(CS)^{2}AI – KPMG Control System Cyber Security Annual Report 2022

The Chairman's Message

Dear Colleagues,

Here we are and another unusual year has passed. We have all been experiencing significant shared challenges around the world and though certainly not limited to cyber security, we know we still have a lot of work to do to secure our modern connected society.

On behalf of the tireless (CS)^{2}AI annual report steering committee, I am proud to introduce the second annual **2022 (CS)^{2}AI-KPMG Control System Cyber Security Annual Report**. This comprehensive report is the result of significant participation from our strategic alliance partner, KPMG, who we owe a heartfelt 'thank you' for helping bring this to life. We must also thank Fortinet, Waterfall Security Solutions and many supporting partners (see page 58) and the steering committee (pages 55–56) for their important contributions from the research phase all the way through the final report. Through their direct support of **(CS)^{2}AI** and this joint project, these companies and individuals continue to demonstrate their commitment to help solve the challenges the control systems cyber security workforce face today.

The report was based on survey results from more than 580 industry members at large and a representative sample of **(CS)^{2}AI's** worldwide membership (approaching 25,000 community members today), with questions regarding control system security events, trends in attack activities and protective technologies, and how organizations are prioritizing their efforts to tackle this challenge.

Most of us cannot 'do it all' and need to choose wisely where our focus goes. The goal of this annual report is to give individuals a clearer picture of what peers are doing and serve as an annual support tool for the many difficult decisions we know are being made.

Good luck!

I sincerely hope many find this report valuable and we welcome feedback of all types. Though we'd all love to hear positive things, constructive criticism is also a necessary ingredient to making this resource the best it can be. For feedback or if you want to get involved in the 2022 report project or any of our initiatives please send us a message at **GetInvolved@cs2ai.org**

Derek Harp
Founder & Chairman
(CS)^{2}AI

Annual report title sponsor foreword

Significant challenges continue to impact cybersecurity in industry and as the frequency and sophistication of threats increase, businesses should mobilize their resources and expertise in bold new ways to protect themselves.

It has indeed been an alarming year for OT cybersecurity amid high-profile attacks that have dominated international headlines, including the Colonial Pipeline, Oldsmar water facility and JBS Foods ransomware cases, to name just a few.

We've seen many companies, in response, rush to review and remediate their OT environments — typically dedicating some much-needed investment, talent and technology towards immediate solutions while working to maintain their critical operations and agility. The enhanced focus on OT security includes a particularly sharp lens on the growing threat of ransomware amid its alarming potential to disrupt sensitive OT environments and industrial targets.

While ransomware and other cyber threats are gaining momentum, businesses are also turning their attention to incidents and potential threats among state actors. While our survey respondents cite 'negligent insiders' as the single most common threat actor in control system security compromises, state-sponsored attacks have also become a significant concern.

As noted, these disturbing trends are prompting more companies to continue their pursuit of new investment in OT cybersecurity programs that may help them combat today's persistent and increasingly aggressive adversaries. But overall investment to protect OT infrastructure is showing evidence of budget constraints.

Most respondents reported a budget increase of about 10 percent, down from approximately 30 percent in our previous survey, while 10 percent of businesses actually reported a budget decrease, compared to about 1 percent a year earlier.

Meanwhile, roadblocks to true progress remain in the area of knowledge and expertise, as revealed in the survey. About half of the respondents (49.1 percent) cited 'insufficient control system cyber security expertise' as the greatest obstacle to reducing their control system cyberattack surface, while more than one third also cited 'insufficient personnel.'

At the same time, adequate investment in training is also lacking amid a trend to third-party outsourcing, which itself is providing limited solutions as service firms also struggle with personnel and skills shortages amid the global pandemic's labor supply disruption. While organizations are combining limited in-house expertise with outsourced personnel to solve today's challenges, it's important to note that managed services are not yet a sure bet in the OT space, with few SOC service offerings, for example, adequately designed for the complexities of today's critical OT cybersecurity needs.

This brings us back to the inevitable — and increasingly urgent — need for in-house training. The good news here is that some companies are indeed making progress amid the overall lack of investment in this crucial area, with a variety of training methods being used. While lower-maturity organizations still rely on traditional computer-based and instructor-led programs, we see more mature players turning to 'live' table-top incident-simulation exercises. This ultimately enables them to move from simply *understanding* OT security to understanding how *well prepared* they are to manage today's expanding threat landscape.

This trend speaks to the critical need for 'security awareness' training. Unlike security training — developing the skills and capabilities of specialized security practitioners — security awareness training aims to improve the security culture organization-wide, ideally enabling all employees to recognize their role in reducing risk exposures. While progress is unfolding, however, we still see nearly one in five organizations (18 percent) with no OT cybersecurity awareness training. That's worrisome when you consider the high threat of 'negligent insider' incidents that can involve something as simple as an uninformed employee clicking on a dangerous email link.

As for the current state of organizational planning, it's encouraging to note that more than 85 percent of organizations say they have management/response plans at some stage of development. And while implementation and testing percentages remain low, this is still a significant improvement over 2020, when 18–27 percent did not even have such planning in place.

As the latest comprehensive survey shows, considerable ground remains to be covered in today's perilous environment as the threat landscape grows and the pace of change accelerates. A heightened sense of urgency has become critical and the need for highly skilled OT-security practitioners cannot be overstated. True progress will require a strategic balancing act that manages costs, system availability and modern measures to combat today's growing threats — and we believe there is no time to lose.

Walter Risi
Global Cyber IoT Leader
KPMG in Argentina

Contents

The Chairman's Message 2

Annual report title sponsor foreword 3

Executive summary 6

- Project objective 6
- Survey methodology 7

Survey results 9

- Top priorities 9
- Key performance indicators (KPIs) tracked 10
- Pre-acquisition risk assessments 12
- Greatest obstacles to reducing the (CS)^2 attack surface 15
- Top three areas for ROI on (CS)^2 investments 17
- Top three areas of greatest expenditure on (CS)^2 18
- Budgets 19
- Services in use 23
- Awareness training 25
- Training 26
- Accessibility of control system components 27
- Control system components most susceptible to compromise 28
- State of organizational plans 28
- Managed services 30
- Current control system network activity monitoring 31
- Assessments 33
  - Frequency 33
  - Inclusions 33
  - Follow-up activities 35
- Frameworks in use 36
- Technologies in use 37
- Recent incidents 37
- Recent incident impacts 39
- Recent attack vectors 40
- Threat actors 41
- Sources of cyber threat information 43
- Confidence in network visibility 44
- Confidence in cyberattack response processes 45
- Investments in the coming year 45

Chief recommendations 47

Appendix A: Participant demographics 48

Respondent demographics 49

- Gender participation 50
- Age distribution 51
- Respondent educational level 52
- Respondent employment type 52
- Organization category 53
- Organization workforce size 53

Appendix B: Annual report steering committee 54

Appendix C: About (CS)^{2}AI 56

Appendix D: Report sponsors 57

Executive summary

This report is the latest in a series of annual projects, drawing from ongoing research by the Control System Cyber Security Association International ((CS)²AI) and its community of members and Strategic Alliance Partners (SAPs). Based in decades of Control System (CS) security survey development, research and analysis led by (CS)²AI Founder and Chairman Derek Harp and Co-Founder and President Bengt Gregory- Brown, the (CS)²AI team invited participation from our 24,000+ global membership and thousands of others in our extended community. We asked them key questions about their experiences in the front lines of operating, protecting, and defending Operational Technology (OT) systems and assets costing millions to billions in capital outlay, impacting as much or more in ongoing revenues, and affecting the daily lives and business operations of enterprises worldwide. Over 580 of them responded to our primary survey and many others participated in numerous secondary data gathering tools which we run periodically.

This pool of data, submitted anonymously to ensure the exclusion of organizational politics and vendor influences, has offered insights into the realities faced by individuals and organizations responsible for CS/OT operations and assets beyond what could fit into this report. We hope the details we have selected to include serve the decision support need we set out to answer.

Project objective

The (CS)²AI-KPMG Control System Cyber Security Report Steering Committee launched the project to collect, analyze and report on data from professionals working in control system cyber security in the first quarter of 2021, with the goal of producing another in our annual series of informative decision-making tools for everyone involved with this work, whether end-users or vendors, leaders or operational.

To gather our data we invited participation in the survey component through a wide range of broadcast and direct channels, targeting all parties actively engaged in the cyber security of Control Systems. Our respondents included professionals at all organizational levels: cyber security specialists and subject matter experts (SMEs) as well as those whose work includes but does not necessarily consist solely of securing and protecting control systems.

This Report uses the overarching term 'Control Systems' to refer to any/all systems that manage, monitor and/or control physical devices and processes. CS or (CS) should be considered to include Industrial Control Systems (ICS), Supervisory Control & Data Acquisition (SCADA), Process Control Systems (PCS), Process Control Domains (PCD), Building/Facility Control, Automation & Management Systems (BACS/BAMS/FRCS…), network-connected medical devices, etc.

Similarly, the term (CS)² refers to the Control System Cyber Security field, profession and workforce.

Key highlights

Respondents from organizations who self-identified as having higher-maturity ('High M') control system cyber security programs stood out from those in Low M organizations in numerous ways. Of particular note, High M participants are:

- *Nearly twice as likely to include IEC62443-4-1 Compliance* in their control system product/service pre-acquisition risk assessments (**34.8 percent** High M vs **17.6 percent** Low M).
- More than twice as likely as to use *Internal security teams under CISO/CSO/CTO* (**49.3 percent** vs **21.4 percent**).
- Nearly four times as likely to leverage managed control system security services (**44.3 percent** High M vs **12.8 percent** Low M).
- Nearly three times as likely to have implemented network monitoring of all control system network activity (**35.7 percent** High M vs **13 percent** Low M) and to plan increasing the degree of that monitoring within the next 18 months (**17.1 percent** High M vs **6.5 percent** Low M).
- More than twice as likely to continuously monitor all devices, users and applications on their networks (**27.5 percent** High M vs **12.5 percent** Low M).

Survey methodology

The (CS)²AI-KPMG Control System Cyber Security Survey and Report was a collaborative effort of the following entities:

— **(CS)²AI:** As the originator of the project, (CS)²AI held the primary role in developing, leading and implementing the project, including producing the project deliverable of authoring this report.

— **KPMG:** As the Title Project Sponsor, KPMG provided primary support in the form of funding and human and organization resources to augment (CS)²AI's own capabilities.

— **Additional sponsors:** non-Title Sponsors provided additional funding and human and organization resources where possible. (See Appendix D: Report sponsors.)

Pursuant to the project objectives stated above, (CS)²AI and the project sponsors distributed multiple online surveys to members of the CS/OT working in the field during the second and third quarters of 2021, collecting key data around CS events, activities and technologies as well as regarding how organizations are responding to ongoing developments in the threatscape.[1] (CS)²AI invited participation from its associated members, known OT security defenders and researchers, distributed the survey through various social media channels, and promoted it on sites serving the CS cyber security workforce, with the intent to collect as wide a sample as possible. Respondents self-selected by affirming their involvement with the field of CS Cyber Security.

The ability to parse our participants into different groups and consider their responses in light of their group associations is key to the insights derived from this annual research project. In our view, the survey participants' control system cyber security program maturity is the most important dimension. We asked each participant to choose which of the following descriptors best fit the situation in their organization.

[1] Threatscape: the sum of all possible threats to CS/OT operations and assets. The threatscape is dynamic, continually shifting as vulnerabilities are discovered and protections are developed to counter their exploitation.

Level 1 — Fire-fighting. Cybersecurity processes are unorganized and undocumented, not organized in a 'program.' Success depends on individual efforts; it is not repeatable or scalable because processes are not sufficiently defined and documented. Passive Defense

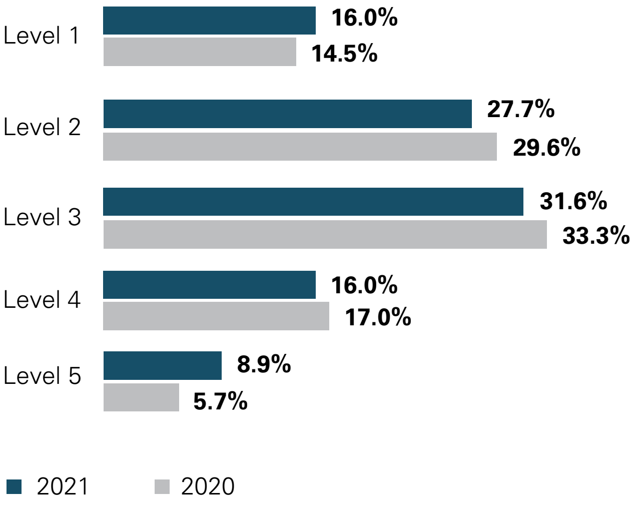
Level 2 — Basic project management practices are followed in cybersecurity implementations; success continues to require key individuals, but a body of knowledge is developing. Best practices are performed but may be ad hoc. Passive Defense

Level 3 — Cybersecurity both produces and works from documented processes and procedures. Key stakeholders are identified and involved. Adequate resources are provided to support the process (people, funding and tools). Standards and/or guidelines have been identified to guide the implementations. Passive Defense

Level 4 — The Cybersecurity program uses data collection and analysis to improve its outcomes. Activities are guided by documented organizational directives; policies include compliance requirements for specified standards and/or guidelines. Personnel responsible for control system security duties have training and experience. Program is managed, proactive, tracks metrics, some automation. Active Defense, SIEM, Anomaly and Breach Detection

Level 5 — Cybersecurity processes continually improved via feedback from existing processes and adapting to better serve organizational needs. Personnel performing the processes have adequate skills and knowledge. Optimizing, automated, integrated, predictable. Active Defense, Threat Intelligence, Incident Management

In your view, which of these best describes your control system cyber security program?



We then look at how the responses of those self-identifying as *Level 1 or Level 2* ('Lower Maturity' or 'Low M') differ from those identifying as *Level 4 or Level 5* ('High Maturity' or 'High M'). The two groups do not differ significantly in responses to all questions but, where they do, we show this in charts comparing the two.

The annual cycle of these research projects also enables us to examine our data longitudinally in search of trends and changes from year to year. Refinement and revision of surveys and their component questions sometimes prevents direct comparisons but, where possible and when interesting deltas between annual data sets are found, we bring those to the attention of our readers.

> The range in the data set responses with respect to Cyber Security Program Maturity is consistent with Industrial Defender's experience. Industries/verticals that have either chosen a standard via corporate or regulatory edict tend to fall within the Level 3 categorization of Cyber Security Programs. Unfortunately, industry verticals such as water and midstream gas typically tend to land in the Level 1 and Level 2 categories due to lack of funding and regulatory oversight.

George Kalavantis
COO at Industrial Defender

Survey results

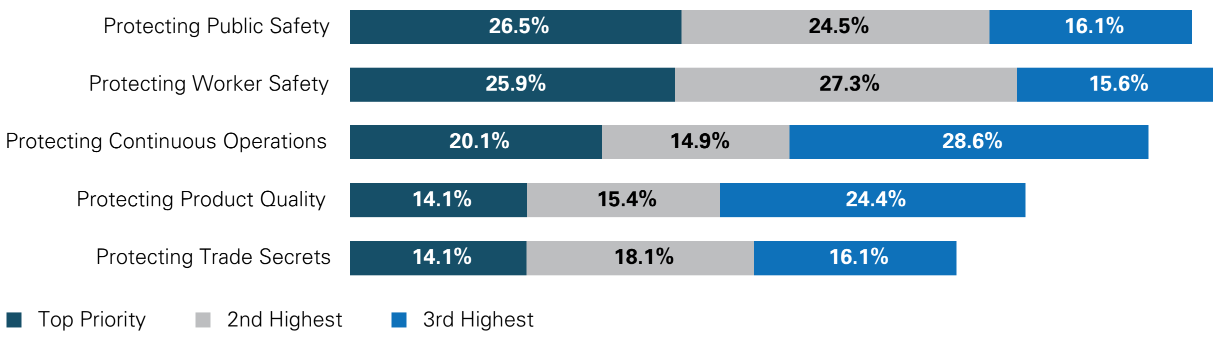
Top priorities

To increase the utility of this research as a decision-making tool we incorporated more categorization questions than in its predecessor. Notably, we isolated responses from end users to analyze them separately from security technology and service vendors. In many questions we found responses from these groups to be quite similar but, in areas with greater divergence, we may present the end user responses specifically.

The topic of top control system cyber security priorities is one of these. With all options receiving some support from various end users, it is clear there continues to be a strong prioritization placed on protecting the safety of workers and the public.

Some of our Subject Matter Expert Steering Committee members expressed surprise that *Safety* did not receive a much higher ranking, as it has always been central to OT security considerations. As is often true, the underlying question of *why* participants responded this way is not entirely clear. It may be that many do not consider their Safety Instrumented Systems exposed to cyber threats (despite ample evidence that many are) and well-known cases of cyberattacks on SIS.[2]

Rank your organization's top control system cyber security priorities (End Users)



> When critical infrastructure is hacked daily, it's no surprise there's an ever-rising concern among OT stakeholders related to secure, continuous operations. We see the network solutions that worked in the past, like adding yet another firewall, are no longer effective. These factors alone point to an ongoing need for cyber security solutions like zero trust and secure remote access to reduce attack surfaces and mitigate negative financial impact to an organization.
>
> **Keith Beeman**
> CEO, Tempered Networks

[2] https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

Key performance indicators (KPIs) tracked

The metrics an organization uses to track performance of its cyber security program can carry valuable information regarding its priorities, its level of maturity, likely past incident experiences, and current security posture. For example, a glance at the table below will show that High M organizations use many key performance indicators more than less mature programs, with some KPIs tracked almost twice as often by the former (e.g., *Reducing the number of Security Incidents:* 50.7 percent High M versus 25.6 percent Low M). At the same time, the Low M organizations are more than twice as likely to not track any KPIs at all (*My organization does not track KPIs,* 10.4 percent Low Maturity vs. 4.2 percent High Maturity). High M organizations have much greater visibility into their environments, enabling them to compute more meaningful metrics, identify and track their KPIs more consistently.

