Publication date:
December 2023

Authors:
Anna Ahrens
Hollie Hennessey

Moving Beyond Visibility

Providing protection to industrial automation networks

OMDIA

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Belden

Contents

Introduction

In the realm of operational technology (OT), unconnected devices created “air gaps,” serving as the paramount defense entrusted by organizations with safeguarding the reliability, safety, and availability of their operations. However, the contemporary OT landscape has undergone a profound metamorphosis, and it now embraces a myriad connected devices, spanning legacy systems and cutting-edge innovations.

Debates surrounding the wisdom of connecting these devices may persist, but the undeniable truth is that a seismic shift is underway. Across industries, an overwhelming majority of organizations are forging unprecedented links between their operational bastions and IT systems. This union is propelled by a strategic imperative for heightened efficiency and unwavering sustainability. The stakes are elevated, the challenges are immense, and the imperative for adaptation is nonnegotiable. In this era of convergence, connectivity between operational and information technologies is not merely a choice but a compelling necessity, propelling organizations to a new frontier where resilience and innovation intersect.

In the relentless pursuit of operational and technological synergy, a cybersecurity risk labyrinth emerges with the convergence of OT and IT connectivity, compounded by the proliferation of interconnected devices. The awareness of this challenge looms large, casting a shadow over the ambitious aspirations of seamless integration. However, the struggle extends beyond mere awareness to grappling with a trifecta of concerns. First, adherence to ever-evolving mandates creates a regulatory tightrope to traverse. Second, the scarcity of resources demands precious allocation of expertise and time. Third, the intricacies of deploying a defensible cybersecurity architecture that can withstand the relentless onslaught of modern threats add an additional layer of complexity, testing the mettle of even the most seasoned organizations. In the OT cybersecurity evolution, the imperative of visibility traditionally took center stage, guided by the principle that “you can’t secure what you can’t see.” Consequently, a multitude of OT and Internet of Things (IoT) cybersecurity solutions have arisen, providing the ability to illuminate the once-shadowy realm of connected devices. These solutions are equipped with the ability to peer into the network and unravel the intricacies of both time-honored legacy systems and cutting-edge Industrial Internet of Things (IIoT) devices.

However, in this dynamic landscape, mere visibility proves insufficient. A new vanguard of controls emerges, reshaping the narrative from reactive to protective fortification. Among these is network access control (NAC), a protector against the incursion of unauthorized devices and users into the network. Far beyond mere observation, these controls introduce multiple layers of defense, unleashing the power to not only identify but prevent cybersecurity breaches. In doing so, they provide a safeguard that mitigates cybersecurity and operational risk.

As the battleground of cybersecurity threats continues to evolve, these controls redefine the rules of engagement, beckoning organizations to embrace not just visibility but both reactive and proactive automated protection. In this era of cyber-resilience, when all devices and users are potential entry points, the call to arms echoes louder than ever: fortify and defend the boundaries of cybersecurity norms.

The key to successful orchestration lies not just in technology but in strategic partnerships. The gaze turns to seasoned allies in the industrial domain, whose wealth of experience guides the selection and implementation of the right solutions.

Omdia, in partnership with Belden, conducted the Secure Industrial OT and IIoT Cybersecurity Networks survey (2023) on cybersecurity to better understand the views and approaches of OT and IT teams, challenges related to visibility, improvements in or deterioration of companies' cybersecurity postures, and the effectiveness of automated access control to companies in the industrial sector.

Key recommendations

- Visibility is a key requirement for many OT networks, but other technologies can aid in areas visibility just cannot reach. Specialized inspection of network traffic can support visibility efforts in mission-critical environments. Automated access control technology can combine monitoring functionality and control quickly while preventing rogue device or user connections from having a detrimental impact on operations or safety.

- Cybersecurity is a collective responsibility that transcends individual roles and resonates across a host of stakeholders. The best technology decisions emerge from collaborative endeavors and the convergence of minds. Historically, IT and OT have operated as distinct realms, but building a resilient future depends upon bridging this gap. To unravel the complexity, it is imperative to decipher the varied priorities and divergent perspectives that shape the cybersecurity landscape. Cooperation is the linchpin of success.

