SANS | Research Program

Survey

2025 ICS/OT Cybersecurity Budget: Spending Trends, Challenges, and the Future

Written by **Dean Parsons**

March 2025

OPSWAT.

Executive Summary

For organizations that rely on industrial control system (ICS) and operational technology (OT) environments, ICS/OT is the business. These environments are the backbone of critical infrastructure sectors, managing essential processes such as energy production, water treatment, and manufacturing. Cybersecurity for ICS/OT plays a pivotal role in ensuring safety, reliability, and continuity of operations. Unlike traditional IT systems, ICS/OT environments interact directly with the physical world, making them uniquely vulnerable to cyber-kinetic threats that could lead to operational disruptions, environmental damage, or even loss of life.

Effective ICS/OT security not only prevents potential catastrophic incidents, but also sustains public trust, economic stability, and national security. As such, ICS/OT teams operate under principles and constraints that differ significantly from those of traditional IT. These differences must be carefully understood and respected, as applying conventional IT security processes, technologies, and practices without adaptation can inadvertently disrupt the engineering business and introduce safety consequences.

This white paper will explore actionable insights into the alignment of budgets, high-return-on-investment (ROI) technologies, and cybersecurity strategies to enhance ICS/OT security. It draws from recent SANS survey data to explore the intersection of IT and OT security practices, highlight key vulnerabilities, and present recommendations for ICS/OT cybersecurity specific controls, budget, and processes. By addressing both strategic and operational aspects, the paper can help guide your organization in making informed decisions to protect critical infrastructure.

The survey data revealed several key insights into ICS/OT cybersecurity:

- **Initial attack vectors—**Fifty-eight percent of respondents identified IT compromises as a leading initial attack vector for ICS/OT incidents, reflecting the interconnected and risky nature of IT and OT environments. Additionally, 33% pointed to internet-accessible devices as an attack vector, and 27% identified transient devices as another attack vector of concern.
- **Incident frequency—**Twenty-seven percent of organizations reported experiencing one or more security incidents involving ICS/OT systems in the past year.
- **Budget trends—**ICS/OT cybersecurity budgets have increased in recent years, with 55% of respondents reporting budget growth over the last two years. However, only 9% of professionals dedicate 100% of their time to ICS/OT security, indicating a potential gap in dedicated resources in protecting critical infrastructure.

Survey Methodology

Our respondent population is drawn from security and other professionals who attested that they are professionals working or active in one or more of the following (or related) fields:

- **IT**
- **ICS**
- **SCADA technology**
- **OT**
- **Process Control Systems (PCSes)**
- **Distributed Control Systems (DCSes)**
- **Building/facility automation/control/ management systems (e.g., BCS, FAS, BMS, etc.)**

Population demographics are characterized by four key items:

- **Industry**
- **Organization size in terms of workforce (both employees and consultants)**
- **Respondent role**
- **Geographic presence of the organization**

These items serve as independent variables to help the SANS author in analyzing the survey's research questions to provide actionable insights into the alignment of budgets, high-return-on-investment (ROI) technologies, and cybersecurity strategies that enhance ICS/OT security.

- **Prioritization challenges—**While 65% of respondents view OT cybersecurity as a primary responsibility, only 27% of budget decisions are led by CISOs or CSOs.
- **Budget control and responsibility—**Approximately 37% of respondents reported a shared budget between IT and OT. In contrast, 31% indicated IT controls the budget, while 26% said ICS/OT is responsible.

Based on inputs from more than 180 professionals across multiple critical infrastructure sectors around the globe, this survey's demographics are represented in Figure 1.

