Rockwell Automation

2022 SURVEY RESULTS

Cybersecurity Preparedness in Critical Infrastructure: Avoiding 'The Big Shutdown'

agilix SOLUTIONS

Table of Contents

INTRODUCTION

The Critical Infrastructure sectors are facing a perfect storm in cybersecurity. Operational technology (OT) organizations are challenged with growing vulnerabilities, new and existing cybersecurity gaps, an expanding attack surface, and rising global threats.

Well-resourced, sophisticated actors such as ransomware gangs and nation-state hackers have Critical Infrastructure organizations in their sights. In 2021, 83% of surveyed Critical Infrastructure organizations said they experienced cybersecurity breaches[1]. As attacks continue to escalate and Critical Infrastructure weaknesses remain unmitigated, The Big Shutdown — a large-scale disaster with broad, harmful implications — looms closer to reality. Critical Infrastructure organizations can no longer wait on the sidelines, underprepared.

To understand the state of Critical Infrastructure cybersecurity and gain insights into organizations' preparedness and best practices, Rockwell Automation commissioned ISMG to survey IT and cybersecurity leaders across multiple Critical Infrastructure industries. This report presents our findings, along with lessons learned and recommendations.

We've organized this report into five core themes aligning with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover). This framework is also used by Rockwell Automation as a fundamental roadmap for assessing and strengthening Critical Infrastructure cybersecurity.

[1] Skybox Security (via Yahoo! Finance): 83% of Critical Infrastructure organizations suffered breaches, 2021 cybersecurity research reveals, November 11, 2021

EXECUTIVE SUMMARY

Threat actors who want to wreak havoc or get fast return on investment have found Critical Infrastructure organizations an appealing target. Ransomware gangs, for instance, often target utilities, energy, oil and gas companies. They are the most likely among all sectors to pay ransom[2] because they can't risk any downtime.

The complexities of the IT and OT environment also make it tougher for these organizations to recover, and the harm of shutdowns can be immense, including downtime, financial losses and threats to public safety and well-being.

The ISMG survey shows that Critical Infrastructure organizations are moving in the right direction. They are taking steps to improve cybersecurity preparedness and resiliency. Yet the survey also shows progress is slow compared to the urgency. Many are struggling to overcome hurdles such as budget and talent shortages, lack of management prioritization, and lack of insight about how to best shore up defenses now.

The majority are missing or are going much too slowly on fundamental steps like inventory assessments, network segmentation and threat monitoring. Consequently, widespread vulnerabilities across Critical Infrastructure persist.

Key Findings for Business and Security Leadership Include:

1. **Critical Infrastructure organizations remain largely open to cyberattacks.** The survey found significant gaps in high priority areas like asset inventory monitoring, remote access management, patch management, endpoint security, network segmentation, incident response and recovery planning, supply chain security assessments, and employee security awareness. For example, fewer than 20% of surveyed organizations conduct asset inventory audits with adequate frequency. Only a third have effective OT patch management practices. Additionally, continuous threat detection is a blind spot across the board, with 60% of organizations lacking real-time threat detection. The manufacturing and machinery sector particularly stand out, as only 37% of those respondents cited having any measures in place across all questions. It's astounding that the other 63% are doing nothing – it's only a matter of time before we see disastrous consequences.
2. **Closing gaps must become an urgent priority.** Recently publicized attacks expose the high costs of downtime from cyberattacks, and the potential for not only crippled operations but disruptions of daily life. Attacks on OT (operational technology) ICS (industrial control systems) networks in industries that carry the risk of public safety impacts, like water, food, oil and gas, healthcare and transportation, are growing in volume and intensity, and Critical Infrastructure organizations are not moving fast enough to reduce their risk. For example, only 56% of those surveyed can analyze, contain and mitigate incoming threats today.
3. **Inadequate budgeting increases risk and holds back progress.** Security leaders cited a lack of funding as hindering their ability to apply known risk reduction tools and processes, such as inventory assessments and patch management. Given the threat landscape and potential harm of a cyberattack, organizations must recognize that the cost of doing nothing (or doing something, too slowly), can drastically impact uptime, compromise systems, and ultimately impact end customers, the economy and even national security.
4. **Organizations are not looking far enough ahead.** The US government is narrowing its focus on cybersecurity, especially as geo-political risks are on the rise. The federal government plans to fund $1 billion in cybersecurity grants for Critical Infrastructure organizations, but fewer than 30% of respondents have a cybersecurity plan in place to help identify critical cybersecurity gaps and to support building a grant submission, which could help close these gaps.
5. **Critical Infrastructure organizations must act quickly.** Based on these findings, Rockwell Automation's cybersecurity professionals recommend these core steps:
   - Perform accurate risk and vulnerability assessments to locate the areas of greatest weakness.
   - Develop a cybersecurity plan based on assessment results.
   - Segment and harden networks with IDMZ (Industrial Demilitarized Zone) and firewalls.
   - Implement threat monitoring.
   - Prepare and rehearse incident response plans.

RESEARCH STUDY DEMOGRAPHICS

The survey was conducted in January, 2022 and received 122 responses. ISMG solicited answers from senior industrial security leaders, whose roles ranged from CISO and head of security to plant engineer and business manager. CISOs and directors or heads of security comprised the largest two cohorts, nearly 25% and 19%, respectively.

Industries represented by the survey respondents ranged across nearly 20 OT verticals, 57% representing Critical Infrastructure organizations, including oil and gas, energy, chemical, water/waste water verticals. Manufacturing organizations had the highest number of single-vertical responses at 18%.

[2] Sophos, "The State of Ransomware 2021," April 2021

SECTION 1

Identifying and Assessing Risks

The Critical Infrastructure security has grown more complex in recent years. Threat actors are pouring tremendous resources into understanding how the new, interconnected Critical Infrastructure systems and networks operate, and into finding weaknesses they can exploit. Critical Infrastructure operators, however, are behind in gaining this visibility for themselves so they can identify their risks and prioritize defense strategies.

To avoid The Big Shutdown, Critical Infrastructure organizations need to take immediate, urgent steps to understand risks and close gaps.

Inventory Assessments

Asset inventory auditing is a key first step in risk assessment. It's also an area in which organizations struggle in terms of getting the right insights and the right frequency of reporting. As one respondent shared, "Inventory is really hard to keep. A virtual machine can be stood up and taken down before the governance team even knows it once existed."

Among survey participants, the most-common cadence for installed base inventory assessment was less than quarterly, with nearly 30% of responses pointing to this frequency. This pace was also the most common among three very critical industries: manufacturing and machinery; healthcare, public health sector and emergency services; and pharmaceuticals and chemicals.

Overall, 45% of organizations monitor their inventory quarterly and fewer than 1 in 5 conduct the audits daily, which is the minimum practice Rockwell Automation recommends.

Why is it Important?

Every unaccounted device creates a vulnerable point of entry to your network. A few years ago, quarterly or even monthly assessments may have been adequate. Now, with the speed of today's attacks, daily checks are essential in most cases and some respondents noted they're moving toward real-time assessments, which is possible with the right network design and monitoring tools in place.

We also found a disconnect in organizational awareness about installed based inventory assessments. Surveyed C-level leaders (e.g., CIOs, CEOs, COOs) were more likely to think assessments were conducted hourly, daily or weekly. However, the technologists with better day-to-day view of security operations (e.g., security heads, IT directors and architects or engineers) painted a less positive picture, consistently describing the cadence as monthly, quarterly or less frequent.

RECOMMENDATIONS

Automated asset inventories improve the prevention or stopping of attacks that result from lack of visibility. A variety of automated tools and services are available to simplify the inventory assessment process both for IT and OT at whatever frequency you decide is within your risk tolerance threshold. For Critical Infrastructure organizations with the risk of outsized impacts on the population, real-time inventory is a prudent strategy, delivering complete visibility into their network assets.

Business-Critical Systems

Our survey found only 56% of organizations had business-critical systems identified and prioritized, indicating this is an area of urgency (Figure 1). Additionally, based on Rockwell Automation experience, some organizations underestimate the effectiveness of their protections around business-critical systems. Survey comments reflected some of this ambiguity, with one respondent noting they've solved this step with robust security software.