- The path to resilience is not a destination but an ongoing, endless journey. To remain resistant in the face of evolving threats, organizations must recognize the imperative of regular cybersecurity assessments. Assessments are not isolated events; they are an indispensable scrutiny that punctuates the continuous journey of safeguarding operations. These assessments are not mere checkpoints but dynamic processes that go beyond compliance, delving into the core of organizational defenses. The aim is not just to meet regulatory requirements but to craft a shield that adapts and fortifies against the ever-shifting threat landscape.

- OT incident response and forensic data collection and insights are key to aid in recovery from a breach or incident. The aftermath of an incident persists far beyond the breach itself, but the reality is that many organizations find themselves standing on uncertain ground, lacking the crucial capabilities to navigate the aftermath of an OT breach. The imperative is clear: organizations must fortify their arsenal with the capabilities required for OT incident response and forensic insights.

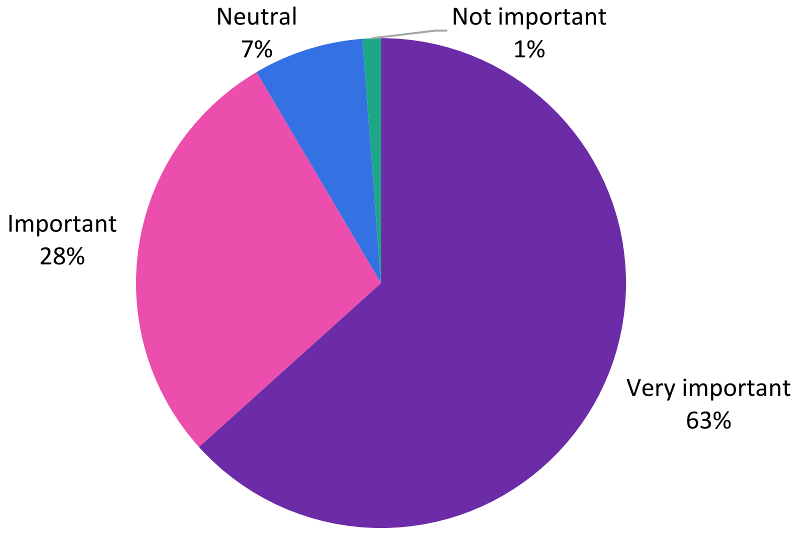
- Technology and services are not mere tools; they are the conduits through which organizations can construct a robust and responsive incident recovery framework. It is not just about filling gaps; it is about transforming weaknesses. The journey toward a resilient cybersecurity posture should be a proactive endeavor, where organizations leverage technology and services to craft a narrative of recovery that outshines the shadow of an incident.

Current visibility in OT networks

To effectively ensure operational safety, comply with regulatory requirements, and support the proactive and systematic strengthening of the network's cybersecurity, organizations require a clear understanding of what is connected, what is happening to these connected assets, and how they are communicating.

Our survey respondents overwhelmingly agreed that this visibility is a critical prerequisite for OT cybersecurity, and this was consistent across all areas of responsibility.

Figure 1: How important is visibility of all devices to your protection?