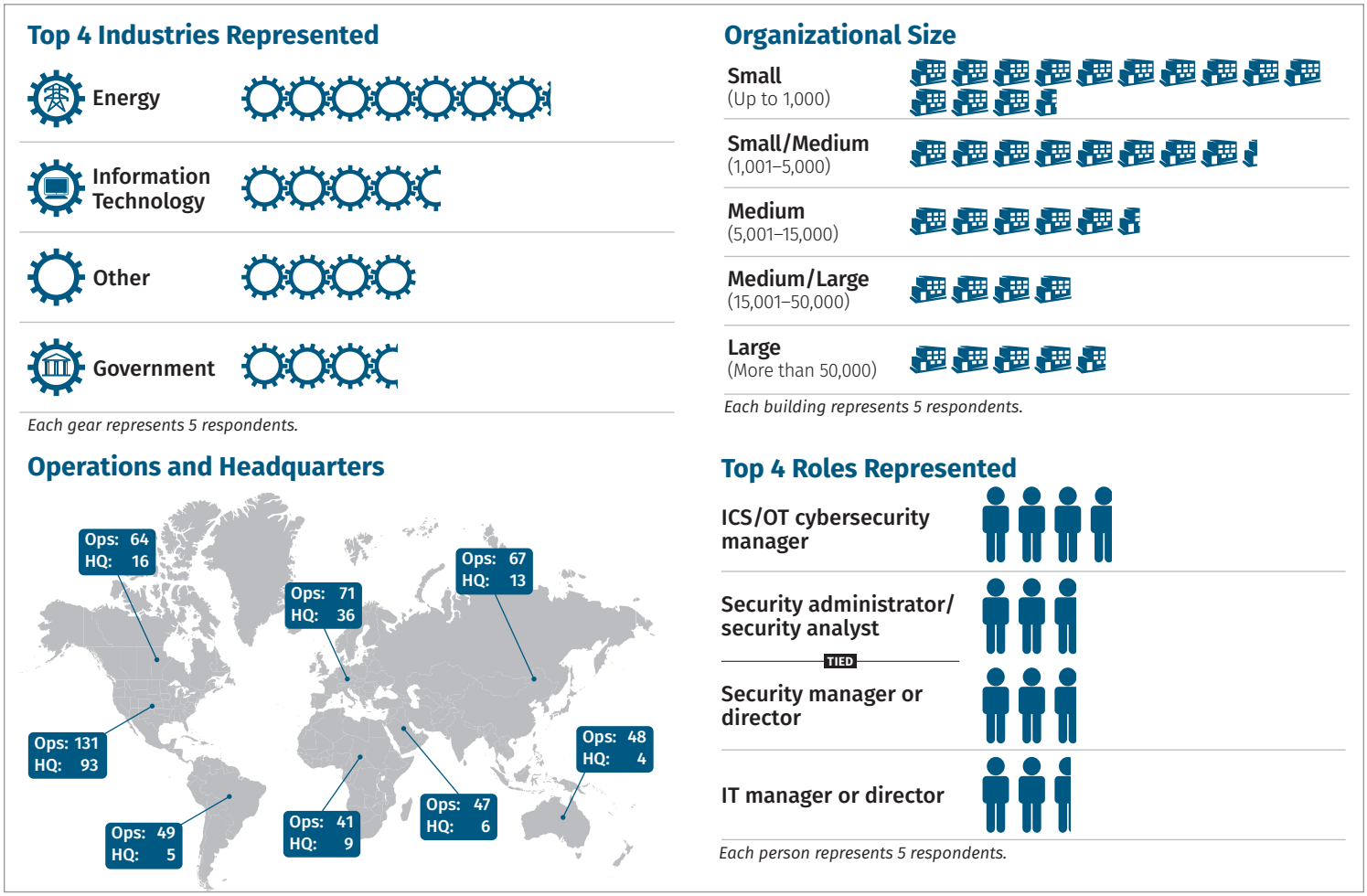

Figure 1. Survey Demographics

IT Controls Risk Safety

Mature organizations understand that IT security controls shouldn't be directly applied to ICS/OT environments. Instead, tailored ICS/OT security practices, aligned with safety, are crucial for effective risk management. Directly applying IT controls presents a false sense of security, disruptive false positives, and suboptimal critical infrastructure defense. See Figure 2.

Therefore, it is essential to focus on specialized strategies and prioritize ICS specific controls such as those outlined in the SANS Five ICS Cybersecurity Critical Controls.[1] That white paper details the five critical controls that are most pertinent to an ICS/OT cybersecurity program based on the current ICS/OT cybersecurity risks. Those controls are engineering-informed and adaptable to an organization's specific risk model to offer practical guidance on effective implementation, ensuring a more robust defense tailored to the unique needs of ICS/OT systems.