In reality, deploying general cybersecurity controls may fail to adequately protect highly critical systems at the levels needed. The operational and business systems with the highest level of criticality must typically be fortified with additional network segmentation, identity and access controls such as multi-factor authentication and related measures. Identifying and prioritizing criticality first ensures that the right additional security strategies are applied appropriately to address risk, system by system.

Zero Trust is a growing security best practice across all sectors. It's also on the radar of the US federal government for Critical Infrastructure organizations to implement, and has a role to play in this step of identifying business-critical systems.

Zero Trust is not an "all or nothing" security model – it can be approached from many angles and applied incrementally, even in small steps. Identifying and prioritizing what's most crucial to the organization is a key step in this incremental journey, generating the insights to put Zero Trust controls where they're needed most.

Are business-critical systems identified and prioritized?

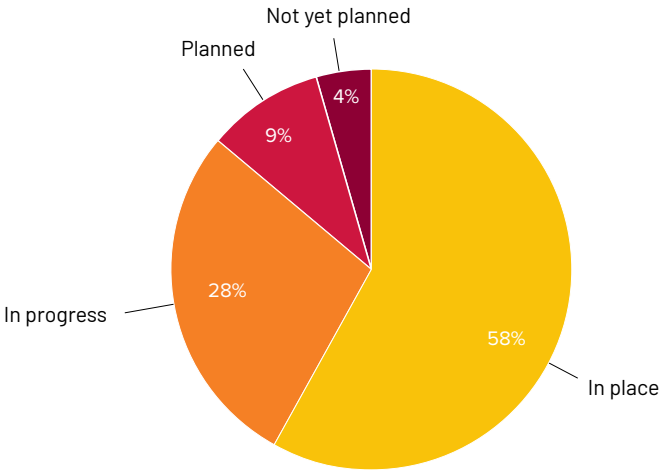


Figure 1

RECOMMENDATIONS

Borrowing from the Zero Trust strategy, examine all of the organization's DAAS elements – Data, Assets, Applications, and Services – and prioritize each based on criticality. These are the organization's 'Protect Surfaces,' each getting the right cybersecurity controls applied in priority order.

In Critical Infrastructure, ICS and production line applications and data are examples of likely business-critical systems. Ask your business, operations, IT and security teams what happens if these systems are locked up in a ransomware attack. What systems enable production operations, data security or integrity, communications, supply chain continuity or simply the ability to provide services to customers to help the prioritization exercise.

SECTION 2

Protecting and Implementing Safeguards

Digital transformation, process digitization and IoT technology, along with the resulting convergence of OT and IT, have improved Critical Infrastructure efficiency and reliability, enabling providers to better serve the public and deliver services more cost-effectively.

While these developments are positive, they've exposed Critical Infrastructure organizations to new threats and vulnerabilities from the increased exposure to the internet through sensors and devices, remote workers, third-party APIs and unsecured programmable logic controllers, gateways, actuators and many other components.

Security controls for OT systems differ from IT practices because many OT components typically lack basic protections. Legacy systems controlling production are often not even patchable, and if they are, not at the speed of normal IT patching - along with other plant floor realities.

Furthermore, OT security is moving toward more CISO ownership, yet many CISOs don't fully understand the implications of managing OT and by extension, IoT security. On the flip side, plant engineering leaders must reliably preserve uptime and can't easily afford to take down OT networks for long periods to patch security flaws, especially not on the fly.

Perhaps this is behind survey results showing only 28% of respondents have a converged IT/OT security roadmap today, with another 35% indicating the step is in progress. Critical infrastructure organizations should follow the lead of the manufacturing and machinery industry, where 84% of surveyed respondents indicated they already achieved this convergence or have it on their roadmap. Clearly, the other sectors must make up a lot of ground to catch up.

Yet the march to convergence will continue. To create a robust converged roadmap, IT and OT leaders need to delve into a true joint planning process together. Rockwell Automation typically recommends to our clients to set aside an entire week where an experienced process driver can walk the two teams through the identification of all the security elements, barriers and requirements. This approach achieves buy-in from all stakeholders as important decisions are made.

Some clients also create a Cybersecurity Center of Excellence (COE), tapping IT, OT and business stakeholder groups to work together on an ongoing basis to create working systems and to troubleshoot together when new issues arise.

Secure Remote Access

Threat actors will exploit any avenue that can produce a foothold inside an organization. With the pandemic's shift to full or hybrid remote workplaces and overall increased worker mobility, under-secured remote access has become an easy target.

Remote access systems often use outdated security, often relying on passwords alone and lacking multi-factor authentication (MFA). In the utilities, oil/gas extraction, and mining sectors, login credentials are the type of data most commonly exposed in breaches[3], and the abundance of stolen and leaked credentials on the dark web makes it easy for malicious hackers to crack remote access systems. So while 69% of survey respondents report having secure remote access in place, the result is potentially misleading in terms of having adequate remote access protection.

The COVID-19 pandemic created both a challenge and a benefit in this regard. One of our respondents noted that hybrid work models made consolidated remote access difficult, while another said the "work from anywhere model" that became standard during the pandemic has forced organizations to pay attention.

RECOMMENDATIONS

A reliable identity and access management (IAM) program is instrumental to a Zero Trust strategy. IAM provides visibility into who is requesting access, to which applications and data, from where, using what device, at what time - and controls for other approved behavioral norms. This allows monitoring and enforcing access policies and controls. An IAM solution that integrates MFA can significantly lower the threat of compromised passwords.

The Industrial Demilitarized Zone (IDMZ)

Creating an 'air gap' between ICS and OT systems and IT using an IDMZ is a baseline of network cybersecurity design that helps ensure threat actors cannot move laterally to OT networks and controllers if they gain access to IT systems - and vice versa. According to survey responses, about 50% of organizations have an IDMZ within their OT architecture, and another 25% are working on it (Figure 2).

The healthcare, public health sector and emergency services industry is especially behind – 38% of respondents don't have an IDMZ planned yet, compared to 16.5% across all industries. These findings align with what Rockwell Automation sees in the broader market.

IDMZ air gaps are not the end game for cybersecurity, especially since OT systems and IoT devices can connect directly to the internet via IT networks. Additional measures must be implemented for a robust defense.

What is the status of implementing an Industrial Demilitarized Zone (IDMZ) within OT security architecture?

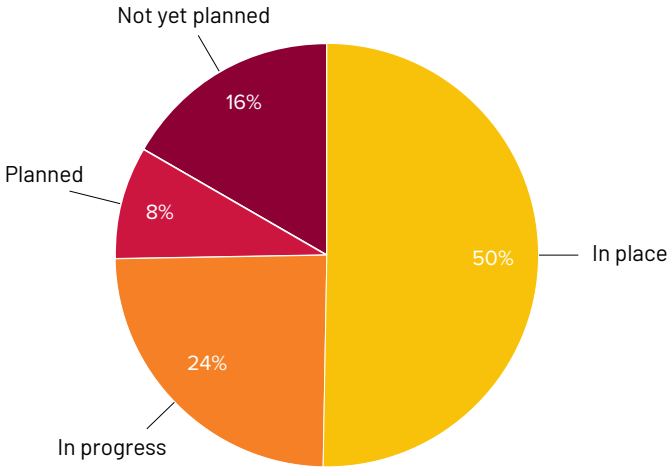


Figure 2

RECOMMENDATIONS

For a secure architecture, implement IDMZ as a basic best practice. Separating IT and OT networks and assets from each other ensures threat actors can't move across the two systems. Yet keep in mind, modern Critical Infrastructure security architecture should include additional defenses, especially around business-critical Protect Surfaces, and across all internet-enabled assets.

[3] Verizon, "2021 Data Breach Investigations Report," May 2021

Patch Management

OT patching is a significant trouble spot. The survey validated what's regularly seen in the field: patch management is either not considered an important practice, not funded, or simply too complicated to undertake. Among our participants, only 37% have implemented effective OT patch management, and 13% haven't even planned a patching approach yet (Figure 3).