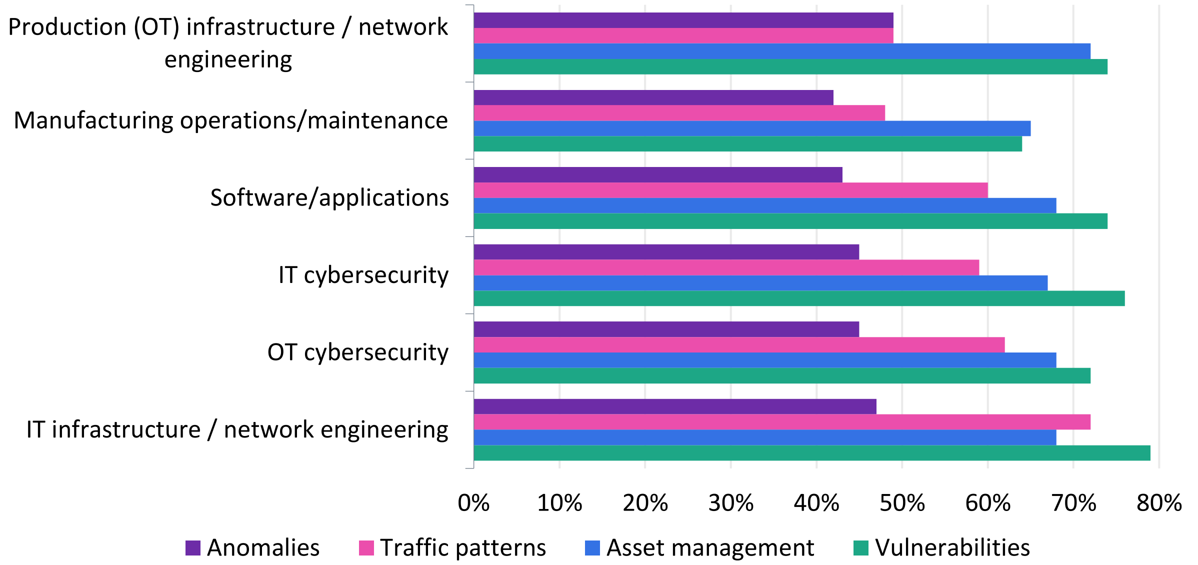
Note: n=330

© 2023 Omdia

Source: Omdia

Visibility is evidently important for many, but often organizations know that they want visibility but not exactly what it is that they want visibility into. Visibility into devices is one criterion, but visibility can also extend to threats, indicators of compromise (IoCs), vulnerabilities, configuration changes, adversary behaviors, log data, misconfigurations, installed software, and anomalies—the list is (almost) endless. Many solutions on the market focus on IP-connected asset visibility and anomaly detection, often using passive data collection techniques, although this has for the most part developed to offer active query methods for more granular discovery. Overall, however, one visibility solution is unlikely to give organizations the comprehensive visibility and coverage that they desire.

Figure 2: Visibility into OT network according to responsibility area



Note: n=330

© 2023 Omdia

Source: Omdia

Omdia’s survey painted a vivid picture of the varied landscape of visibility within the OT network. Across diverse job roles, a hierarchy of visibility emerges with vulnerabilities taking the lead, closely trailed by asset management. However, visibility into anomalies languishes at a mere 43% overall.

This revelation is not just a statistic: it is a resounding alarm. More than half of organizations find themselves navigating uncharted territory, lacking the crucial visibility into anomalies that could signal impending threats to operations and safety. This echoes with potential consequences, a blind spot that demands immediate attention.

The narrative deepens as we delve into the nuances of expertise. IT network professionals, with a commanding view into traffic patterns, stand at a vantage point. Conversely, OT networking professionals find themselves on a lower echelon of visibility. This hints at the imperative for convergence across the network operations center (NOC) and security operations center (SOC). Utilizing both networking and cybersecurity expertise across IT/OT can forge a unified front against the evolving threats.

Access control in OT environments

Though visibility has undeniable value, it is crucial to acknowledge its constraints. The reality is that achieving comprehensive visibility into every facet of networks, especially those traversing both OT and IT realms, is an unrealistic and largely unattained goal for many organizations.

Supplemental controls go beyond visibility into the OT network to protection of the network itself. Though technology is pivotal, effective cybersecurity extends beyond devices to encompass the critical human element, both internally and externally.

Network access control leverages user identity and endpoint data while making network access decisions, defending against unpatched assets, rogue assets, and malware and facilitating controlled guest access for partners and contractors. It achieves this through segmentation and micro-segmentation, proving indispensable in industrial settings by effectively monitoring and securing IoT and OT devices with boundaries.

Modern NAC technologies automate control, easing the burden on cybersecurity professionals in the intricate OT cybersecurity landscape and alleviating the strain of the cybersecurity skills gap. A resounding 88% of respondents recognize the crucial importance of automated network access controls.