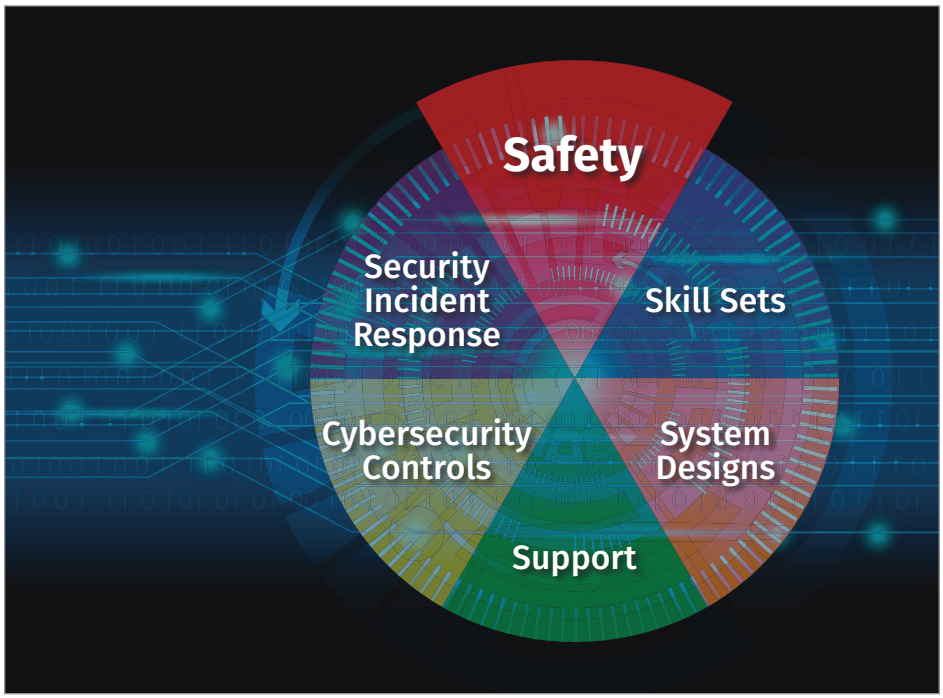

Figure 2. Main IT and ICS/OT Differences

Challenges and Benefits of Convergence

The presence of IT professionals in ICS/OT cybersecurity highlights the convergence of IT and operational technology skillsets, with IT roles expanding to include ICS/OT responsibilities. Although this can enhance security strategies, it may pose safety risks without an optimal approach.

Organizations should promote structured collaboration between IT security and engineering teams. IT professionals can shadow engineers to gain insight into ICS/OT dynamics, to prioritize safety, and to align with engineering-led incident response protocols.

Engineering teams must lead this collaboration, because ICS/OT environments are their domain. IT teams should adopt a supportive role, assisting and aligning with engineering needs.

This cooperative model fosters respect, secures critical infrastructure, and strengthens organizational resilience.

[1] SANS, "The Five ICS Cybersecurity Critical Controls," November 7, 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

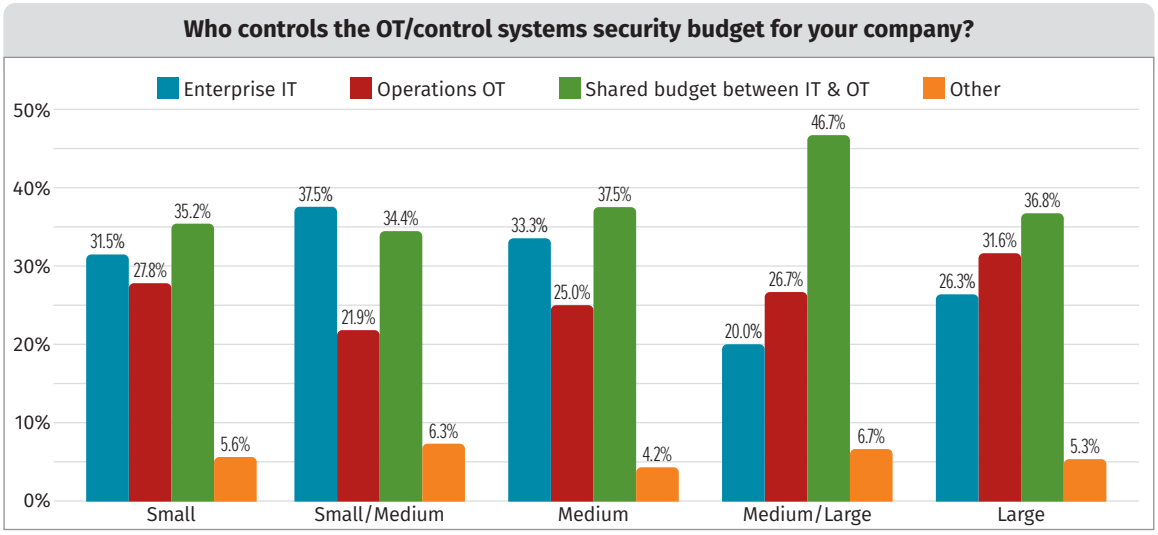

Figure 3. ICS/OT System Security Budget Responsibility

ICS/OT Cybersecurity Budget Allocation and Trends

Insights regarding who holds the primary responsibility for establishing security budgets within organizations shows a trend of collaboration, where caution should be exercised. Control of the ICS/OT systems budget is variable based on organization size (see Figure 3).

Decision-Makers

A portion of these decisions are made at high levels of corporate leadership, with 27% of the budgeting authority resting with CISOs or CSOs, and 26% with CIOs or CTOs (see Figure 4). This high-level involvement is beneficial, as it underscores the strategic importance placed on cybersecurity within these organizations. In mature organizations, these roles are expected to be safety- and engineering-informed.

