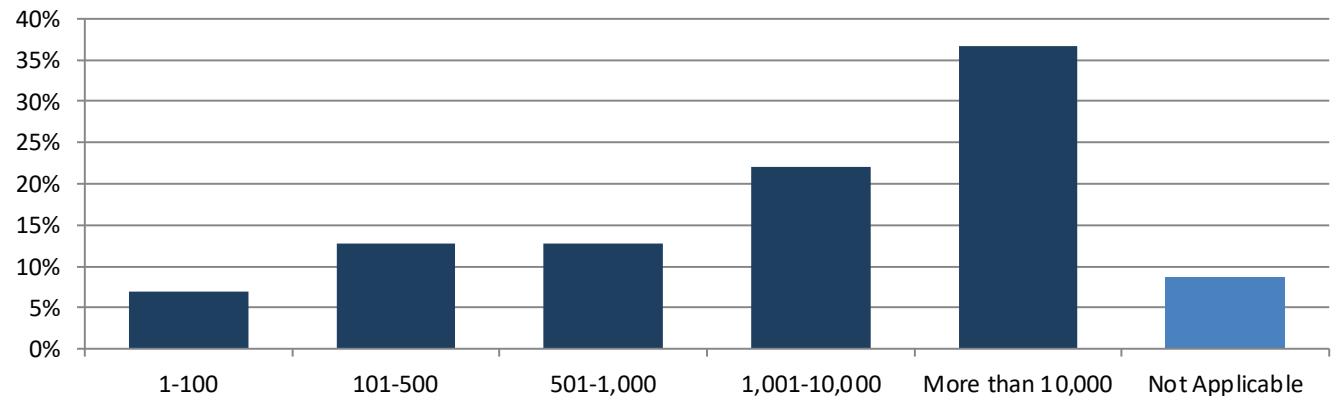
Key Findings

We aimed to understand the scale of the cybersecurity challenge faced by respondents in terms of the number of devices and systems they manage.

The distribution shows a significant skew towards larger asset pools, highlighting the extensive cybersecurity responsibilities shouldered by many of the survey's respondents. The largest proportion of respondents dealing with more than 10,000 assets underscores the critical need for scalable and efficient cybersecurity solutions capable of managing vast networks of operational technology devices. As smaller OT-using companies greatly outweighs the number of larger ones, this also suggests that cybersecurity is a higher priority for the latter.

This trend towards larger asset pools being managed underlines the importance of comprehensive cybersecurity strategies that include not only technological solutions but also processes and training to protect against and respond to cyber threats effectively. It also hints at the potential for significant automation and orchestrated, advanced cybersecurity tools, including artificial intelligence and machine learning, to play crucial roles in managing these large-scale environments.

Q: How many assets (PLCs, Workstations, IIoT devices, etc) do you estimate are in our organization's (or, for service providers, your clients') networks (all sites)?



1-100 assets: 7.19%

A smaller scale, likely indicative of smaller organizations or those with highly specialized operations.

101-500 assets: 12.57%

Representing small to medium-sized operational networks, where the cybersecurity challenges start to grow in complexity.

501-1,000 assets: 12.57%

Suggesting larger operational environments with significant cybersecurity needs.

1,001-10,000 assets: 22.16%

Reflecting very large and potentially multinational organizations with extensive operational technology environments, requiring robust and sophisticated cybersecurity frameworks.

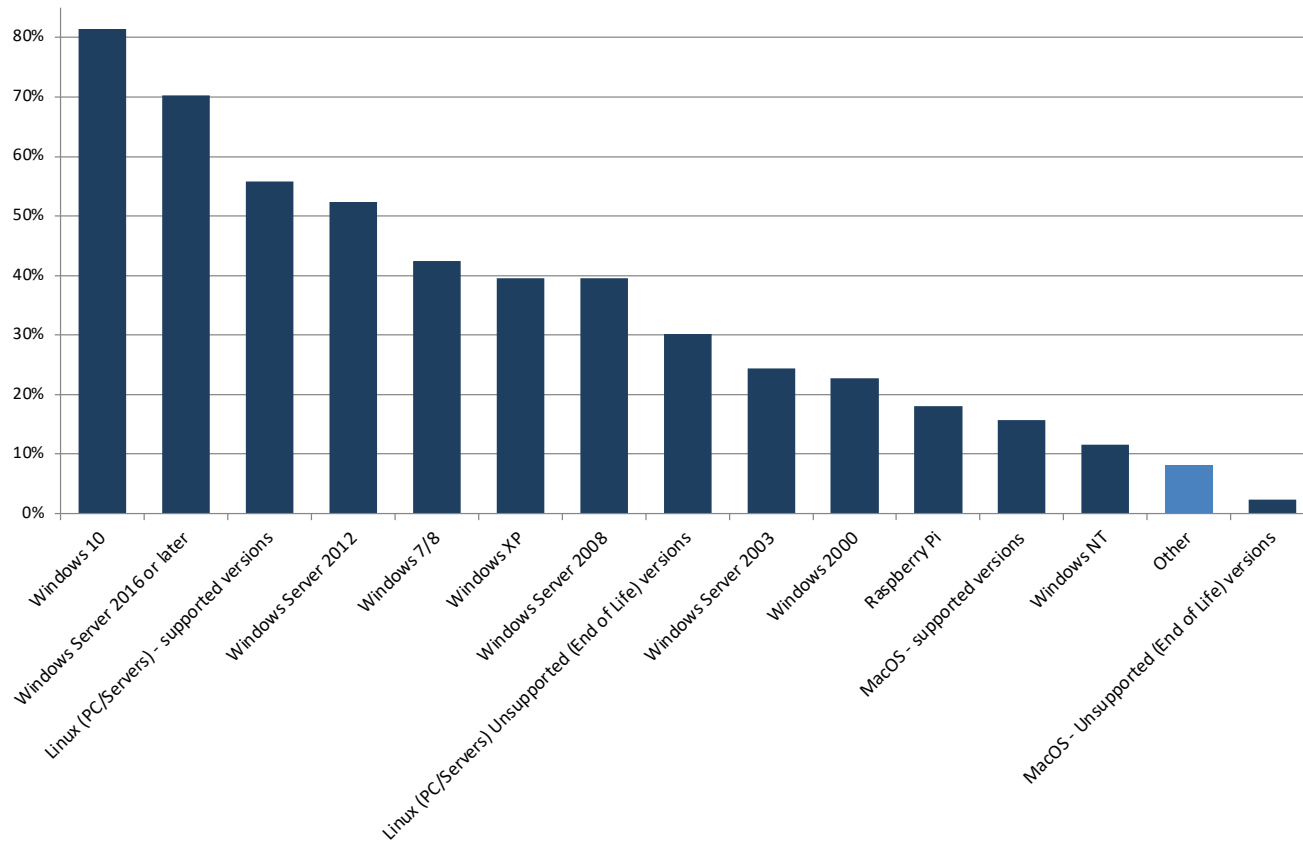
More than 10,000: 37.13%

The largest category, indicating respondents from organizations with vast numbers of assets. This scale suggests significant cybersecurity challenges, given the sheer volume of devices and systems to be secured.

Not Applicable To Me: 8.38%

This category might include consultants, researchers, or professionals in roles not directly involved in managing or securing OT assets but who are involved in the cybersecurity landscape.

Q: Which of the following Operating Systems are in use at sites you support?



The variety of operating systems in use, including a mix of modern and legacy systems, underscores the complexity of OT environments and the challenges in managing cybersecurity risks. Organizations must navigate the demands of operational continuity and compatibility with the imperative to secure their environments against evolving cyber threats. Transitioning away from legacy systems, where feasible, and ensuring all operating systems are supported and regularly updated, are critical steps in strengthening cybersecurity defenses in OT settings.



Operating Systems: Legacy & Updated

Key Findings

Windows 10: The most widely used operating system with 80.84%, underscoring its prevalence in modern IT and potentially OT environments.

Windows Server 2016 or later: Shows a strong adoption rate at 70.06%, indicating a trend towards newer, more secure versions of Windows Server.

Linux (PC/Servers) - supported versions: Utilized by 56.29%, reflecting Linux's significant role in both IT and OT environments due to its versatility and reliability.

Windows Server 2012: Also widely used with 53.29%, suggesting a balanced mix of operating system generations in current infrastructures.

Legacy Systems: Notably, Windows XP (40.12%) and Windows Server 2008 (40.12%) are still in use, highlighting the challenges of upgrading or replacing legacy systems in operational environments.

The data reveals a diverse landscape of operating system usage that spans from legacy systems like Windows XP and Windows 2000 to modern systems like Windows 10 and recent Windows Server versions. This diversity can be attributed to the varied lifecycle and upgrade strategies across different operational environments, as well as the specific requirements of certain applications or processes that may depend on older technologies.

Legacy System Risks: The continued use of unsupported or end-of-life operating systems like Windows XP and Windows Server 2003 poses significant cybersecurity risks, including vulnerabilities to malware and other cyber threats. These systems often remain in use due to compatibility requirements with specialized equipment or software, highlighting the challenge of balancing operational needs with cybersecurity best practices.

Adoption of Modern Systems: The strong presence of Windows 10 and recent Windows Server versions suggests a conscious effort towards modernizing IT infrastructure, likely driven by the need for enhanced security features, support, and performance improvements. This trend is crucial for improving the cybersecurity posture of OT environments.

Linux in OT Environments: The significant use of both supported and unsupported Linux versions points to the operating system's critical role in supporting diverse applications, from servers to embedded

systems. The distinction between supported and unsupported versions underscores the importance of maintaining up-to-date systems to mitigate security vulnerabilities.

Diverse Ecosystem: The somewhat surprising inclusion of MacOS and Raspberry Pi, though less common, reflects the diversity of devices and platforms in today's operational environments, and indicates dated patching strategies. It emphasizes the need for comprehensive cybersecurity strategies that cover all components of the OT infrastructure.

“ These systems may be running for 20 years. But frankly, no one can provide cybersecurity support in obsolete systems. This is where network isolation and other mitigation MUST be applied.”

- Senior IT/OT Solution Cybersecurity Specialist

Key Findings

Wifi: Predominantly used with 62.87%, indicating its widespread adoption in operational settings for its convenience and flexibility.

Cellular: Utilized by 43.11%, this may indicate the growing trend of integrating cellular technologies (e.g., 4G/5G) for remote monitoring and control in OT environments. It might also reflect their use for other purposes, such as direct cloud connectivity.

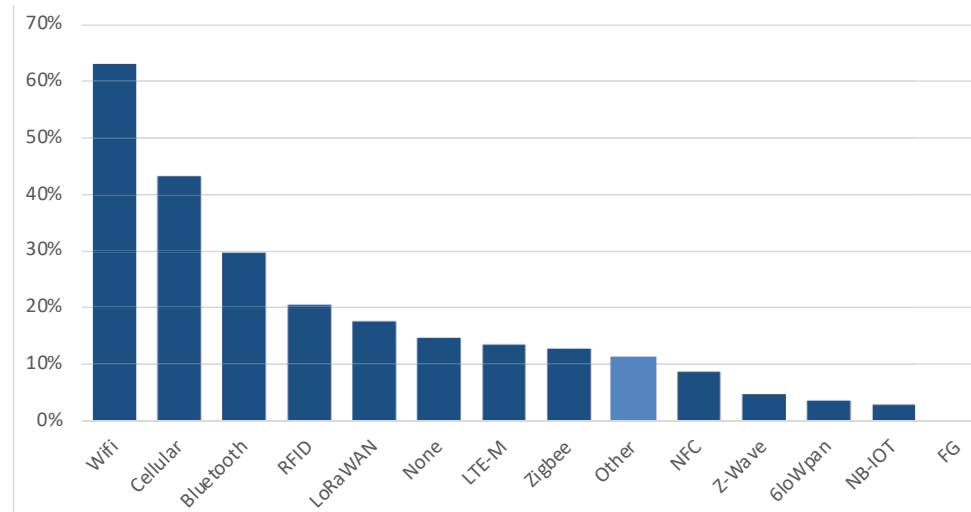
Bluetooth: Reported by 29.34%, suggesting its use in specific applications where short-range communication is sufficient.

RFID: With 20.36%, indicates its role in asset tracking and management within OT operations.

No wireless devices/protocols in use: 14.37% highlight a significant segment that still relies on wired connections exclusively, likely due to security, reliability, or operational requirements.

This analysis highlights the critical role wireless technologies play in modernizing and enhancing OT/ICS operations, along with the importance of implementing stringent security measures to mitigate the risks associated with their use. It underscores a trend towards more connected, efficient, but also potentially vulnerable industrial environments, emphasizing the need for ongoing vigilance and innovation in cybersecurity practices.

Q: Do you use wireless functions (devices/protocols) in OT/ICS operations networks which you support?



Security vs. Convenience: The high adoption rate of Wifi and Cellular technologies underscores the balance OT operators need to strike between leveraging wireless technology for efficiency and managing the potential cybersecurity risks associated with wireless communications. While these technologies offer significant benefits in terms of flexibility and operational efficiency, they also introduce vulnerabilities that must be carefully managed through robust security protocols.

Emerging Technologies: The presence of technologies like LoRaWAN and LTE-M, though less widespread, points to the adoption of newer wireless solutions designed for the Internet of Things (IoT) and industrial applications. These technologies offer low power consumption and long-range capabilities, making them well-suited for specific OT applications, such as remote monitoring of distributed assets.