In only a few areas do the groups of respondents approach parity, notably *Reducing the financial cost of security incidents, Reducing the number of shared accounts, and Reducing the number of security incident false positives.*

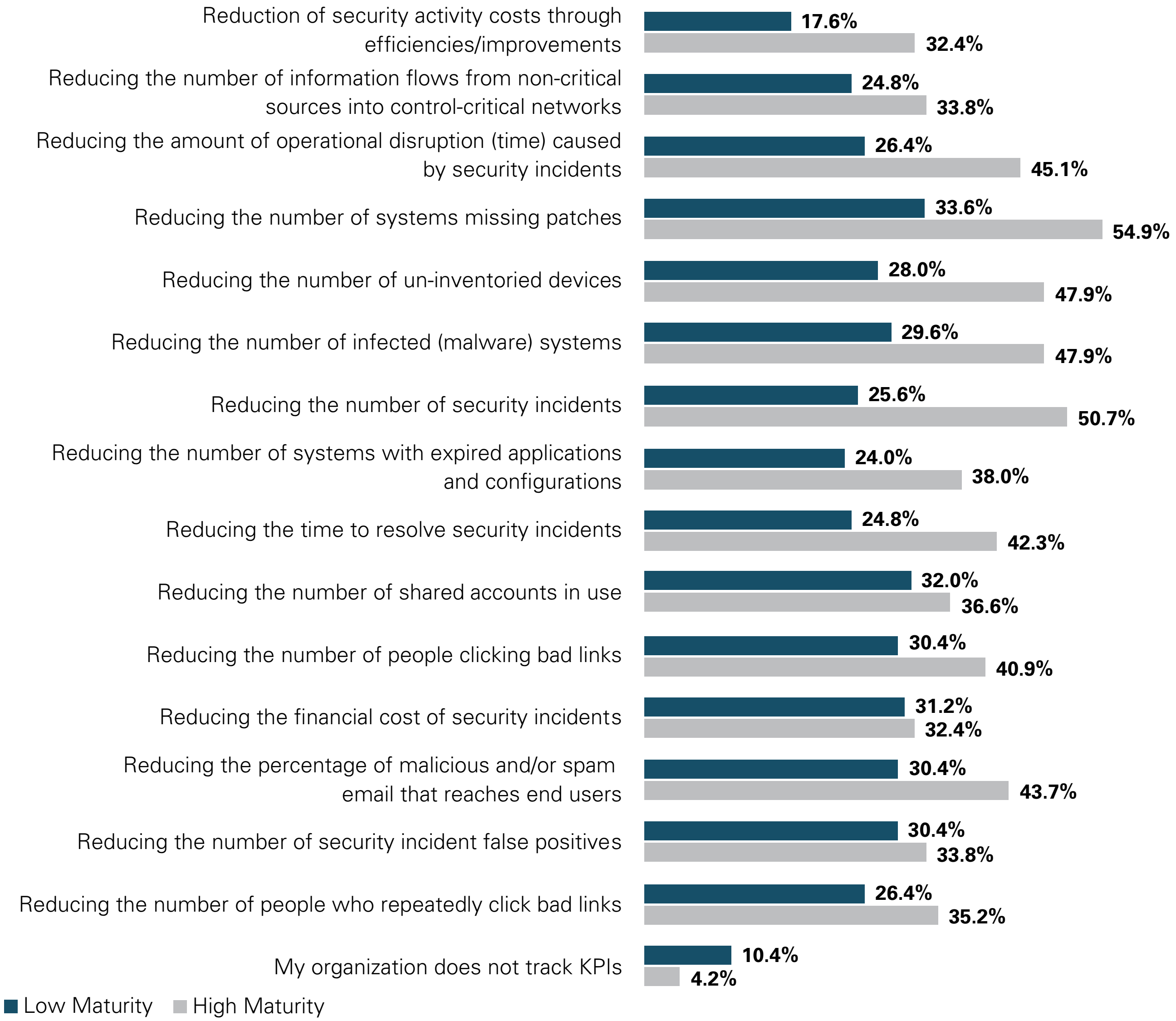
While security program maturity levels were evenly distributed among respondent organizations of all sizes, we noted that larger entities did track a subset of KPIs more than smaller ones, as shown in the next table. The two groups reported use of other KPIs quite similarly, but we found distinct differences in usage of these 11 specific indicators.

We examined how responses of other subsets of participants differed on numerous questions.

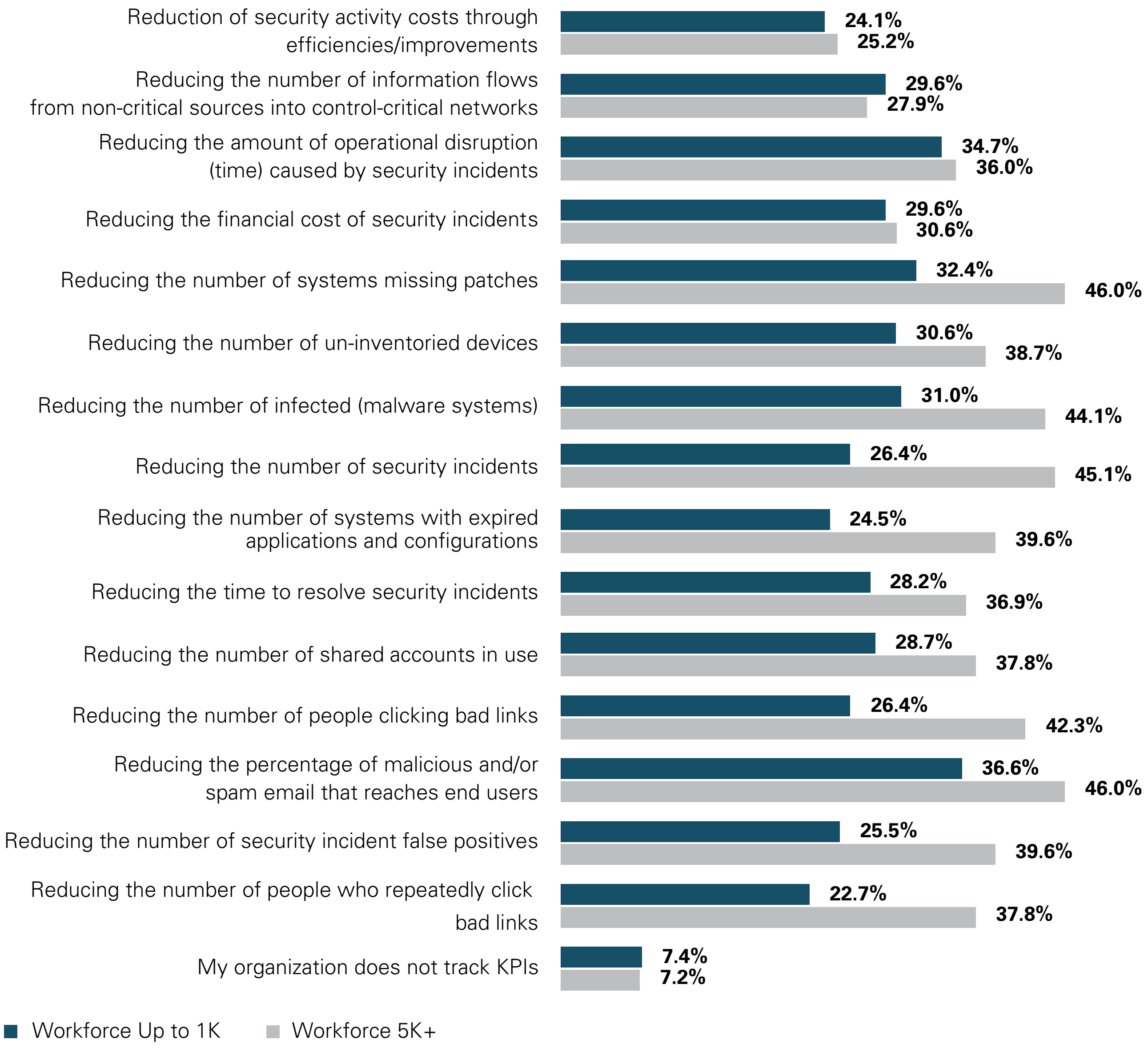
Where a statistically useful correlation was found, we use the symbol “ρ” to call this to the readers’ attention.

ρ

Identify all security program key performance indicators your organization uses (High Maturity vs Low Maturity)



Identify all security program key performance indicators your organization uses (Large vs Small Organizations)



> “A lot of these metrics feed into each other creating a positive feedback loop. Organizations that are proactive about reducing unpatched systems and expired apps/configs will find lower occurrences of ransomware, and swifter resolution. A similar case can be made for user behaviors — orgs tracking user training and results of cyber exercises (like phishing) will most likely see a drop in number of people clicking bad links (once or multiple times) and the incidents that stem from social engineering attack vectors.”

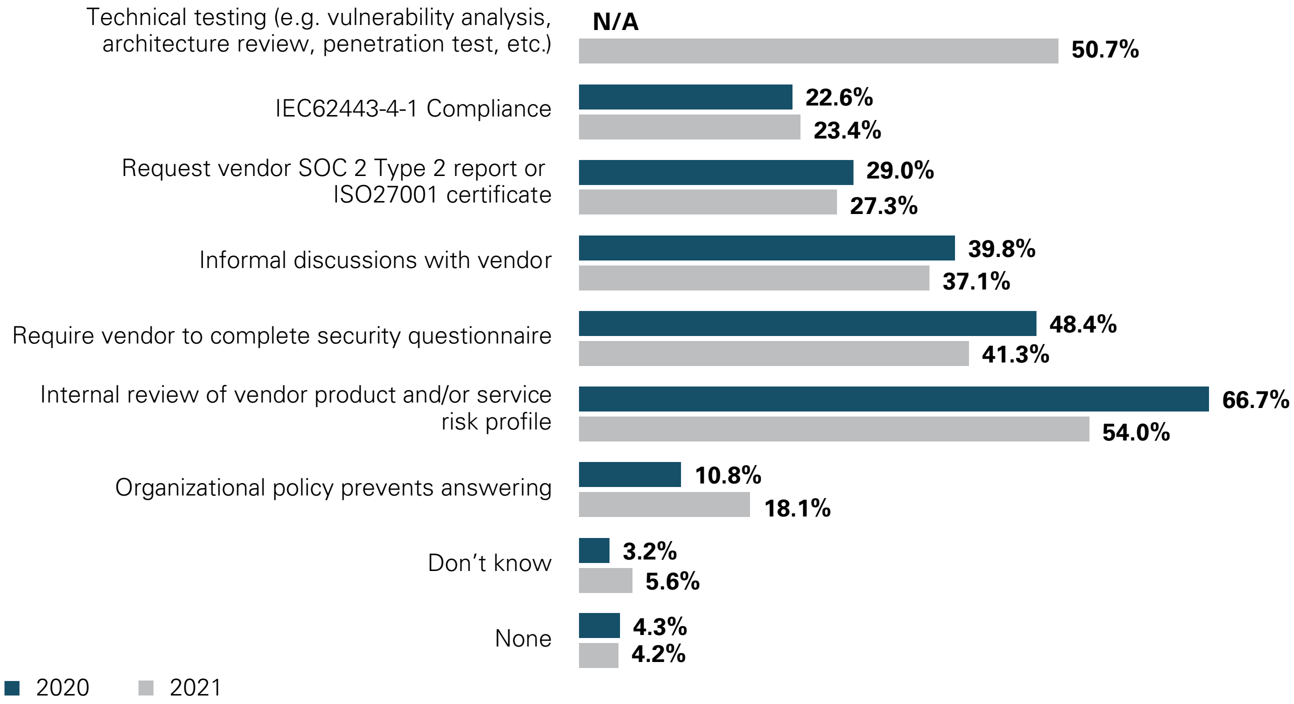
Brad Raiford
Director, Cyber Security, KPMG in the US

Pre-acquisition risk assessments

Internal review of vendor product and/or service risk profile is still the most used pre-acquisition form of risk assessment for control systems owners (54 percent now vs 67 percent in 2020). We added “Technical Testing” as a new option this year, and it is encouraging to see that at least half of the respondent organizations do this. Of that group, most (69.2 percent) also conduct internal reviews of vendor products and/or service risk profiles and (50.6 percent) require vendors to complete security questionnaires. Potential impacts being what they are in many control system settings, the authors of course recommend using multiple approaches to measuring and managing risks.

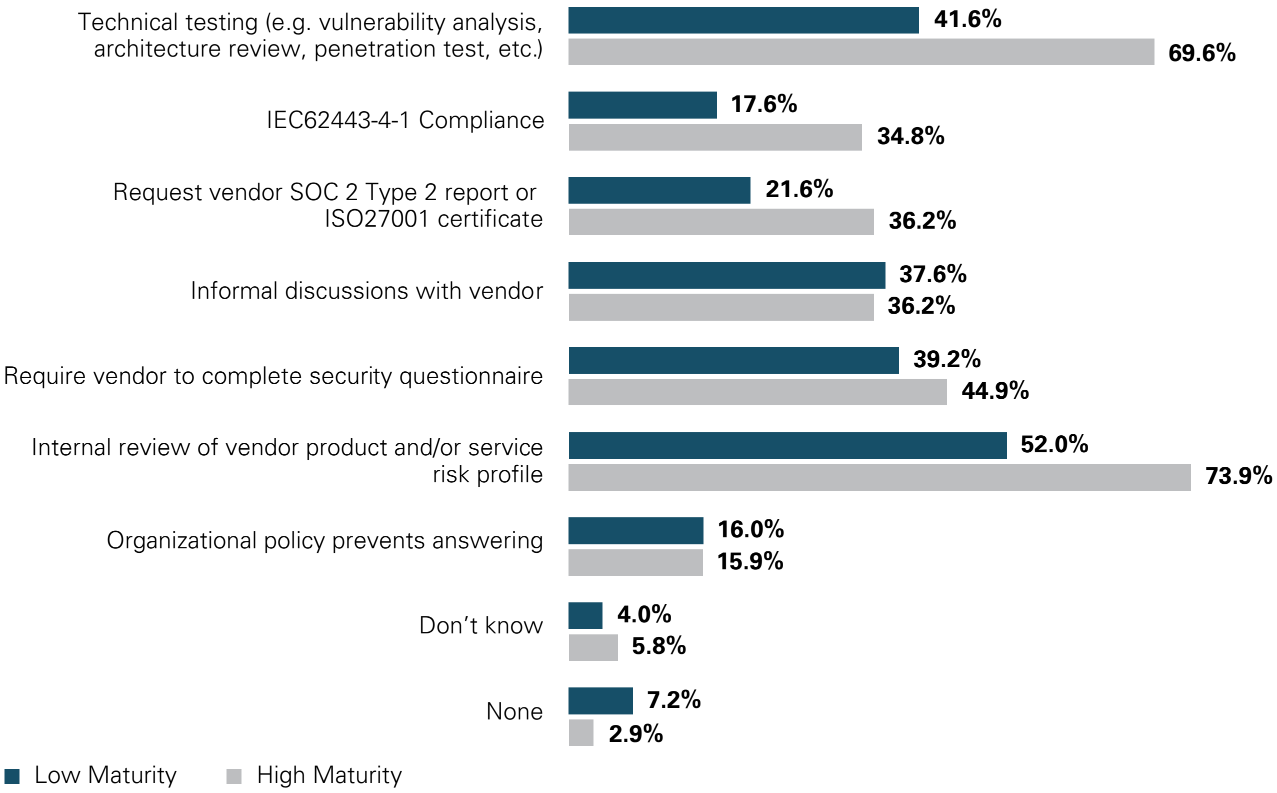
Of particular note in comparison of High and Low M organizations are the broad differences in their assessments of *IEC62443-4-1 Compliance* (34.8 percent High M vs 17.6 percent Low M) and their inclusion of *Technical Testing* (69.6 percent High M vs 41.6 percent Low M). Significantly greater frequency of an *Internal review of vendor product and/or service risk profile* stood out as well (73.9 percent High M vs 52 percent Low M).

Identify all risk assessments your organization performs before acquiring control system products or services



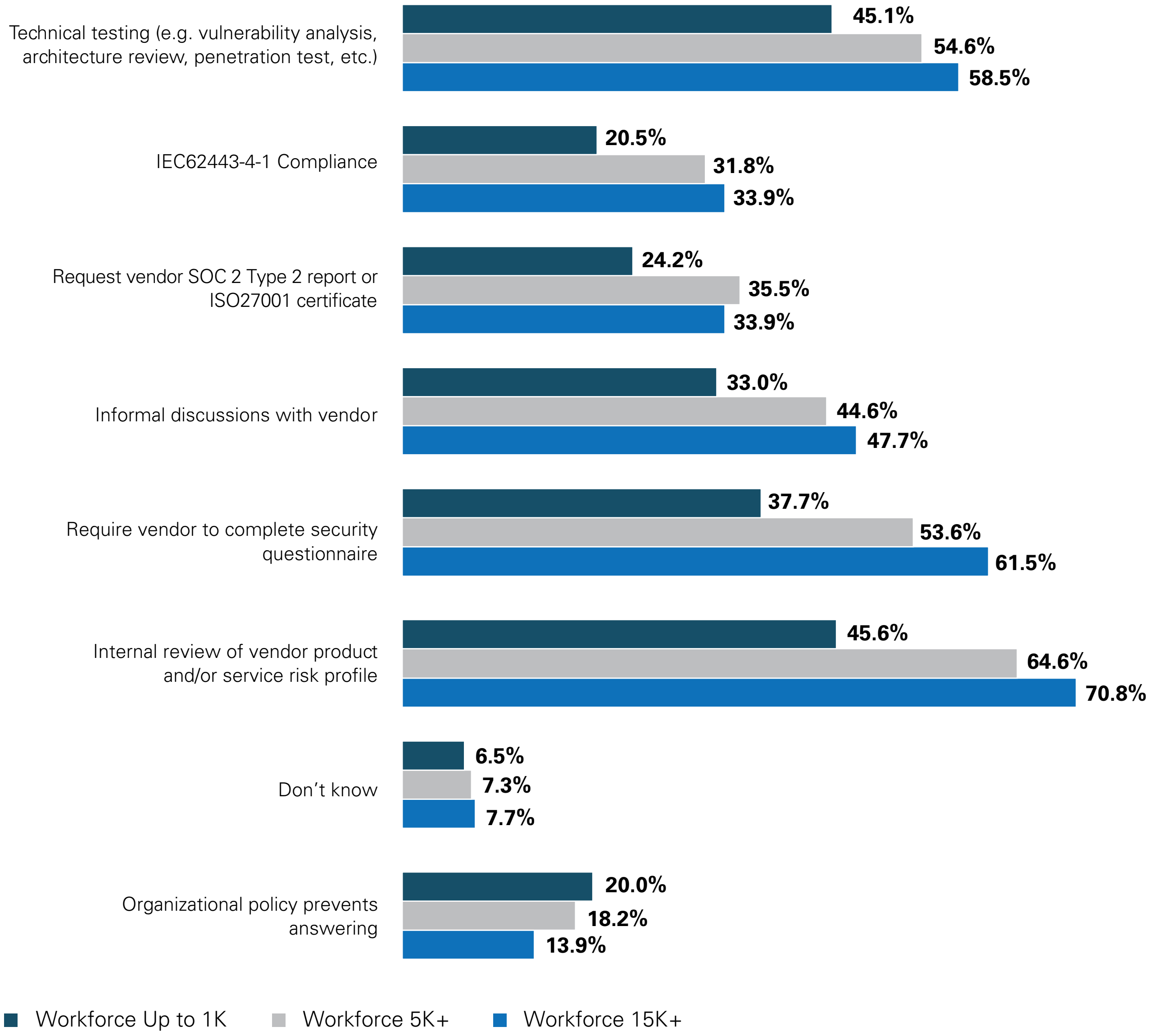
The size of respondent organizations (as defined by size of workforce) clearly influenced the risk assessments carried out prior to acquiring control system products or services as well. Even controlling for cyber security program maturity levels, larger organizations are more likely to conduct **every** type of risk assessment. Perhaps these entities, having greater resources, can and do choose to be more thorough in this aspect of their risk management.