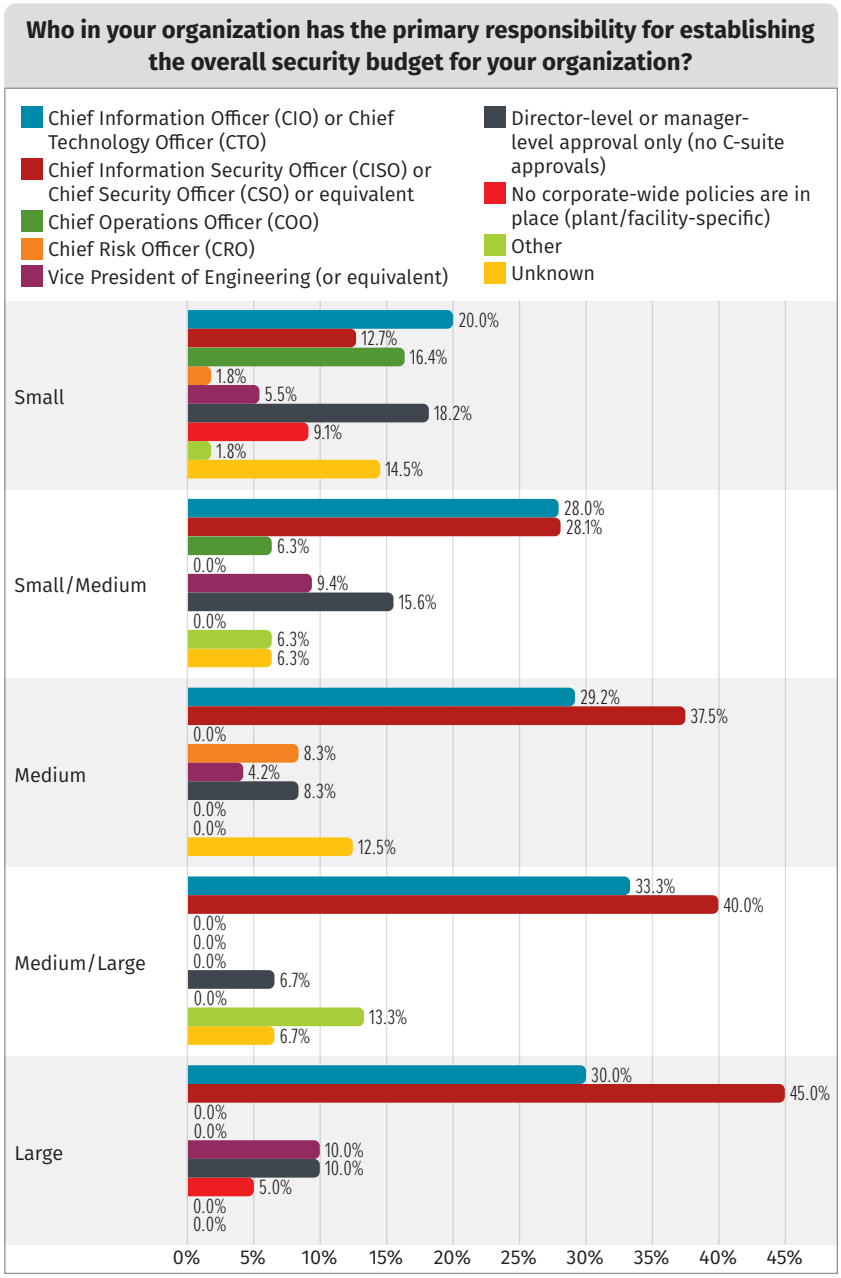

Figure 4. Responsibility for Security Budgets by Organization Size

Budget Variability

The survey revealed that 34% of respondents were unsure about their organization's overall security budget allocations, highlighting potential gaps in budgeting practices that may impact critical infrastructure security. A small percentage of organizations reported budgets of less than $10,000, suggesting that smaller entities or those less aware of cyber threats may face challenges in adequately funding cybersecurity measures.

On the other hand, 21% of organizations reported budgets between $10,001 and $100,000, and 37% exceeded $100,000—figures more common in larger, mature organizations or high-risk sectors. It is also important to recognize that smaller facilities, even those outside major critical infrastructure sectors, remain potential targets. Adversaries may exploit these facilities as test environments to refine attack methods before targeting larger, more critical operations. See Figure 5.