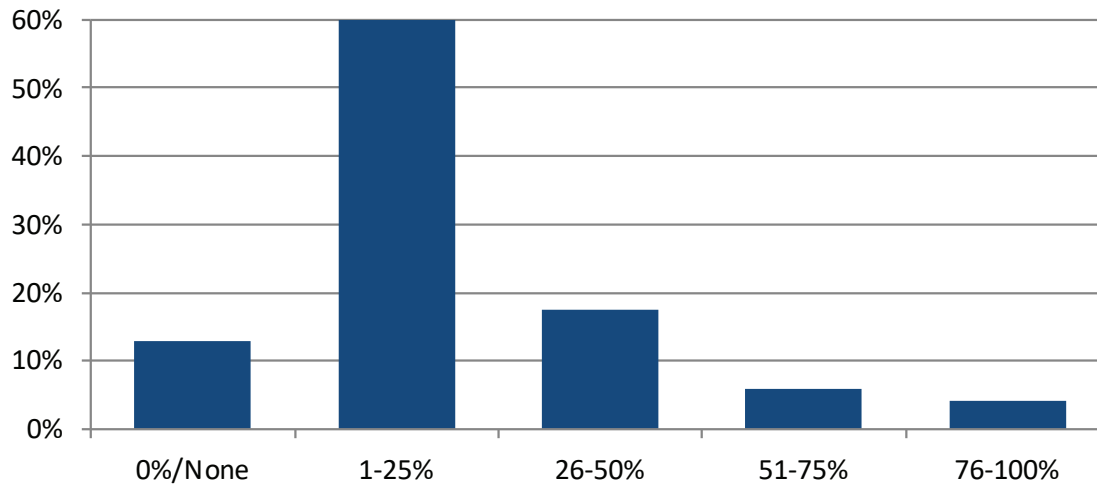
Niche Applications: The use of Zigbee, Z-Wave, and other specified technologies suggests that OT environments are diverse and that operators select wireless solutions based on the unique requirements

of their operations. These technologies, often associated with smart devices and home automation, are finding niches within industrial settings for their ease of deployment and low power requirements.

Risk Management: Wireless technology in OT environments necessitates careful consideration of security risks, including eavesdropping, unauthorized access, and interference. The decision to use these technologies reflects an assessment of their benefits against the potential cybersecurity challenges they present. Operators must employ advanced security measures, such as encryption, access control, and regular monitoring, to safeguard against these risks.

Strategic Integration: The strategic integration of wireless technologies into OT environments reflects a broader trend towards digital transformation in the industrial sector. As companies seek to enhance operational efficiency, reduce costs, and improve data analytics capabilities, wireless technologies become crucial enablers, provided their deployment is accompanied by comprehensive security strategies to protect critical infrastructure.

Q: In your estimation, what percentage of ICS/OT operations networks which you support contain wireless functions?



Selective Integration of Wireless Technologies:

The data suggests that while wireless technologies are integral to modern ICS/OT operations, their adoption is measured and selective. The majority of respondents indicating a 1-25% integration level reflects a cautious approach to wireless technology, likely driven by the operational necessity, security concerns, and the critical nature of many OT environments.

Operational and Security Considerations: The presence of a notable percentage of networks without any wireless functions underscores the prioritization of security and reliability over the convenience wireless technologies might offer. In environments where uninterrupted operation and security are paramount, the potential risks associated with wireless communication, such as interference or unauthorized access, may outweigh their benefits.

Emerging Trends in Wireless Adoption: The data also points to an emerging trend where a significant portion of operations networks are beginning to incorporate wireless functions more extensively (26-50% range and above). This could be indicative of growing confidence in the security and reliability of modern wireless technologies or a shift in operational

requirements that favor the flexibility wireless solutions provide.

Balancing Act: The integration of wireless technologies in OT environments requires a balancing act between leveraging the operational flexibility and efficiency gains they offer and mitigating the security risks they entail, as their use greatly expands the threat surface. This balance is crucial in maintaining the integrity and reliability of critical infrastructure.

Future of Wireless in OT: The trend towards cautious but increasing adoption of wireless functions in OT networks suggests an evolving landscape. As wireless technology continues to advance, offering more secure and reliable options, its integration into OT environments is likely to grow. However, this integration must be accompanied by strong security measures, including the use of secure communication protocols, regular security assessments, and the implementation of network segmentation strategies. AI in wireless networks will add to the threat vectors, and possible remediation as it develops.

Key Findings

1-25% Range: The majority, with 59.88%, indicating that while wireless functions are adopted, they constitute a smaller proportion of the overall network functions for most sites.

26-50% Range: 16.77% of the respondents estimate that a quarter to half of their networks incorporate wireless functions, pointing to higher adoption in certain environments.

51-75% and 76-100% Ranges: Fewer respondents, 5.99% and 4.19% respectively, indicate that wireless functions are predominant or exclusive in their operations networks, highlighting that while significant for some, widespread dominance of wireless technology in ICS/OT networks is less common.

0%/None: A significant 13.17% of networks reportedly do not utilize wireless functions at all, suggesting a cautious approach or specific operational requirements that preclude the use of wireless technologies.

This data highlights the nuanced approach to the adoption of wireless technologies in OT environments, emphasizing the critical importance of security and reliability in these decisions. As the landscape of industrial operations continues to evolve, the role of wireless technologies will likely become more pronounced, necessitating ongoing attention to cybersecurity practices and innovations.

Key Findings

From the Internet: Reflects the most cautious approach for remote access, with a high percentage of components having Neither/No Access (N), especially PLCs, IEDs, RTUs (80.90% N), and HMIs (78.41% N). This indicates a strong security posture to minimize exposure of critical OT components to the public internet. Monitoring (M) and control (C) capabilities are notably limited, underscoring the heightened awareness of cybersecurity risks associated with internet-facing access.

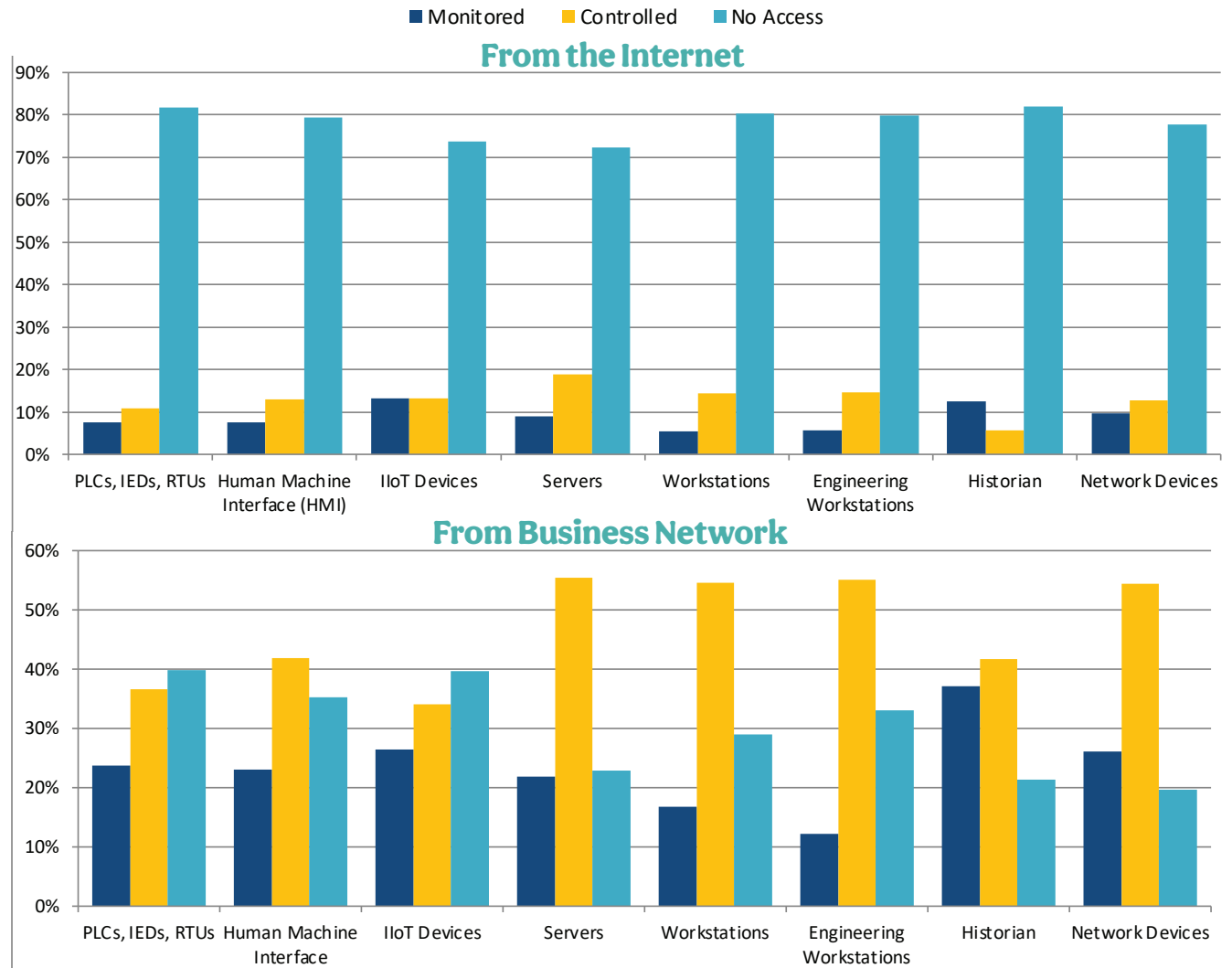
From the Business Network: Demonstrates higher accessibility, with significant percentages for monitoring and control across devices, highlighting the business network as a common vector for remote interactions. This is particularly evident with servers (20.22% M, 57.30% C) and workstations (14.94% M, 56.32% C), suggesting a balance between operational flexibility and security within the confines of the business network.

Remotely by Vendor/Service Provider:

Shows a moderate level of remote access, indicative of vendor involvement in the maintenance and support of OT systems. This reflects a reliance on external expertise while also pointing to the necessity of stringent access controls and security protocols to manage vendor interactions securely.

From the Cloud: Indicates generally lower levels of remote access, except for historians (19.05% M, 8.33% C), which may suggest cloud-based data aggregation and analysis activities. The cautious approach to cloud access mirrors the security concerns associated with exposing OT systems to potentially insecure external networks.

Q: Please identify whether each of these in your (or, for service providers, your clients') network(s) can be monitored (M), controlled (C), or Neither/No Access (N) remotely...



Roughly 50% of all types of assets are either monitored or monitored / controlled by vendors, presumably across the Internet. This means that remote access systems, to be used by vendors across the Internet, must be exposed to potential exploits of known vulnerabilities and zero-days across the Internet. Threat reports show that tens of thousands of

VPN servers, "secure" remote access servers, firewalls and other parts of Internet-based vendor remote access have been breached in recent years. What the world needs is hardware-enforced remote access - where even if software vulnerabilities are exploited, no harm can come to the industrial / OT network, because the hardware saves us."

Insight from: Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Integrating the internet access data into the overview highlights the nuanced approaches to remote accessibility across different vectors, with a clear emphasis on security and risk management, especially for internet-facing access points. The stark contrast in remote accessibility “From the Internet” compared to other vectors underscores the prioritization of OT networks. It must be noted that compromised devices in the business network are potential pivot points to attack OT, should the latter be accessible from the former. By limiting internet-based remote interactions, organizations aim to protect critical infrastructure from the array of threats present in the wider internet environment, while still leveraging internal and vendor-supported remote capabilities to maintain operational efficiency and support.

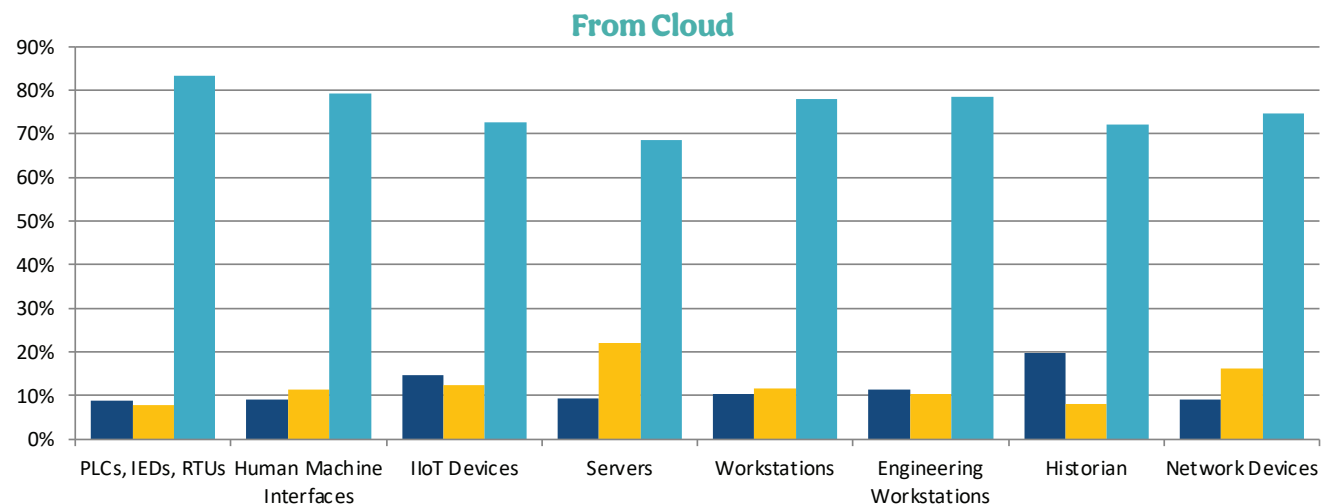
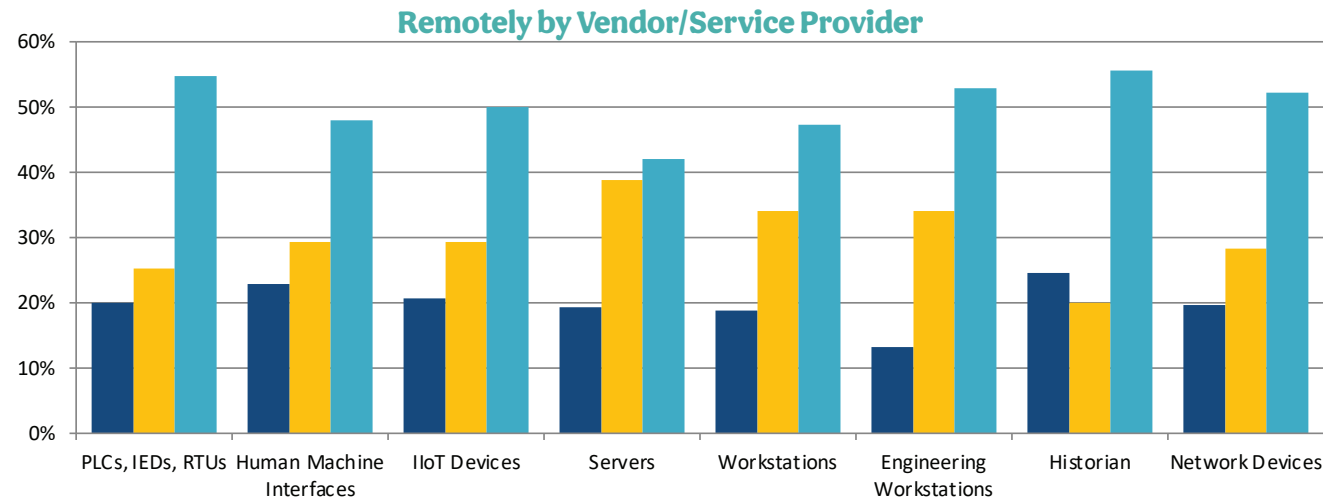
This careful management of remote access pathways reflects a broader cybersecurity strategy within OT environments, balancing the need for connectivity and remote operational capabilities with the imperative to secure critical systems against unauthorized access and cyber threats.