Identify all risk assessments your organization performs before acquiring control system products or services (High Maturity vs Low Maturity)

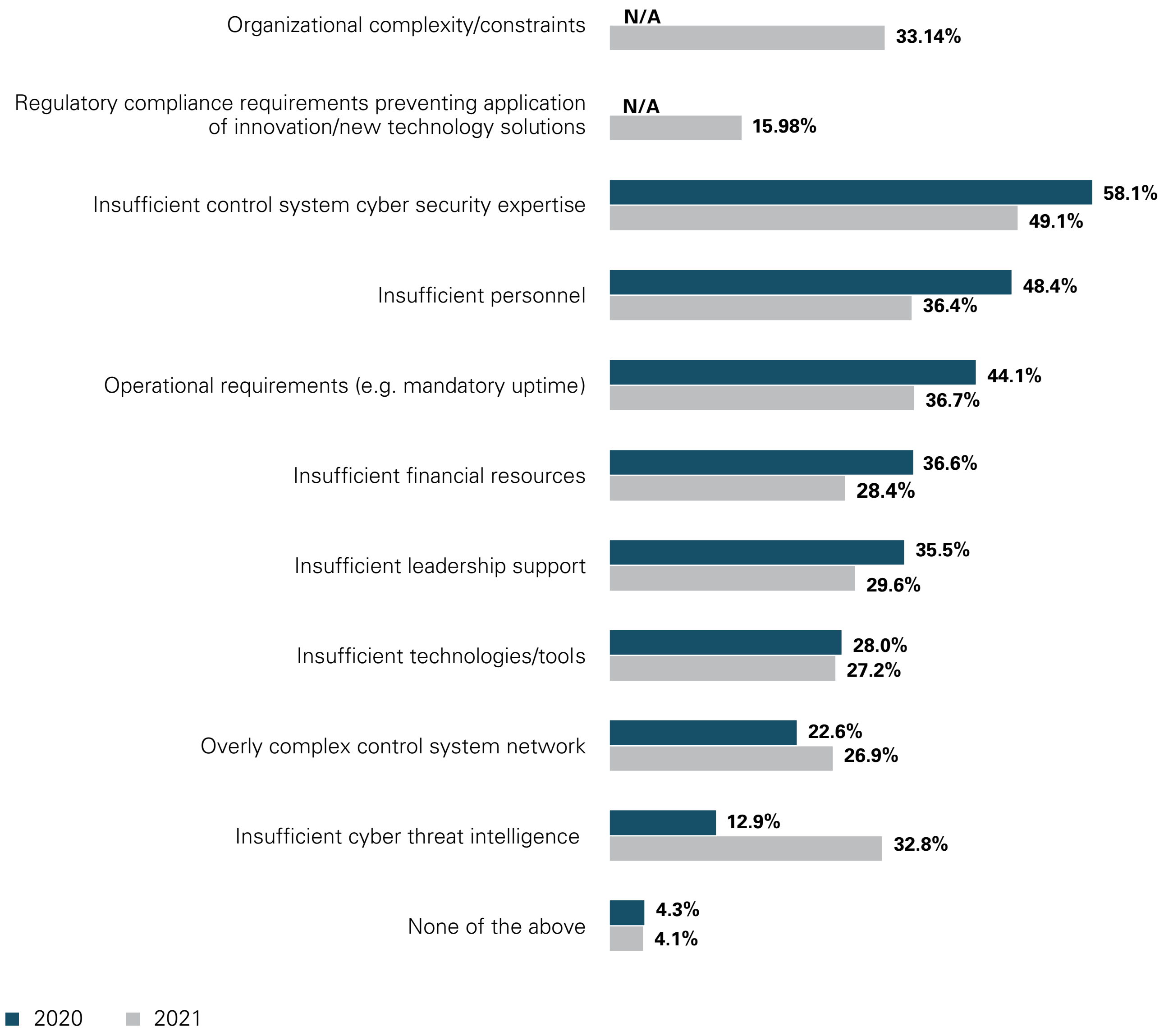


Available resources notwithstanding, challenges that reliably increase with organization size are vendor portfolio size and maintaining a current awareness of risks. Pre-acquisition risk assessments may be called for only once, but the periodic post-acquisition assessments of an ever-growing list of vendors and their equipment, software and services may swell into the thousands or tens of thousands over time.

ρ Identify all risk assessments your organization performs before acquiring control system products or services (by Organization size)



Select the greatest obstacles to reducing the control system cyber security attack surface (2020 vs 2021)

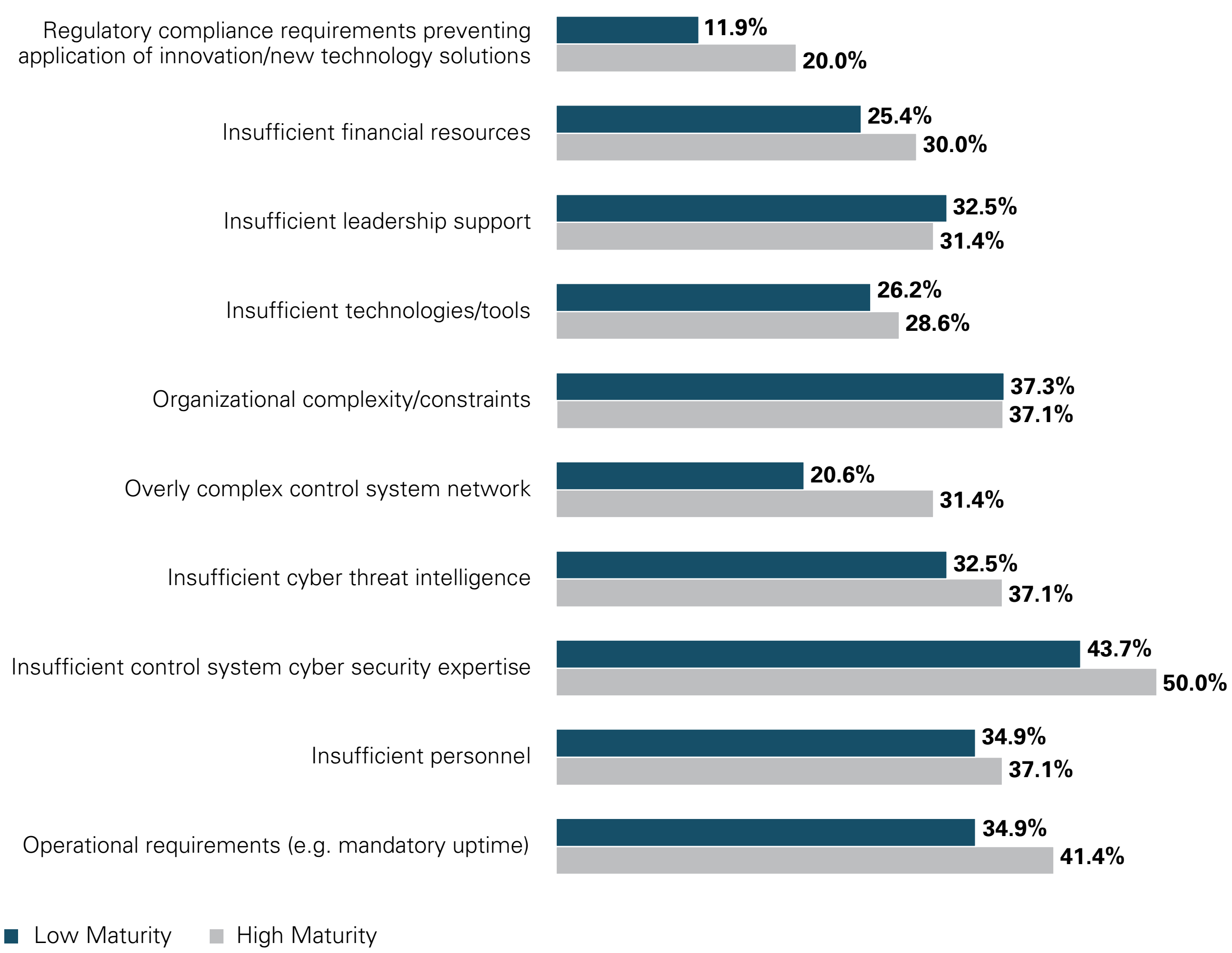


Greatest obstacles to reducing the (CS)^2 attack surface

Insufficient control system cyber security expertise continues to be widely considered the greatest obstacle to reducing the control system cyber security attack surface.

In longitudinal analysis, almost all factors received a lower percentage of responses than in our 2020 report, an unsurprising effect of having added two new answer options to this question this year. It is worth noting that *Insufficient Technologies/Tools* was nearly unchanged (27.2 percent this year vs 28.0 percent in 2020) and two others received a larger share of responses. *Insufficient Cyber Threat Intelligence* jumped to 32.8 percent (2021) from 12.9 percent (2020) and *Overly Complex Control System Network* rose slightly to 26.9 percent (2021) from 22.6 percent (2020). Many organizations, of course, do experience frustration from greater administrative complexity and new barriers to network visibility when implementing greater levels of network segmentation.

Select the greatest obstacles to reducing the control system cyber security attack surface (High Maturity vs Low Maturity)



Common write-ins (entered by respondents using our *Other* field on this question) included *Supply chain issues, Lack of secure OT products,* and *Insufficient support below the leadership level of the organization.*

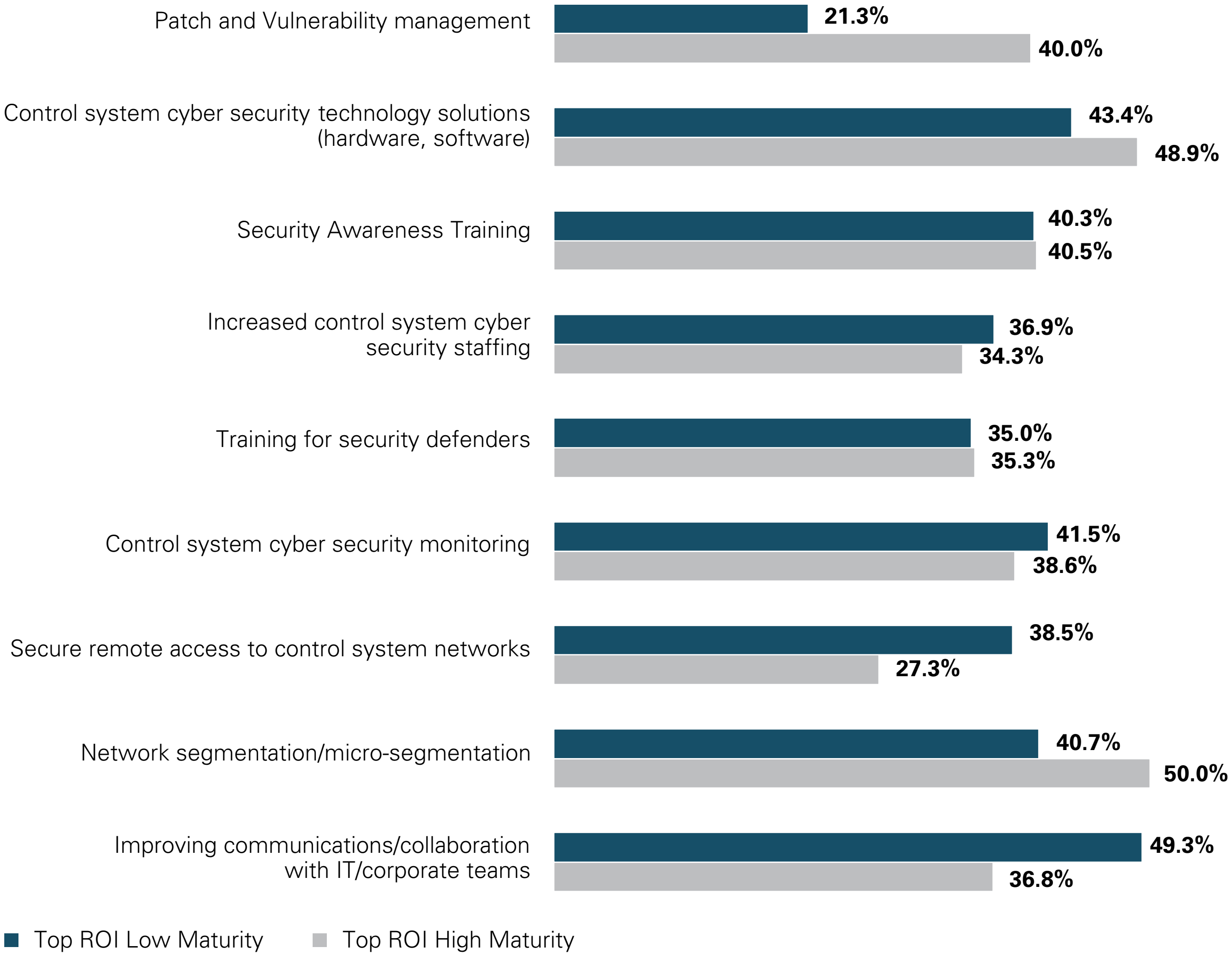
> From this survey result, we can see that as IT and OT continue to network, the complexity of the organization related to OT security is a major obstacle, along with the lack of ICS cybersecurity expertise.
>
> Adversaries attack regardless of IT and OT environment, and organizational silos do not give a complete picture of the risk. Asset owners need to improve their ICS cybersecurity expertise and combine it with IT security expertise. The ability of the situation awareness across IT and OT is essential to ensure resilient critical operations. A security platform that integrates IT and OT telemetry to provide one vision will effectively enhance the protection, detection and response capabilities of the critical infrastructures.

William Malik
Vice President of Infrastructure Strategies,
Trend Micro

Top three areas for ROI on (CS)² investments

Respondents differed significantly on where they considered the best places to spend their cyber security dollars based on the relative maturity of their control system cyber security programs. Both groups place very similar emphasis on *Security Awareness Training, Training for security defenders* and *Increased control system cyber security staffing*. Outside of those three related areas, we see deltas ranging from nearly 3 percentage points (*Control system cyber security monitoring*: 38.6 percent Low M vs 41.5 percent High M) up to nearly 20 (*Patch and Vulnerability management*: 21.3 percent Low M vs 40 percent High M).

What area provides the greatest returns on control system cyber security investments? (High Maturity vs Low Maturity)



High Maturity organizations are nearly twice as likely to believe that *Patch and Vulnerability Management* provide high ROI.

> “The study suggests that further scrutiny is warranted to determine whether there are lower ROI expectations on improving communication and collaboration between OT organizations and their corporate IT counterparts. In Fortinet’s 2021 The State of Operational Technology and Cybersecurity research report, findings indicated IT-OT convergence was well underway pre-pandemic, and the pandemic only accelerated digital transformation and increased the need for connectivity.
>
> The study also revealed that the few companies who reported zero intrusions were more likely to adhere to several best practices. They were:
>
> — more likely to use orchestration and automation and have security tracking and reporting in place.
>
> — more likely to have 100 percent centralized visibility in their security operations center.
>
> — more prepared, earlier, to accommodate working from home during the pandemic.
>
> As the old adage goes, what gets measured gets improved. Financial implications to security vulnerabilities were tracked and reported by 74 percent of top-tier organizations. They also track vulnerabilities found and blocked (74 percent) and tangible risk management outcomes (60 percent).”
>
> **William Noto**
> Global Product Marketing Leader for Operational Technology, Fortinet

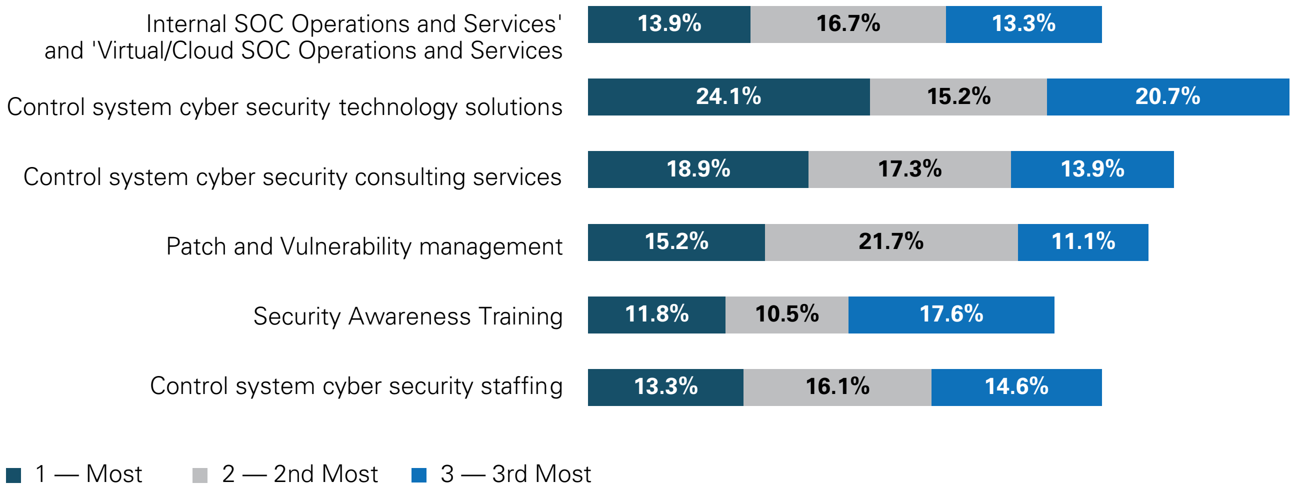
In addition to recognizing where programs of different levels of maturity see their best returns, it is worth considering *why* they do so. Do organizations with less mature cyber security programs focus more on remote access because this is a problem area for them or because they rely more often on outsourced security? Do organizations with more mature cyber security programs place lower ROI expectations on *Improving communications/collaboration with IT/corporate teams* because they have established protocols and processes largely overcoming the challenges of this activity and are moving on, because past work in this area has yielded disappointing results, or for other reasons? Further research to investigate underlying rationales will be needed to answer these questions.

Top three areas of greatest expenditure on (CS)²

Control System Cyber Security Technology Solutions continues to be reported as the area on which the greatest amount of control system cyber security resources is spent, albeit with a significantly smaller percentage of respondents selecting this as their highest spend (24.1 percent this year vs 48.3 percent previously). *Control System Cyber Security Consulting Services, Patch and Vulnerability Management* held the same relative positions as 2020.

Security Awareness Training and Control System Cyber Security Staffing have swapped places as the second lowest and lowest areas of expended resources, respectively. Across the board, some dilution effect must be recognized for the addition of *Internal SOC Operations & Services and Virtual/Cloud SOC Operations & Services* as a new option in the survey this year. It is also possible that we are seeing the impact of improved processes and technology implementations decreasing the amount of human labor required to perform security functions. We see this as an interesting area for further research.