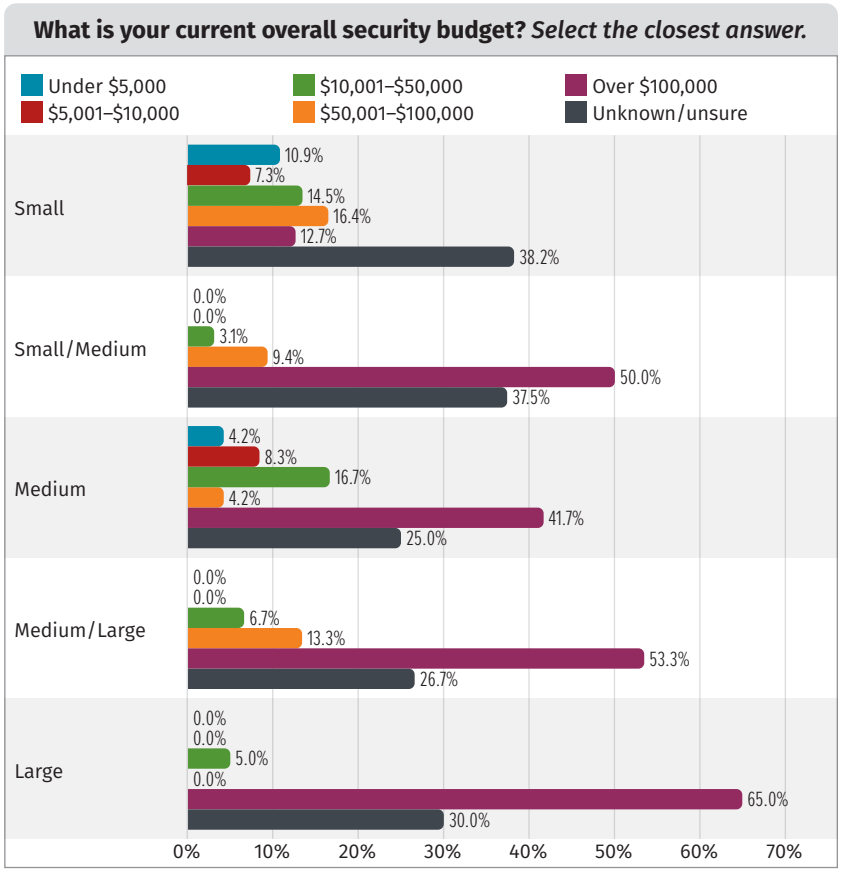

Figure 5. Budget Allocation

In terms of budget distribution, 41% of respondents allocated 0–25% of their overall budgets to ICS/OT security, and 40% allocated 26–50%, indicating a moderate investment approach by the majority. Meanwhile, 10% allocated 51–75%, and only 9% allocated more than 75%, illustrating that few organizations prioritize higher investments in ICS/OT security, potentially increasing operational and safety risk.

To address these disparities and verify budget for risk management strategies, leadership could reevaluate budgets, recognizing that ICS/OT environments are the backbone of businesses.

Budget Trends in Recent Times

Positively, the data on changes in the OT/control system budget for the past two years indicates an overall trend toward increased investment, with 23% of respondents reporting a significant increase and 31% noting a minor increase. See Figure 6. This suggests a strong and growing widespread acknowledgment of the need for enhanced resources to protect what makes, moves, and powers our world. Meanwhile, 21% have seen no change, implying stability in their funding, possibly due to satisfaction with existing measures or a stable budget strategy.

On the other hand, a minority of 5% experienced a minor decrease. As well, 5% reported not having a budget prior to the last two years, reflecting potential recent realignment, or augmentation in their financial commitments. Another 15% were unsure about budget changes in the last two years, indicating potential gaps in financial oversight.

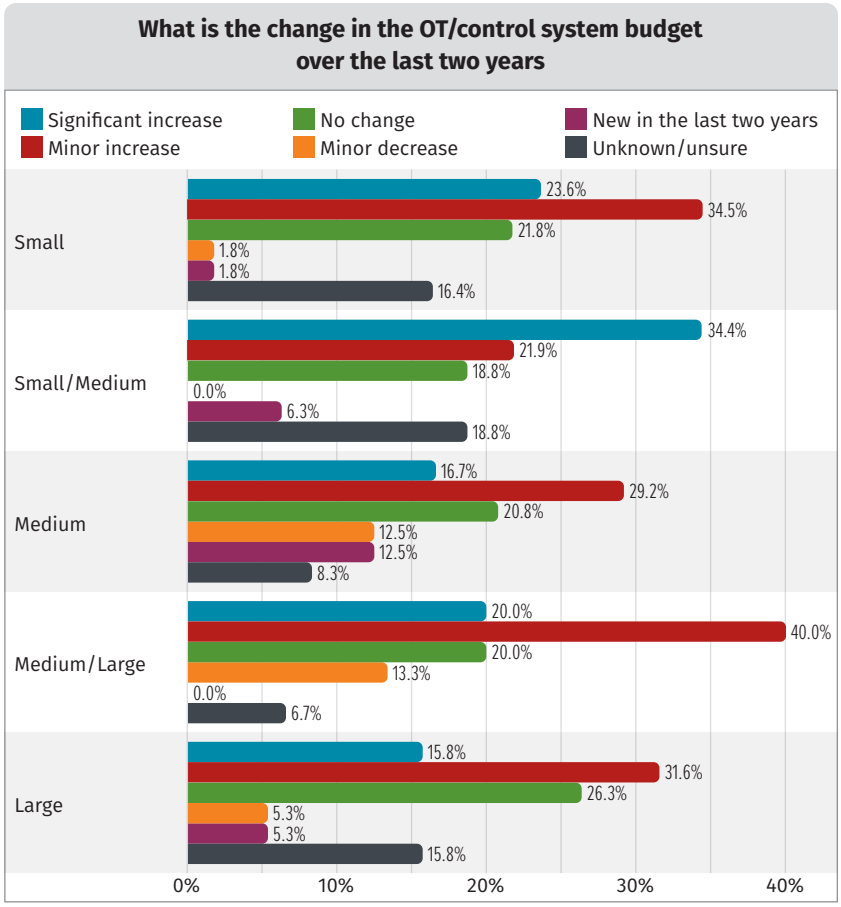

Figure 6. Budget Changes in the Past Two Years by Organization Size

Prioritized Areas of Investment

ICS/OT cybersecurity budgets focus on foundational security, but raise concerns, as seen in Table 1. The following key ICS/OT controls can improve ROI for critical infrastructure protection:

#1. Ranked first, ICS/OT defensible network architecture is crucial for robust segmentation, as per survey respondents, 58% of attacks stem from IT compromises breaching over into ICS/OT networks.