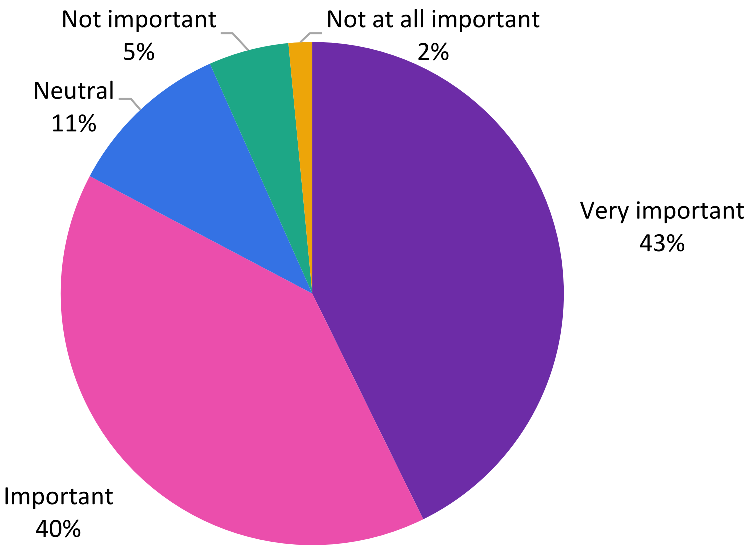
Protecting the industrial environment with purpose-built firewalls

Modern IT firewall technology commonly incorporates signature-based deep packet inspection (DPI) that protects only against known behavior, but its value in OT networks is limited. Off-the-shelf IT networking technology may offer some control, but it often lacks protocol sanity checking support for crucial industrial protocols (e.g., Ethernet/IP, ModbusTCP, DNP3, OPC). The cybersecurity importance of this gap is acknowledged by 83% of organizations, emphasizing that while signature-based DPI is valuable, it falls short without coverage of proprietary industrial protocols in mission-critical deployments that protect against zero-day attacks.

IoT and OT cybersecurity vendors excel by specializing in industrial protocols, down to function codes, from the outset, providing granular protection tailored for OT networks. Their solutions are crafted with an understanding of unique OT communications and network architecture. By contrast, some traditional IT firewall vendors are catching up by incorporating this capability into their portfolios.

Ninety-five percent of those designing or specifying solutions said DPI of industrial protocols is important, perhaps because they have a more niche understanding of requirements. Those involved or contributing to final decisions were more likely to feel neutral on the capability (17%).

Figure 3: How important is DPI capability of industrial firewalls for protocols?