Identify the top 3 areas on which your organization expends the most control system cyber security resources



Budgets

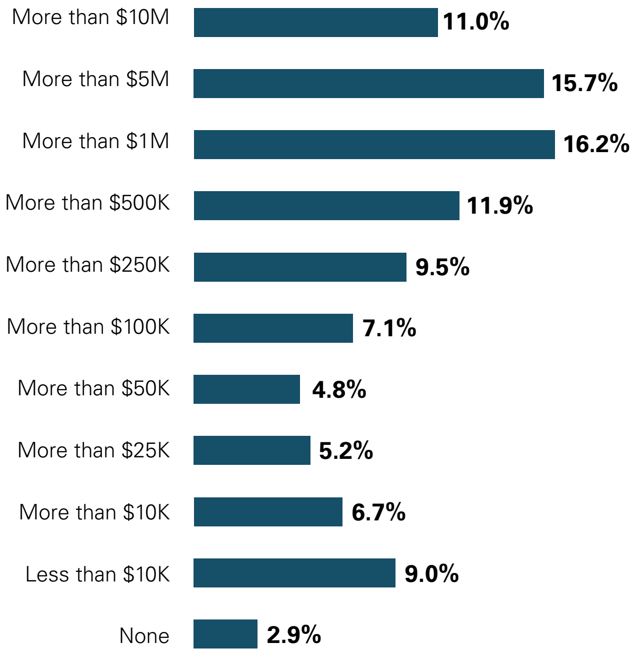
Over 43 percent of our respondents who provided budget data reported control system cyber security budgets exceeding US$1M for fiscal year 2020, which is comparable to our previous report.

We found some evidence of constraints on budgets in this past year. Most respondents indicated that their organizations did increase control system cyber security budgets in the past year but a total of 10 percent of respondents indicated a decrease in 2020, far more than the 1.1 percent in the previous annual study, which looked at 2019 budgets. Further, the concentration of budget growth has lowered from the 30–50 percent range into the 10–30 percent range, for an overall tightening of cyber security budgets, most likely deriving at least in part from pandemic impacts on the market.

Overall trends did continue upwards, with nearly two-thirds (60.4 percent) reporting at least a 10 percent increase in resource allocations, and budgetary pressures for many organizations will have included the rapid rise in need for remote worker access driven by COVID-19, requiring increased network segmentation and Identity Access Management expenditures.

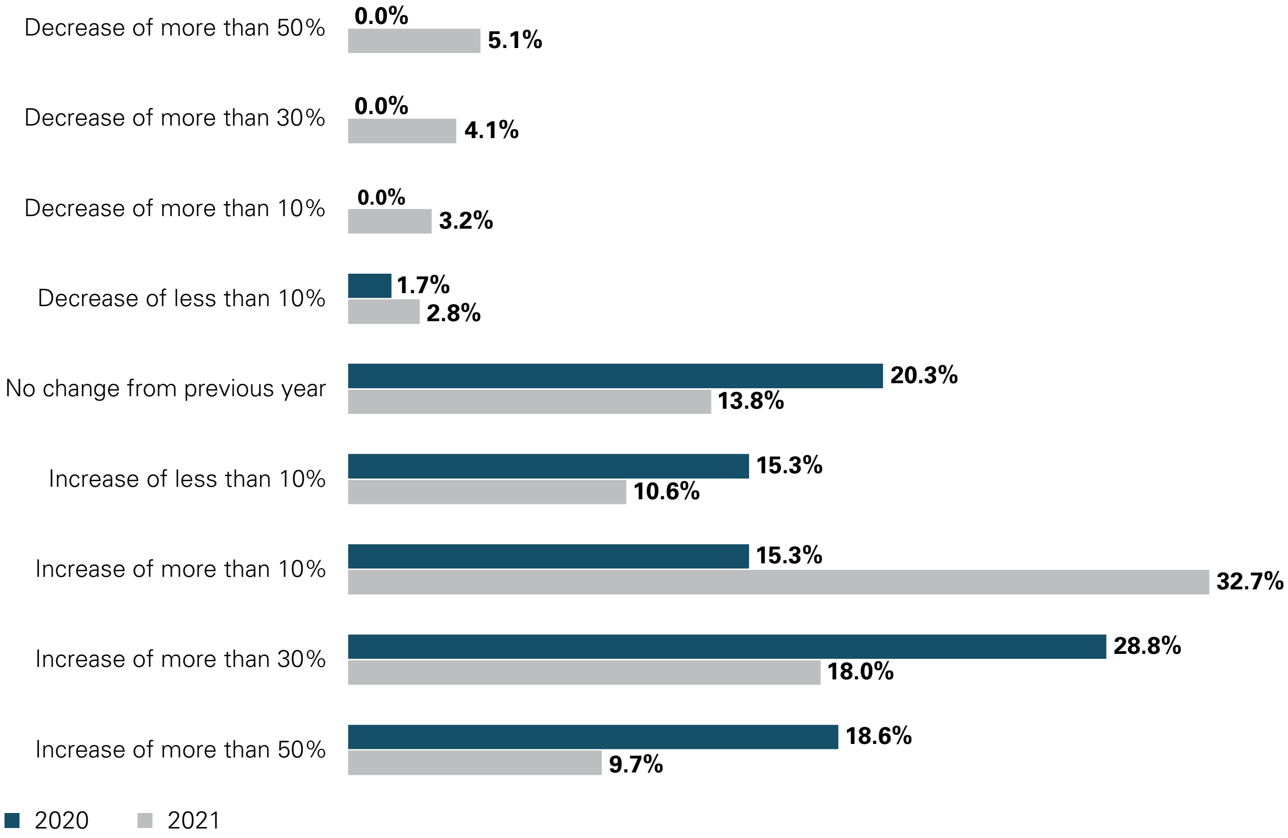
> “I think the messaging of ‘no silver bullet’ is finally starting to sink in. Many vendors have claimed to have ‘the’ solution to improve cyber holistically or within a particular capability and to great effect. What was not happening was a deep dive into understanding the true nature of the problem space for which the organization needed to solve. Technology enables processes executed/administered/supervised by people; technology does not solve process gaps/immaturities; technology does not inherently solve for people and skill gaps/shortages.”
>
> **Brad Raiford**
> Director, Cyber Security, KPMG in the US

Provide your best estimate of your organization's total annual control system cyber security budget



That being the case, we dove deeper into the data to find what we could about relative impacts on different organizations and found some distinct patterns in budget deltas based on company workforce size. The most significant belt tightening, with *Decrease of 50 percent or more* occurred almost exclusively in the small-to-medium sized business, those with up to 1,000 employees. These SMBs were quite diverse, obviously, as they are also highly represented in the *more than 10 percent and more than 30 percent increase* groups. The largest entities, those with workforces greater than 15,000, were not immune to economic headwinds, but the programs exhibiting the largest growth do mostly come from this subset, with 12.9 percent reporting an *Increase of 50 percent or more*.

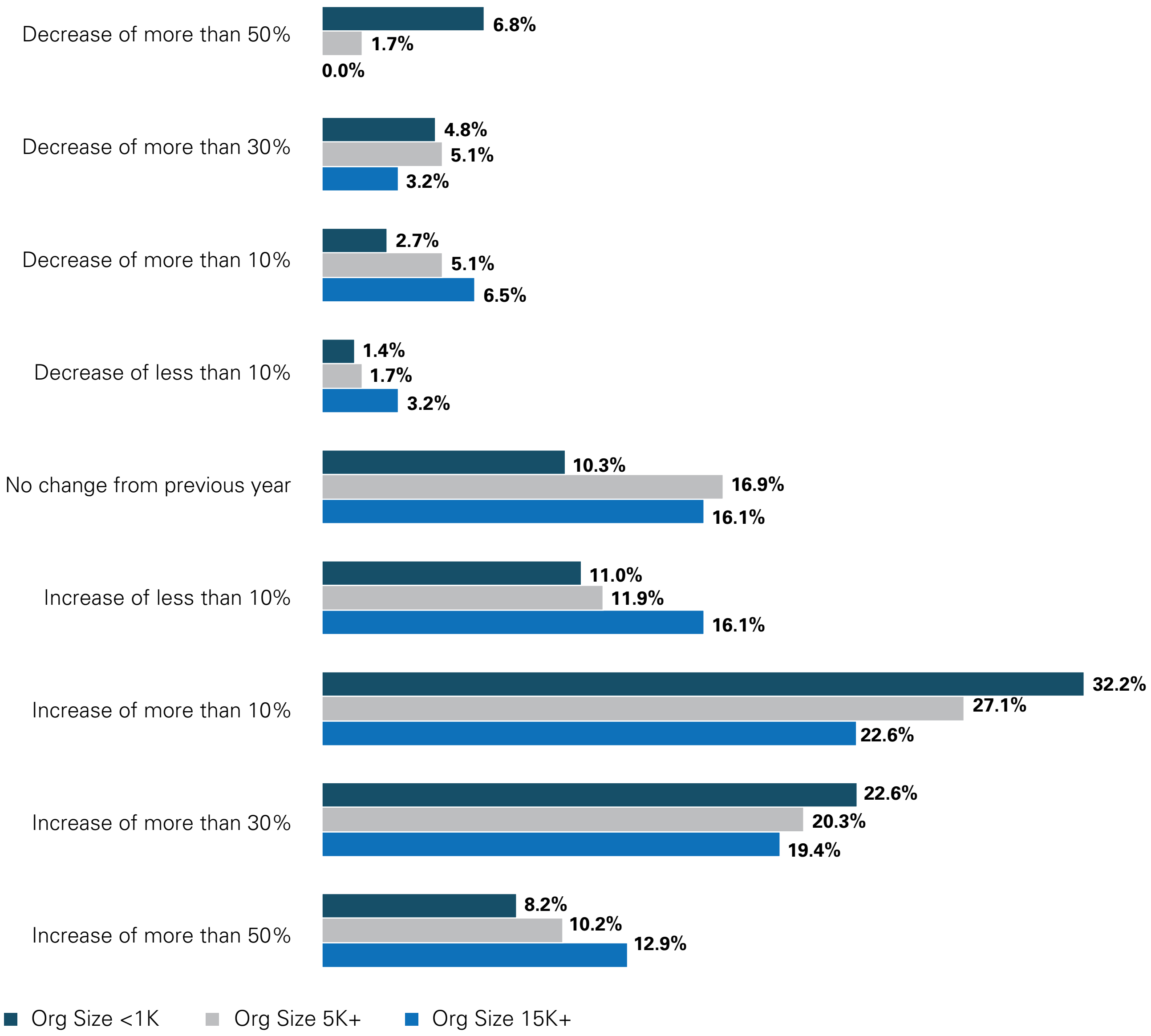
Provide your best estimate of how this year's control system security budget compares with last year (2020 vs 2021)



> Any organization with responsibility for protecting critical infrastructure must take security seriously. The 2022 CS2AI survey data illustrates that budget limitations, insufficient expertise, and the need for control systems to remain online 24/7 can become major obstacles to strong cyber security. But it does not have to be this way.
>
> We're going to see a trend in the next 12 months towards hardware-based security, as security leaders demand the strongest protection without the need for maintenance or patching. There's a real hunger for elegant solutions that can future-proof critical infrastructure against all types of remote attacks.

Dr. Ron Indeck
CEO, Q-Net Security

Provide your best estimate of how this year's control system security budget compares with last year (by Organization Size)



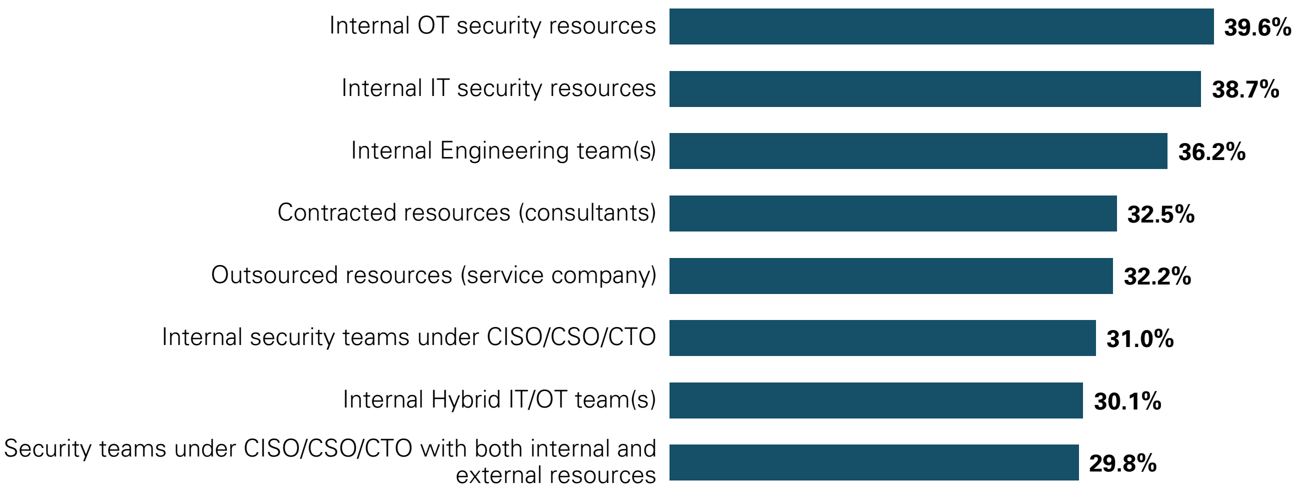
Services in use

We observed no major changes from last year's survey results on the question of control system cyber security services in use. Organizations continue to depend most heavily on their internal resources for control system cyber security services, with *Internal IT Security Resources* at 38.7 percent and *Internal OT Security Resources* at 39.6 percent as the most common answers.

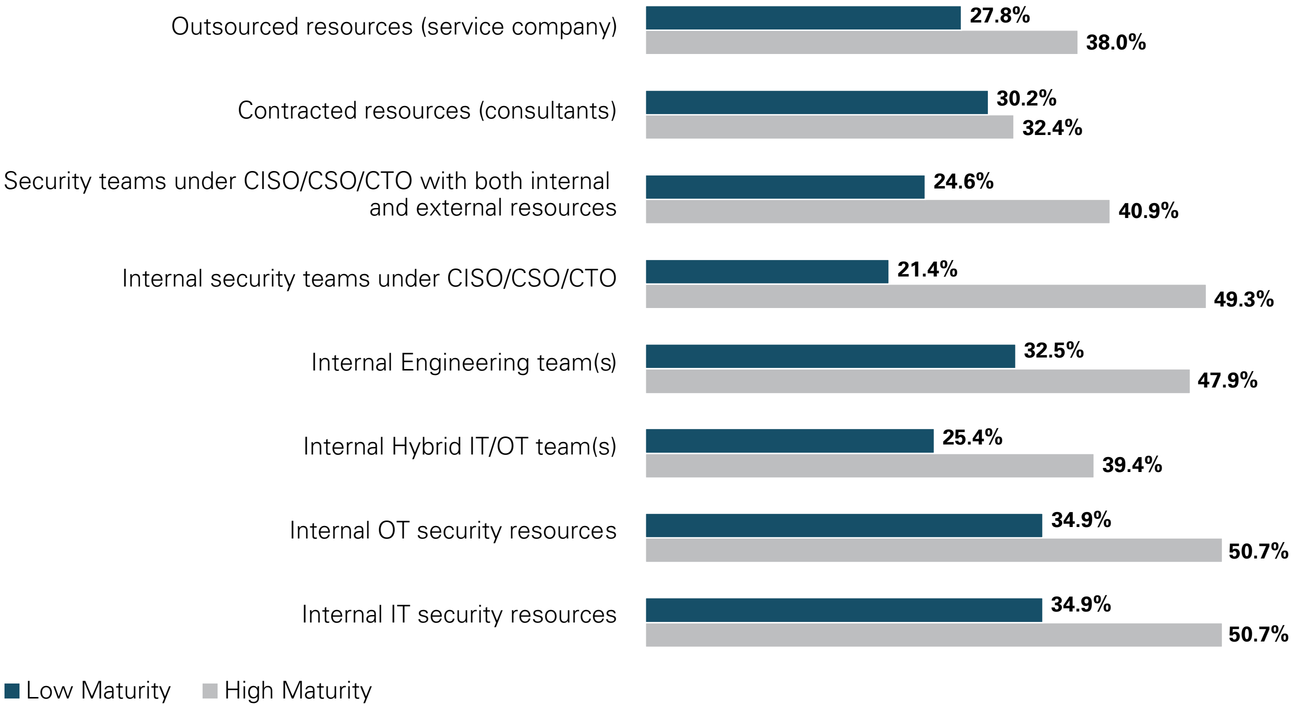
One observation made is that each respondent, on average, reported a combination of 2–3 different services in use in their organization.

Breaking our respondents into subset by maturity of their control system cyber security programs, it became immediately clear that the higher-maturity programs have a much more comprehensive approach, using **all** services more often than their counterparts in lower-maturity programs, often by a wide margin.

Select all sources of control system security services your organization uses



Select all sources of control system security services your organization uses (High Maturity vs Low Maturity)



High M organizations are more than twice as likely as the Low M group to use *Internal security teams under CISO/CSO/CTO.*

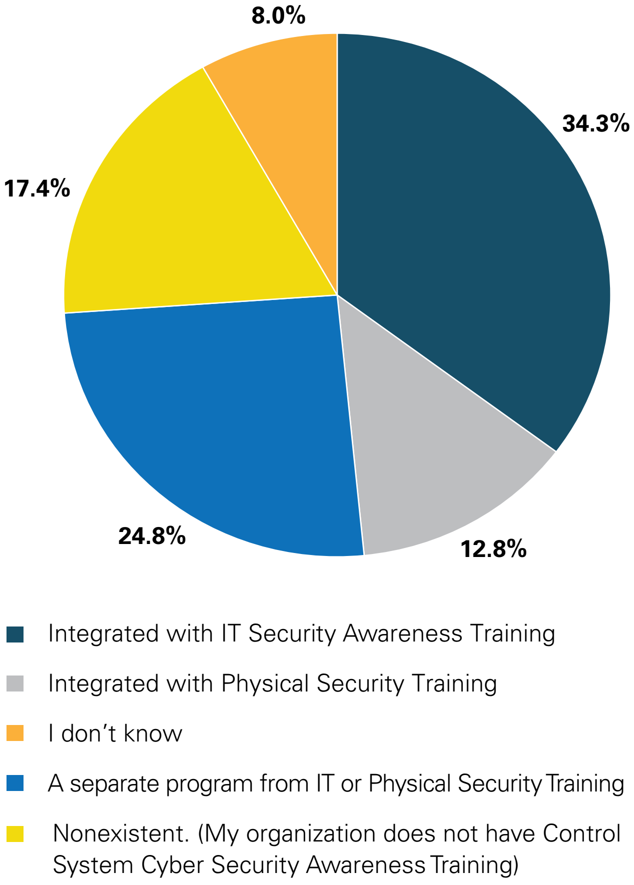
Awareness training

Security awareness training, which aims to improve the security culture of an organization and enable all employees to recognize their role in reducing risk exposures, as opposed to security training which is designed to develop the skills and capabilities of the specialized security practitioners in defending the organization, its assets and resources, is a maturing field in control system settings. Training for IT security awareness and OT safety awareness often have deeper histories of development.