#2. Ranked second, ICS specific incident response emphasizes engineering-driven recovery within the ICS network, ensuring response plans cover both standard ICS assets and specialized engineering devices.

#3. Ranked third is architectures that support visibility, reflecting the priority placed on preparing for real-time network visibility and monitoring situational awareness deep inside operational technology networks.

#4. Ranked fourth, removable media and transient device security protects engineering laptops and portable tools used for ICS maintenance, as well as ICS network operations. This is crucial, as 27% of attacks were revealed to stem from this vector.

Table 1. Control Based on Budget Spend

Rank	Control
1	Control system ICS/OT defensible network architecture
2	ICS specific Incident response
3	Architectures that support visibility
4	Removable media and transient device security and protection for the ICS/OT environment
5	Network security (internal segmentation)
6	Asset identification
7	Network security (perimeter segmentation)
8	Log collection
9	Antimalware
10	Endpoint access control
11	ICS/OT-specific visibility and monitoring capabilities
12	Secure remote access into the ICS/OT control system environment
13	Process-communication enforcement
14	Data security
15	Dedicated ICS/OT risk-based vulnerability management

Current ICS/OT cybersecurity budgets align with key priorities, notably ICS specific incident response and defensible network architecture reinforcing strong engineering recovery and safety measures.

However, ICS network visibility and monitoring, crucial for detecting threats, identifying vulnerabilities safely, and aiding engineering network troubleshooting, ranks lower, despite its high ROI. Encouragingly, investment in architectures that support visibility (ranked third) shows growing recognition of this need.

Secure remote access, essential for preventing unauthorized access in increasingly remote operations, remains underfunded, despite rising attacks on unsecured connections. A more ICS threat-informed approach, aligned with the SANS Five ICS Cybersecurity Critical Controls,[2] could enhance protection against real-world threats.

Budget Allocation Based on Region

The survey highlights significant regional differences in ICS/OT cybersecurity budget allocation. The U.S. (40%) and Europe (38%) allocate 26–50% of their cybersecurity budgets to ICS/OT, demonstrating a strong recognition of its importance. Canada (30%) also falls into this range, but with 30% of organizations spending only 0–10%, suggesting a change in prioritization. Africa (35% in 26–50% and 37% in 11–25%) shows growing investment, indicating an increasing awareness of ICS/OT security needs. Asia, Australia/New Zealand, and Europe (38%) also allocate 26–50%, reinforcing a moderate investment approach to ICS/OT cybersecurity.

Latin America and the Middle East have higher concentrations of organizations (29–30%) spending only 0–10%, reflecting less rapid investment growth in ICS/OT cybersecurity. Higher budget allocations (51–100%) remain rare, with the U.S. leading at 12%, followed by Africa (17%) and Australia/New Zealand (17%), suggesting that although ICS/OT security is acknowledged, some organizations and regions still allocate a moderate portion of their budget to these protections.

Overall, the data indicates that many organizations recognize the importance of ICS/OT cybersecurity, but relatively few allocate more than 50% of their budgets toward it. The findings highlight the ongoing challenge of balancing ICS/OT and IT cybersecurity investments and underscore the need for continued advocacy, regulatory incentives, and awareness efforts to drive increased protections of critical infrastructure.

[2] SANS, "The Five ICS Cybersecurity Critical Controls," November 7, 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Budget Allocation Over Time: Controls

in the past two years, ICS/OT cybersecurity investment has focused on network security, secure remote access, and visibility. The U.S. (44.1%), Canada (55%), Europe (48%), and the Middle East (54%) have prioritized defensible network architectures, for example. Incident response funding has grown in the U.S. (36%), Africa (36%), and the Middle East (32%), emphasizing attack mitigation. Secure remote access is a key focus, with major increases in Asia (52%), Australia/New Zealand (42%), Europe (46%), Latin America (44%), and the Middle East (47%), reflecting a widespread push for stronger remote access controls across regions.

Log collection, process-communication enforcement, and endpoint access control budgets remain stable, while data security has seen slight declines in Africa (12%), Asia (8%), and the Middle East (8%). ICS/OT visibility investments have risen in the U.S. (42%) and Canada (44%).

Overall, network security and secure remote access remain top priorities, while incident response and visibility investments vary by region. Budget constraints, regulations, and shifting priorities continue to shape ICS/OT cybersecurity trends globally.