Note: n=330

© 2023 Omdia

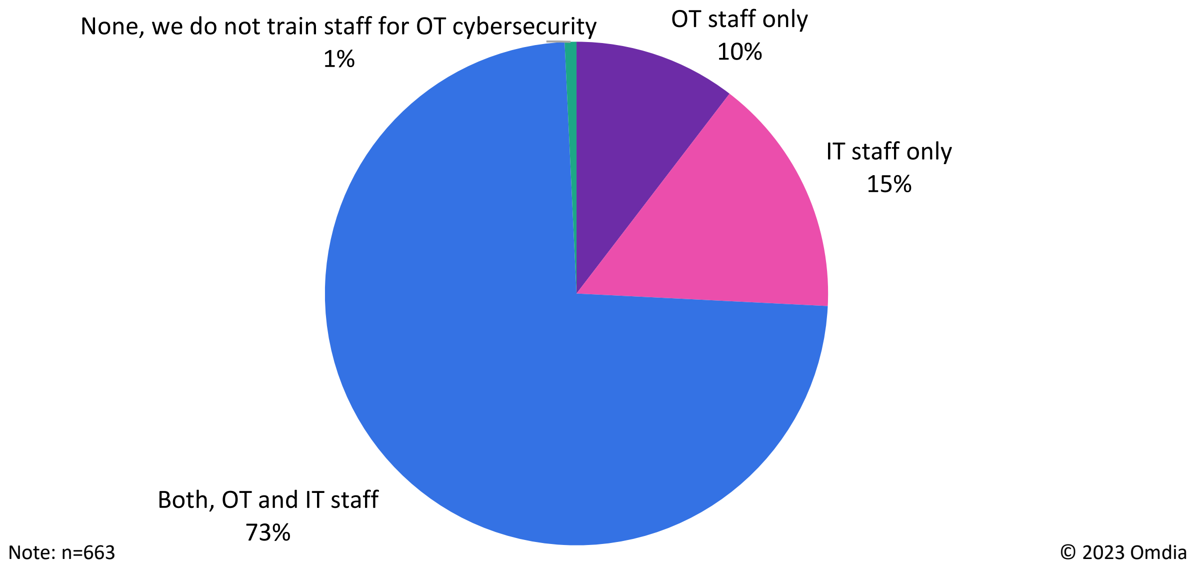
Source: Omdia

Addressing the OT cybersecurity skills gap

Introducing IT-based cybersecurity in OT demands intense interdepartmental collaboration, knowledge transfer, and education on both sides. Historically, OT and IT systems operated in isolation, each with distinct priorities. OT systems prioritize synchronized deterministic control for production continuity and operational safety, historically closed and isolated for protection. Cybersecurity was not a primary concern in OT until recently. By contrast, IT systems, connected and lacking autonomy, faced cybersecurity threats earlier, fostering awareness and the development of dedicated cybersecurity tools.

As companies digitally transform, the convergence of IT and OT is imperative. Teams must integrate, learn new skills, and understand each other’s needs to jointly ensure uninterrupted, safe, and secure operations. Both teams share responsibility for this critical mission.

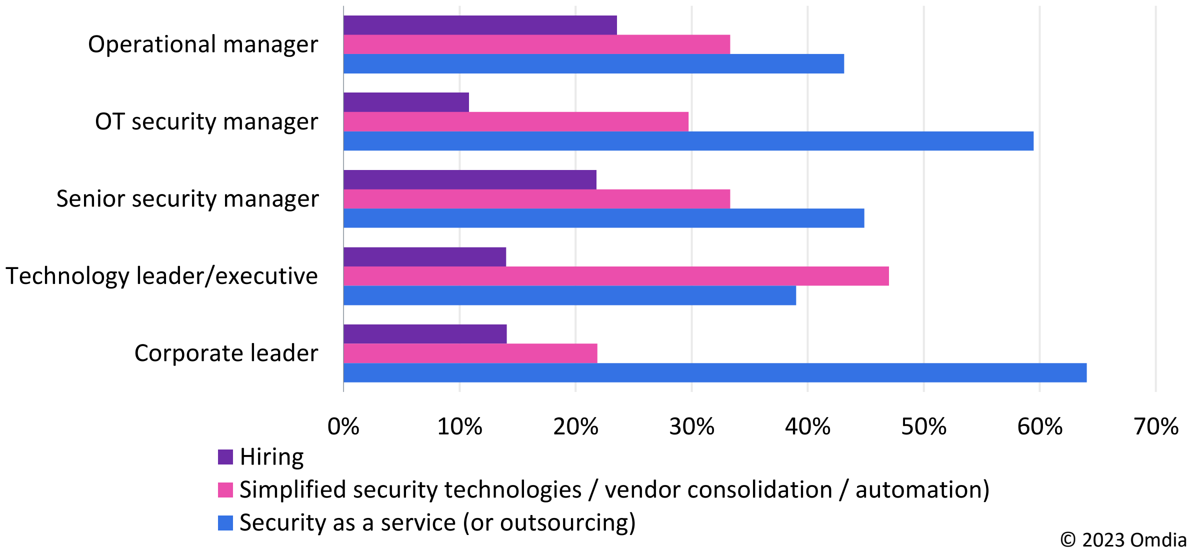
Figure 4: Most train both IT and OT staff on OT cybersecurity, but a significant minority do not



Source: Omdia

Many organizations address the skills gap through simplified security technologies, vendor consolidation, and automation or by using security as a service (or outsourcing).