In the manufacturing and machinery vertical, 42% of surveyed organizations don't have effective patch management in place or even in progress. The top industries that are ahead of the rest in making good headway are manufacturing in the US and UK/Ireland, and financial in the Middle East and Asia-Pacific (APAC).

These findings are – alarming across the board, considering the rate of discovered vulnerabilities and the risk of stealthy malware lying in wait.

Many OT systems can't be patched normally because of limited, narrow functionality, and/or legacy structures don't allow for embedding security components. Patching can also take an entire day [each] when you have dozens or hundreds of network servers - incredibly costly in terms downtime, so plant operators have historically resisted IT approaches to patching.

What is the status of effective OT patch management?

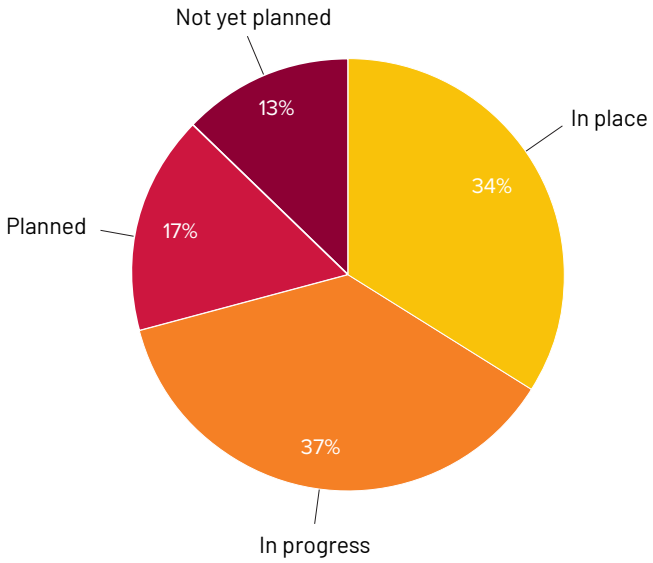


Figure 3

Additional Security Gaps

- **Removable media.** Just over half of organizations cited effective security procedures for removable media. For the rest, anyone can effectively walk out with data anytime, or walk in and potentially insert malware onto networks. Look no further than the Snowden and Manning insider cases to understand the potential implications. One respondent, whose organization is working on a fix, offered this excellent insight: "Configure your next generation of endpoint detection and response (EDR) tools to not allow memory sticks."
- **Network segmentation.** In a similar story, only 49% of organizations have implemented segmentation or microsegmentation to protect business-critical systems. This is an essential best practice required by many government policies and a core component of Zero Trust. Given the effectiveness of the Zero Trust approach, more mandates are likely to be required of Critical Infrastructure providers to effectively segment networks.
- **Employee awareness.** 69% of organizations have implemented employee security awareness, training and testing programs. The APAC and Middle East financial and banking sector leads the way here, while the US travel and transportation industry cited no training at all. Nearly ⅓ of organizations overall have not implemented security training, which is a NIST framework best-practice and is highly recommended. Awareness training is a proven protection measure for preventing and stopping attacks that begin with phishing (a whopping 86% of confirmed breaches). Whether your program is in the hands of HR or IT, make sure it covers cybersecurity threats and best practices specific to OT. We also recommend penetration testing to help identify the areas where employees need more training.

RECOMMENDATIONS

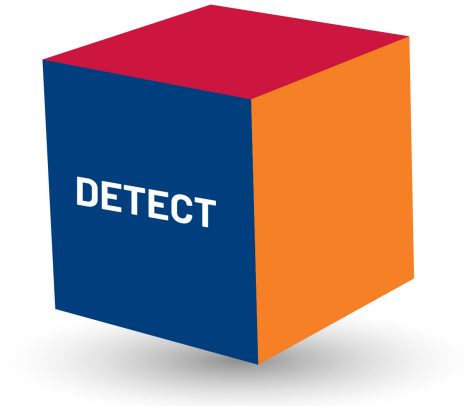
Threat actors are constantly looking for vulnerabilities. No organization, especially those in Critical Infrastructure, can go forward in a 'business as usual' style. As downtime risk from cyberattacks increase, the risk-reward balance between doing nothing and finally addressing the complexities of OT patching should naturally tilt towards prevention, given high potential loss and damage.

Efficient and effective OT patch management starts with heavy industrial experience and OT cybersecurity expertise. This expertise helps to avoid common pitfalls and leverages best practices from multiple successful implementations. Working with a partner who understands the dynamics of production environments along with the acute implications of cyberincident downtime can streamline this complex but necessary process and execute OT patching with minimized disruption.

[4] Verizon, "2021 Data Breach Investigations Report," May 2021

SECTION 3

Detecting Threats and Identifying Cybersecurity Events



A core tenet of Zero Trust security is the assumption that a breach has already occurred; no connection or access request should be trusted until it's verified and authenticated, dynamically, each and every time. This principle relies on constant monitoring for malicious activity in real time to detect and mitigate threats.

Unfortunately, survey responses show that threat detection is a blind spot for Critical Infrastructure organizations. This means attacks on OT systems can go unnoticed, and organizations are not addressing frequent attack risks such as ransomware that could debilitate operations; nation-state actors who are conducting long-term espionage activities; and attackers who may be moving through systems and supply chains preparing for a large-scale attack.

Detecting Threats and Anomalies through an OT SOC

An OT Security Operations Center (SOC) brings together the technologies, tools, talent and other resources for 24/7 threat monitoring and response. An OT SOC is indispensable for detecting threats and anomalies quickly and minimizing impact on business-critical systems. Our survey found that 43% of organizations don't currently have real-time threat and anomaly detection via an OT SOC in place (Figure 4), revealing a broad shortcoming in cybersecurity preparedness.

The APAC, Australia and New Zealand region lags in OT SOC implementation, with "not yet planned" as the top answer. Among respondents in this region, 31% don't have an OT SOC planned, compared to 16% across the globe. Drilling farther into the data, we found no organizations in the region's energy, power and nuclear industry with a SOC in place or even planned. For comparison, 74% of organizations in Middle East and Africa have implemented an automated SOC or are working on it, with two verticals blazing the trail: financial and banking; and energy, power and nuclear.

Additionally, 47% of respondents haven't implemented a security information and event management (SIEM) platform for analyzing security alerts from applications and network hardware. While most SIEM systems don't generate alerts in true "real time," some get very close, making them a staple in your SOC tool stack and a critical component of effective Critical Infrastructure defense.

What is the status of implementing real-time threat and anomaly detection via OT SOC (owned or managed services) for malware, ransomware, vulnerabilities?

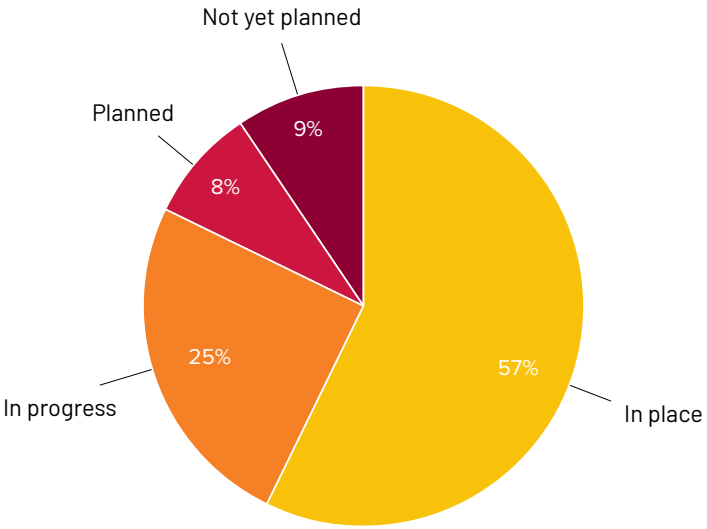


Figure 4

RECOMMENDATIONS

Resource constraints such as lack of in-house talent can create insurmountable hurdles for many organizations' ability to monitor and detect threats, yet this is a cornerstone necessity in today's evolving OT threat environment. Take advantage of third-party OT SOC solutions that include services such as continuous threat monitoring and incident response.