Cybersecurity Implications: The varying levels of remote accessibility across different access points underscore the complex cybersecurity landscape in OT environments. While remote access provides operational flexibility and efficiency, especially for maintenance and monitoring, it also introduces potential vulnerabilities. The data highlights the need for robust security measures, including multi-factor authentication, encryption, and strict access controls, to safeguard OT systems against unauthorized access and cyber threats.

Trend Towards Business Network and Cloud

Integration: The data shows growth in integrating OT systems with business networks and cloud services, facilitating enhanced data analytics, operational visibility, and efficiency. However, this integration requires careful consideration of the cybersecurity implications, particularly in ensuring that OT networks are resilient against threats propagated through business IT systems or cloud services.

Vendor Access for Support: The moderate levels of remote access by vendors/service providers highlight the reliance on external entities for system support and maintenance. While beneficial for operational efficiency, this



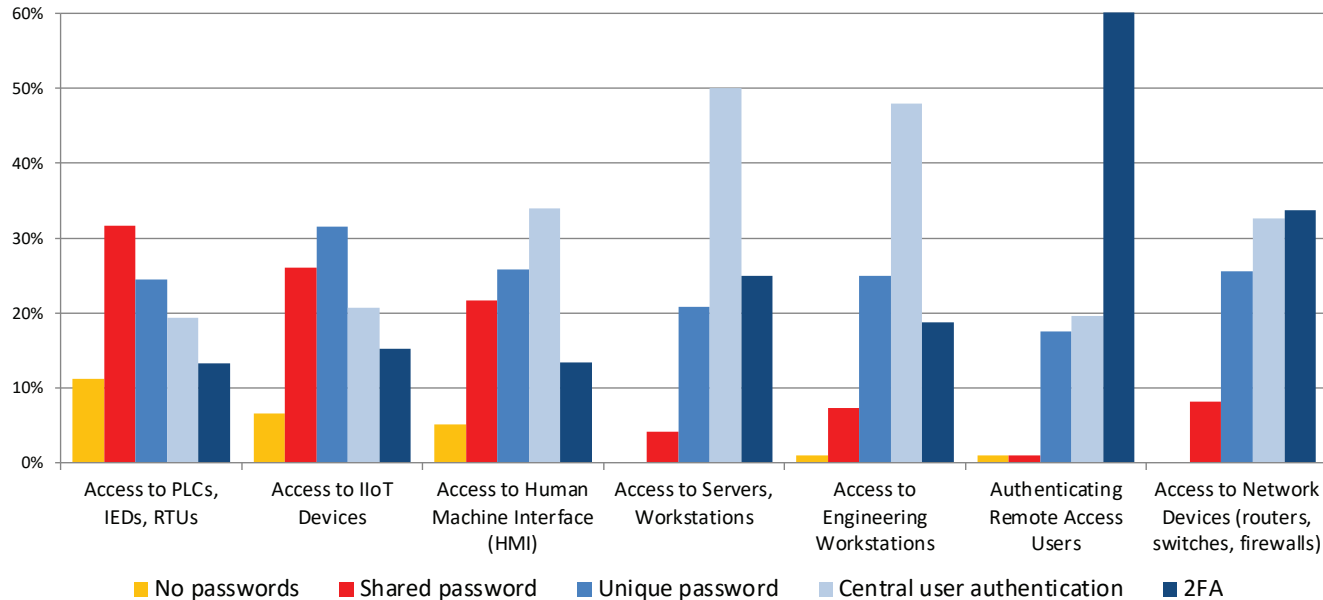
reliance necessitates clear agreements on cybersecurity responsibilities and protocols to ensure that vendor access does not become a weak link in the security posture

Risk Management in Connectivity: Essential components like PLCs, IEDs, RTUs, and HMIs are less exposed to remote control, especially from the Internet and cloud, mitigating risks associated with external cyber threats. The prioritization of monitoring over control for remote access from less secure points suggests an effort to maintaining operational integrity while leveraging remote capabilities. That, in almost

a third or our respondents organizations, those same devices can be controlled from the business network does leave a potential route for a determined attacker.

This comprehensive view into the remote accessibility of ICS/OT components underscores the critical balance between operational flexibility and cybersecurity risk management. As OT environments become increasingly interconnected, the data emphasizes the importance of adopting advanced cybersecurity strategies tailored to the unique challenges of OT systems, ensuring that remote access capabilities enhance operational efficiency without compromising security.

Q: What type of user authentication methods are you (or, for service providers, your clients) using for the following?



Balancing Usability and Security: The data illustrates the ongoing challenge of balancing ease of access for operational efficiency with the need to secure critical systems against unauthorized use. While shared passwords are still in use, particularly for devices like PLCs, IEDs, and RTUs, there's widespread use of more secure authentication methods, such as unique passwords, central user authentication, and 2FA, especially for systems with broader network access or critical operational roles.

Shift Towards Stronger Authentication for Remote Access: The emphasis on 2FA for authenticating remote access users reflects some recognition of the heightened risks associated with remote connectivity. That this should be much closer to 100% is a given. This approach is particularly crucial in the context of increasing remote operations and the need to ensure secure access for users connecting from outside the traditional network perimeter.

Adoption of Central Authentication Services: The widespread use of central user authentication mechanisms, like Active Directory, for servers, workstations, and network devices indicates a move towards more centralized and manageable security practices. This centralization not only enhances security but also improves administrative efficiency, allowing for more consistent policy enforcement and user management across the OT environment. It also increases the security and resiliency requirements on those same centralized services to prevent them being the single points of failure whose compromise or disruption does not impact operations.

Diverse Authentication Practices Across Device Types: The varied authentication methods across different device types highlight the complexity of OT environments and the need to tailor security practices to the specific operational and risk contexts of different systems. While, with few exceptions (such as emergency safety shutdown systems), 2FA represents best practice, the continued use of shared and unique passwords reflects the operational realities and constraints within which these environments operate.

Key Findings

Central User Authentication and 2FA: Predominantly used for servers, workstations, and network devices, possibly indicating a higher security standard for these critical components, reflecting the technical difficulties and reliability risks inherent in using central anything in distributed/critical systems.. Servers and workstations see a combination of central user authentication (48.35%) and 2FA (25.27%), emphasizing the importance of secure access controls in protecting sensitive systems.

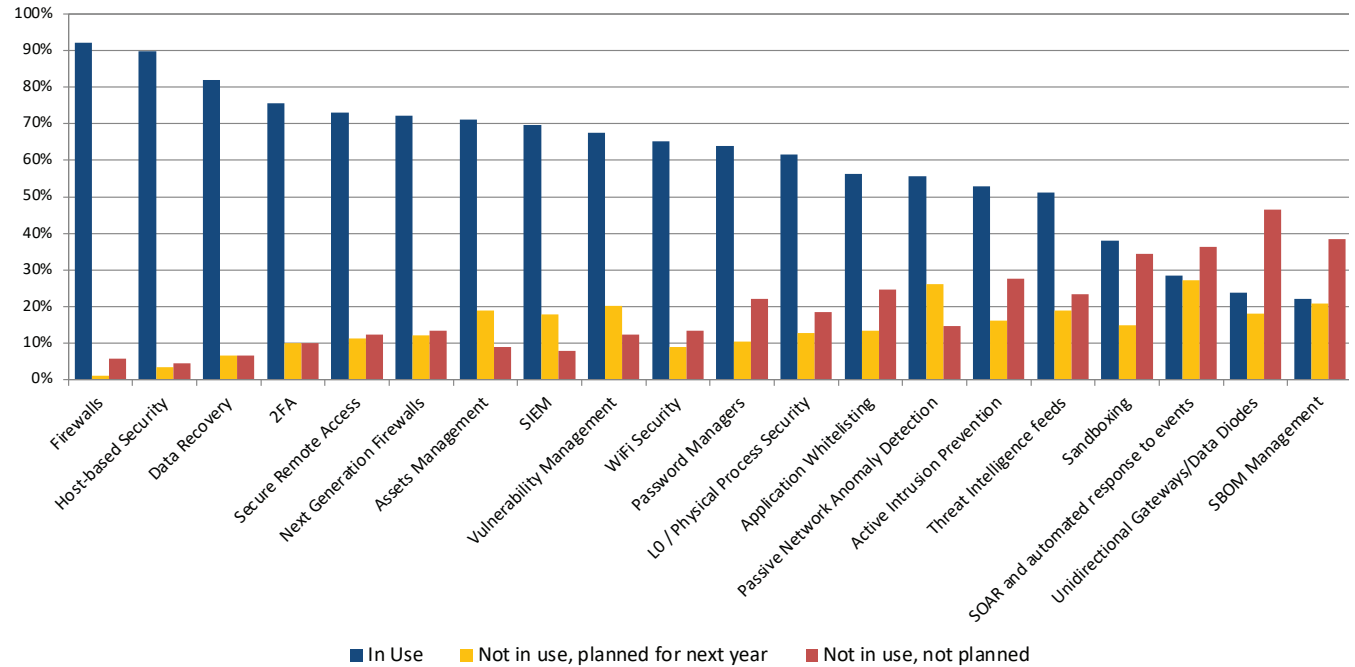
Access to PLCs, IEDs, RTUs, and IIoT Devices: Displays a diverse approach, with a notable reliance on shared passwords for PLCs, IEDs, RTUs (31.18%), and a preference for unique passwords per user for IIoT devices (31.03%). This variation might reflect the differing operational contexts and security challenges associated with these device types.

Authenticating Remote Access Users: Shows a strong preference for 2FA (60.22%), underscoring the heightened security measures applied to remote access to mitigate the risks of unauthorized access from external networks.

Engineering Workstations: Also emphasize central user authentication (47.83%) and 2FA (18.48%), pointing to the critical role these systems play in the design and maintenance of OT environments and the necessity of protecting them from cyber threats.

These insights underscore the importance of adopting robust and flexible authentication strategies to secure OT networks effectively. As OT environments continue to evolve and integrate more closely with IT systems and the Internet of Things (IoT), the need for advanced authentication methods that can adapt to the diverse and dynamic nature of these environments becomes increasingly critical.

Q: Which of the following technologies/solutions are in use in networks you support?



This analysis sheds light on the user authentication methods employed across various ICS/OT components. The findings illustrate a broad application of diverse authentication strategies, reflecting a heightened focus on security in operational technology environments. Notably, the most prevalent method is the use of central user authentication mechanisms, such as those integrated with Active Directory, indicating a shift towards more centralized and manageable security practices that can offer improved control and oversight across multiple components, as well as possible introduction of tools such as Privileged Access Management (PAM) platforms.

An interesting trend observed is the considerable adoption of two-factor authentication (2FA), especially for accessing critical components such as servers and engineering workstations. This trend towards multi-factor authentication underscores the increasing recognition of the need for enhanced security measures to protect sensitive OT environments from unauthorized access. Varied use of authentication methods, including less secure options like shared passwords for less critical components, suggests a strategic, risk-based approach to authentication, where the level of security implemented shows sensitivity and exposure of the system component.

The analysis reveals a dynamic and nuanced approach to cybersecurity within OT environments, with a blend of foundational security practices and innovative solutions to meet the unique challenges of these networks. As OT environments continue to evolve and integrate more closely with IT systems and the broader digital landscape, the strategic selection and implementation of cybersecurity technologies will remain critical in safeguarding operational integrity against an ever-expanding threat landscape.

Key Findings

Widely Adopted Technologies: Firewalls (92.77%), Host-based Security (EDR, Antivirus, etc.) (89.16%), and Data Recovery (82.14%) are among the most commonly implemented solutions, reflecting their foundational role in network security and data integrity.

Emerging and Advanced Solutions: While traditional security measures like firewalls and antivirus remain prevalent, there is notable adoption of Next-Generation Firewalls (70.59%) and Two-factor Authentication (2FA) (74.12%), indicating a shift towards more sophisticated security frameworks. Solutions such as SIEM (67.86%) and Secure Remote Access (72.62%) also highlight the importance of advanced monitoring and secure connectivity in modern OT networks.