Figure 5: How the skills gap is addressed, by job role



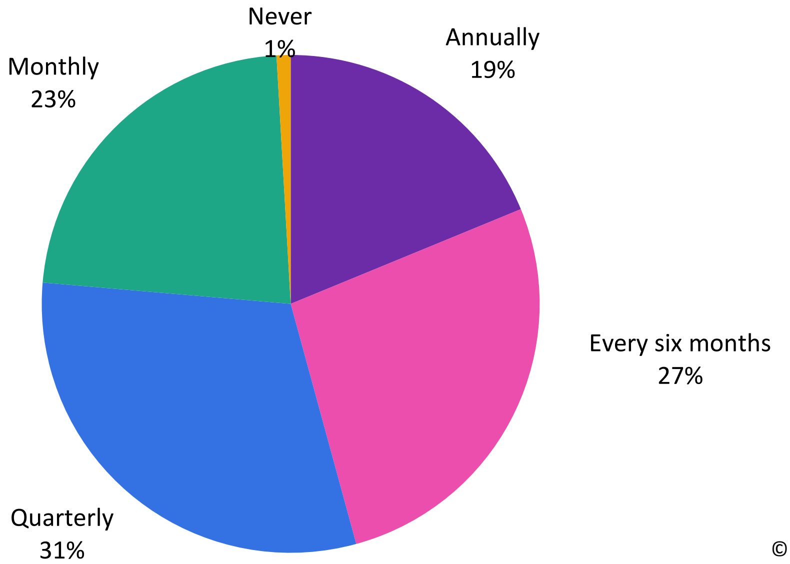
Source: Omdia

For accelerated adoption of OT cybersecurity, companies use diverse approaches. Technology leaders prioritize simplified cybersecurity technologies, vendor consolidation, and automation. Those in technical roles, likely to be closer to and more skilled in technology, align with this preference. Conversely, those in less technical and operationally focused roles lean toward outsourcing, possibly indicating a lack of in-house expertise and a greater reliance on external support. Companies with revenue exceeding $1bn prioritize building in-house competencies through simplified technologies and vendor consolidation, hiring experts. By contrast, smaller enterprises predominantly opt for security as a service. Larger firms have the capability to strategically leverage their resources to develop scalable expertise, while for their smaller counterparts introducing third-party management of cybersecurity can be more effective.

Continuous assessment leads to continuous improvement

Many OT organizations are advancing in their technology deployment, but without proper assessment the risk of ineffective cybersecurity looms. Cyber assessments are essential, and 99% of respondents conduct them annually, following frameworks for continuous improvement. The evolving threat landscape and OT environment necessitate a strategic approach. The level of detail and methodology, crucially, must align with resourcing and skills. Partnering with cybersecurity service providers can guide organizations on the right assessment frequency and level, and they can offer a valuable assessment as a service.

Figure 6: How often are cyber assessments performed in OT cybersecurity?



Note: n=330

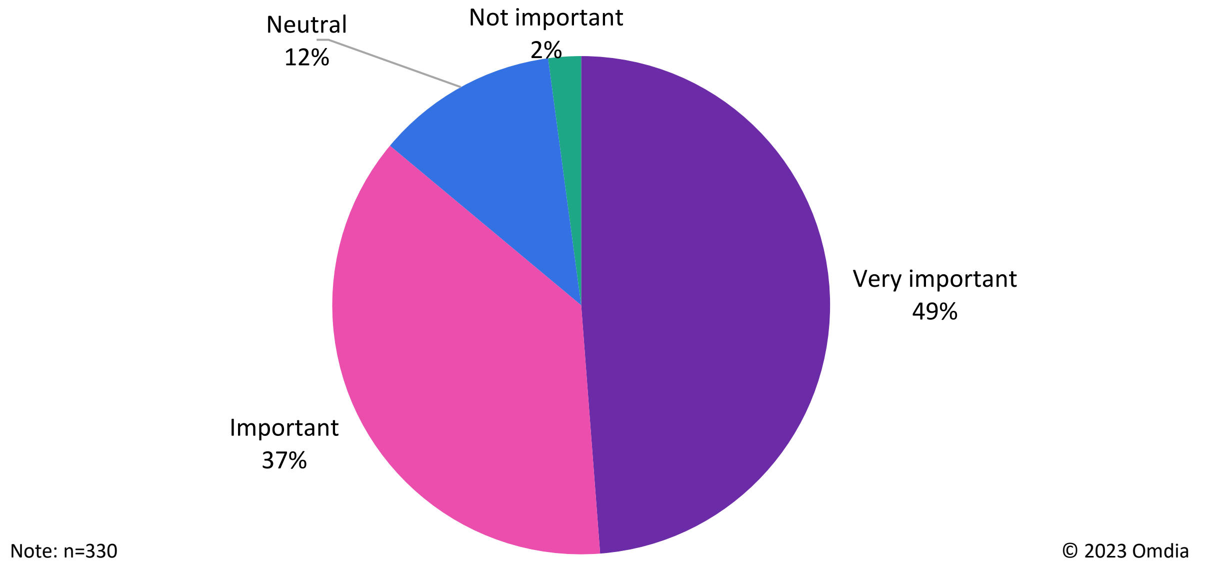
© 2023 Omdia

Source: Omdia

Ensuring regular assessment is in place can also help cybersecurity and organizational leaders maintain compliance with standards and dynamically improve their cybersecurity as their networks converge and evolve.