When you work with a reliable OT SOC partner, you're getting the on-the-ground expertise of a highly trained security team, but also real-time insights gained from all customers using being served by the SOC. A managed OT SOC also avoids high CapEx costs and ensures that the latest tools, techniques and threat intelligence insights are deployed on your behalf – advantageous considering the worldwide shortage of trained security professionals that is estimated at 2.72 million ((ISC)^2 2021 Cybersecurity Workforce Study).

Securing Endpoints

From industrial IoT sensors and personal employee devices to controllers, the proliferation of endpoints vastly expands the OT attack surface. Protecting operations in this environment is a mounting problem. Among surveyed security leaders, 46% don't monitor and control endpoints 24/7 in real time today (Figure 5). That means a large portion of devices connected to OT systems aren't configured properly or contain security flaws. Organizations may get lucky, but in most cases it's only a matter of time before threat actors use these unsecured and unmonitored endpoints in cyberattacks.

What is the status of having all endpoints access-controlled and monitored in real time 24/7?

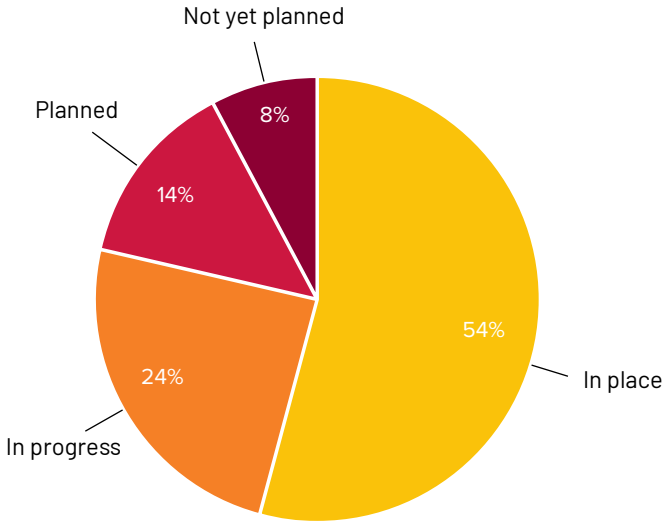


Figure 5

RECOMMENDATIONS

Endpoints are an area to shore up quickly. Start by conducting the network asset inventory assessment discussed earlier to identify all endpoints connected to your network. Once identified and evaluated for their security risks, you can develop a plan, based on your identified business-critical systems and security priorities, for the tools, staff and services required to harden perimeters around these entry points.

SECTION 4

Responding to Cyber Incidents

Incident response planning and preparation are crucial. The right preparations will minimize downtime, financial losses, customer disruptions and other negative impacts of cybersecurity incidents. For Critical Infrastructure providers, the speed of response is especially urgent because of the extent of damage possible, including public service and safety issues, in some cases for up to millions of people.

Critical Infrastructure organizations are making strides as 57% reported capabilities for analyzing, containing and mitigating cyber threats (Figure 6). However, we also detected this is an area of angst, perhaps due to the constant and rapid change of the threat landscape. One participant remarked, "Does anyone have this figured out?" Another respondent asks: "How do Critical Infrastructure organizations plan to address business continuing and resiliency while they're still figuring out how to develop a basic incident response strategy?"

What is the status of cyber threat analysis, threat containment, and threat mitigation capabilities?

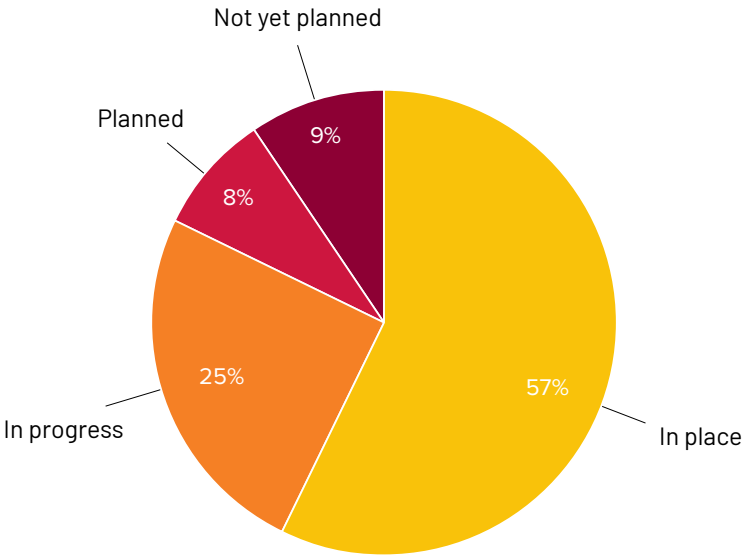


Figure 6

RECOMMENDATIONS

If resources and expertise are an issue in developing your incident response strategy, consider a managed services provider - such as an OT SOC partner - to move quickly and avoid hitting walls in efforts to hire experienced cybersecurity talent directly, given the global staffing shortage. An experienced OT SOC partner with deep industrial heritage, such as Rockwell Automation, can assure you have an effective incident response plan ready but can also spring into action on your behalf to help block and mitigate attacks if needed. Expert teams also perform ongoing training and scenario testing to validate the ability to respond quickly. Additionally, a top-quality OT SOC partner will bring deep understanding of OT compliance requirements and reporting.

SECTION 5

Recovering After an Incident

46% of survey participants said they are ready with recovery processes today, with systems, data and operational procedures in place to restore operations quickly after a cyberattack.

In terms of recovering from a cyberattack, what counts as "fast?" In some cases, a week may be considered adequate. In others, every minute matters.

For example, when power companies experienced outages during the major 2021 snowstorm in Texas, a week of downtime meant hundreds of lives lost. In the case of Colonial Pipeline's ransomware attack, even 24 hours without recovering meant millions of dollars in costs and untold economic impact from the loss of gas supplies on the East coast of the US.

While returning to normal operations is the key focus of your incident recovery phase, it's also an opportunity to identify areas needing improvement. Implementing meaningful changes based on the learnings from incidents creates a culture of continuous improvement of cybersecurity, yielding ever more resilient and protected systems.

Leveraging Federal Funding

In November 2021, the US Congress enacted an infrastructure bill (H.R. 3684, Infrastructure Investment and Job Act) earmarking about $2 billion for cybersecurity upgrades and enhancements in Critical Infrastructure. $1B of the amount is slated for funding grants for state, local, tribal and certain non-profit organizations. Grant submission guidelines are pending, however Rockwell Automation expects grants to align to the NIST Cybersecurity Framework capabilities given the framework's use by federal Cybersecurity and Infrastructure Security Agency (CISA).

About a third of survey respondents (29%) have a cybersecurity plan in place adaptable for grant submission. Another 25% have a plan in development. That leaves approximately 40% of organizations without this level of preparation.

A cybersecurity plan not only enables those in target organizations to apply for grants quickly when available, but also helps set in motion the right kind of systematic cybersecurity program that will expose gaps, lower risk, and help to prioritize efforts for protecting the organization and its customers from harmful impacts.

Rockwell Automation encourages all Critical Infrastructure leaders to familiarize themselves with this legislation, prepare a baseline plan and seek funding if the grants are applicable to their organization. Don't wait until grant requirements are released — take steps now to start preparing and developing your plan. Rockwell Automation has created a cybersecurity planning template and checklist using the NIST framework: **Download Planning Template**

RECOMMENDATIONS

Recovery and restoration planning should be as common of an operational practice as asset maintenance, central to reliable operational uptime. The financial and human costs of downtime continue to escalate, and you can't count on shifting the burden of risk to your insurance company. As liability grows and insurability becomes more limited, the burden will revert to the insured to cover the bulk of the losses and recovery costs.