The reasoning and importance of IT security awareness concepts such as validating email sources before clicking unknown links are widely known and understood, for example. Less well understood are the exposures often created when connecting business systems to operational technology, and it is crucial that all organizations address this lack of awareness by delivering control system cyber security awareness training to all their employees, whether they accomplish this by integrating that training with a broader program or as a stand-alone deliverable.

The authors' key concern is with the over one-sixth (17.4 percent) of respondents whose organizations lack any control system security awareness training at all. While there is a very slight improvement (20.6 percent in 2020 report), we must stress the importance of educating all personnel regarding their responsibilities in keeping control systems secure.

My organization's control system security awareness training is...



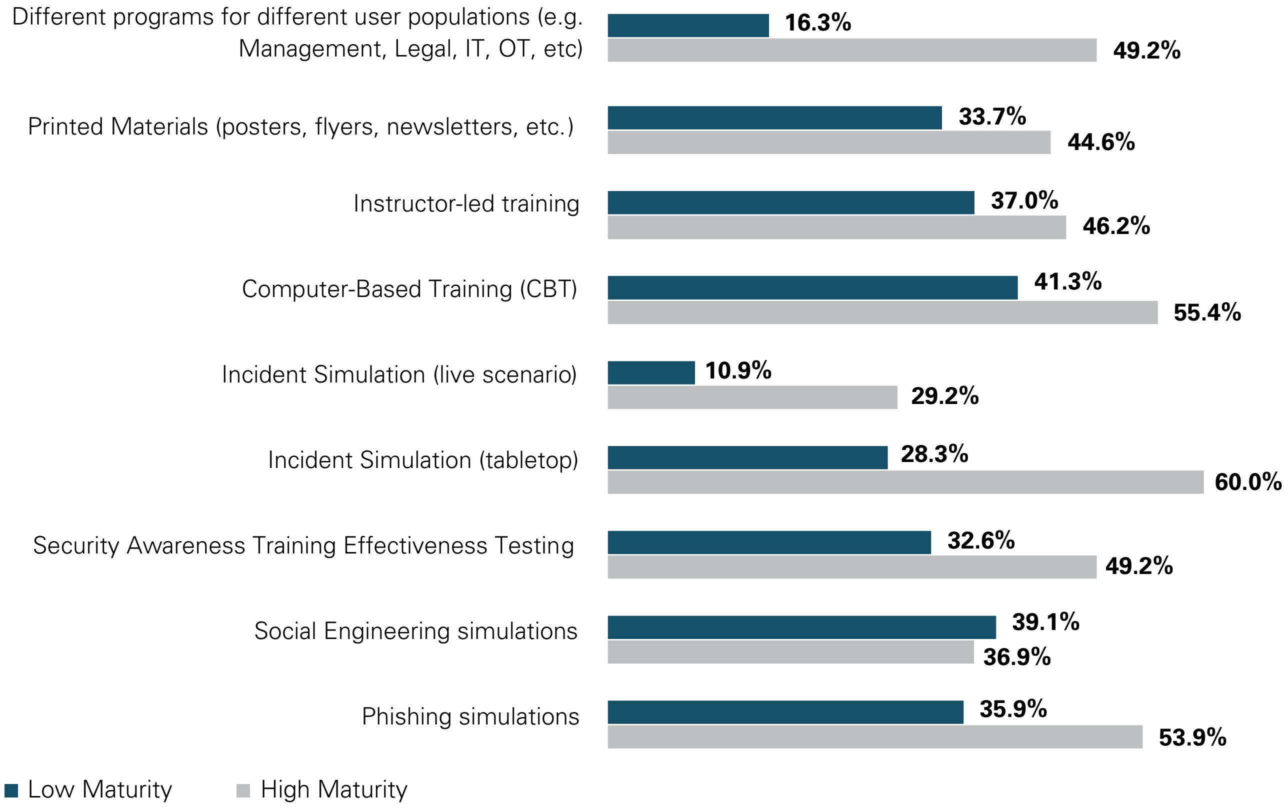
Training

Respondents reported on average more than three of the training components being included in their respective training programs. With known differences in utility of diverse training methods on different populations, this combination of approaches is definitely recommended, with similar content and messaging delivered across multiple channels, hopefully in an effective system of reinforcement.

Incident Simulation (live scenario) was selected by the fewest participants, particularly in the less mature (Maturity Level 1–2) programs. While recognizing that these are certainly the most complex and expensive training exercises, the authors do wish to stress that they are also generally much more effective than others, particularly at finding gaps in incident response and business continuity plans.

A clear reason that High Maturity programs are far more likely to conduct Incident Simulations is these are not easy to start from scratch. As a precursor, the relevant Plans (e.g., DR/BC/IR) must exist and be relatively mature in terms of documentation, with all roles defined and understood by all entities with parts to play before tabletop simulations become possible. These should be practiced multiple times (with Lessons Learned and improvements/updates made to Plans with each iteration) before progressing to live scenarios, with the involvement of operational systems.

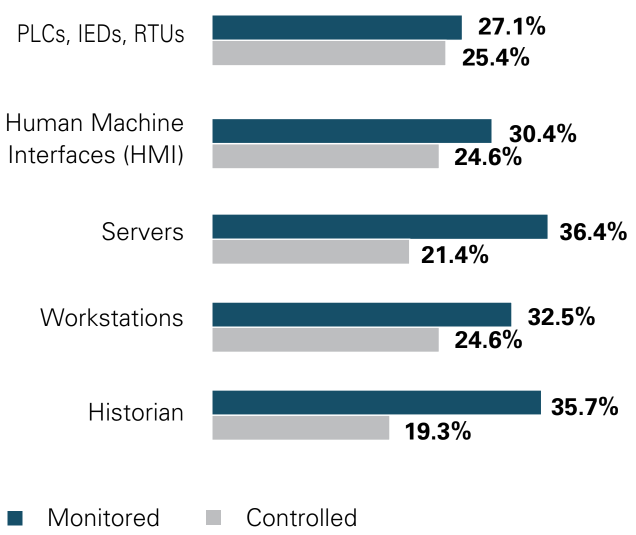
Select all components included in your control system security-related training (High Maturity vs Low Maturity)



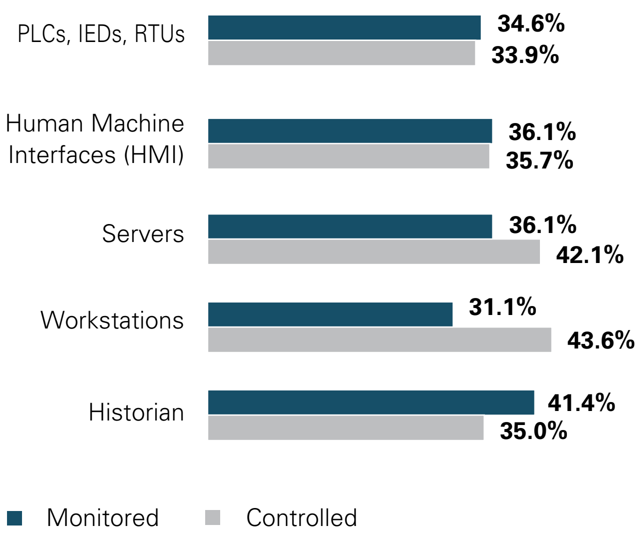
Accessibility of control system components

With it already well established that at least some accessibility from outside of the control network is common in most environments, we asked respondents to identify whether each control system component can be monitored or controlled remotely.

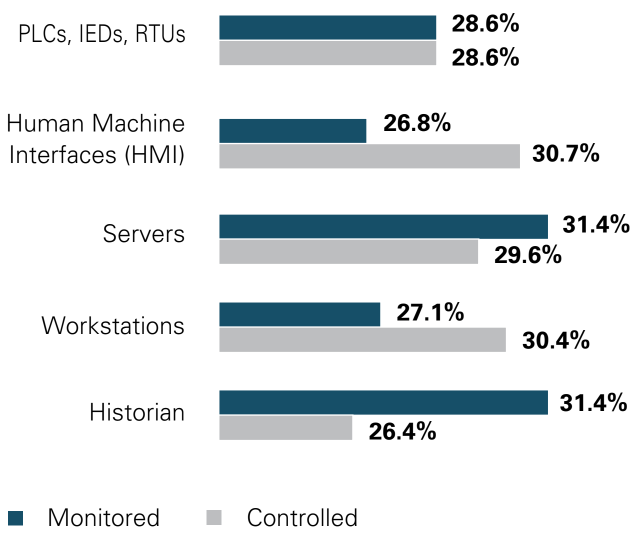
From internet



From business network



Remotely by vendor



Control system components most susceptible to compromise

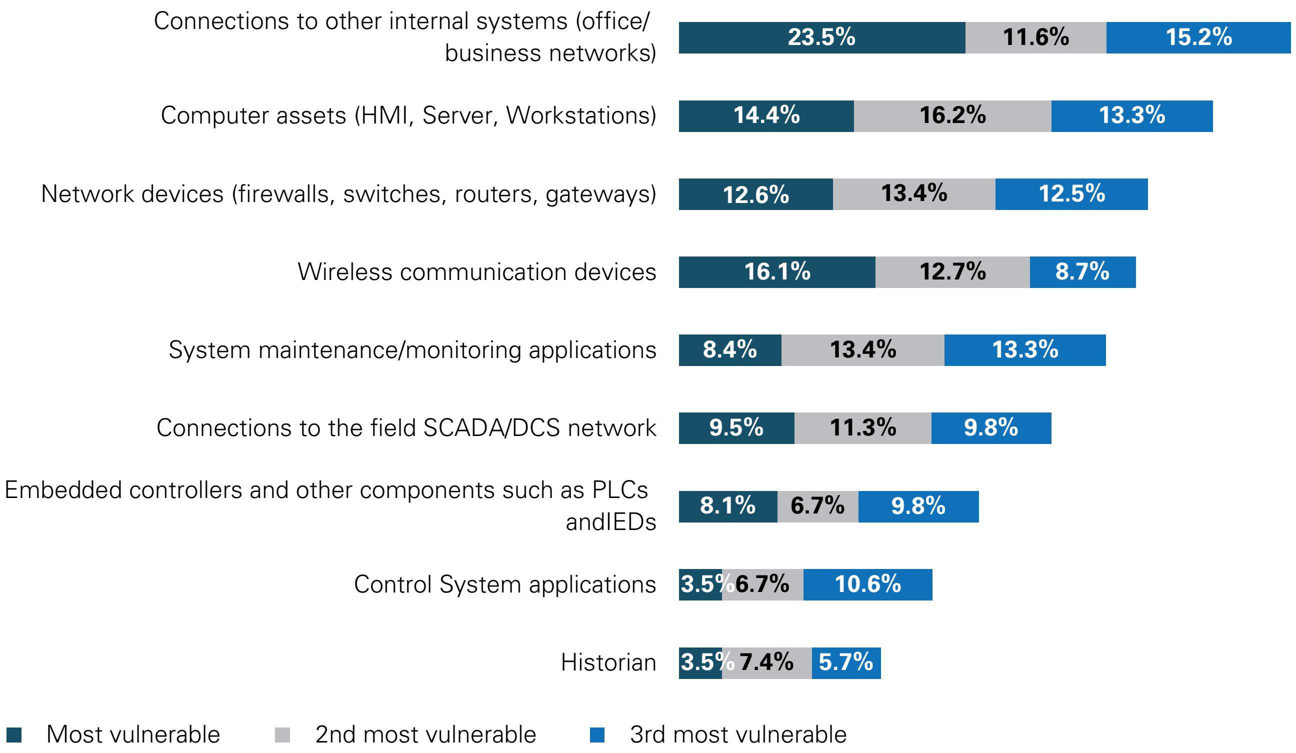
Whatever progress has been made in securing systems in the past year, our respondents continue to consider *Connections to other internal systems (office/business networks)* and *Computer Assets (HMI, Server, Workstations)* their weakest points. *Wireless communications devices* received nearly 50 percent more attention than a year ago, suggesting increased awareness of the proliferation of insecure or weak security wireless devices over that period.

State of organizational plans

The positive take is that over 85 percent have all their plans at some stage of development, with roughly 20 percent *Documented* and 26–30 percent *Implemented*. This is a significant improvement over 2020, when we found 18–27 percent did not even have the various management/response plans in their organizations.

It is noteworthy how few reported having actually *Tested* any of their plans, particularly in *Vulnerability Management* and *Supply Chain Risk Management*. Testing plans is essential to finding and closing gaps before they become failures during real, consequence-bearing incidents.

Identify which control system components your organization considers MOST susceptible to compromise based on current protections and configuration



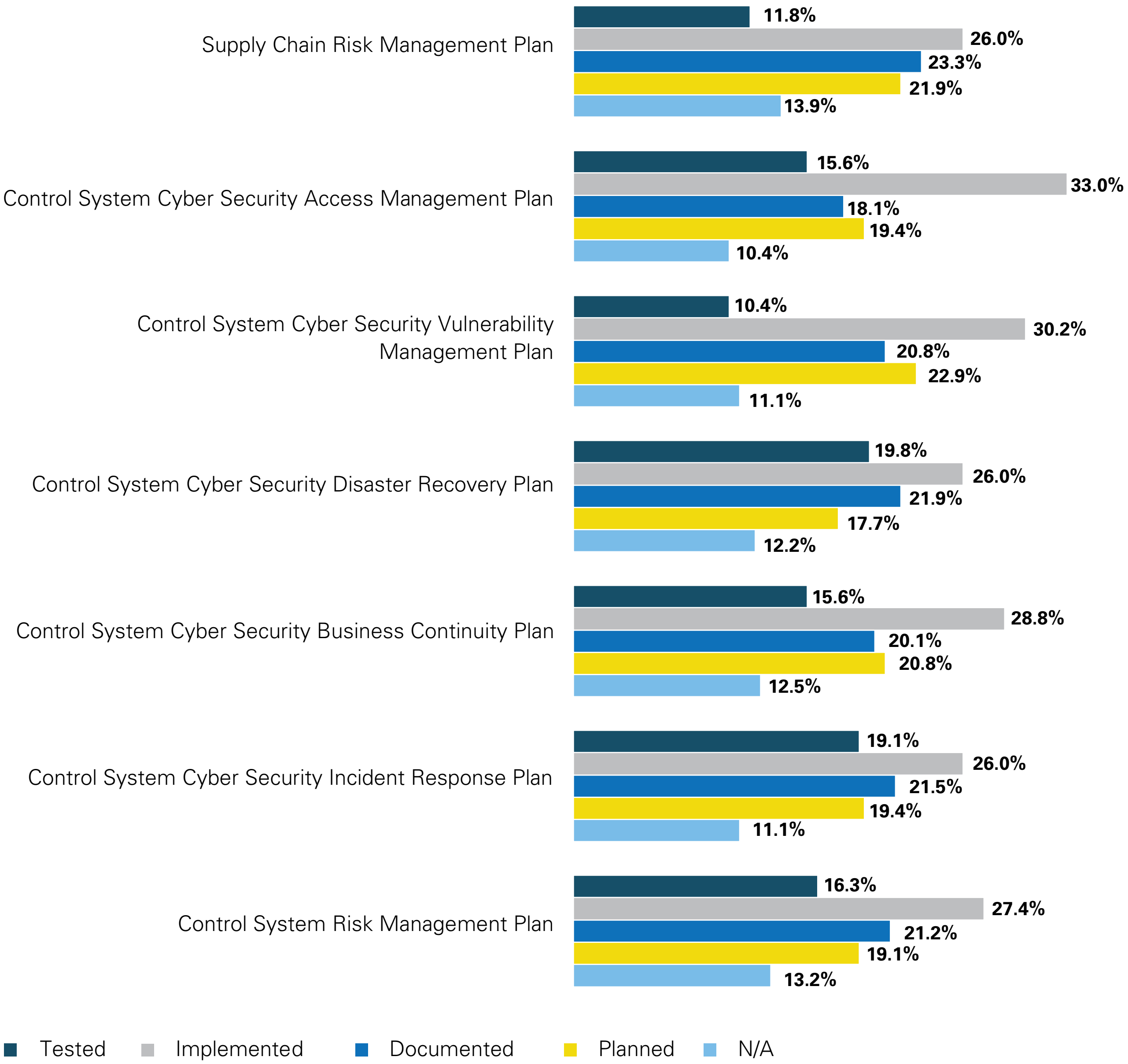
> “That ‘connections to other systems’ is the top result for the ‘most susceptible to compromise’ question confirms the premise of my 2019 book Secure Operations Technology. All connections and other information flows are attack vectors. Secure industrial sites work hard to minimize the number and kinds of information flows entering their control systems from less-critical networks. And these sites universally deploy outbound-only unidirectional gateways between control-critical and business-critical networks.”

Andrew Ginter
VP Industrial Security, Waterfall Security Solutions

> OT presents a more complicated security environment versus IT since there are both IT (OS-based servers) and pure industrial OT devices. This separation of devices creates an interesting division of ownership, skillset and budget between IT and OT teams. The IT and OT 'gap' is real, yet there are forward-leaning businesses who are closing this gap by integrating across the gap to give IT teams exposure to industrial devices to assist in managing the basic controls necessary in the relatively immature OT spaces while the industrial teams are getting access to additional personnel, established security practices and much needed budget. As we've witnessed over the past year, cyber risk and production risk are intermingled and it behooves companies to address these risks together by rapidly closing the IT and OT gap.