In addition, organizations can use these standards to validate the security of the products they offer or use in their environment. Having a globally recognized standard, such as IEC 62443 certification, helps assure that products and services are safer and better protected against attacks.

Figure 7: How important is it that products you buy are certified against such standards such as IEC 624443?



Note: n=330

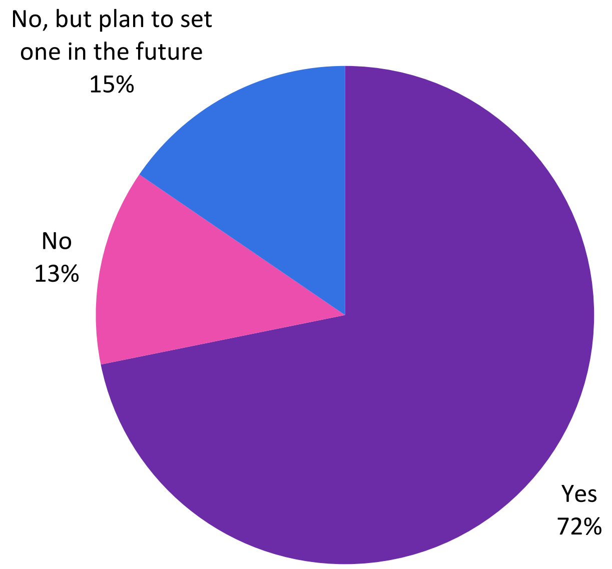
© 2023 Omdia

Source: Omdia

Effective incident response fosters resilience

According to Omdia's 2023 Cybersecurity Decision Maker survey, 92% of organizations have experienced cybersecurity incidents, and 47% suffered serious breaches that had an impact on business. While the incident's impact is a top concern, learning from it is equally crucial. Risk assessments evaluate likelihood and impact, allowing for acceptance, mitigation, or transfer of risk. One mitigation tactic is robust incident response, crucial for minimizing the mean time to response (MTTR) and preventing operational downtime in industrial settings. Omdia's survey underscores the necessity for tailored OT incident response processes; 72% of organizations are adopting unique approaches.

Figure 8: Do you have an incident response process that is unique to OT?



Note: n=330

© 2023 Omdia

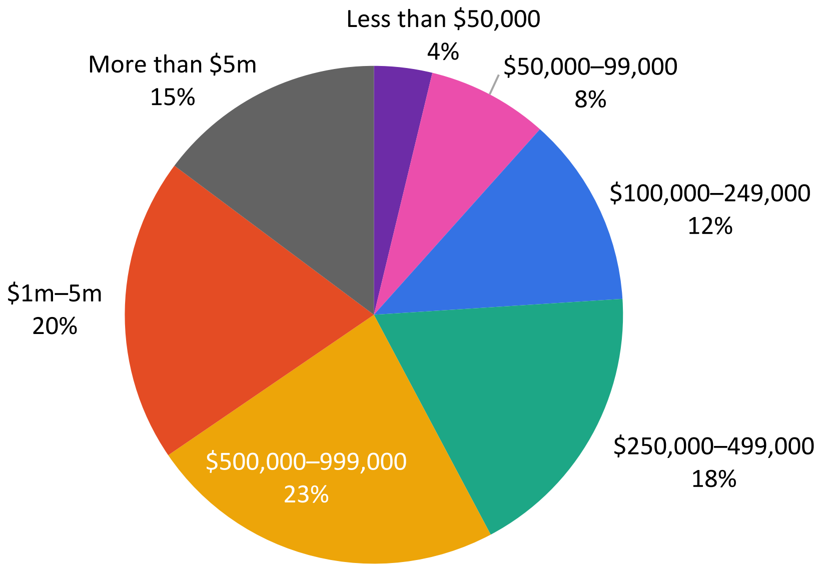
Source: Omdia

However, there is evidently significant work to be done by almost one-third of organizations to get to a point of resilience in the event of an incident or attack, given that 13% of survey participants responded “no,” and 15% only have plans to set one in the future.