Drivers for ICS Technology Implementation

The data indicates several drivers for ICS/OT technology deployment. Primarily the drivers are a combination of organizational priorities, compliance mandates, and responses to evolving threats. Understanding these drivers provides valuable insight into the factors shaping cybersecurity strategies in critical infrastructure sectors.

Current Drivers for Control Implementation

Currently, the leading driver of ICS/OT security control implementation is organizational requirements (Rank #1), as companies shape security controls based on internal policies, risk management frameworks, and executive decisions. The evolving threat landscape (Rank #2), including ransomware incidents, ICS targeted malware frameworks, and geopolitical risks, significantly impacts security planning, pushing organizations to strengthen defenses proactively. Compliance requirements (Rank #3) remain a strong influence, with frameworks like NERC CIP, IEC 62443, NIS2 Directive, and NIST CSF. While vendor recommendations (Rank #4) still play a role in guiding product-specific decisions like patches and technology solutions, they carry less weight compared to internal policies and regulatory pressures.

Planned Priorities for the Next 12 Months

Looking ahead, ranked #1, the evolving threat landscape is expected to be the top driver for security control implementation. This marks a significant shift, with organizations prioritizing cyber threat mitigation more than in the past year. Ranked #2, organizations are expected to maintain a steady focus on aligning security measures with corporate objectives, ensuring security strategies support broader business goals. In contrast, regulatory compliance, ranked #3, is expected to become less of a primary driver as organizations shift toward proactive risk management rather than solely focusing on meeting compliance mandates. Reliance on vendor-driven guidance, ranked #4, is anticipated to decrease over the next 12 months; companies may place greater emphasis on their own risk assessment approaches rather than only vendor-provided security measures.

ICS/OT Incident Trends

Of the surveyed organizations, over the last 12 months, 27% reported experiencing one or more security incidents involving their control systems. This can be defined as unauthorized access; security breach; loss of OT relevant data; or operational disruption, damage, or destruction of product, process, or property involving the OT/control systems (see Figure 7). The majority, 43%, indicated no such incidents, while 11% were unsure, and 20% were unable to answer due to company policies.

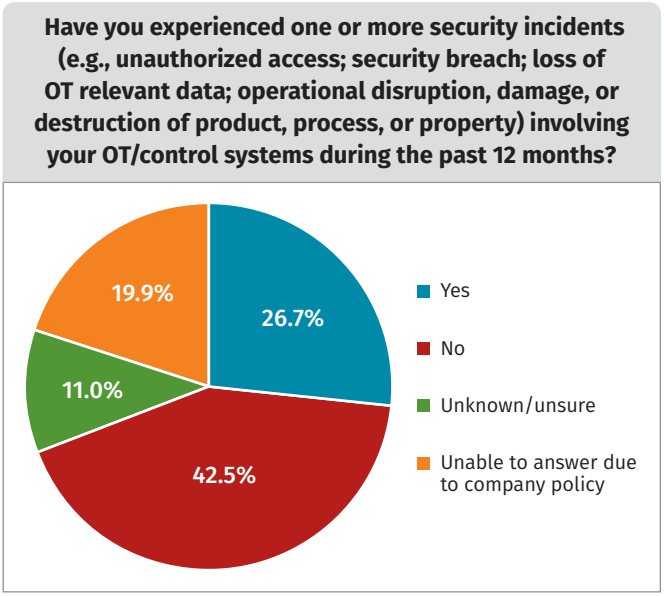

Figure 7. ICS/OT Security Incidents in the Past Year

Regarding the frequency of these incidents, the most common scenario, reported by 44%, was encountering fewer than five incidents. This suggests that although breaches are occurring, they tend to be relatively infrequent for most respondents. However, categories included 15% experiencing 6 to 15 incidents, and fewer respondents reported higher numbers, with only 3% encountering 26 to 50 incidents.

Most Common Attack Vectors

In terms of attack vectors, the most prevalent initial attack vector was a compromise in IT that allowed threats into OT/IT networks, identified by 58% of the respondents. This highlights the interconnected nature of IT and OT environments and the need for integrated security measures to protect ICS/OT environments from risky IT networks and the internet.

Other notable attack vectors included internet-accessible devices (33%), engineering workstation compromises (30%), and exploits of public-facing applications (27%). Also at 27% is the attack vector of transient cyber assets including vendor laptops. See Figure 8.