Richard Springer
Director of Business Development, Industrial,
Tripwire

Please select the best descriptor for the current state of each of your organizational Plans

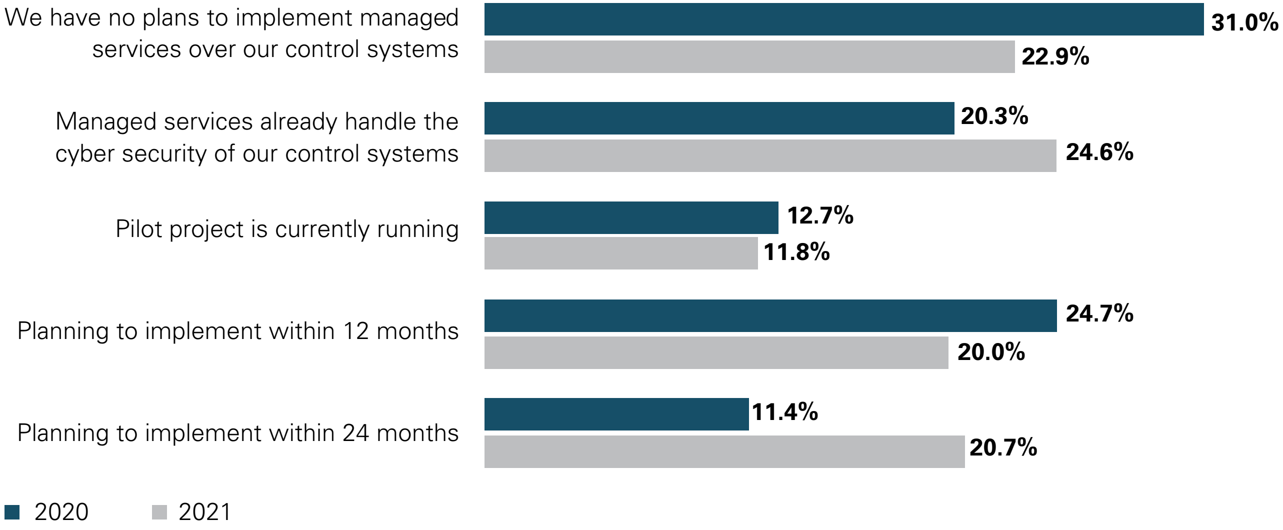


Managed services

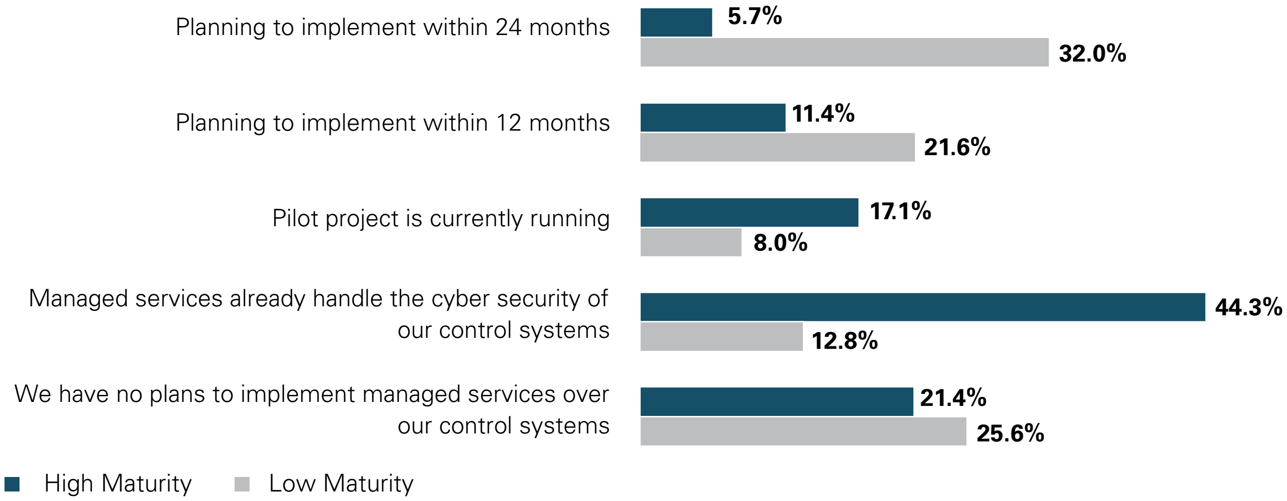
We are seeing a small shift in respondents planning to implement managed control system cyber security services (about a 5 percent increase) and fewer who have no plans at all (over an 8 percent decrease in *'We have no plans to implement managed services… systems'),* with some differences between Low Maturity and High Maturity programs. There were no clear trends among organizations based on size of their workforces.

Lack of internal resources with sufficient training and expertise continues to be the primary motivator for organizations to implement managed control system cyber security services, selected as the sole factor for nearly 44 percent and altogether by 68 percent of respondents. In comparing the data longitudinally, it appears more entities have established clear, single factor support than previously. This is supported by the number of respondents who, in selecting *Other* in the 2020 report, specified that they did not have clear business cases to implement managed services.

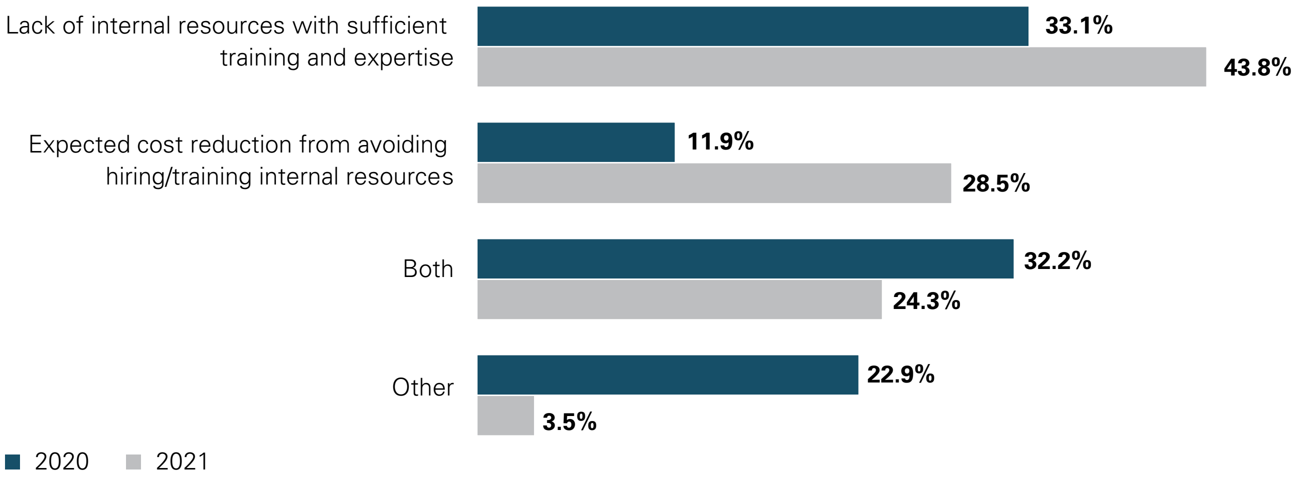
What is the current state of managed control system security services in your organization?



What is the current state of managed control system security services in your organization? (High Maturity vs Low Maturity)



Why do you have (or plan to have) managed control system security services?



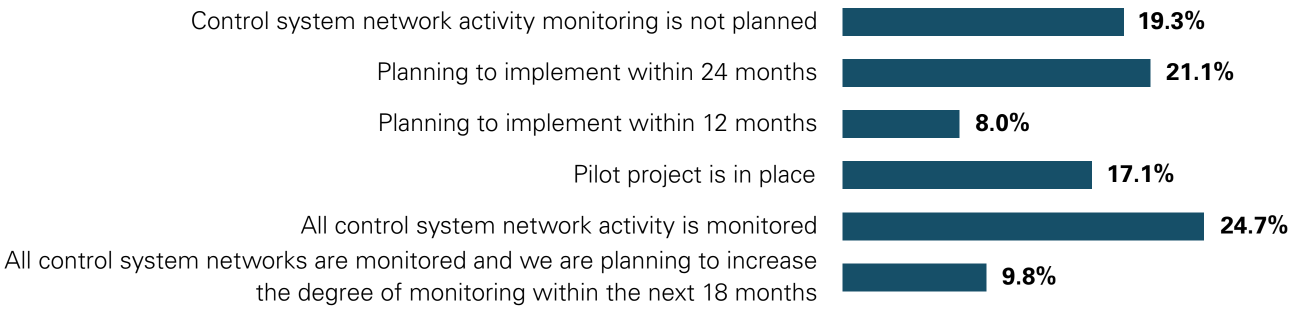
Current control system network activity monitoring

The positive view of our data is that over half of respondent organizations have at least begun to monitor their control system network activity (51 percent) and nearly another third (29 percent) are planning to implement this important awareness tool. Unfortunately, the remainder of almost one-fifth (19.1 percent) are unmonitored and have no plans to change that. Lacking awareness of the traffic in this area means that the first indication of compromise these organizations have will be operational disruptions, by which time threat actors will have had an indeterminate amount of time dwelling in their systems to reconnoiter and establish their presence with the network environment. Many case studies have shown that attackers are often unnoticed for several months for exactly this reason, with the extent of damage and the difficulty in removing them much greater because of the extended period of free action granted by their invisibility.

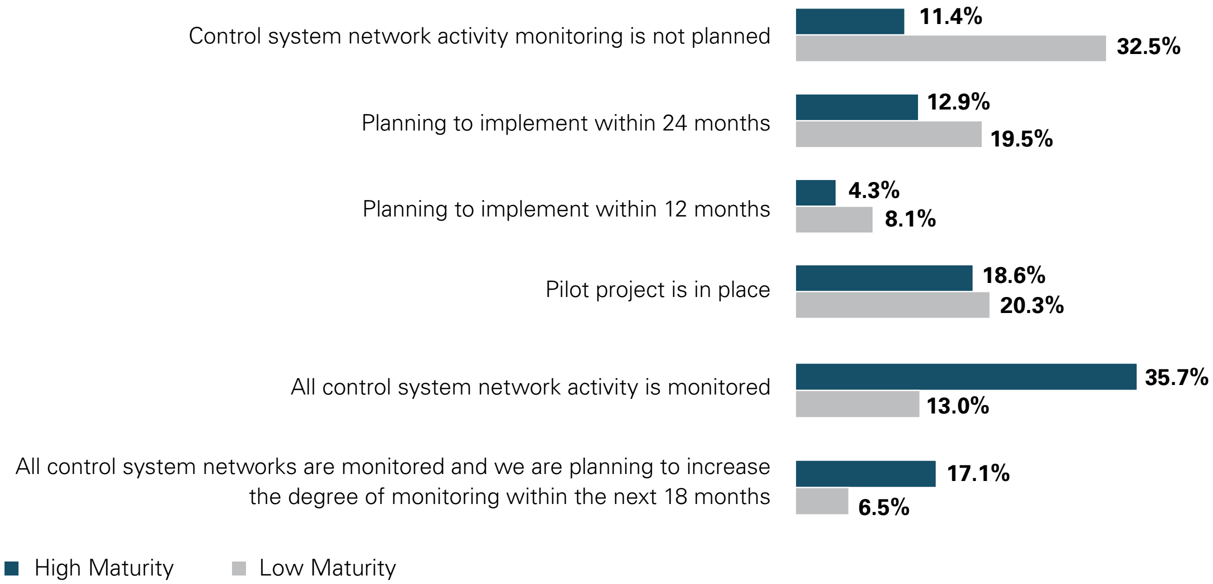
Perhaps more interesting are the distinct differences between inputs from Low Maturity and High Maturity respondents, with the latter significantly more likely to have implemented control system network monitoring, and even to be increasing what is currently in place.

It is given that many experienced control system professionals remain wary of monitoring solutions, in some cases stemming from historical issues in the application of IT-derived scanning tools to OT environments. What must be recognized, however, is that control system-specific intrusion detection and prevention tools (IDS/IPS) have made great advances in recent years and, with knowledgeable practitioners involved, bear little of the risk once associated with them. They are increasingly considered a base essential component in protecting control system assets and operations.

What is the current state of control system network activity monitoring in your organization?



ρ What is the current state of control system network activity monitoring in your organization? (High Maturity vs Low Maturity)



Assessments

Frequency

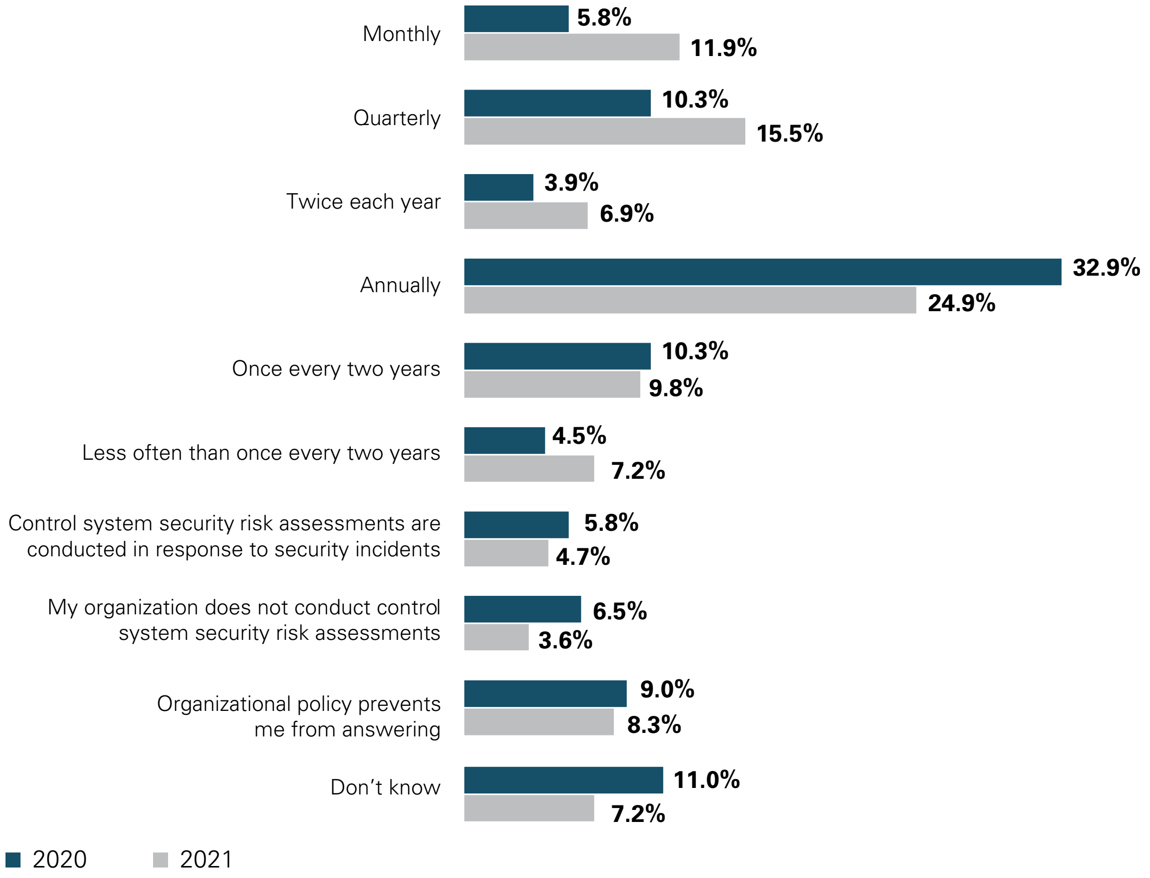
While the greatest frequency of control system cyber security assessments reported continues to be *Annual* (24.9 percent), there has been an overall increase in every higher rate of occurrence, which can only be seen as a positive. The number of respondents conducting these *Monthly* has approximately doubled (to 11.9 percent), and *Quarterly* rose by nearly half (to 15.5 percent).

We did not see a significant difference in the frequency of assessments conducted by organizations with highly mature cyber security programs relative to those of less mature ones. The distinction became more evident when we considered the question of what was included in those assessments, however.

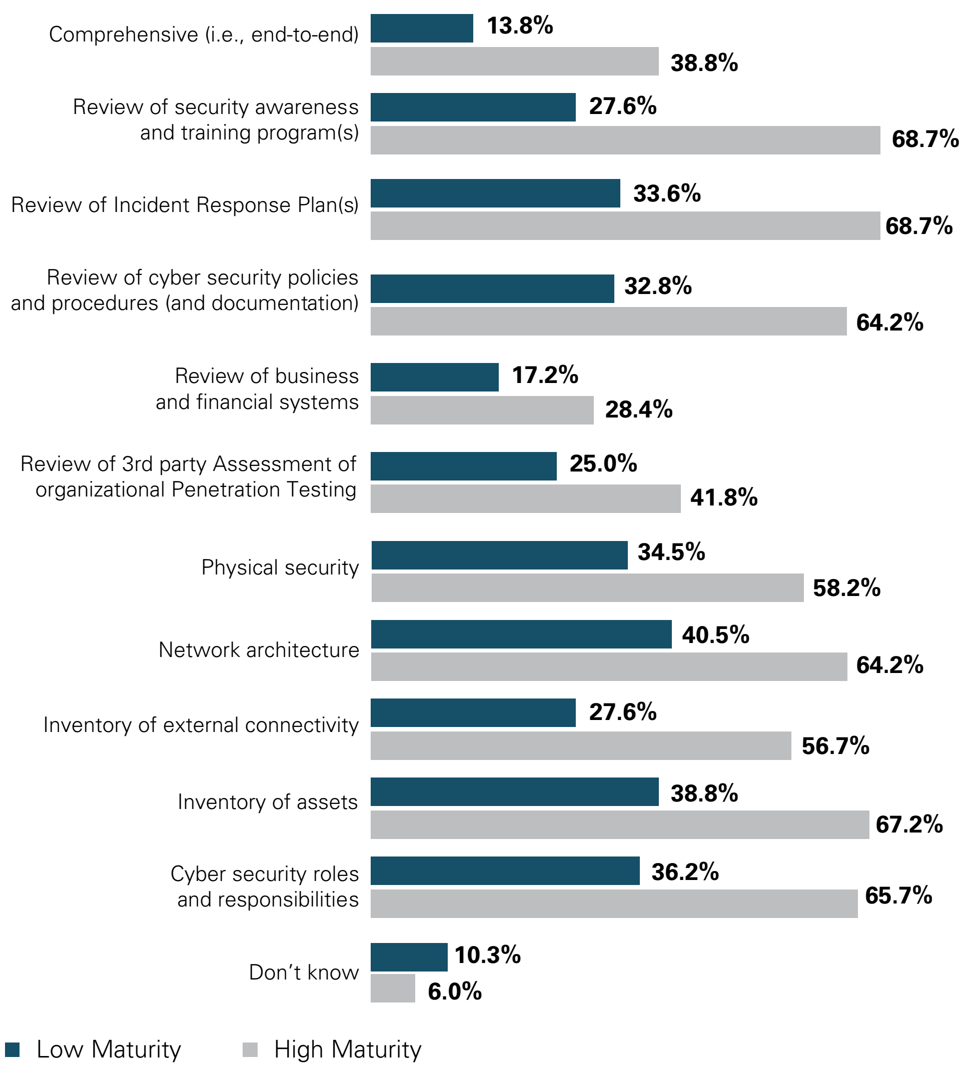
Inclusions

Organizations with more mature security programs evidently conduct more thorough cyber security assessments, not only including every component more frequently than those with less mature programs, often by wide margins, but also nearly three times as likely to conduct *Comprehensive (i.e., end-to-end)* assessments (High M 38.8 percent vs Low M 13.8 percent).

How often does your organization conduct control system security assessments?