Those with the highest cybersecurity budgets (more than $1m) are more likely to have this specialist process in place (83%). This suggests that perhaps cost constraints are reducing the likelihood of incident response retainers or the availability of the funds to build in-house incident response activities in organizations with lower budgets.

Interestingly, those with the very lowest budgets (less than $50,000) are most likely to have or to plan to have this process in place: 81% already do so, and the remaining 19% are planning on setting one. One potential explanation is that those organizations with the lowest cybersecurity budgets are choosing their top priorities based on recovering from the worst-case scenario rather than spending extensively to build out a range of preventive, reactive, and proactive controls.

Figure 9: What is your annual budget for OT/IIoT cybersecurity (excluding internal staffing costs)?



Note: n=663

© 2023 Omdia

Source: Omdia

Forensic capability is crucial for disaster recovery and improvement efforts. Processing data provides intelligence for remediation and preventing future attacks. Though 77% of organizations have identified data sources for forensics, a significant 23% have not. Collecting insights is valuable, but analysis and improvement require the right skills and expertise.

Conclusions

Visibility is a key requirement and often a starting point for many organizations in their OT cybersecurity journey. However, 100% visibility into a wide range of data and cyberthreats provides no protection to operations and is unrealistic for one single solution to offer.

Preventive controls are pivotal for addressing many challenges in OT network cybersecurity. NAC is a key protective technology, seamlessly and effortlessly integrating monitoring and control across critical segments, safeguarding both users and devices. It effectively mitigates cybersecurity and operational risks while restricting the potential impact of various events, including malware, ransomware, and nonsecurity incidents such as misconfigurations. Access controls, specifically preventing unauthorized or unknown devices, enhance protection against transient assets—such as laptops or mobile devices—connecting to the industrial control network without authorization.

For sustained success, organizations must deploy cybersecurity practices tailored to the complexity of industrial automation. These practices should secure from the IO block to the edge and cloud, employing a blend of active and passive methods alongside robust endpoint and systems protection.

An OT-specific approach should extend to incident response and forensic capabilities, minimizing the impact of cyberattacks, hastening system recovery, and preventing future breaches. The survey reveals significant improvement needs in these areas. To enhance cyber-resilience, companies should invest in in-house incident response and forensic capabilities or make use of third-party services.

Solutions must be accessible to both IT and OT workers, simplified for reduced complexity, and tailored with expertise from trusted partners in the industrial domain to de-risk implementation.

Cybersecurity is an ongoing journey, demanding continuous improvement. Companies must assess the effectiveness of their controls at various stages, not just at the beginning. Regular assessments set baselines, assist in planning and design, meet standardization requirements, and enhance overall resilience.

Appendix

Methodology

Omdia conducted an online survey of 300 decision makers in North America, Europe, and Asia & Oceania with a focus on IT, OT, technology, networking, security, and operations to explore the key cybersecurity challenges, pain points, gaps, and investment plans of industrial firms. Omdia senior analysts in cybersecurity and manufacturing provided analysis of the primary research data against a background of current market knowledge and previous primary research results.

Author

Anna Ahrens
Principal Analyst, Government & Manufacturing
customersuccess@omdia.com

Hollie Hennessy
Senior Analyst, IoT Cybersecurity
customersuccess@omdia.com

Get in touch

Omdia
www.omdia.com
customesuccess@omdia.com

Belden
www.belden.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Belden

Belden Inc. delivers the infrastructure that makes the digital journey simpler, smarter and secure. We're moving beyond connectivity, from what we make to what we make possible through a performance-driven portfolio, forward-thinking expertise and purpose-built solutions. With a legacy of quality and reliability spanning 120-plus years, we have a strong foundation to continue building the future. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia, and Africa. For more information, visit us at www.belden.com; or follow us on Facebook, LinkedIn and X/Twitter.

Belden helps safeguard operations and safety by providing cybersecurity solutions that deliver less complex, automated protection from inadvertent and malicious behavior from the IO block to the edge, helping our customers embark on their Industry 4.0 journey.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.