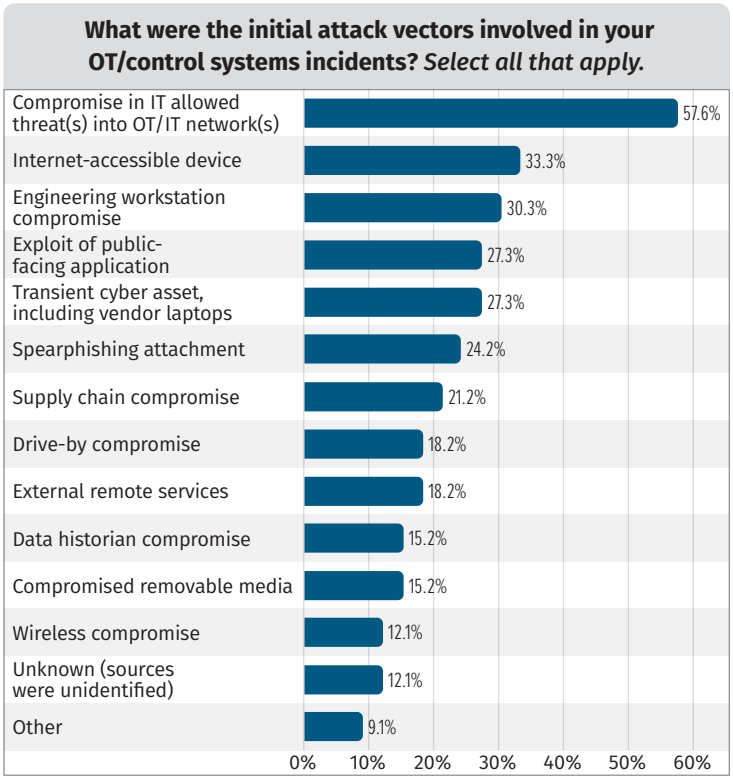

Figure 8. Common ICS Attack Vectors

Cybersecurity Areas of Focus

The insights on time allocation for ICS specific cybersecurity shows that professionals dedicate an average of 52% of their time to ICS/OT cybersecurity. A notable segment spends between 26% and 50% of their time on ICS cybersecurity, balancing these responsibilities with other tasks.

The survey data strongly emphasizes the critical role of ICS/OT cybersecurity in some organizations, with 65% of respondents identifying it as their primary responsibility. Additionally, 50% of participants are involved in IT cybersecurity, presenting a potential collaboration opportunity.

This distribution of responsibilities showcases a cybersecurity ecosystem where professionals are increasingly tasked with converging IT and ICS/OT expertise to implement extensive protective measures across all technological and operational aspects of their organizations. This could be a positive trend, provided the respective groups are learning from each other and collaborating, rather than pushing respective workflows and controls onto the other domain outside their expertise.

However, there is a concerningly small proportion—only 9%—of professionals who dedicate 100% of their time to ICS/OT cybersecurity. Given that industrial control systems underpin the essential services that power, move, and sustain our world, this figure is alarmingly low.

Considerations for Enhancing ICS/OT Cybersecurity

Reevaluate Budget Allocation to Focus on Core ICS/OT Systems

Organizations may wish to reevaluate their cybersecurity budgets to ensure what makes them a business, the ICS/OT networks and processes (in ICS/OT organizations), are protected given the current threat landscape. Maturing facilities can emphasize the risk-based Five ICS Cybersecurity Critical Controls[3] including defensible network architectures that support passive network visibility tools for real-time asset inventory and threat detection. As well, they can focus on high-risk vectors such as IT and ICS/OT network connectivity and transient device protections.

Leadership would do well to align budget decisions with the specific risks, safety consequences, and evolving threats unique to ICS/OT environments rather than adopting disruptive generalized IT strategies.

[3] SANS, "The Five ICS Cybersecurity Critical Controls," November 7, 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Leverage Specialized ICS/OT Controls to Address Unique Risks

Organizations are best positioned to adopt ICS specific controls to safeguard critical infrastructure networks effectively. This includes implementing tailored incident response plans that prioritize safety, deploying passive vulnerability management tools that avoid active scanning and operational disruptions, and using engineering-focused measures like ICS-aware firewalls and industrial intrusion detection systems to defend against cyber-kinetic threats.

Encourage Collaboration Between IT and OT Teams

Effective ICS/OT security requires structured collaboration between IT and OT teams. Cross-training programs can enhance mutual understanding, with IT professionals gaining operational insights into the core business, and engineers developing cybersecurity awareness for supporting organization functions. Establishing joint and engineering focused incident response teams with defined roles promotes a culture of respect that ensures IT methodologies are not applied to ICS/OT.

Conclusion

The evolving critical infrastructure threat landscape necessitates a proactive and strategic approach to securing what makes, moves, and powers our world—the ICS/OT environments, the backbone of our modern way of life. This white paper underscores the importance of reassessing budget allocations to prioritize core ICS/OT systems and human safety, leveraging specialized controls tailored to their unique risks and fostering collaboration between IT and ICS/OT teams to develop holistic security strategies. With only a small percentage of professionals fully dedicated to ICS/OT cybersecurity, organizations should invest in specialized ICS/OT cybersecurity skillsets and talent to address these high-stakes challenges effectively.

By implementing the insights and recommendations outlined in this white paper, organizations can strengthen the resilience of their ICS/OT systems, safeguard operational continuity, and enhance their overall cybersecurity posture in an increasingly interconnected world, while prioritizing safety.

Sponsor

SANS would like to thank this survey's sponsor:

OPSWAT.