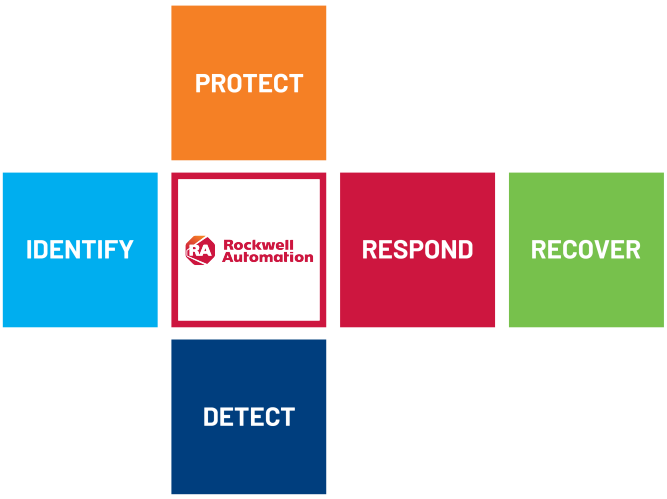
NEXT STEPS

Preparing for the Future

Every Critical Infrastructure provider must act now to avoid The Big Shutdown. Lives, wellbeing, safety, and livelihoods depend on it.

OT cybersecurity is not easy. On the other hand, most breaches have known defenses. Critical Infrastructure organizations have made great strides in efficiency and reliability through digital transformation and automation; now they must tackle cybersecurity with the same tenacity. Survey findings show the sector waking up to the need for modern, focused cybersecurity, although slowly - with heavy remaining gaps, ill-defined priorities and lack of clarity regarding risks and best practices.

Yet Critical Infrastructure leaders are starting to pay attention. Many respondents reported planning or having important protections in progress. The sector is moving from low awareness, to reactivity after significant attacks in the news and the accompanying government response, to asking how cybersecurity can be accelerated in their organizations.



Rockwell Automation: Securing What The World Relies On.

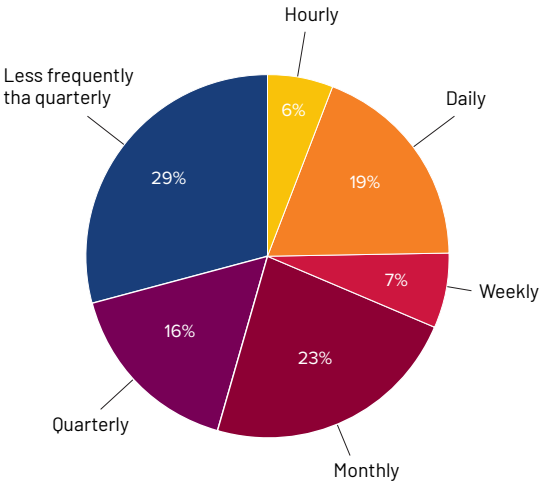
Rockwell Automation provides a range of industrial security solutions and services to help you manage threats and boost the resiliency of your OT and IT ecosystem. Our experts can help you build a robust and secure network infrastructure while helping to defend against threats and rapidly respond to incidents. In addition to deep expertise and knowledge of the latest best practices, we bring production operations wisdom from more than 100 years in industrial automation. Our worldwide locations enable customers to apply cybersecurity protections on a global scale across multiple sites with logistics as finely tuned as you'd expect from the industry leader in industrial automation.

RECOMMENDATIONS

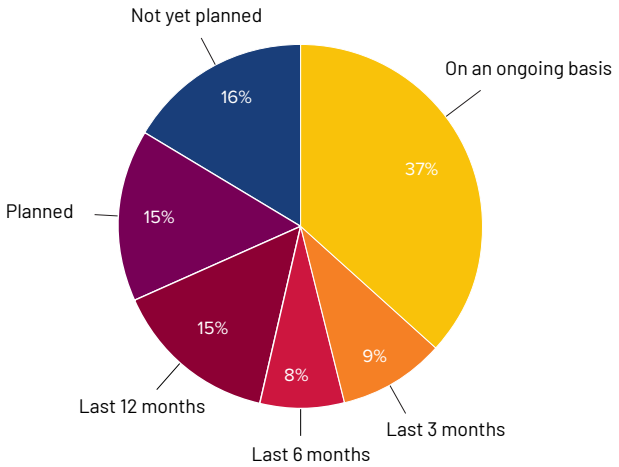
- Take the **Rockwell Automation Cybersecurity Preparedness Assessment** and receive a custom report, benchmarked against original survey respondents. See how your organization compares by industry, company size and region.
- Download our **OT Cybersecurity Plan Template** for advance insight on tools, services and staffing to defend your operations effectively. US Critical Infrastructure organizations: use the Plan Template to help prepare for grant funding that can support closing cybersecurity gaps.
- **Talk to a Rockwell Automation professional** and learn how we can help you with the right OT cybersecurity program to best protect your industrial operations.

APPENDIX

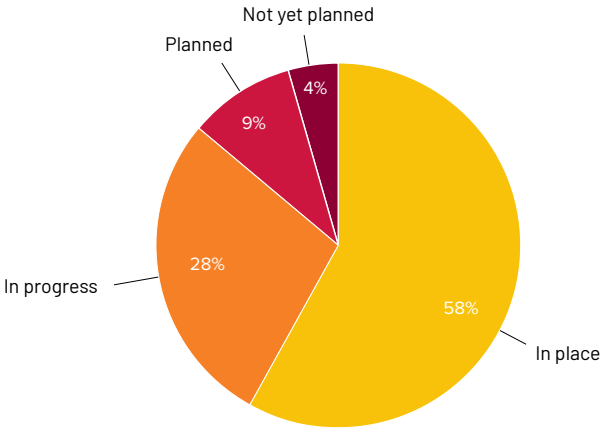
How often is the installed base inventory assessed?



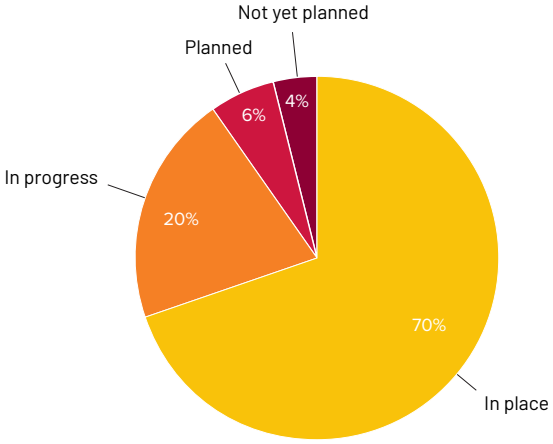
How often is a supply chain risk assesment performed?



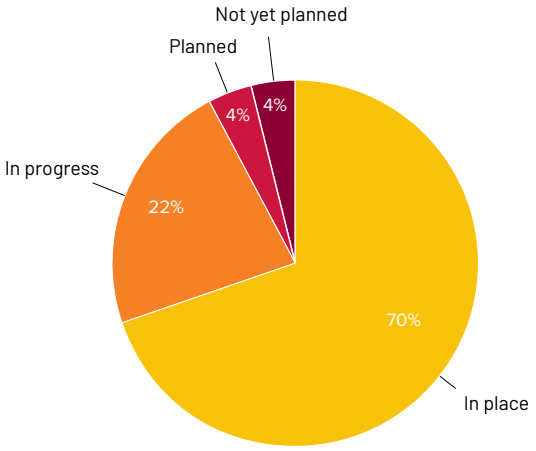
Have business-critical systems been identified and prioritized?



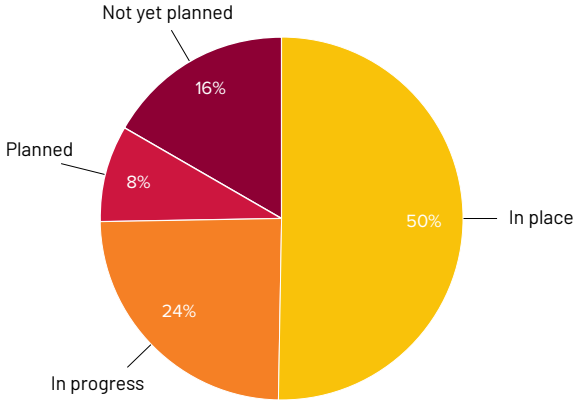
What is the status of remote access controls for secure offsite login?