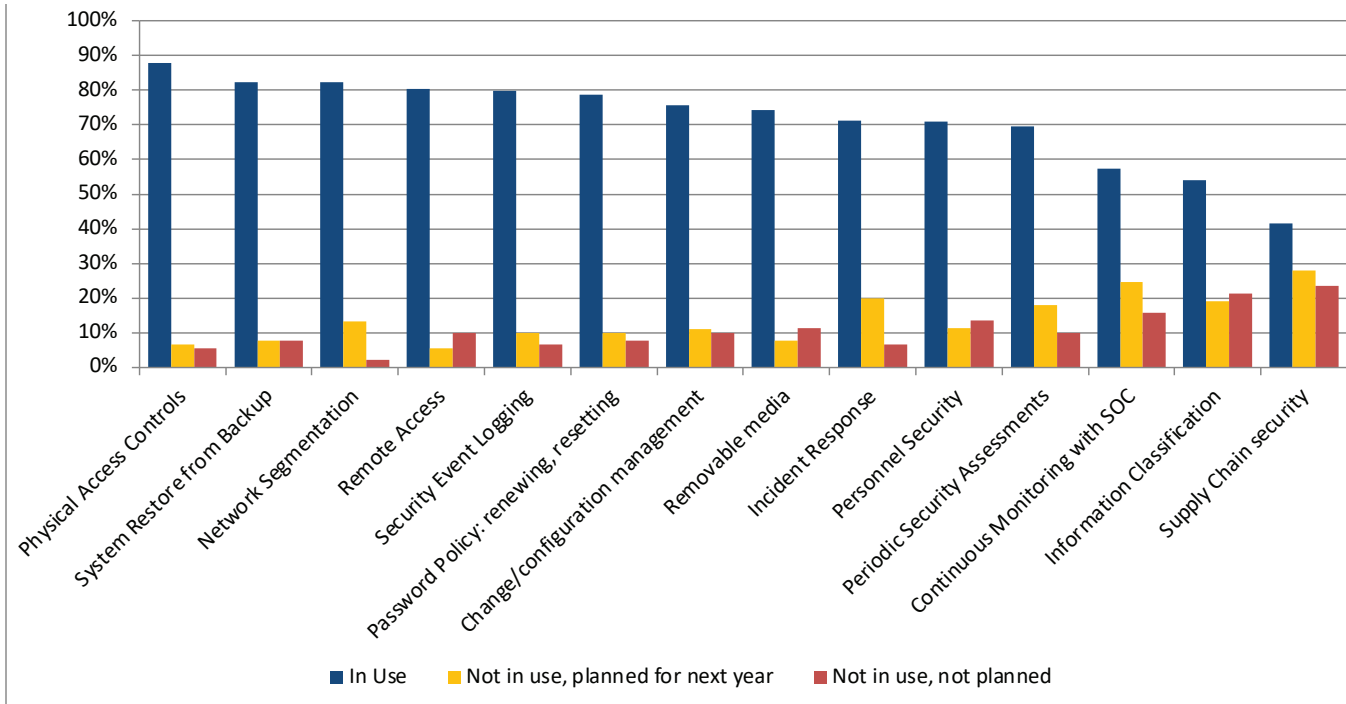
Innovative and Niche Solutions:

Technologies like SBOM Management (23.46% in use) and Unidirectional Gateways/Data Diodes (22.89% in use) demonstrate a growing interest in addressing specific security challenges unique to OT environments, albeit with a lower adoption rate compared to more established security measures.

Planned Implementations:

Passive Network Anomaly Detection (26.51% planned for next year) and Threat Intelligence feeds (18.82% planned for next year) show significant interest in adopting advanced monitoring and threat detection capabilities, indicating a proactive stance towards evolving cybersecurity threats.

Q: Which of the following procedures are in use in networks you support?



Strategic Layering of Security Procedures: The adoption patterns reflect a layered approach to security, combining foundational practices like backups and physical controls with advanced strategies such as SOC monitoring and supply chain assessments, creating a robust defense against a wide range of cyber threats.

Prioritizing Resilience and Recovery: The prioritization of System Restore from Backup and Network Segmentation underscores the importance of resilience to cyber incidents. By preparing for the possibility of breaches, organizations may reduce downtime and mitigate the impact of attacks.

Focus on Personnel and Remote Access Security: The emphasis on Personnel Security and Remote Access management (80.23% in use) highlights the recognition of human factors and the risks posed by remote connectivity. Through background checks, cybersecurity training, and secure protocols, organizations aim to address

both insider threats and the vulnerabilities associated with remote operations.

Adaptation to Evolving Cybersecurity Landscapes: The attention to Information Classification and Supply Chain Security reflects the evolving cybersecurity landscape, where information handling and third-party relationships are increasingly critical. As cyber threats become more sophisticated and pervasive, understanding the flow and storage of sensitive information, and security of suppliers, is paramount.

Comprehensive Cybersecurity Culture: The wide range of procedures in use indicates the development of a comprehensive cybersecurity culture within OT environments, where security is integrated into various aspects of operations, from the ground up. This culture is essential for ensuring that cybersecurity considerations are embedded in daily operations, decision-making processes, and strategic planning.

Key Findings

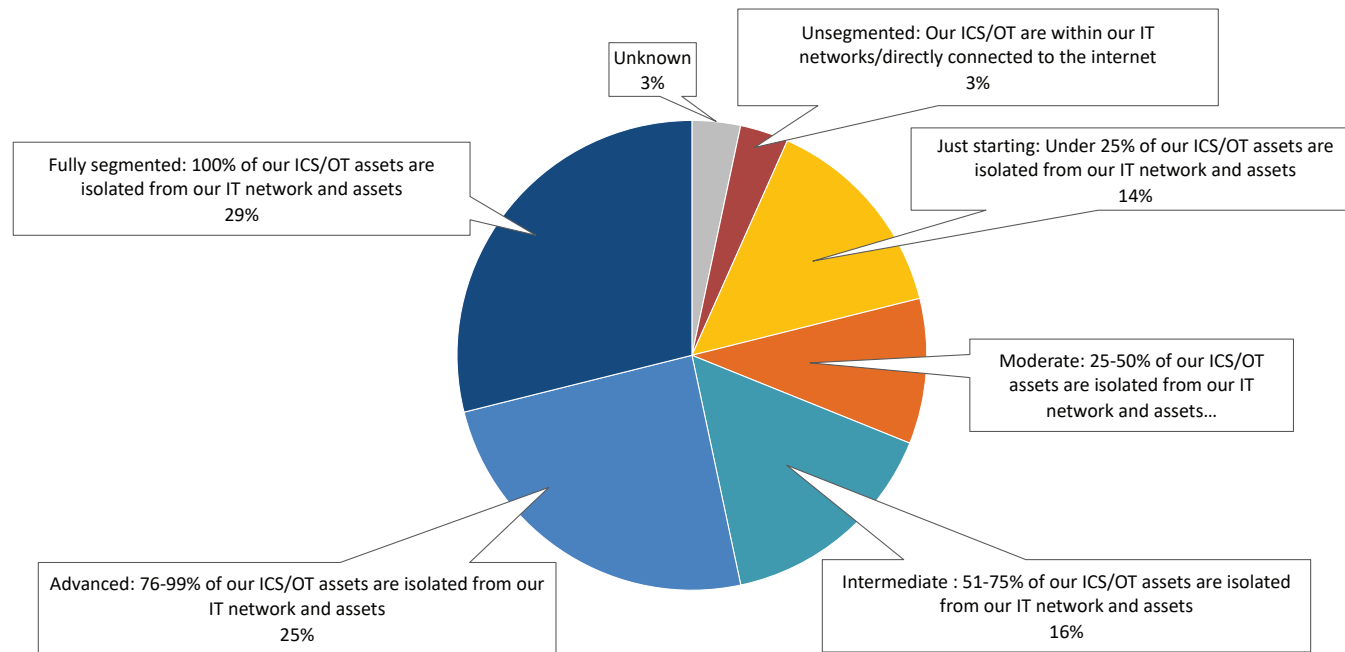
Widely Adopted Procedures: High rates of adoption for System Restore from Backup (82.35%), Network Segmentation (82.35%), and Physical Access Controls (87.06%) illustrate a strong foundation in basic cybersecurity and operational resilience practices. These are critical for ensuring system integrity, data recoverability, and the physical security of OT assets.

Incident Preparedness and Response: A significant percentage of networks implement Incident Response procedures (70.59%) and Periodic Security Assessments (69.05%), indicating a proactive stance towards identifying vulnerabilities and responding to security incidents.

Operational Security Measures: Continuous Monitoring with a Security Operations Center (SOC) (55.95%), Password Policy management (77.38%), and Security Event Logging (78.57%) highlight the emphasis on ongoing vigilance and user access control as part of the security posture.

Emerging and Advanced Strategies: The data shows a growing focus on Supply Chain Security (41.67% in use) and Information Classification (53.57% in use), pointing to an expanded security view that encompasses the entire lifecycle and sensitivity of information and assets.

Q: What degree of network segmentation is implemented (i.e., isolation of OT/ICS from other IT assets, within controlled access networks) in networks you support?



Strategic Importance of Network Segmentation:

The responses underscore the strategic importance of network segmentation in safeguarding critical OT environments. By isolating OT systems from less secure IT networks and the internet, organizations can significantly reduce the attack surface and limit the potential for cybersecurity threats to propagate across networks.

Challenges and Progress in Segmentation: The varying degrees of segmentation reflect the challenges organizations face in achieving complete isolation, often due to operational dependencies, legacy systems, and the complexity of existing network architectures. However, the data also indicates some recognition of the value of segmentation and concerted efforts toward achieving more advanced levels of isolation.

Operational Impact and Considerations:

Implementing network segmentation involves not just technical changes but also operational considerations,

including the need for robust access controls, secure communication between segmented networks for necessary data exchange, and the management of potential impacts on operational efficiency.

Correlation with Maturity and Risk Management:

The degree of network segmentation can serve as an indicator of an organization's overall cybersecurity maturity, with higher levels of isolation reflecting a proactive approach to risk management and a commitment to protecting critical infrastructure from cyber threats.

Future Directions: As OT environments continue to evolve with increased digitalization and connectivity, the role of network segmentation as a foundational security measure will likely grow in importance. Organizations will need to continuously assess and adjust their segmentation strategies in response to changing operational requirements and emerging threats.

Key Findings

Advanced Segmentation Levels: A significant proportion of respondents indicate an advanced degree of network segmentation, with 24.71% stating that 76-99% of ICS/OT assets are isolated, and 28.24% reporting complete isolation (100%) of ICS/OT assets from IT networks. This highlights a strong commitment to securing OT environments against potential cyber threats propagated through IT systems.

Beginning and Moderate Implementation:

There's a noticeable effort in initial stages of segmentation, with 15.29% of participants in the early phase (under 25% isolation) and 10.59% at a moderate level (25-50% isolation), suggesting ongoing initiatives to enhance the security posture through increased isolation.

Intermediate Isolation Efforts:

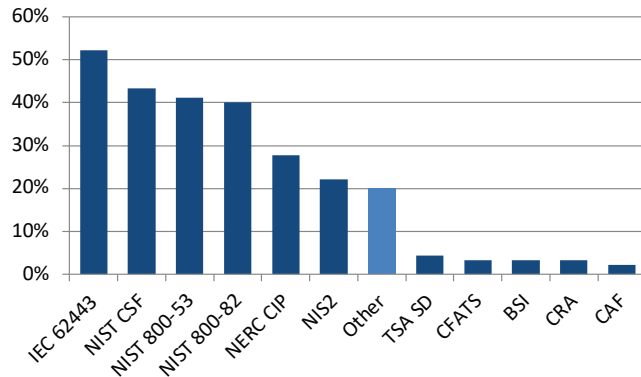
Additionally, 14.12% of respondents are at an intermediate stage, with 51-75% of ICS/OT assets isolated, reflecting progress toward more comprehensive network segmentation strategies.

Minimal or No Segmentation:

A small fraction report minimal or no segmentation, with 3.53% not distinguishing ICS/OT from IT networks or having them directly connected to the internet, and another 3.53% uncertain about the extent of segmentation. This scenario underscores potential areas for significant security enhancements.

Standards & Regulations

Q: Which regulations does your organization target for compliance?



The Role of IEC 62443: The prominence of IEC 62443 underscores its role as a cornerstone in the cybersecurity strategy for industrial control systems (ICS) and OT networks. Its comprehensive coverage of cybersecurity principles, from system design to operations and maintenance, makes it a critical framework for organizations looking to safeguard their operational technologies against cyber threats.

Balancing Compliance and Operational Needs: While compliance is essential, organizations must balance regulatory requirements with operational realities. The wide range of standards and regulations targeted reflects the need to navigate a complex compliance landscape while ensuring that cybersecurity measures are tailored to the specific needs and challenges of OT environments.

Evolving Compliance Landscape: The data points to an evolving compliance landscape, where traditional standards like NIST and emerging frameworks like NIS2 coexist. This evolution reflects the dynamic nature of cybersecurity threats and the continuous development of regulatory and industry standards to address these challenges. Organizations must remain agile, updating their compliance and security strategies to align with both current and future regulatory environments.

Sector-Specific Regulations: Compliance with sector-specific regulations such as NERC CIP highlights the critical importance of safeguarding infrastructure deemed vital to national security and public welfare, for each critical sector. The trend toward additional sector-specific regulations is increasing in the US, where broader multi-sector regulations are becoming more common in Europe.

Portability of Compliance Reporting: As external pressures mount on OT organizations, especially those within critical infrastructures, many are choosing to assess their cybersecurity positions against well-known frameworks such as IEC 62443 and NIST that can act as a “Rosetta Stone” for the variety of external reporting needs (e.g., compliance enforcement authorities, public commissions, mergers and acquisitions, cyber insurance policy questionnaires or claim processing).

Key Findings

IEC 62443 Leading: The most targeted standard for compliance is IEC 62443, with 54.12%, indicating its significance as a global benchmark for the security of industrial automation and control system networks.

NIST Frameworks Popular: A significant proportion of organizations also target compliance with various NIST frameworks: NIST CSF (42.35%), NIST 800-53 (42.35%), and NIST 800-82 (41.18%). These frameworks are widely recognized for their comprehensive approach to cybersecurity risk management.

Sector-Specific Regulations: NERC CIP compliance is targeted by 29.41%, showcasing the emphasis on securing the North American electric grid. Other sector-specific or regional regulations, like TSA SD and CFATS have a lower emphasis, indicating a potentially narrower applicability or focus within the respondent base.

Emerging and Other Standards: NIS2, a regulation indicating the growing importance of network and information security within the European Union, is targeted by 23.53%. The presence of “Other” specifications at 17.65% suggests a diverse compliance landscape that may include industry-specific standards, regional regulations, or internal corporate governance frameworks.