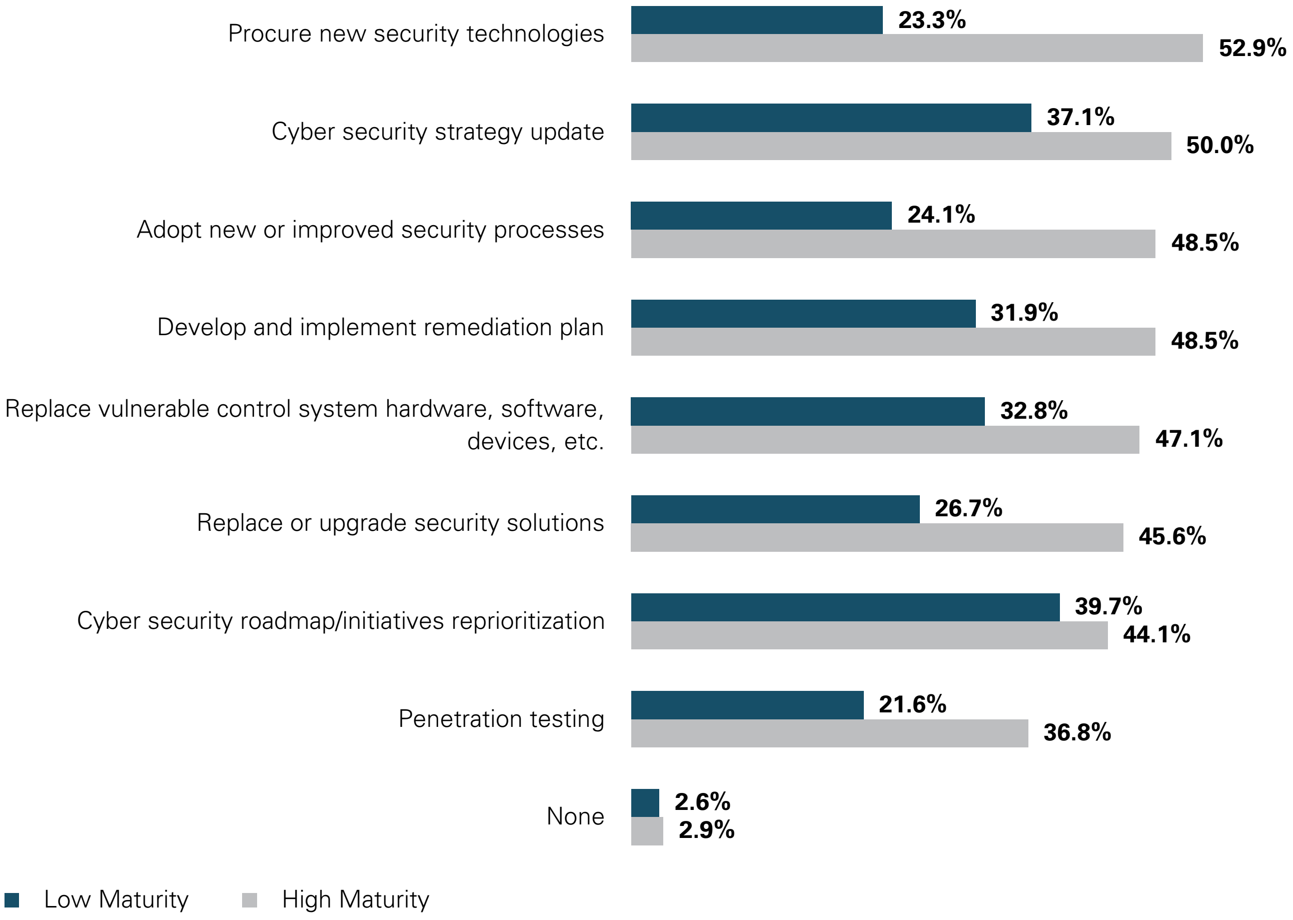
Identify all the components included in your organization's control system security assessments (High Maturity vs Low Maturity)



Follow-up activities

Similarly, the higher-maturity programs are more likely to carry out a wide range of follow up actions responsive to the findings of those security assessments.

Select all activities your organization carried out (or plans to) in response to security assessments carried out within the last 12 months (High Maturity vs Low Maturity)



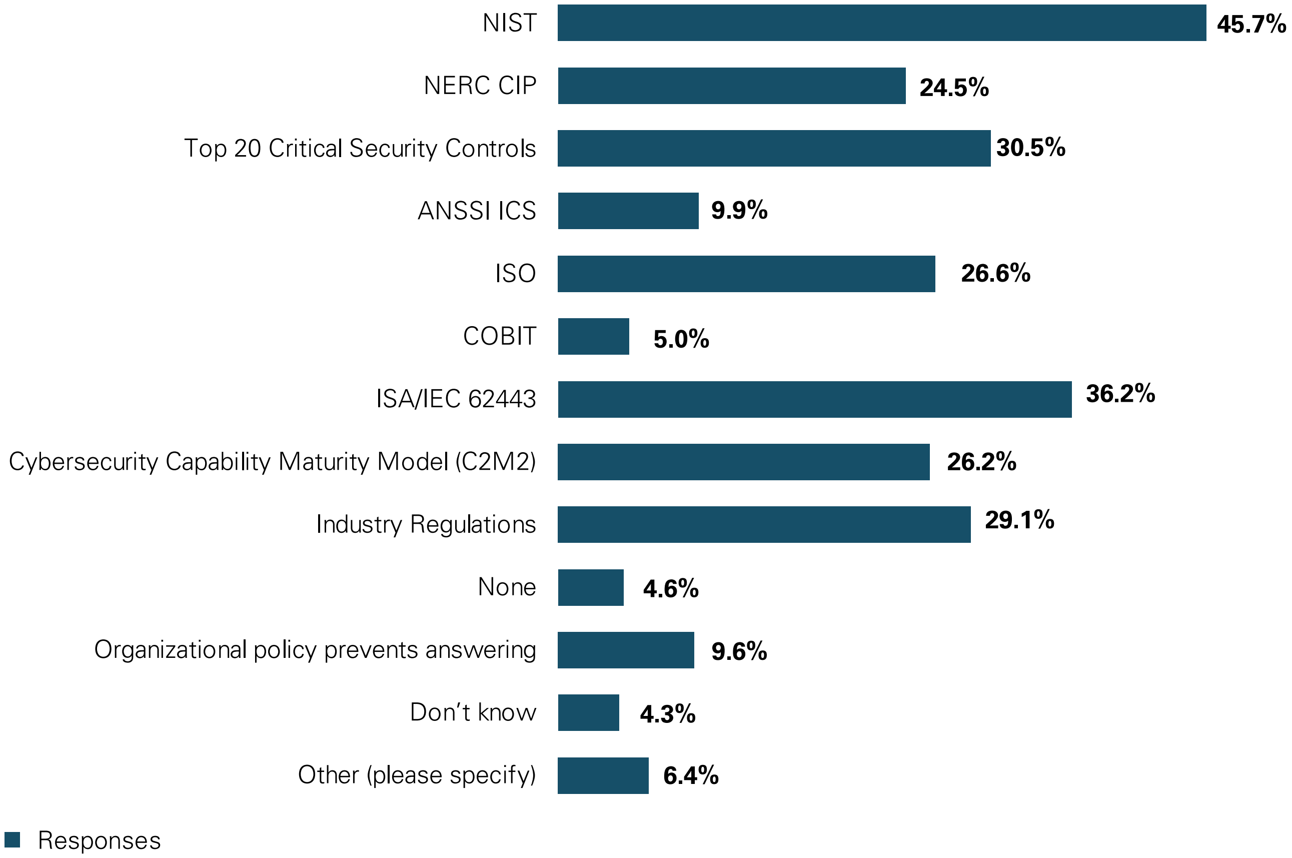
Frameworks in use

The NIST cyber security framework continues to be the most used. Direct comparison with our previous report is not possible due to changes in this question, but it is worth noting that two answer choices not offered on our original survey, the *Cybersecurity Capability Maturity Model (C2M2)* and *ISA/IEC 62443*, are both in widespread use as well (26.2 percent and 36.2 percent, respectively).

The Top 20 Critical Security Controls stood out as the only framework cited more often by respondents with Low Maturity security programs than High Maturity ones (30.1 percent vs 28.6 percent). The High Maturity security program participants reported using every other framework at higher rates, strongly suggesting that their organizations use multiple sources of expertise to guide their programs more often than their counterparts.

The clear takeaway is not that all Low Maturity programs should adopt particular frameworks to improve their security posture, but that these organizations should incorporate **more** sources of guidance into best practices and processes.

Please select all of the following framework(s) used by your control system security team



Technologies in use

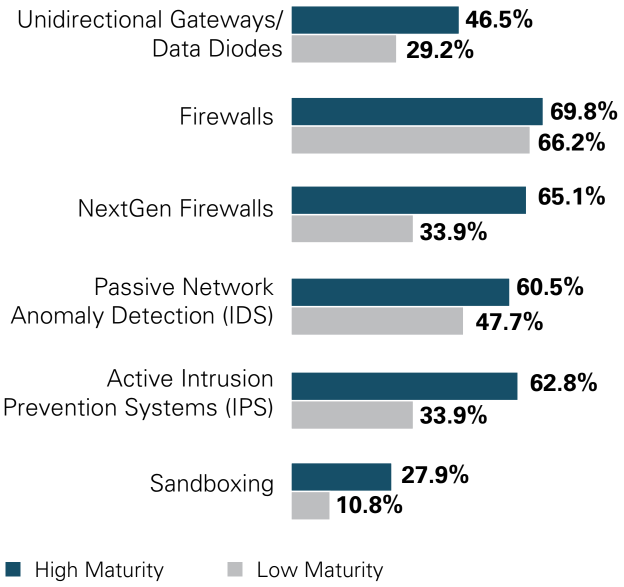
We found several notable trends in security technology use among High Maturity security program organizations. They are roughly half again as likely to use *Unidirectional Gateways/Data* Diodes (46.5 percent High M vs 29.2 percent Low M), nearly twice as likely to use *NextGen Firewalls* (65.1 percent High M vs 33.9 percent Low M) and *Active Intrusion Prevention Systems (IPS)* (62.8 percent High M vs 33.9 percent Low M), and more than twice as likely to use *Sandboxing* (27.9 percent High M vs 10.8 percent Low M).

Recent incidents

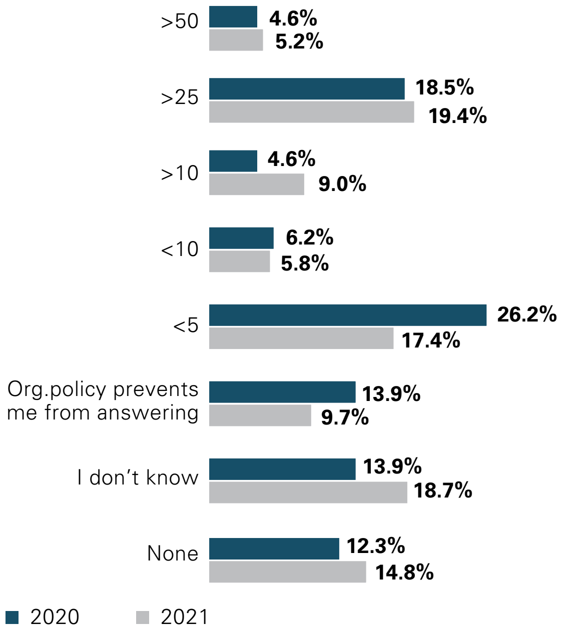
Longitudinal analysis revealed a statistical jump in respondents reporting more than 10 control system cyber security incidents in the past year (4.6 percent in 2020 vs 9.0 percent in 2021) and a drop in reports under five incidents (26.2 percent in 2020 vs 17.4 percent in 2021).

Breaking respondents' organizations into subset by workforce size it quickly becomes clear that their experiences differed. The distinctly higher number of entities in the 500–1,000 employee range reporting more than 25 control system cyber security incidents in the past 12 months (40.9 percent), bracketed by very similar numbers in the 100–500 and 1,000–5,000 ranges (28.6 percent and 28 percent, respectively), along with the sharp drop outside of that range, suggests the possibility that malefactors are targeting companies around this size.

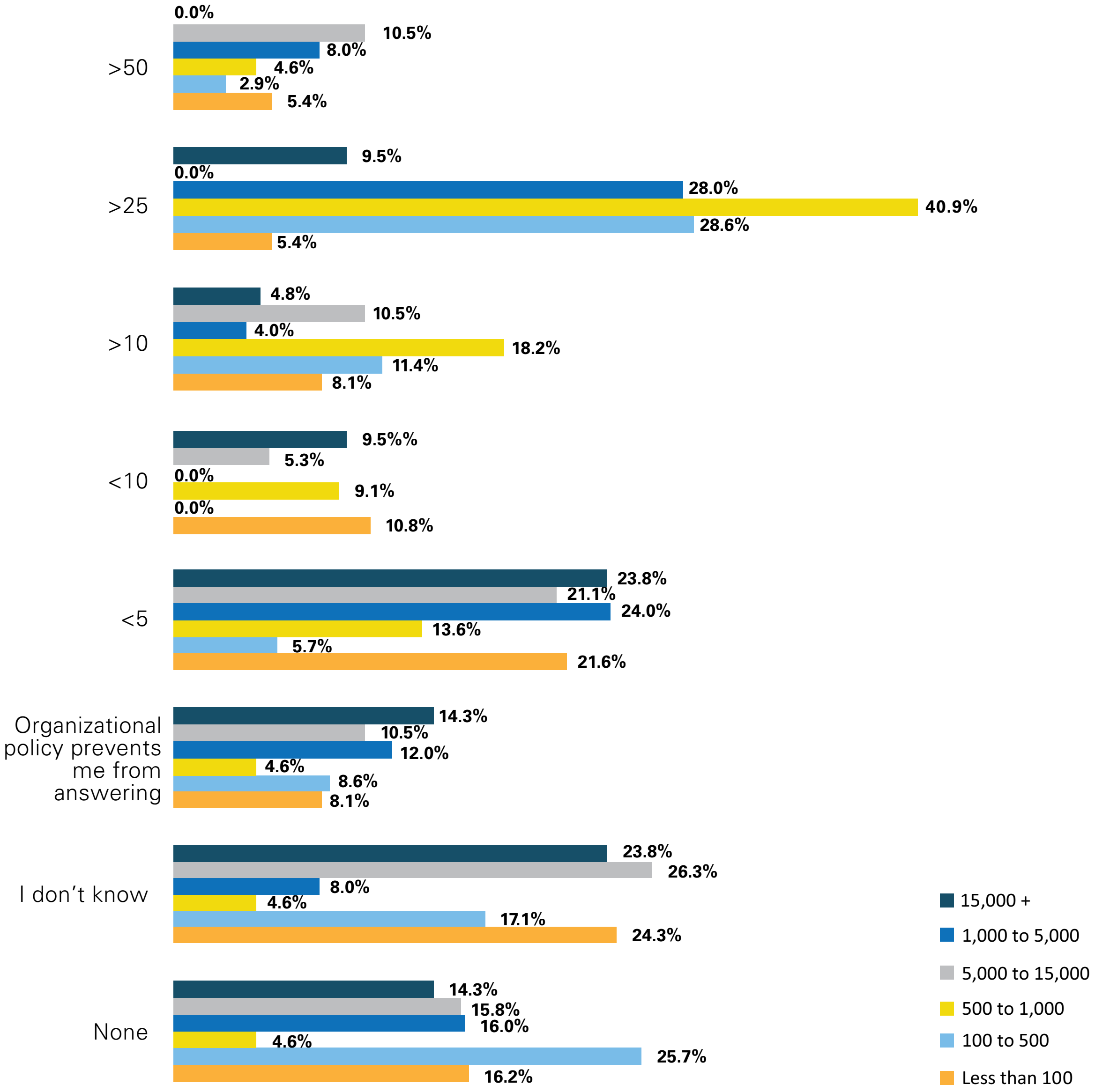
Indicate all security technologies in use to protect your organization's control system assets against cyber threats? (High Maturity vs Low Maturity)



What is your best estimate of how many control system cyber security incidents have occurred in your organization within the past 12 months?



What is your best estimate of how many control system cyber security incidents have occurred in your organization within the past 12 months? (by Organization size)

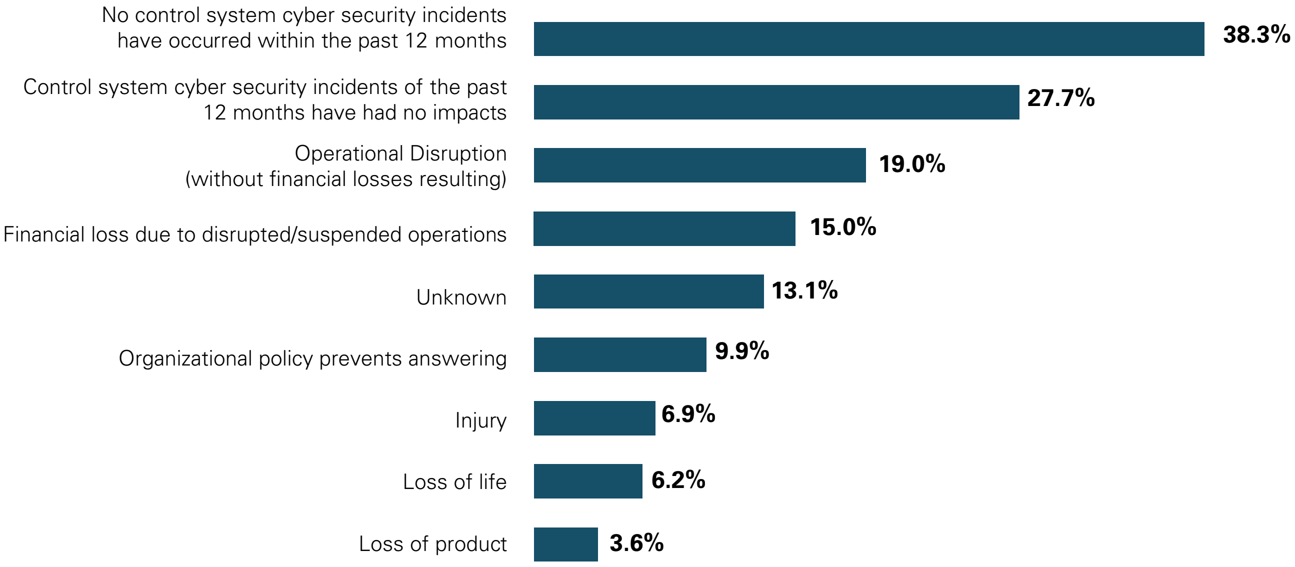


Recent incident impacts

While direct comparisons between this year's survey and the previous reporting on this question are not possible due to changes in survey design, there is clear increase in the number of respondents indicating either *"Injury"* (up from 1.3 percent to 6.9 percent) and *"Loss of Life"* (up from 1.3 percent to 6.2 percent) resulting from a control system security incident within the past year. Some portion of this may be attributable to greater representation of participants in health care (over 12 percent of 2021 survey respondents do at least some of their work with or in hospitals) and the enormous growth in ransomware attacks on health care systems[3] in recent history.

Additional trends observed included fewer respondents citing organizational policies or lack of knowledge preventing them from answering (down from 30.9 percent to 19.0 percent and from 34.9 percent to 13.1 percent, respectively). That more people are contributing information to this research, both in overall numbers and in actual data provided, can only be seen positively.