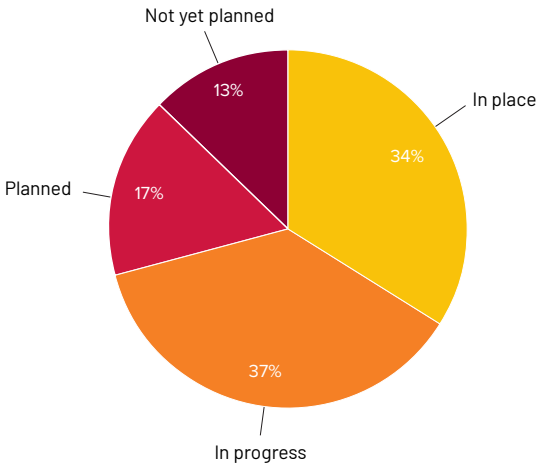
What is the status of physical access controls that discern and prevent unauthorized system access?



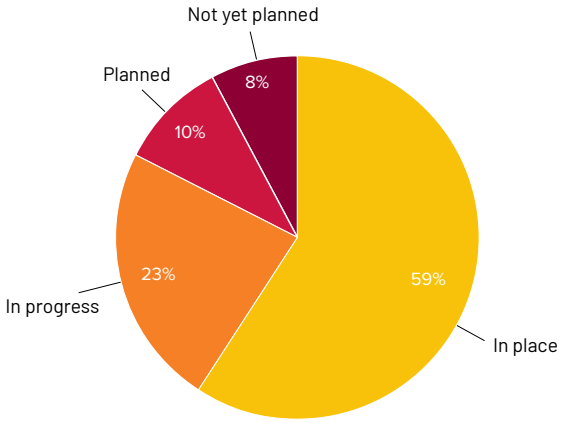
What is the status of implementation of an Industrial Demilitarized Zone (IDMZ) within OT security architecture?



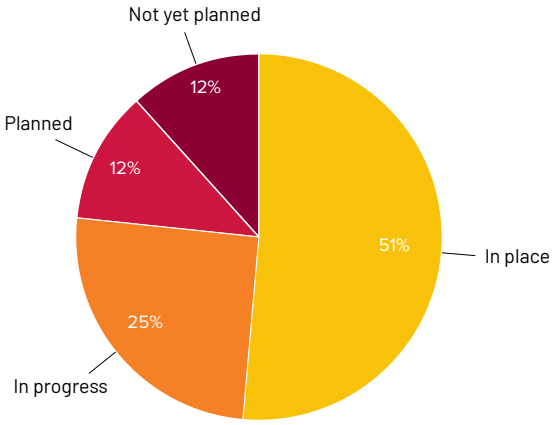
What is the status of effective OT patch management?



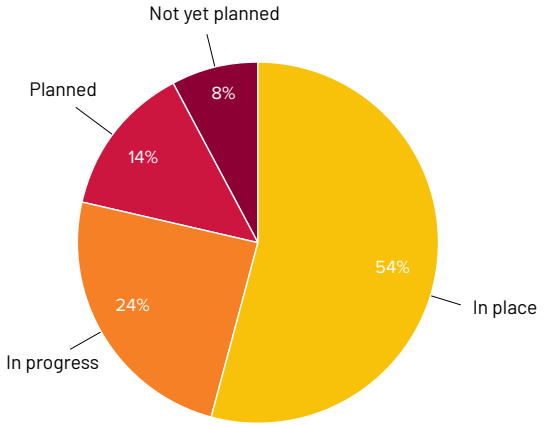
Operational systems data backup processes are regularly executed?



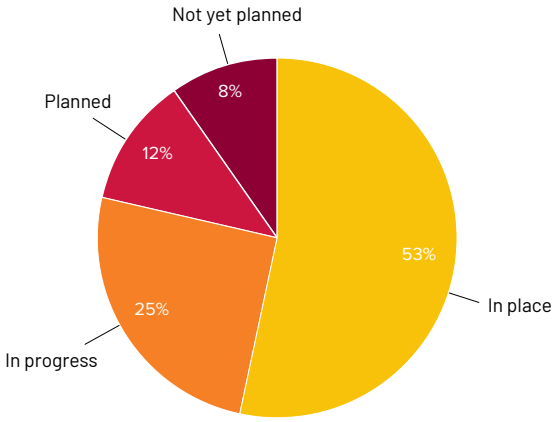
Protective technology: What is the status of effective removable media security procedures?



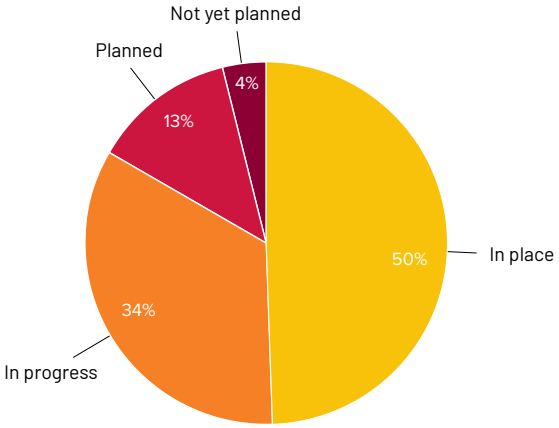
What is the status of having all endpoints access-controlled and monitored in real time 24/7?



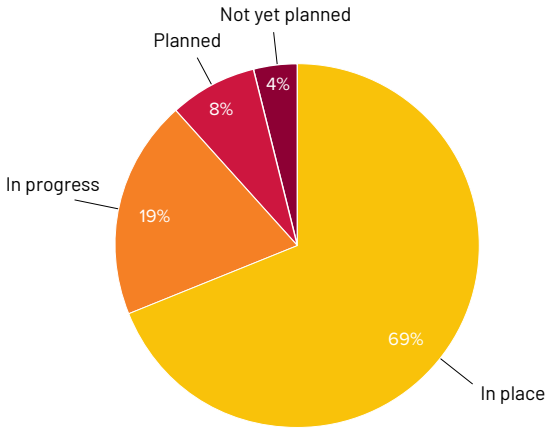
What is the status of a Security Event Information Management (SIEM) system, providing real-time analysis of security alerts generated by applications and network hardware?



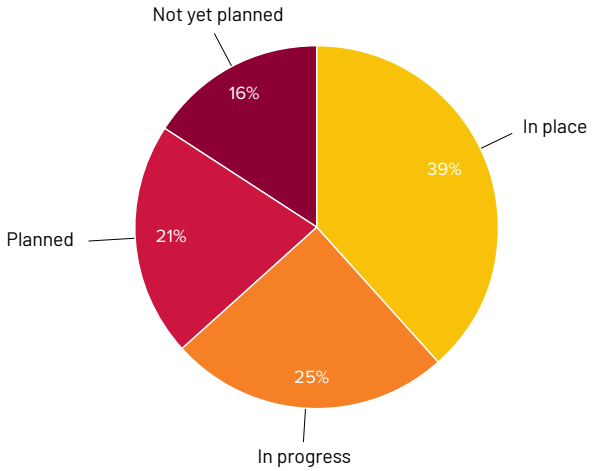
What is the status of network segmentation/ microsegmentation architecture implementation, placing security perimeters around business-critical systems?



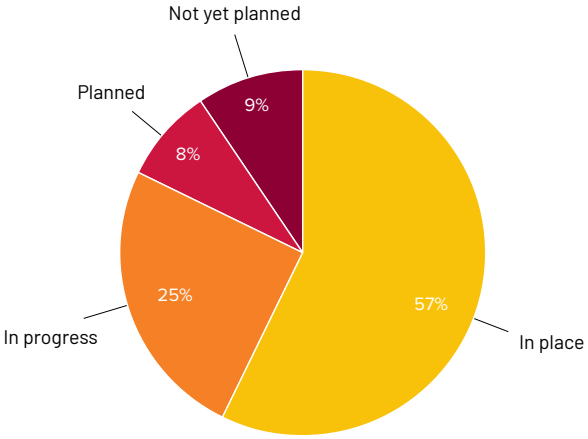
Do you have employee security awareness training and testing?