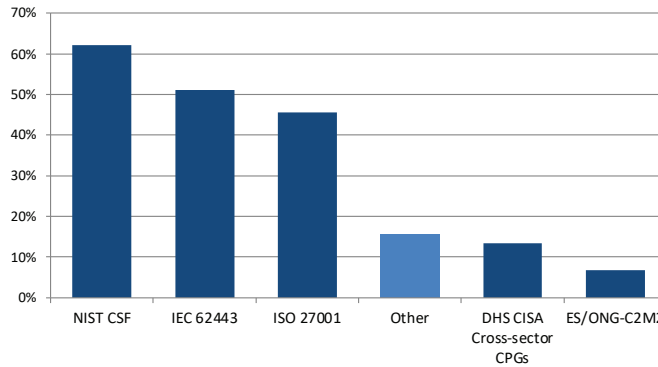
Key Findings

NIST CSF Leads: The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) is the most adhered-to framework, with 61.18%, reflecting its comprehensive approach and adaptability across various sectors.

IEC 62443 and ISO 27001: Following closely, IEC 62443 is adhered to by 52.94% of the respondents, showcasing its importance in industrial control system security. ISO 27001 also has significant adherence at 48.24%, underscoring its role in establishing information security management systems.

Other Frameworks and Practices: DHS CISA Cross-sector Cyber Performance Goals (CPGs) and ES/ONG-C2M2 show lower adherence rates at 12.94% and 7.06%, respectively. "Other" frameworks specified by 14.12% indicate a diverse range of additional standards and practices in play, tailored to specific operational needs or sector-specific risks.

Q: What industry security frameworks (or common practices) does your organization (or, for service providers, your clients) adhere to?



Strategic Framework Selection: The selection of frameworks like NIST CSF, IEC 62443, and ISO 27001 highlights a strategic approach to cybersecurity, where organizations opt for standards that offer both broad guidelines and industry-specific recommendations. This strategic selection is crucial for developing a robust cybersecurity posture that addresses the unique challenges of OT environments.

NIST CSF's Broad Adoption: The broad adoption of NIST CSF underscores its versatility and effectiveness in providing a framework for improving cybersecurity across different types of organizations. Its popularity suggests that it serves not only as a guideline for cybersecurity practices but also as a benchmark for cybersecurity maturity.

IEC 62443's Specialized Focus: The adherence to IEC 62443 emphasizes the importance of securing industrial automation and control systems. This

framework's detailed guidance for OT environments makes it a critical resource for organizations aiming to protect critical infrastructure from cyber threats.

ISO 27001's Comprehensive Approach: The adherence to ISO 27001 reflects an organizational commitment to establishing, implementing, maintaining, and continuously improving an information security management system (ISMS). This adherence indicates a comprehensive approach to managing information security risks, including those related to OT.

Adaptation to Evolving Threats and Practices: The inclusion of "Other" frameworks and practices, along with adherence to newer or less common frameworks like DHS CISA CPGs and ES/ONG-C2M2, points to the dynamic nature of cybersecurity. Organizations must continually adapt to evolving threats and assess their practices through various measuring tools.

The Importance of Customized Security Strategies: The diversity in adherence across different frameworks highlights the necessity of customized security strategies that align with organizational goals, regulatory requirements, and the specific risks associated with OT environments. This customization ensures that cybersecurity measures are not only compliant with industry standards but also effectively mitigate the unique threats faced by each organization.

The survey data sheds light on the critical role of industry security frameworks in shaping cybersecurity strategies within OT environments. As organizations navigate the complex landscape of cybersecurity threats, the choice and implementation of these frameworks provide a consistent, structured, and measurable approach to managing risks, enhancing security, and ensuring operational resilience.

Key Findings

Annually/Semi-Annually: The majority of respondents, 37.65%, conduct control system security assessments annually or semi-annually, indicating this as the most common frequency for thorough security evaluations.

Quarterly and Monthly Assessments: A smaller yet significant portion of organizations opt for more frequent assessments, with 15.29% conducting them quarterly and 5.88% on a monthly basis. These frequencies suggest a proactive approach to cybersecurity, allowing for timely identification and remediation of potential vulnerabilities.

Less Frequent and Absent Assessments: 14.12% report conducting assessments less than once a year, while 18.82% do not perform periodic assessments at all, highlighting areas for improvement in cybersecurity practices.

Other Frequencies: 8.24% specified other frequencies or approaches to security assessments, which may include ad-hoc, event-driven, or risk-based assessments that do not adhere to a fixed schedule.

Q: How often does your organization (or, for service providers, your clients) conduct control system security assessments?

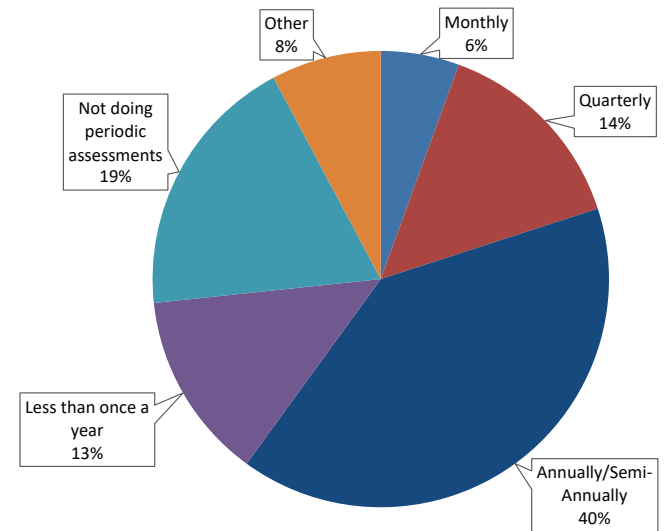
Strategic Importance of Regular Assessments: The data underscores the strategic importance of regular security assessments within OT environments. Periodic assessments serve as a critical component of a dynamic cybersecurity strategy, enabling organizations to adapt to evolving threats and technological changes.

Balancing Assessment Frequency with Operational Impact: Choosing the optimal frequency for security assessments involves balancing the need for thorough security evaluations with the potential operational impact. While more frequent assessments can provide timely insights into security posture, they must be managed to minimize disruption to critical operational processes.

Challenges in Assessment Frequency: The presence of organizations not conducting periodic assessments reflects potential challenges, including resource constraints, lack of awareness, or underestimation of cybersecurity risks. It underscores the need for increased awareness and prioritization of cybersecurity within the OT domain.

Customized Approaches to Security Assessments: The variation in assessment frequencies, including those specified under “Other,” points to the need for customized approaches that consider the unique operational, regulatory, and risk landscapes of each organization. Tailoring assessment frequency to specific organizational needs allows for more effective management of cybersecurity risks.

The Role of Assessments in Cybersecurity Maturity: Regular security assessments are indicative of higher cybersecurity maturity levels, as supported by another of our research projects, the (CS)²AI-KPMG Control System Cyber Security Annual 2024 Report 2024 (pg 33). They provide the foundation for continuous improvement in security practices, informing strategic decisions on security investments, policy adjustments, and technological enhancements.



The survey responses highlight the critical role of control system security assessments in maintaining and enhancing the cybersecurity posture of OT environments.

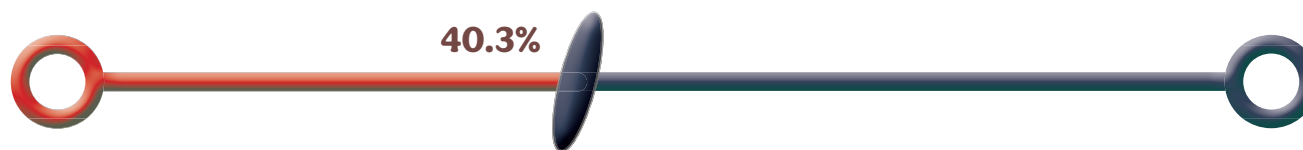
As organizations navigate the complex cybersecurity landscape, the frequency and approach to these assessments become key factors in ensuring the security and resilience of critical infrastructure.

Key Findings

High Proportion of Legacy Assets: The average percentage of 40.3% legacy, outdated, or EOL assets indicates a substantial portion of the operational technology landscape that may not be operating under the latest standards of security, efficiency, or compatibility. Many organizations struggle to manage and update their asset base amid rapidly evolving standards and cybersecurity threats.

Significant Visibility Gap: Lack of visibility into over 38% of the network indicates a substantial portion of OT/ICS/IloT environments remains unmonitored by existing tools. This can obscure potential vulnerabilities, ongoing unauthorized activities, or inefficiencies within these critical networks.

Q: What percentage of your OT/ICS/IloT asset base is legacy, outdated or end of life (EOL) (for service providers, your clients'?)



Q: How much of your (or, for service providers, your client's) overall OT/ICS/IloT network is not currently visible (e.g. no telemetry from host or network based visibility tools)?



The prevalence of legacy and outdated systems within OT environments illustrates a substantial challenge in maintaining modern cybersecurity standards across critical infrastructure systems. Whether due to the long life spans of some OT/ICS technologies, or the short life span of the IoT/IloT companies/manufacturers, this high percentage points to legacy technologies that are intertwined with critical operational processes.

The persistence of outdated systems is a serious concern, as these systems may not support modern security measures or receive necessary updates to defend against contemporary cyber threats. The presence of a large proportion of legacy systems underscores the need for specialized approaches to cybersecurity that can accommodate the unique vulnerabilities of older technologies. It highlights a crucial area for improvement in terms of resource allocation, technology upgrades, and strategic planning for secure and updated solutions.

The extent of network visibility in OT environments is concerning. This substantial visibility gap poses significant challenges for effective cybersecurity management, as unidentified or unmonitored parts of the network can easily become hotspots for security breaches. The data underscores the critical need for comprehensive network monitoring tools that can provide deeper insights into all aspects of OT infrastructures, for all network traffic.

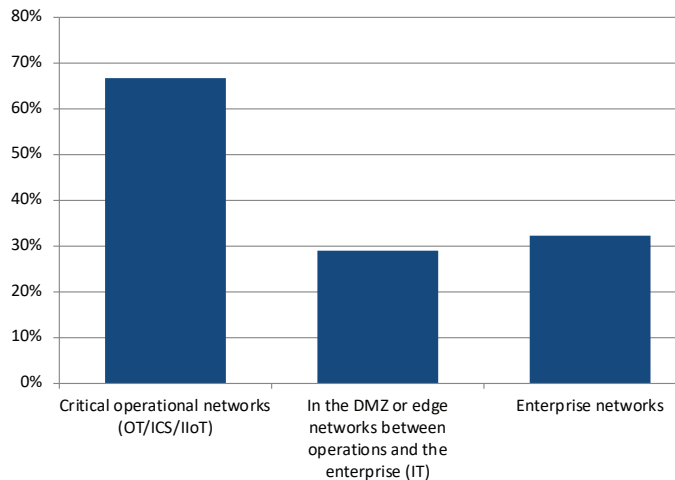
This lack of visibility affects overall network performance. The survey suggests that network visibility should be a priority for organizations aiming to bolster their cybersecurity defenses and improve operations. Investing in advanced monitoring technologies and integrated security platforms could help bridge this visibility gap, enabling more informed cybersecurity strategies. This approach would enhance operational efficiency by providing a clearer understanding of operational behavior, network activities, and potential vulnerabilities.

The survey data highlights a critical area of concern within OT/ICS/IloT security and operations, emphasizing the need for strategic investments in updated technologies and visibility-enhancing technologies and practices. As organizations strive to close the visibility gap, a comprehensive approach that incorporates technological, procedural, and strategic elements will be key to securing and optimizing these vital networks.

“ If we consider the rough estimates that 70% of enterprise customers with OT environments are struggling to define security programs, it's clear that past efforts at achieving basic visibility—relying on serviceable but mostly passive technologies—have had limited benefits and high rates of false positives. These efforts have taught us several key lessons. First, true visibility can only be attained through a combination of passive, active (despite its various marketing euphemisms), and integration-based discovery methods. This includes leveraging existing infrastructure, software, and network artifacts to enhance context awareness and asset detail. Second, no single vendor can address these challenges alone. We are now witnessing niche vendors integrating, collaborating, and partnering with ecosystem and infrastructure providers to offer more comprehensive solutions. Finally, cultural biases between OT and IT continue to cause significant issues, including breaches and incidents, largely due to poor cyber hygiene and neglected attack surface management. It's encouraging to see more organizations recognizing the need for IT and OT to work together, share information and processes, and adopt frameworks that promote organizational maturity, ultimately leading to better security and more effective investments.

Insight from: Jay Gignac, Head of Global Sales & Marketing
Framatome Cyber, Cyberwatch & Foxguard

Q: If you have network blind spots, are they in... (for service providers, please answer for your clients' networks)



Implications for Security and Risk Management:

The prevalence of blind spots within critical operational networks underscores a significant security and risk management challenge. Lack of visibility in these areas means potential vulnerabilities or ongoing unauthorized activities may go undetected, increasing the risk of successful cyberattacks with severe consequences for safety and productivity.

Enterprise Network Visibility as Part of a Holistic Strategy:

While the focus on OT/ICS/IIoT network visibility is critical, the findings also emphasize the importance of maintaining visibility across enterprise IT networks. Comprehensive security strategies should therefore encompass both OT and IT domains, recognizing that vulnerabilities in one area can have implications for the other.

Future Directions in Network Visibility: As OT and IT networks continue to converge, and as the complexity of cyber threats evolves, enhancing network visibility will remain a pivotal aspect of cybersecurity strategies. The integration of advanced analytics, artificial intelligence, and machine learning technologies may offer new opportunities to identify and address blind spots across operational and enterprise networks to detect issues that may originate (or pivot) in IT with a trajectory toward the OT environment.

Key Findings

Critical Operational Networks Most Affected:

A significant majority, 66.67%, indicate that their network blind spots are primarily in critical operational networks. This highlights the challenges in achieving comprehensive visibility within these environments, which are crucial for the safe and efficient operation of industrial processes.

DMZ/Edge and Enterprise Networks:

Both DMZ/edge networks and enterprise networks are identified as areas with blind spots by 28.89% and 32.22% of participants, respectively. This suggests that while efforts may be made to secure the core operational environment, the interfaces between OT and IT, as well as the broader IT networks, also suffer from visibility issues.