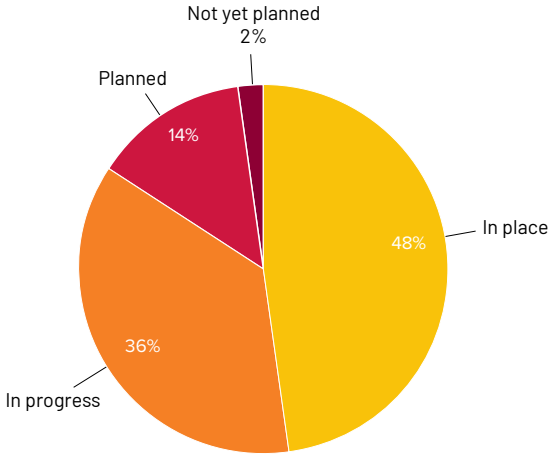
What is the status of implementing real-time threat and anomaly detection via OT SOC (owned or managed services) for malware, ransomware, vulnerabilities?



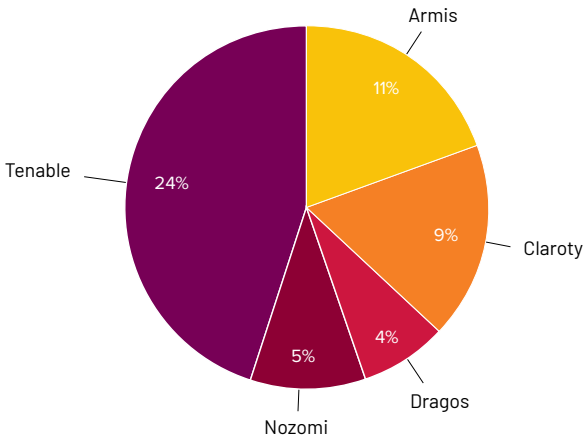
What is the status of cyber threat analysis, threat containment, and threat mitigation capabilities?



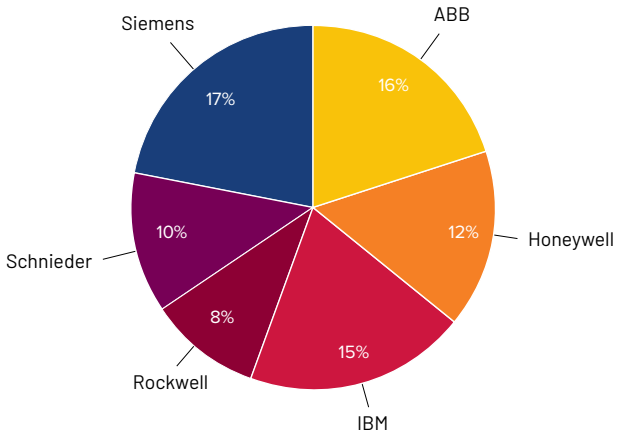
Status of systems, data and operational procedures to restore operations quickly in the event of a cyberattack?



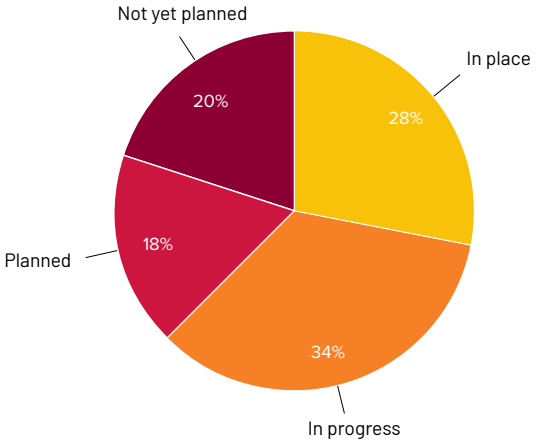
OT Threat Detection platforms or services in use?



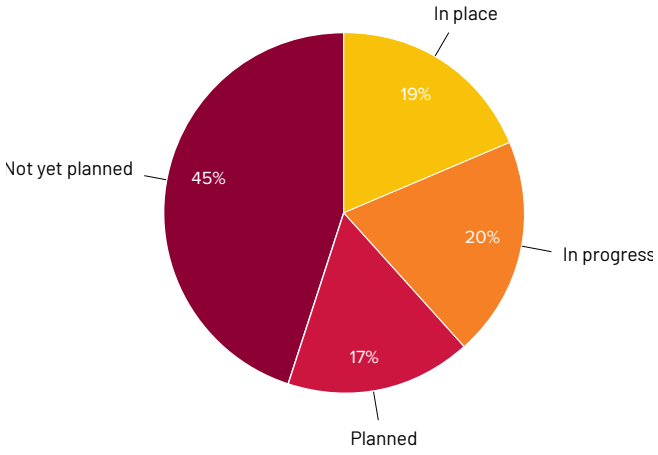
Industrial Automation service providers in use?



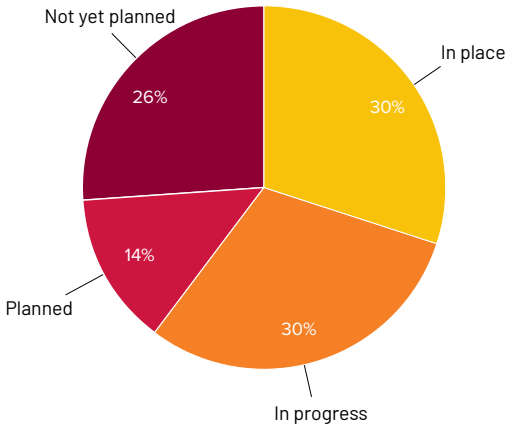
What is the status of implementing a converged IT/OT cybersecurity roadmap?



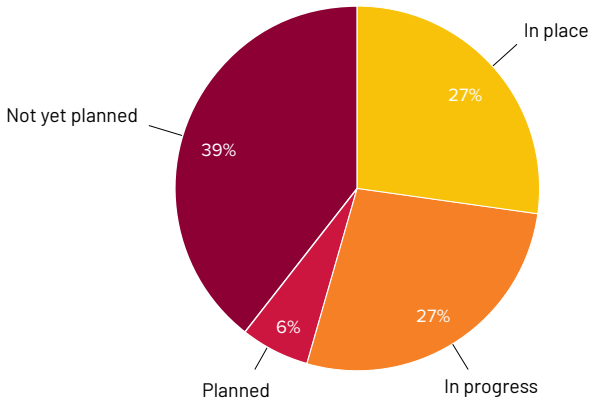
What is the status of using Common Industrial Protocol (CIP) certified products to secure and encrypt Ethernet communications?



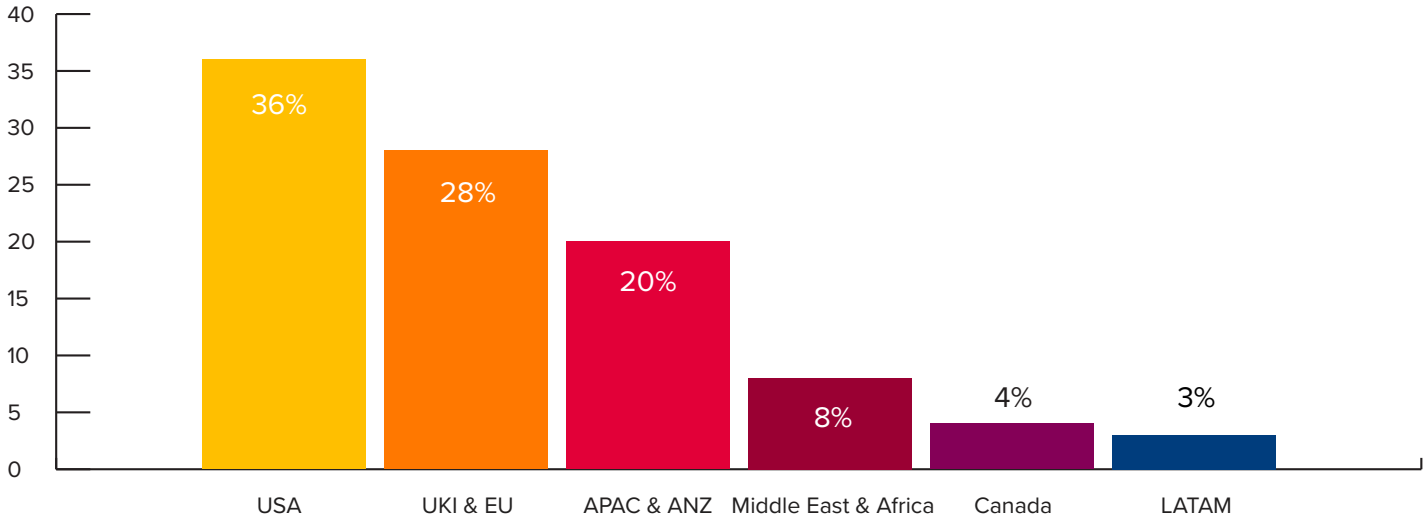
Does your organization work with one or more established cybersecurity partners, delivering dynamically updated and scalable OT SOC services?