Implementation

2



Key Findings

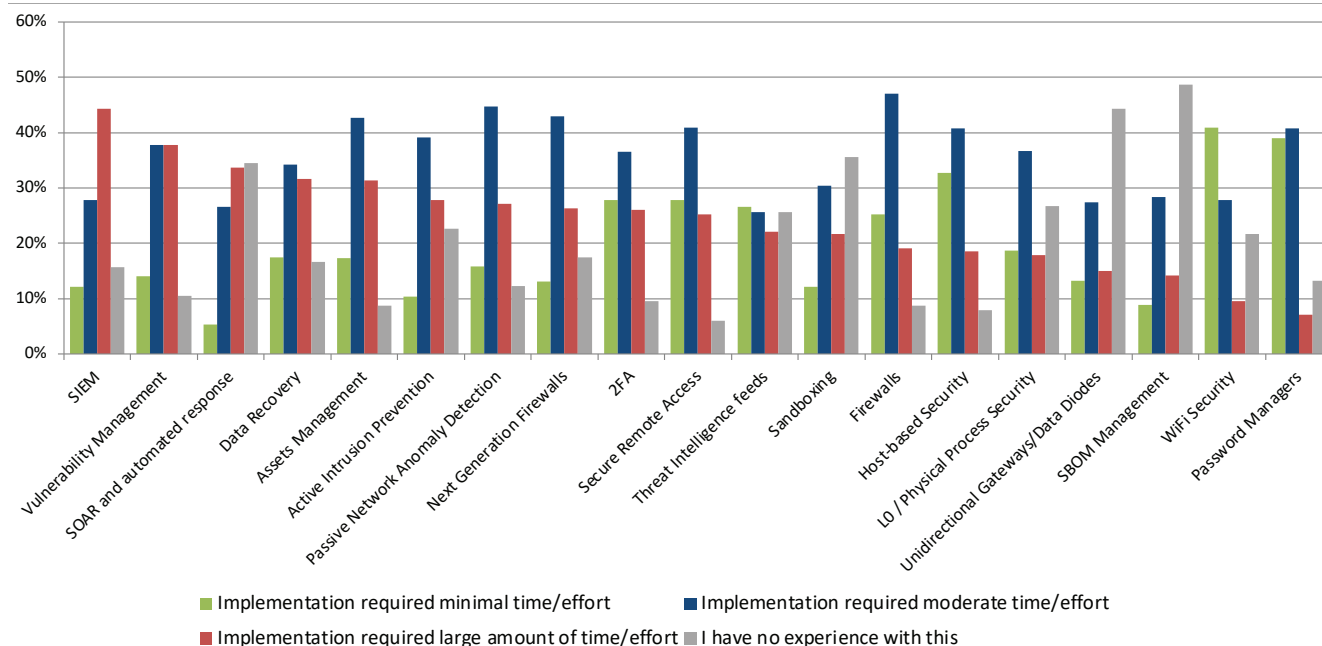
Easier to Implement: Password Managers (38.68% minimal effort) and WiFi Security (39.81% minimal effort) are seen as the easiest technologies to implement, suggesting that their deployment processes are well-understood and straightforward, potentially due to mature technology solutions and widespread adoption in both IT and OT contexts.

Moderately Challenging: Technologies such as Firewalls (47.22% moderate effort) and Secure Remote Access (42.59% moderate effort) are perceived to require a moderate amount of time and effort for implementation. This could reflect the necessity to tailor these solutions to specific operational contexts and security requirements.

Considerably Challenging: SIEM systems (46.30% large effort) and SOAR (33.96% large effort) are viewed as requiring significant implementation efforts. These technologies, essential for advanced threat detection, management, and response, may pose challenges due to the complexity of integrating vast amounts of data and the need for customization.

High Variability in Experience: The implementation effort for Next Generation Firewalls, Passive Network Anomaly Detection, and Vulnerability Management shows considerable variability, suggesting differences in organizational capabilities, the specific technologies selected, and possibly the scale of deployment.

Q: In your experience, how is the implementation effort of these technologies/solutions?



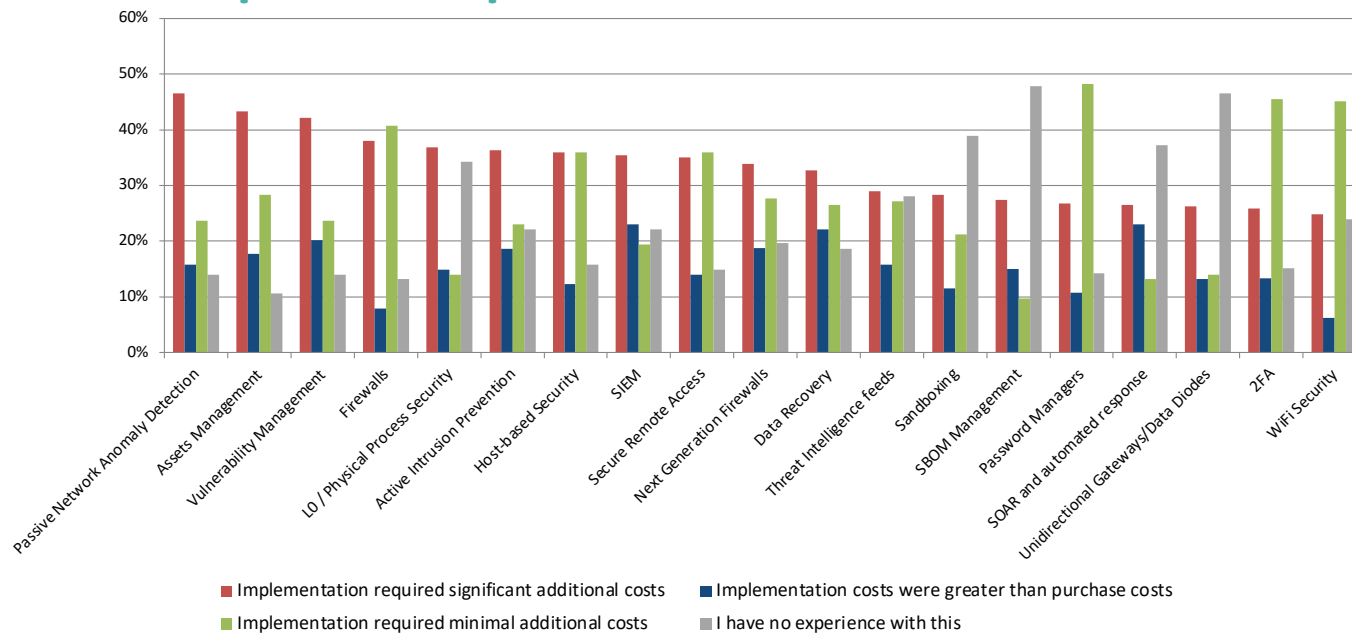
Correlation with Technological Complexity and Integration Depth: Technologies perceived as more challenging to implement often involve deeper integration with existing systems and processes or require a significant amount of customization to meet specific security needs. This complexity underscores the importance of comprehensive planning, skilled resources, and vendor support in successful technology deployments.

Influence of Organizational Maturity: Organizations with advanced cybersecurity practices may find it easier to implement complex technologies due to existing expertise and infrastructure. Conversely, those in the earlier stages of cybersecurity maturity might struggle more with implementation, reflecting a learning curve and the need for capacity building.

Impact on Adoption Decisions: The perceived effort required for implementation can significantly impact adoption decisions, especially for resource-constrained organizations. Technologies perceived as less challenging may be more quickly adopted, while those viewed as requiring more effort might see delayed or hesitant adoption, potentially leaving security gaps unaddressed.

Strategic Implications for Cybersecurity Planning: Understanding the implementation effort is crucial for strategic cybersecurity planning. Organizations must balance the need for advanced security capabilities with the realities of implementation challenges, ensuring that the chosen technologies align with operational capacities and long-term security objectives.

Q: In your experience, how does the implementation cost of these technologies/ solutions compare with their purchase cost?



Strategic Investment Considerations: The survey data underscores the importance of considering the total cost of ownership when selecting cybersecurity technologies for OT environments. Organizations must weigh not only the purchase price but also the anticipated costs associated with integration, customization, ongoing maintenance, and potential operational impacts.

Complexity and Customization Factors: Technologies requiring significant additional or greater implementation costs often involve complex integration challenges or need extensive customization to align with specific operational requirements. This complexity underscores the necessity for comprehensive planning and potentially specialized expertise to ensure successful deployment.

Value of Simplified Solutions: The relative ease of implementing solutions like Password Managers and WiFi Security reflects a market preference for technologies that offer straightforward deployment. This preference signals a broader trend towards adopting cybersecurity solutions that balance effectiveness with ease of integration.

Impact on Adoption Decisions: The perceived implementation cost can significantly impact adoption decisions, particularly in resource-constrained environments. Technologies perceived as having high implementation costs may face longer evaluation periods or require more substantial justification based on their expected value and ROI.

Evolving Cost Dynamics: As cybersecurity technologies evolve, so too do their implementation costs relative to purchase costs. Emerging solutions may initially present higher implementation challenges and costs, but these can decrease over time as solutions mature, integration practices improve, and organizations gain experience.

The data highlights critical considerations for organizations as they navigate the cybersecurity technology landscape within OT environments. Understanding the full spectrum of costs associated with deploying these technologies is crucial for making informed decisions that align with both security objectives and financial constraints. As organizations continue to prioritize cybersecurity, aligning strategic investments with operational needs and total cost considerations will be key to ensuring robust and cost-effective security postures.

Key Findings

Technologies with Minimal Additional Costs: Password Managers (47.62%) and WiFi Security (44.34%) are perceived to require minimal additional costs beyond purchase, suggesting their implementation is straightforward and does not significantly increase the total cost of ownership.

Significant Additional Costs: Technologies like Passive Network Anomaly Detection (46.73% significant additional costs) and Assets Management (42.45%) are seen as requiring significant extra investment beyond the purchase price, indicating that their deployment may involve complex integration or extensive customization.

Costlier Implementation than Purchase: For some technologies, a notable percentage of respondents indicate that implementation costs were greater than the purchase costs, such as Next Generation Firewalls (19.05%) and Data Recovery (23.58%). This suggests that the total cost of ownership for these solutions can be considerably higher than initial acquisition expenses.

Variability in Experience: The responses also highlight a variability in experiences with implementation costs, as evidenced by the proportion of respondents without experience in these implementations across various technologies.

We Asked ICS/ OT Cybersecurity Professionals...

What do you wish all cyber security technology providers understood better about your environment or business?

What practice or approach do you wish cybersecurity technology providers would stop doing?

Are there any practices or approaches you think the most effective cybersecurity technology providers use?





Direct Feedback

Key Findings

This question addresses respondents' satisfaction with cybersecurity technology providers' efforts to understand and address the specific challenges of OT environments. The data reflects a significant positive response, indicating that a majority of respondents feel that providers are genuinely attempting to tailor their solutions to meet the unique demands of OT systems. This suggests a growing alignment between technology providers and the operational needs of these environments, likely influenced by increased dialogue and collaboration between these entities.

However, while the overall sentiment is positive, there remains a segment of the OT community that is less satisfied with the providers' efforts. This divergence in perceptions may highlight areas where providers can improve, such as deepening their technical engagement, enhancing support services, or developing more specialized solutions that address less common but critical OT challenges.

These responses convey a clear message for cybersecurity technology providers: a deep understanding of the unique aspects of OT environments, coupled with a collaborative, flexible, and strategic approach, is crucial for developing and implementing effective cybersecurity solutions. As the OT cybersecurity landscape continues to evolve, fostering strong partnerships between technology providers and OT professionals will be key to addressing the complex challenges and ensuring the resilience of critical infrastructure.

Q: What do you wish all cybersecurity technology providers understood better about your environment or business?

Not everything is connected to a network. A lot of devices may not be air gapped but data exchange to the "outside" world (IT and above) is minimal.

What the OEM says is acceptable

How their products create ROI

Understand that OT Staff in the plant should be well trained, engaged and it is key to be involved early in the projects. It seems they only focus on IT Staff and just promote network based security.

As a System Integrator, I miss an specific and direct approach "to me". I mean, in conferences, advertisements, etc. the target is always the final client (usually a great company) and providers are only mentioned as the weak link in the chain so "they" must be controlled and must be required to (bla bla) by "you" (the great company). As an Integrator, I have different clients with different needs and different requirements; but I'm trying to find a common base criteria in order to anticipate and be prepared to reduce the work when accomplishing the specific requirements of a new client or installation.



“ I have more production impact due to security tools breaking my environment than hackers.”

- SVP, Cyber Defense

That there are things that are not my fault, but are my problem.



Strategic Collaboration: The feedback underscores the importance of strategic collaboration between OT professionals and cybersecurity technology providers. Providers should strive to become partners in securing OT environments, understanding the specific challenges and requirements of their clients, and working together to develop effective cybersecurity strategies.

Sector-Specific Solutions: Given the wide range of industries within the OT domain, as indicated in previous questions, there's a need for sector-specific cybersecurity solutions. Providers that understand the unique threats and operational challenges of specific sectors can offer more relevant and effective security measures.

Advancing OT Cybersecurity Maturity: The insights from respondents highlight a collective effort to advance the cybersecurity maturity of OT environments. This involves not just implementing technological solutions but also addressing organizational, procedural, and human factors that influence cybersecurity outcomes.

Empowering OT Personnel: Emphasizing training, education, and the engagement of OT personnel in cybersecurity initiatives can empower those who are on the front lines of operating and protecting critical infrastructure. This approach fosters a culture of security awareness and collective responsibility for cybersecurity within organizations.

Navigating Resource Constraints: The responses also reflect a realistic understanding of the resource constraints often faced in OT cybersecurity, including budget limitations and staffing challenges. Providers that offer efficient, scalable, and easy-to-implement solutions can help organizations maximize their cybersecurity investments and achieve better security outcomes with limited resources.



Key Findings

Avoid Solution-first Approaches: A common theme is the frustration with providers who push solutions without fully understanding the unique context and needs of the client's environment. This includes fear-based marketing and offering one-size-fits-all solutions that may not align with challenges specific to OT environments.

Importance of OT vs. IT Distinction: Several responses highlight the critical difference between OT and IT environments, emphasizing that availability and reliability often supersede confidentiality and integrity in OT. Providers are encouraged to tailor their approaches and solutions to respect these priorities.

Skepticism Towards Overhyped Features: There is a clear call for honesty and transparency, with criticisms directed at providers overhyped capabilities or claiming exclusivity in offerings that are widely available. The use of buzzwords and exaggerated security claims, without substantial evidence or understanding of practical implementation, is also discouraged.

Challenges with Implementation and Integration: Respondents express concerns over the complexity and cost associated with implementing and integrating new cybersecurity technologies. They wish providers would acknowledge the real-world challenges of fitting new solutions into existing OT infrastructures, especially considering legacy systems and the importance of seamless operational continuity.

Desire for Meaningful Engagement: There is a plea for providers to move beyond transactional interactions, such as cold calls and unsolicited calendar invites, towards more meaningful and consultative engagement that genuinely addresses the needs and challenges of OT environments.

Q: What practice or approach do you wish cybersecurity technology providers would stop doing?

Saying that they are the *only* ones who do something, when in reality, many others offer the same solution. I'd rather hear what they do better - acknowledging that there are multiple approaches.

Recommending the latest, rather than a staged approach. Please do not dump all the new products you got on your shelves"

Selling point solutions outside of the context of a holistic program/strategy.

Thinking their technology has no affect or effect on production.

They should refrain from making exaggerated or unsubstantiated security claims about their products. Honesty and transparency about a product's capabilities and limitations are essential to building trust with customers. Providers should also not operate in isolation. Collaborating with security researchers, industry peers, and customers can help identify and address vulnerabilities and threats effectively.



STOP

“ **Claiming Air Gap. In today’s environments, it is very rare to have an actual air gapped network.** ”

Fear mongering. While true, it turns a lot of people off. They stop listening.



Strategic Partnership over Vendorship: The feedback underscores a desire for cybersecurity technology providers to act as strategic partners rather than mere vendors. This partnership involves a deeper understanding of the client’s operational context, collaborative planning for security implementations, and support throughout the technology lifecycle, including transparent communication about product limitations and collaborative problem-solving.

Educational Approach to Cybersecurity: Professionals wish for an approach that educates and informs rather than alarms, highlighting the need for cybersecurity education and awareness that complements technological solutions. Providers are encouraged to focus on building knowledge within client organizations, helping them understand their own cybersecurity landscape better and make informed decisions, leveraging innovative tools like cyber ranges and immersive labs.

Customization and Flexibility: The diverse needs of different OT environments call for customizable and flexible solutions. Providers should focus on offering modular and scalable options that can adapt to varying levels of cybersecurity maturity, from foundational practices to advanced threat detection and response capabilities.

Holistic Cybersecurity Strategy: Emphasizing the need for a holistic approach to cybersecurity, respondents advocate for solutions that fit within a broader strategic framework rather than isolated point solutions. This approach acknowledges the interconnected nature of cybersecurity challenges and the importance of addressing them through comprehensive strategies.

Building Trust through Transparency and Collaboration: Trust emerges as a crucial factor in the provider-client relationship, with a call for greater transparency, honesty, and collaboration. Cybersecurity technology providers can foster trust by openly discussing the strengths and limitations of their offerings, engaging in collaborative problem-solving, and actively participating in the broader cybersecurity community to address



Q: Are there any practices or approaches you think the most effective cybersecurity technology providers use?

Regular system audits for segmentation and user anomalies. Change tracking and asset health monitoring are value adds that can help engage onsite teams to ensure security programs stay active and useful to them.

Start talking about cybersecurity at the start of the earliest design phase, use IEC-62443-2-4

Really in depth and slow and patient training for on-premises staff

When they have a scalable product/solution/service that a customer can adopt at their level of cyber maturity.

Mature secure programming practices, and clear understanding and disclosure of all 3rd party libraries included in their products -- and notification if vulnerabilities/updates in any of these have been identified.

Listening to Real-Life Situations: Emphasizing the importance of understanding the unique operational realities of clients, highlighting the need for cybersecurity solutions to be grounded in the practical challenges and requirements of OT environments.

Simplicity and Clarity: The call for keeping solutions and communications simple underscores the importance of accessibility and ease of integration for cybersecurity technologies, ensuring they can be effectively utilized without undue complexity.

Collaboration and Coordination: A strong theme of collaboration amongst all stakeholders, including vendors, clients, and industry partners, points to the value of a cooperative approach to cybersecurity, where knowledge and resources are shared for mutual benefit.

Early Inclusion in Design Phases: Incorporating cybersecurity considerations at the earliest stages

of system design and development is highlighted as a critical practice, enabling the proactive mitigation of risks and integration of security measures.

Threat Intelligence-Based Approaches:

Leveraging threat intelligence to inform cybersecurity strategies and product development is recognized as beneficial, allowing for more targeted and effective defenses against evolving threats.

Transparency Over Vulnerabilities: Openness about vulnerabilities and sharing best practices for mitigation reflect a trust-building approach, where providers support their clients not just with tools but with valuable knowledge for enhancing security.

Certification and Standards Alignment: The alignment of products and services with recognized standards like IEC/ISA 62443 and ensuring certification are viewed as marks of quality and reliability in cybersecurity solutions.



Operational
Security
Engineer
Risk
Head
Industrial
Consulting
Specialist
Analyst
Trends
Automation
Division
SSE
Operations
Services
Working
Vertical
Defense
Junior
Practice
CCO
Leader
System
CISO
NIS2
QA
audits
Software
Cibersecurity
Crypto
Sales
CEO
Solutions
Manager

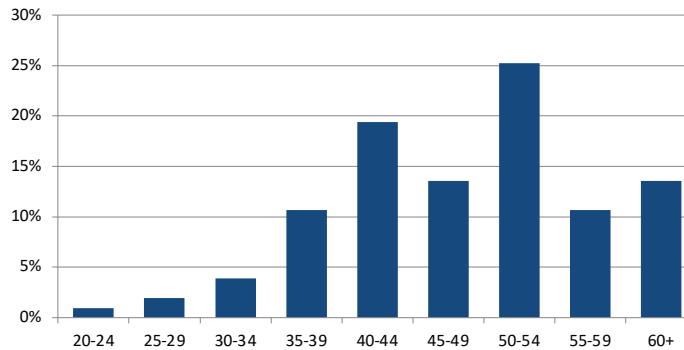


+

Demographics

Basic Demographics

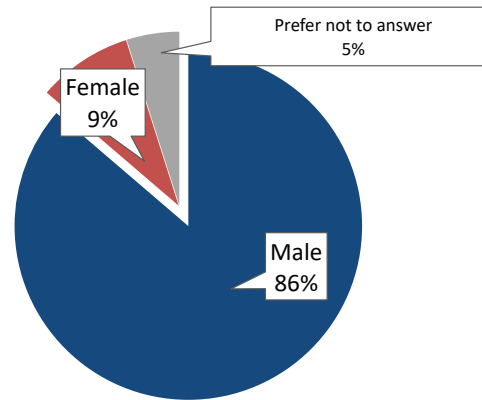
Q: What is your age?



Age: The survey data reveals a predominantly mature workforce, with a significant proportion of respondents aged 50-54, followed by those in the 55-59 age bracket. This trend highlights the accumulation of extensive experience and expertise within the sector.

Interestingly, the survey also shows participation from younger age groups, although to a lesser extent, adding validity to the ongoing efforts to attract new talent into the field. The presence of these younger professionals is essential for the continual infusion of fresh ideas and contemporary skills, which are necessary to keep pace with rapid technological advancements and evolving cyber threats. This age diversity within the cybersecurity workforce suggests a dynamic intergenerational exchange that can create some communication challenges, but also enhances the robustness and adaptability of cybersecurity strategies in OT environments.

Q: What is your gender?



Gender: We polled the gender distribution of professionals working within the cybersecurity field of operational technology (OT). The data shows a significant predominance of male professionals, making up 85.57% of respondents, which aligns with the broader trend often observed in the tech and cybersecurity sectors. This highlights a continuing gender disparity within the field, underscoring the need to better understand the skills, improve hiring and application processes, and make available jobs more attractive to a broader talent pool.

Interestingly, while the female representation remains low at 9.28%, the survey indicates efforts to recognize and perhaps bridge this gap, with initiatives or discussions possibly underway to increase gender diversity. This demographic snapshot not only sheds light on current workforce composition but also potentially sets the stage for future diversity and inclusion efforts aimed at enriching the cybersecurity domain with a wider range of perspectives and skills.

Further Note on Gender

Implications for Diversity and Inclusion:

The gender distribution within the OT cybersecurity workforce underscores the importance of continuing efforts to enhance diversity and inclusion within the field. A more diverse workforce can contribute a wider range of perspectives, experiences, and solutions to the complex challenges of cybersecurity, fostering innovation and resilience.

Addressing Gender Diversity Challenges:

The relatively low percentage of female respondents reflects broader challenges in attracting and retaining women in cybersecurity roles. Addressing these challenges requires concerted efforts across education, recruitment, retention, and career development processes to create more inclusive and supportive environments for women and other underrepresented groups.

Educational and Career Pathways:

In the context of the educational background and age distribution data previously discussed, the gender distribution prompts further consideration of how educational and career pathways into OT cybersecurity might differ. Encouraging diverse participation from an early educational stage, offering mentorship opportunities, and highlighting role models from underrepresented groups could help broaden the talent pipeline.

Q: What is the highest level of school you have completed or the highest degree you have received?

Key Findings

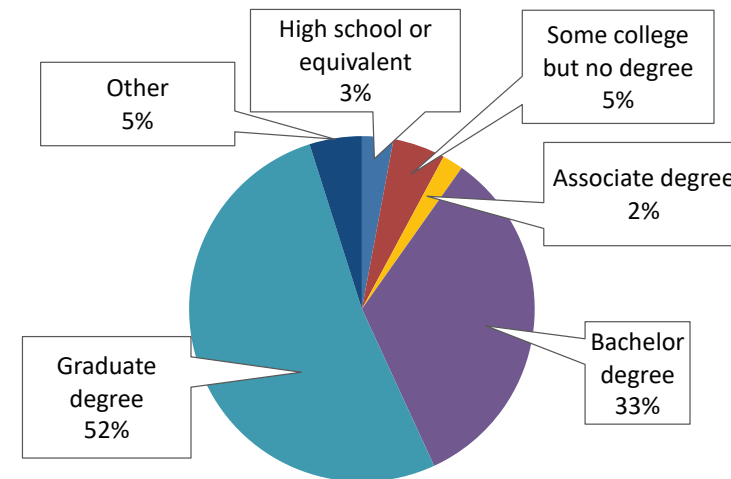
Broadening the Talent Pool: While the data shows a highly educated workforce, the presence of professionals with varied educational backgrounds highlights the diverse paths through which individuals can enter the field of OT cybersecurity. This diversity is essential for building a robust talent pool with a wide range of skills and perspectives.

Future Trends in Education and

Cybersecurity: The demand for advanced cybersecurity skills in the OT domain may continue to influence educational trends, with an increasing number of professionals seeking graduate-level education or specialized training in cybersecurity. Furthermore, the integration of OT-specific content into cybersecurity education and training programs could further enhance the preparedness of the workforce.

Linking Education to Implementation

Challenges: The educational background of professionals may also inform the implementation efforts and costs associated with cybersecurity technologies, as seen in previous data. A higher level of education could correlate with a more effective and efficient implementation process, though challenges related to complex technologies and integration requirements remain.



Education: We examined the educational backgrounds of the cybersecurity professionals engaged in protecting operational technology environments. The survey results highlight a highly educated workforce, with a significant portion of respondents holding graduate degrees. This underscores the complexity and critical nature of OT cybersecurity, requiring a deep understanding of technology, engineering/safety, and security practices.

Notably, the prevalence of advanced degrees among respondents suggests a strong correlation between higher education and the roles that

demand sophisticated skills in threat assessment, system protection, and compliance with rigorous industry standards. This trend indicates that the OT cybersecurity sector values formal education, which likely provides the theoretical and practical foundations necessary for handling the intricate challenges present in securing industrial control systems. The educational background of these professionals not only enhances their ability to design and implement effective security measures but also prepares them to innovate and operationally adapt to the rapidly evolving cyber threat landscape.

The survey data highlights the highly educated nature of the workforce involved in OT cybersecurity, emphasizing the role of advanced education in equipping professionals to address the sophisticated challenges of securing operational technology environments. As the field continues to evolve, the educational qualifications of cybersecurity professionals will remain a critical factor in advancing cybersecurity practices and ensuring the resilience of OT systems against emerging threats.

Industry and Sector Profiles

Q: In which sector do you primarily work??



Information Technology: Following closely with 17.66%, this sector's strong presence reflects the intertwined nature of IT and OT cybersecurity, underscoring the importance of securing information systems that support operational technologies across all industries.

Energy (Electric): The largest single-industry segment representation at 13.77%, indicating a significant concern for cybersecurity within the electric energy sector. This could be due to the critical nature of energy infrastructure and the high stakes associated with potential cyber-attacks.

Manufacturing (Critical): With 11.98%, critical manufacturing sectors are also significantly represented, highlighting concerns over the cybersecurity of systems that are essential for the production and distribution of critical goods.

Energy (Oil & Gas): With 7.78%, the oil and gas sector shows notable participation, similar to the electric sector, emphasizing the importance of cybersecurity in protecting energy resources and infrastructure.

Other: This category garnered 13.47%, indicating a variety of sectors not explicitly listed in the survey but which still hold significant interest in OT cybersecurity.

The significant presence of respondents from the Information Technology sector signals the growing recognition of cybersecurity as a critical component of IT operations, reinforcing the need for advanced protective measures in this area. Similarly, the substantial focus on the Energy sector, particularly electric, points to the strategic importance of securing energy infrastructures, which are often targets of sophisticated cyber-attacks due to their critical role in national security and economy. These findings reflect a broader trend towards prioritizing cybersecurity efforts in sectors that are crucial to national and economic stability, driving demand for tailored cybersecurity solutions that address the specific risks and regulations of these industries.