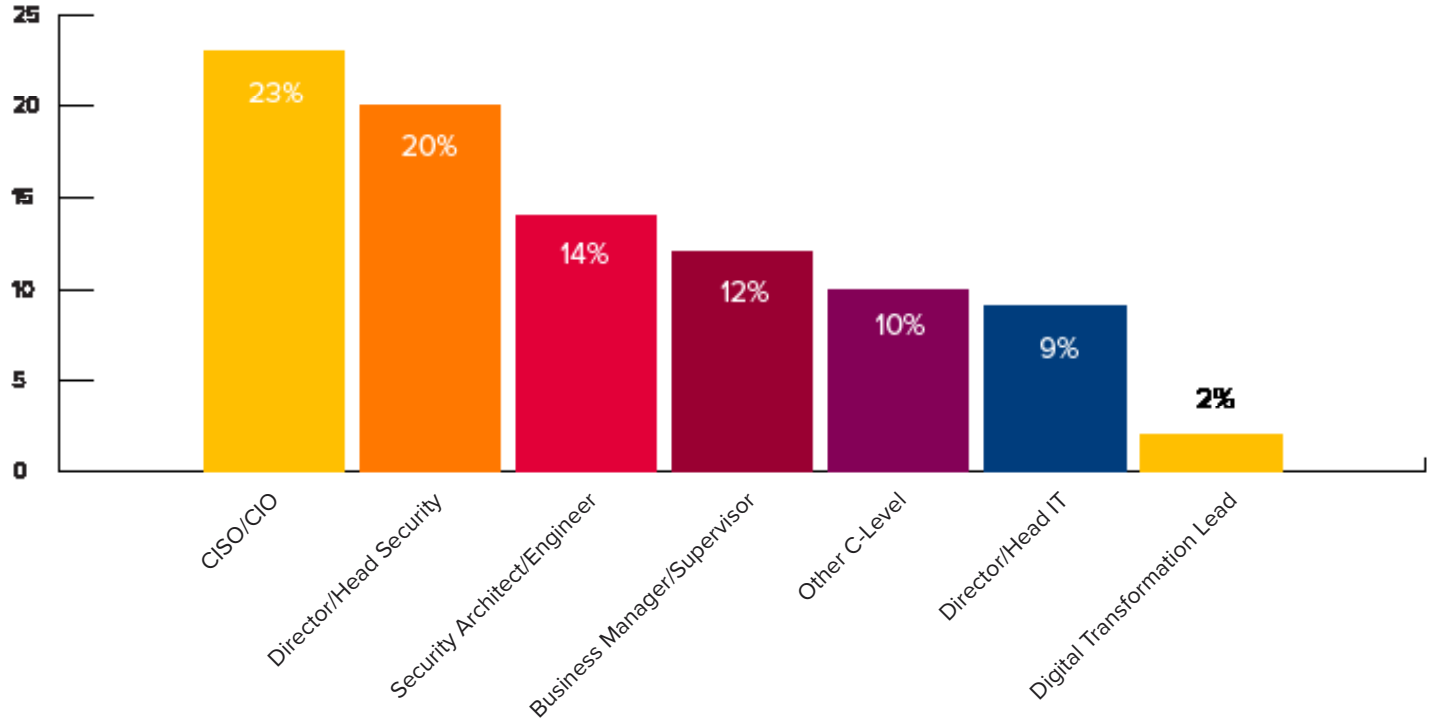
Does your organization have a cybersecurity plan, suitable for submission for US Infrastructure Bill funding grants?



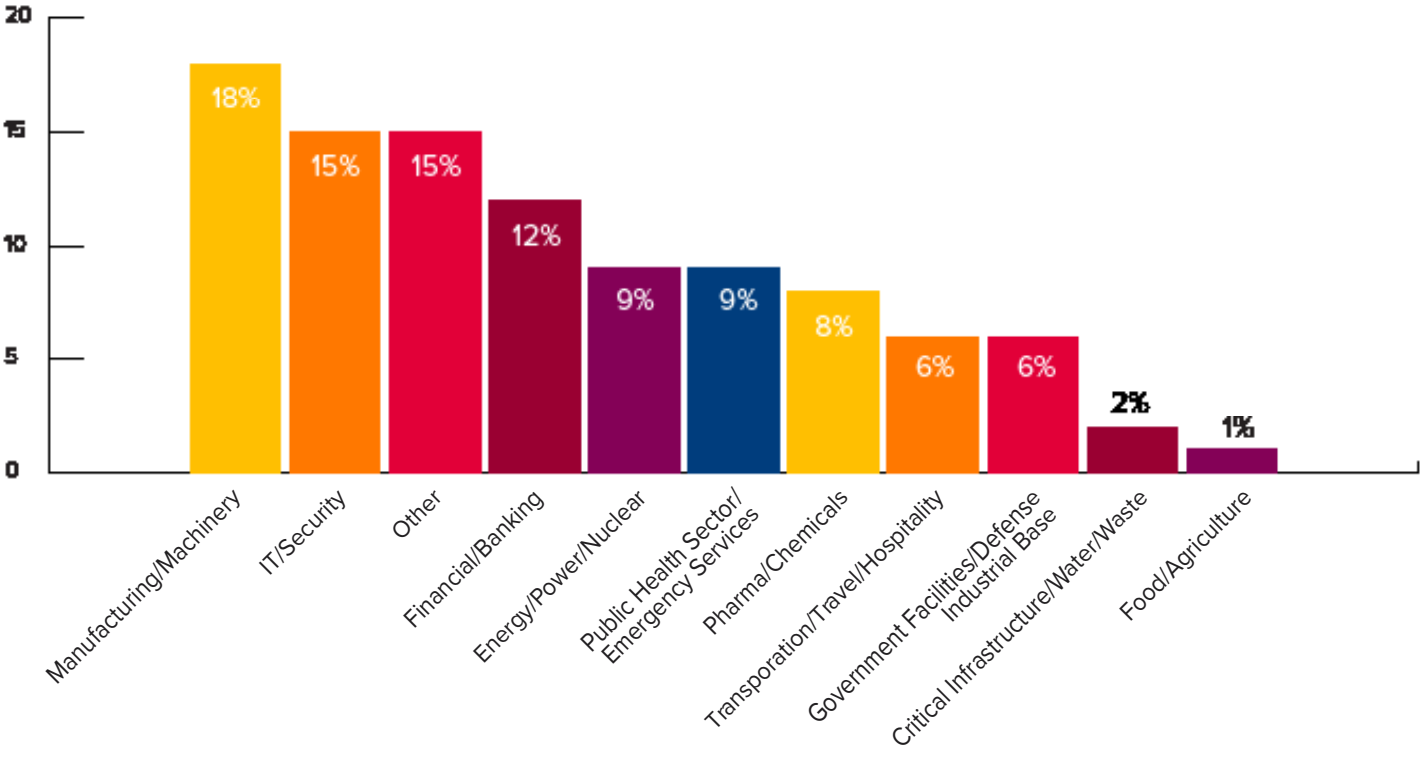
Survey Participants by Region



Survey Participants by Role



Survey Participants by Industry Sector



Kelly McLure
Sales Specialist
kmclure@goAgilix.com
Office: 901.334.4832
Mobile: 901.530.6534
www.goAgilix.com

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-SP016A-EN-P - June 2022