Key Findings:

Sector-Specific Cybersecurity Challenges:

The varied industries highlight subsector-specific challenges in OT cybersecurity. For instance, the Electric Power sector faces the dual challenge of ensuring the reliability of power distribution and safeguarding against cyber-physical threats, whereas the Manufacturing sector must contend with protecting industrial control systems alongside ensuring product integrity.

Importance of Cross-Sector Collaboration:

The presence of professionals from a broad spectrum of sectors underscores the potential benefits in sharing best practices, threat intelligence, and technological solutions to common cybersecurity challenges.

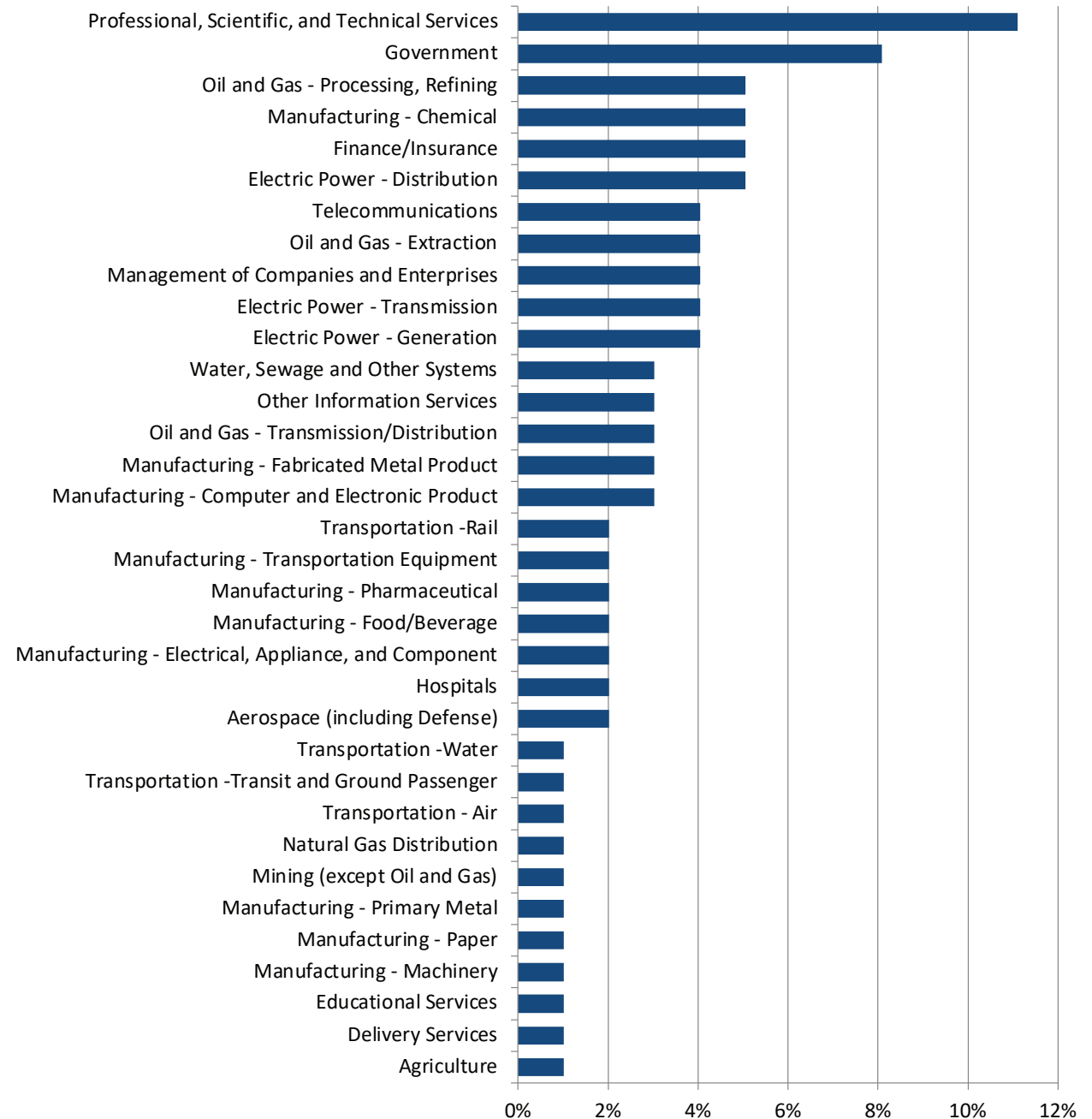
Impact of Regulatory and Compliance

Requirements: Different sectors face varying regulatory and compliance requirements, influencing their cybersecurity strategies and priorities. For example, the Government and Electric Power sectors may be subject to more stringent regulations.

Future Trends in Sector-Specific

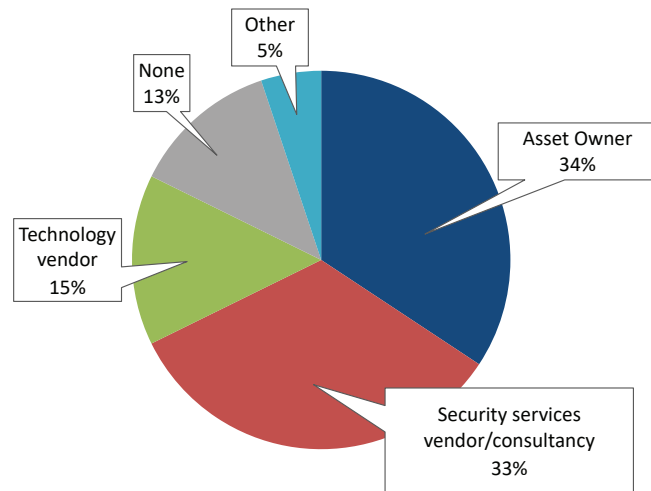
Cybersecurity Needs: As technology continues to advance and the threat landscape evolves, sector-specific cybersecurity needs will also change. Keeping abreast of these trends and fostering a dynamic approach to cybersecurity will be crucial for organizations in all sectors.

Q: To help us gain more detailed industry data, please indicate in which subsector(s) you primarily work



Domain Authority

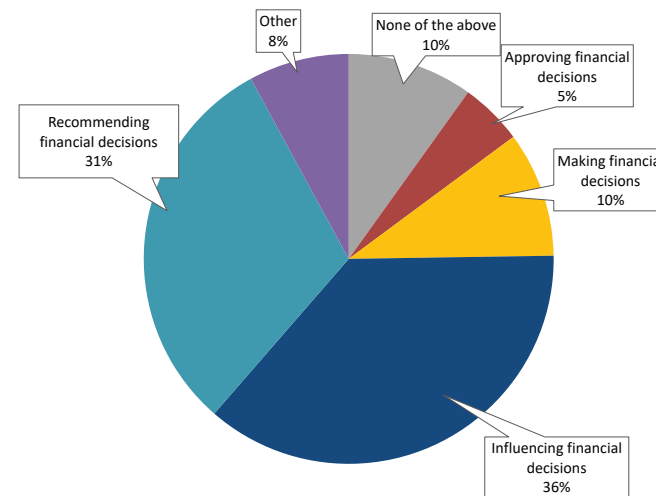
Q: What is your or your organization's category in relation to control system cyber security?



The balanced representation between asset owners and security services vendors/consultants highlights the survey's comprehensive coverage of key stakeholders in OT cybersecurity. This distribution suggests a valuable mix of insights from those who manage and operate OT systems daily and those who advise or support these entities in securing their operations against cyber threats.

The technology vendors' responses are also significant, as they provide the tools and solutions integral to protecting OT environments. Meanwhile, the presence of respondents outside these categories indicates this topic's reach to professionals interested in OT security who may be employed at companies that currently do not focus on it.

Q: Please identify your role in making decisions on control system security-related expenditures?



A significant portion indicated that they are primarily involved in influencing or recommending decisions, rather than having direct authority. This trend suggests that while many OT cybersecurity professionals are key contributors to the cybersecurity strategy, final financial authority often resides with higher executive levels, such as CISOs, IT/OT directors, or facility managers.

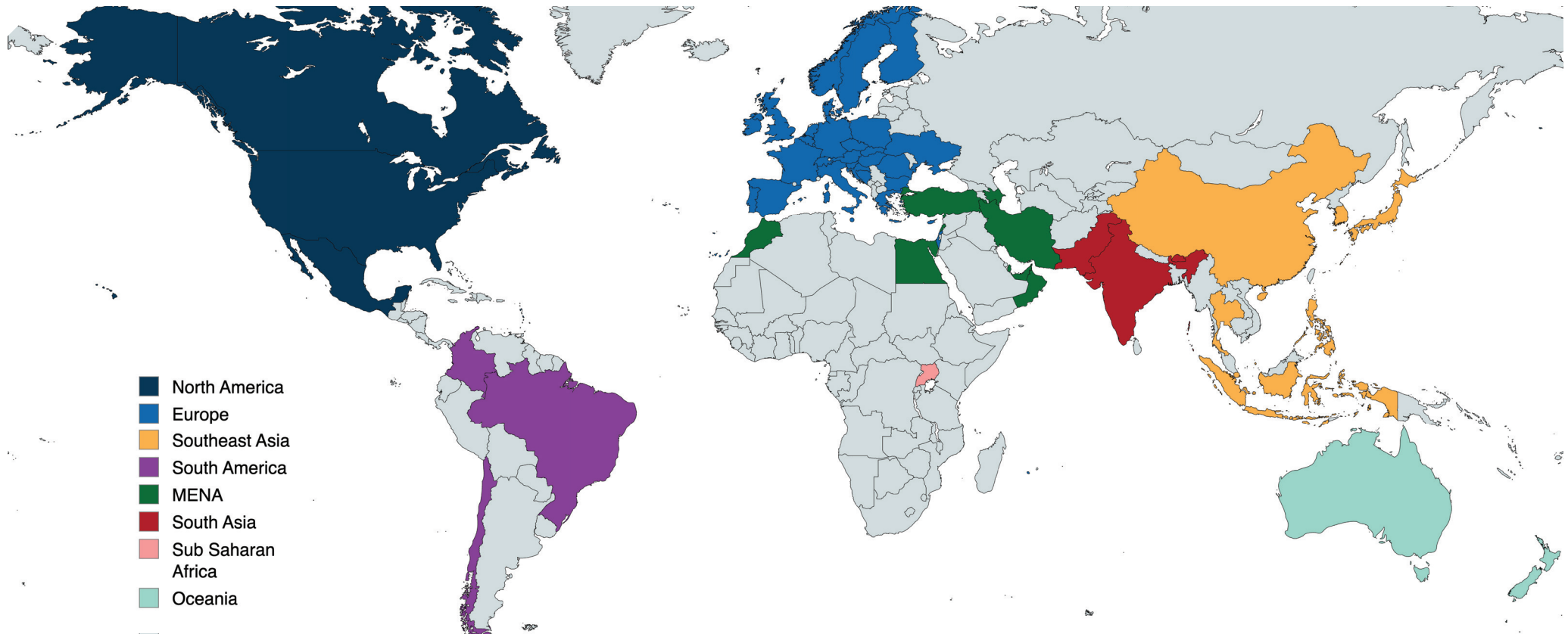
The data also illustrates a collaborative decision-making process within organizations, where multiple roles contribute to the cybersecurity budgeting and strategy discussions. This reflects the complex nature of cybersecurity in OT environments, where understanding the technical, operational, and strategic aspects is crucial for effective risk management. The involvement of various levels within the organization in these decisions underscores the recognized importance of cybersecurity as a critical component of the operation.

Survey Segments

All survey participants were asked to identify their organization's primary function at the beginning of the questionnaire.

Shown in the chart on the left, this breakdown resulted in a nearly even split between individuals working at asset-owning organizations, and security services vendors. The questions were worded so that vendors could answer technical questions on behalf of their clients (or a majority thereof).

Asset owners and security services vendors (comprising more than two thirds of our overall audience) were given access to the entire survey. Technology vendors were asked a limited set of questions wherein their perspective would add to the quality of the feedback and analysis, primarily centered around implementation and maintenance costs of various technological solutions.



Global Survey Participants

This data reveals intriguing trends about the geographical distribution of the respondents. Nearly half (49%) of our responses came from participants in North America, which may reflect this being the region with the greatest concentration of our membership. While this might introduce some NA-centric bias to our results, it remains that technology is a world market, with the same devices and software available without regional distinction.

Europe follows with 29%, highlighting its role as another key player in the global cybersecurity landscape, likely driven by stringent regulatory frameworks such as NIS2, the EU Cybersecurity Act,

and even GDPR, which have broader implications for cybersecurity practices.

Another interesting aspect is the representation from regions such as Asia-Pacific (10%), Latin America (4%), and Middle East/North Africa (4%), which suggests a growing awareness and investment in cybersecurity across diverse geopolitical landscapes.

Varying levels of participation from these regions might indicate differences in cybersecurity maturity, regulatory pressures, or technological adoption rates. This geographic distribution provides valuable insights into where cybersecurity solutions are being prioritized and the potential for market expansion in less represented regions.

In order of percentage of responses: United States of America | Canada | Brazil | India | Spain | Netherlands | Belgium | Germany | Italy | United Kingdom | Australia | Denmark | Ireland | Philippines | Qatar | Israel | Poland | Finland | France | Singapore | Switzerland | United Arab Emirates | Indonesia | Portugal | Sweden | Thailand | Czech Republic | Mexico | Norway | Oman | Austria | Azerbaijan | Bhutan | Bosnia and Herzegovina | Chile | China | Colombia | Croatia | Egypt | Greece | Iran | Japan | Lebanon | Morocco | New Zealand | Pakistan | Republic of Korea | Romania | Turkey | Uganda | Ukraine

(CS)²AI™ Radiflow

This report is a publication of Control System Cyber Security Association, International, (CS)²AI.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The Control System Cybersecurity Association International, a.k.a. (CS)²AI names and logo are registered trademarks.

(CS)²AI is a 501(c)6 nonprofit organization registered in the United States of America.

Report Design by Marsden Media LLC.

© 2024 Control System Cyber Security Association, International. All Rights Reserved.