Select all impacts resulting from control systems security incidents in the past 12 months



> In July 2021, the TSA ordered US pipeline operators to improve security to the point where pipelines continue operating, even when their IT networks are compromised. After all, what does 'shut down in an abundance of caution' mean? It means that we do not trust the strength of our OT security programs. The time has come to add a layer of hardware-enforced unidirectional gateways into our defense in depth, OT/ICS security designs.
>
> **Andrew Ginter**
> VP Industrial Security, Waterfall Security Solutions

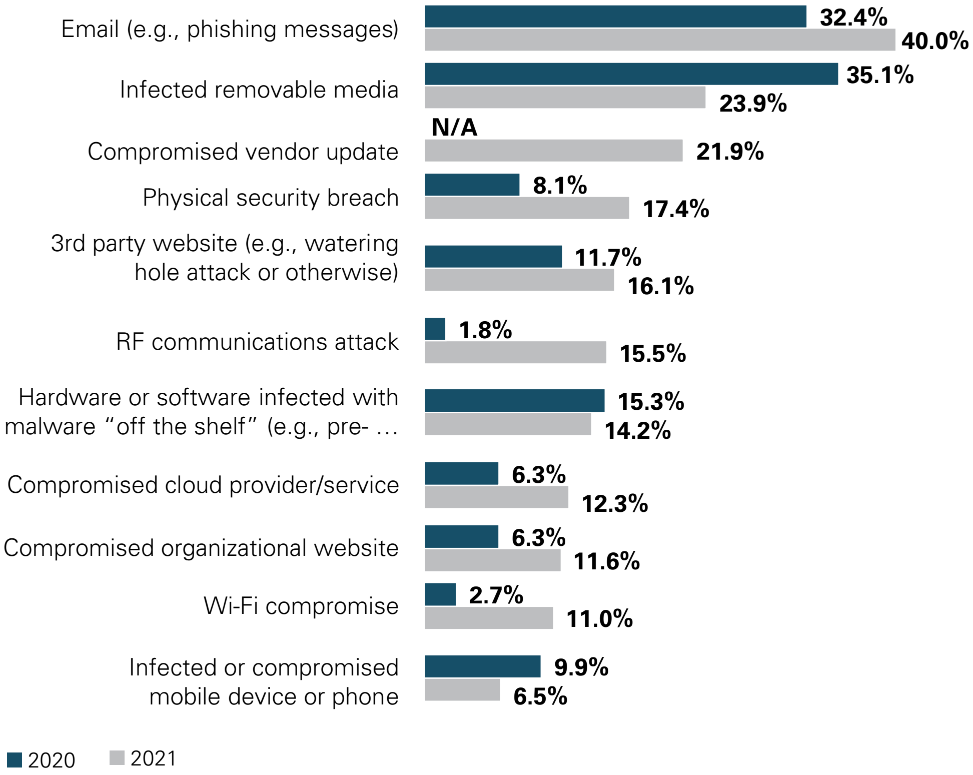
[3] https://thecrimereport.org/2021/08/18/hospitals-cyberattacks/

> “Successful operations organizations run on metrics, targets, detailed procedures, and tactical results monitored on an hourly, daily and weekly basis. Cyber security objectives tend to be subtle or aspirational: reduce vulnerabilities, identify potential malware, identify attackers, improve incident response, etc. Successful OT cyber security approaches transform these subtle objectives into very tactical targets and metrics that can be displayed on simple red, yellow, green charts.”
>
> **Rick Kaun**
> VP Solutions at Verve Industrial Protection

Recent attack vectors

Compromised Vendor Update, a newly added vector on our survey this year, impacted a larger number of respondents than anticipated, at 21.9 percent. Unlike some questions which showed a possible dilution effect from additional answer options, several other vectors rose markedly, particularly *RF Communications Attack* (1.8 percent in 2020 vs 15.5 percent in 2021), *Wi-Fi Compromise* (2.7 percent in 2020 vs 11.0 percent in 2021), *Physical Security Breach* (8.1 percent in 2020 vs 17.4 percent in 2021) and *Compromised Cloud Provider/Service* (6.3 percent in 2020 vs 12.3 percent in 2021).

Please select all attack vectors used in any of the control system cyber security incidents occurring in your organization within the past 12 months



> The COVID-19 pandemic has further blurred the lines between the physical and digital worlds, exposing fault lines in cybersecurity infrastructure and unravelling a host of new challenges. In the post-pandemic context, workforce shortages on site are one such challenge. One of the key reasons for the lack of personnel at sites is that companies are adopting hybrid work arrangements and split teams amid COVID-19 related restrictions. This often leads to extended maintenance cycles and workarounds like contractor remote service support. As a result, supply chain risks have also heightened.
>
> Wireless communications present another avenue for attackers to gain entry into an ICS network. Radio frequencies such as 5G have been deployed to facilitate communications between devices/equipment that are mobile or deployed over long distances. Other radio frequencies could be used for manual control on a day-to-day basis or for troubleshooting. The risk of using radio frequencies for communications is that they are usually broadcast and could be recorded, reverse engineered, manipulated and replayed in ways that could have impact to safety and production. A Wi-Fi access point, commonly used in home network, when deployed in ICS network could undermine the use of data diode intended to establish an airgap. Knowing what technology is deployed on our ICS network and understand what risks they present to the business cannot be understated. ”

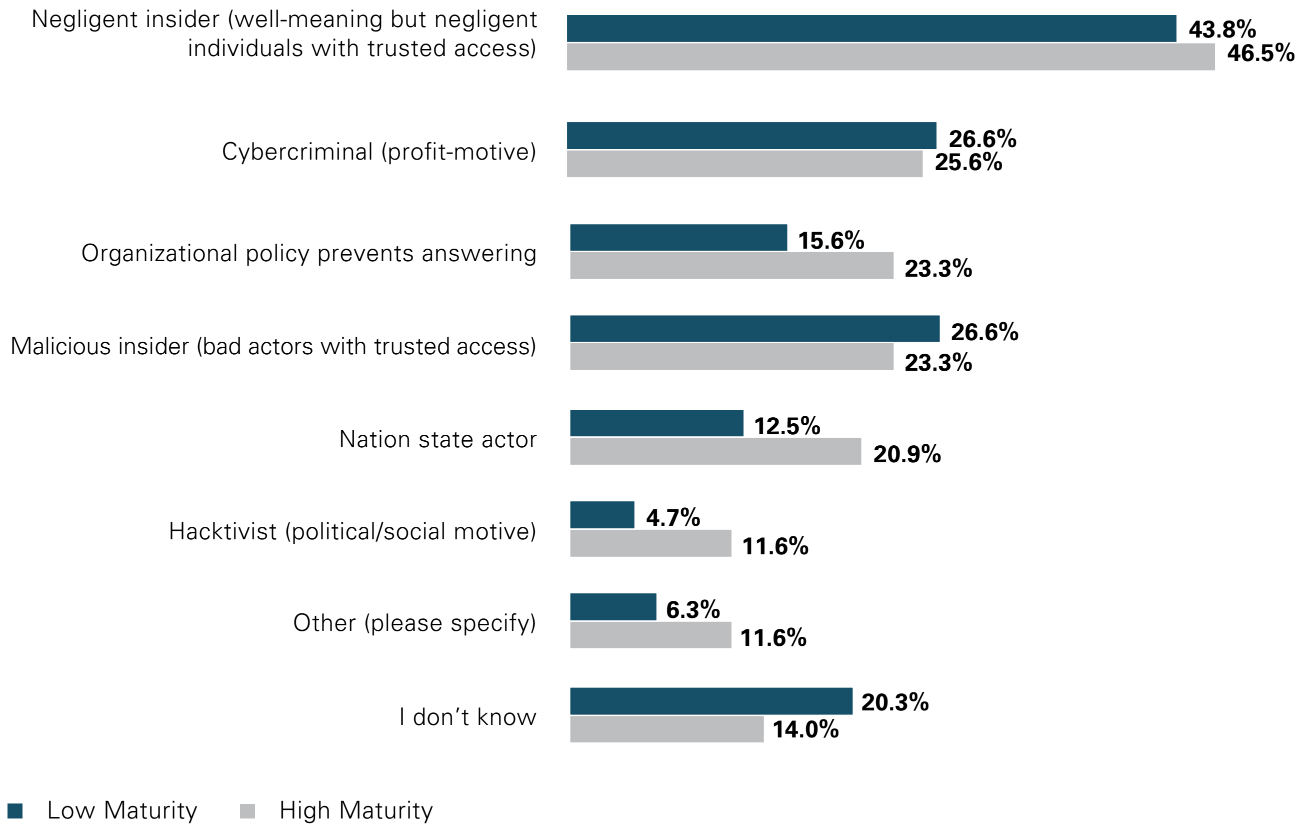
Eddie Toh
Partner, Head of Forensic Technology, Asia Pacific, Advisory, Cyber, Advisory,
KPMG Singapore

Threat actors

The *Negligent insider* continues to be the single most commonly identified threat actor in control system security compromises. It is part of our working environments that these *well-meaning but negligent individuals with trusted access* can cause disruption to systems and processes by the nature of their roles. Reducing the **likelihood** of them doing so calls for a two-pronged approach:

- Where possible, implementing safeguards to force confirmation of potentially disruptive actions. Dependent on situation/environment, these may take forms such as parameter limits, physical controls, or authorization checks requiring second party approval to enact.
- Training, including technical operations and security awareness components, to ensure those with trusted access know both how to perform their roles without disruption and the potential impacts of mistakes if they are negligent.

Select all of the following which describe threat actor(s) in your recent control system cyber security compromises (High Maturity vs Low Maturity)

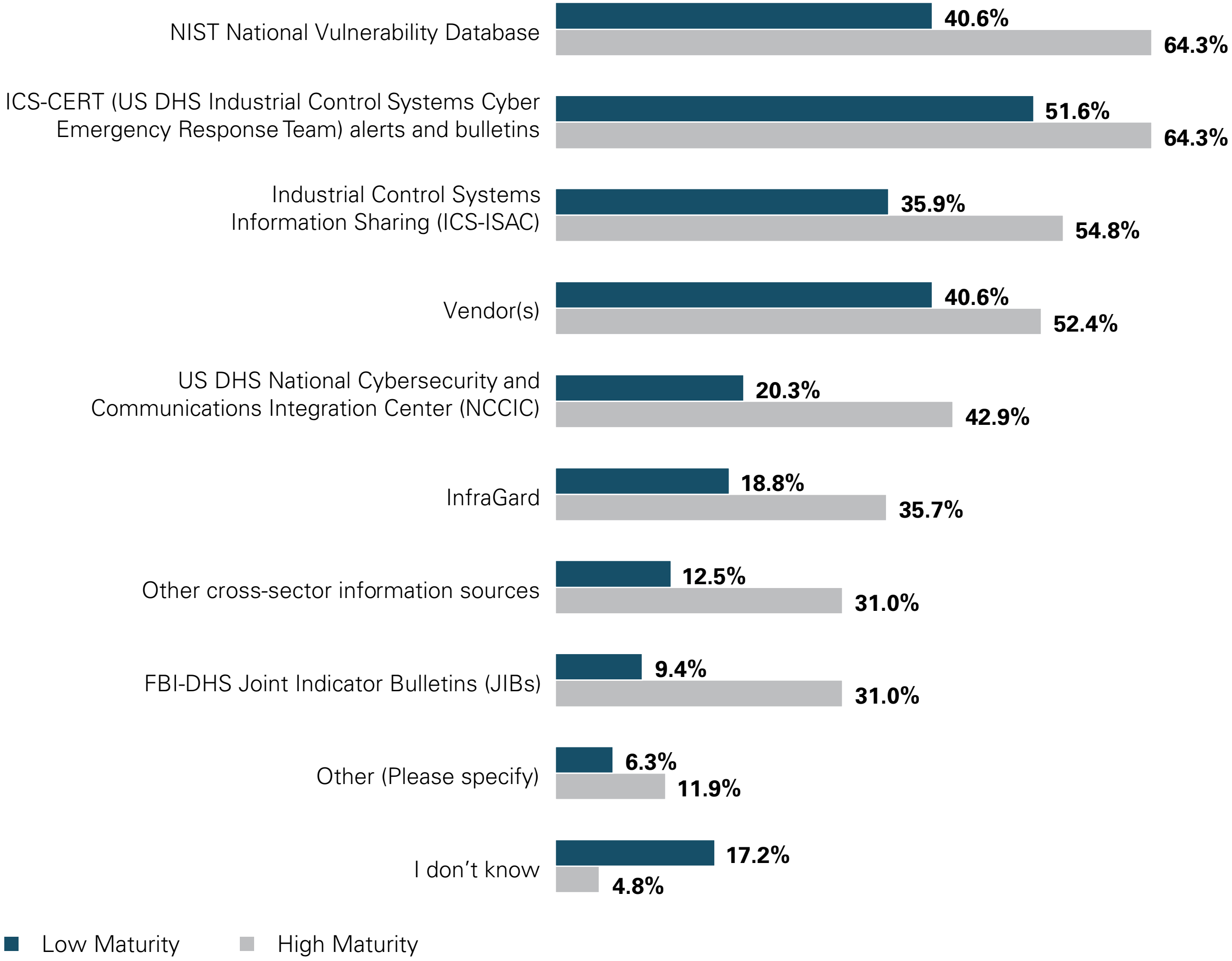


Sources of cyber threat information

It is clear that respondents from High Maturity control system cyber security programs draw on more sources of threat information than those in Low Maturity programs, are much less likely to lack knowledge of sources in use at their organizations (4.8 percent High Maturity vs 17.2 percent Low Maturity), and nearly twice as likely to use additional sources beyond our list (11.9 percent High Maturity vs 6.3 percent Low Maturity).

The greater visibility into their environments available to High M organizations is likely a factor in this, as it enables them to make greater use of the threat intelligence from the various sources available.

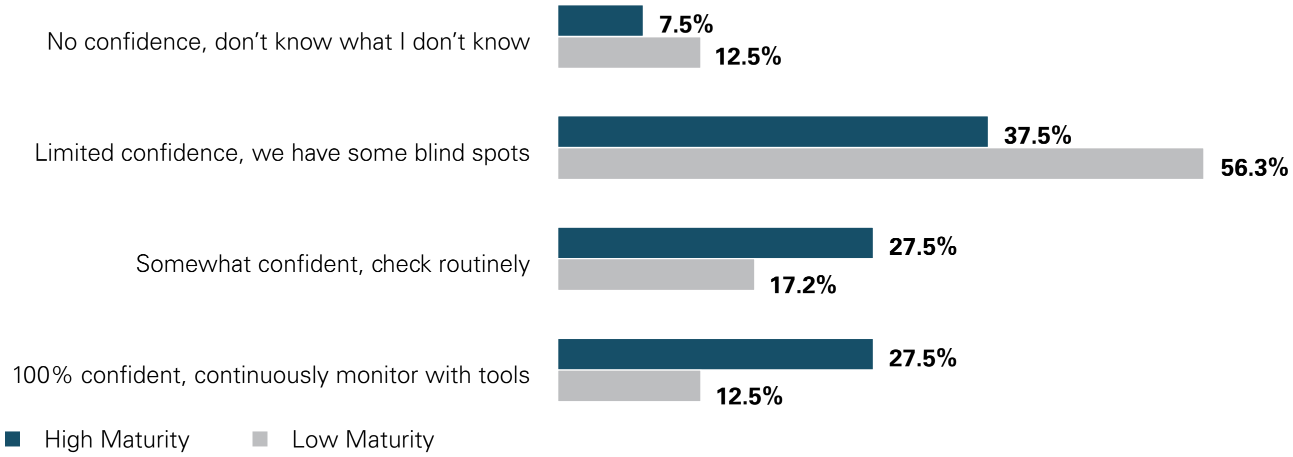
Please indicate which of the following sources of control system cyber security threat information your organization uses (High Maturity vs Low Maturity)



Confidence in network visibility

The greatest number of respondents recognize that they have some blind spots in their networks, whether discussing devices, applications or users. Those from more mature cyber security programs do more often have higher levels of confidence in their visibility into what's going in the areas for which they are responsible, but it is good to see that nearly two-thirds of even this group recognize that work remains to be done (total of 65 percent of High Maturity respondents indicated either *Limited Confidence* or *Somewhat Confident*). Conjecture based on ongoing incidents and assessments of SMEs in the field suggests that those who are *100 percent Confident* should be more cautious in their estimation, but we wish them all success.

How confident are you with the visibility of the devices, users and applications on your network? (High Maturity vs Low Maturity)

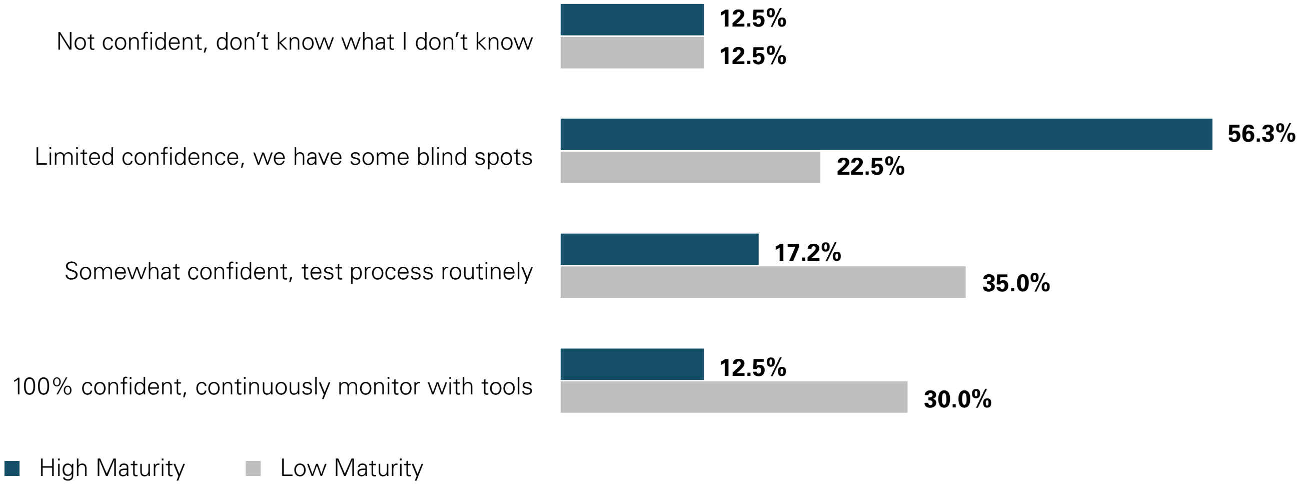


> “Most organizations have limited to no confidence in the visibility of their network and assets due to the growing complexity and size of their environment. It's important to understand that there are two types of network visibility: active traffic monitoring and independent architecture review. The former requires to deploy sensors in the field, which often takes years to complete. The latter can be achieved with a sensorless network modeling solution that requires only the configuration files of firewalls and routers, which means organizations can leverage it to gain visibility on their network architecture much faster and at a lower cost.”

Robin Berthier
CEO, Network Perception

Confidence in cyberattack response processes

How confident are you in your response processes should your organization suffer a cyberattack? (High Maturity vs Low Maturity)



Investments in the coming year

As a particularly key point of interest for many of our readers, we looked at responses to the question of planned OT cyber security investments. Perhaps the greatest surprise, given the number of well-publicized and impactful supply chain incidents of the past year, is how few of our respondents intend to focus resources on that area.

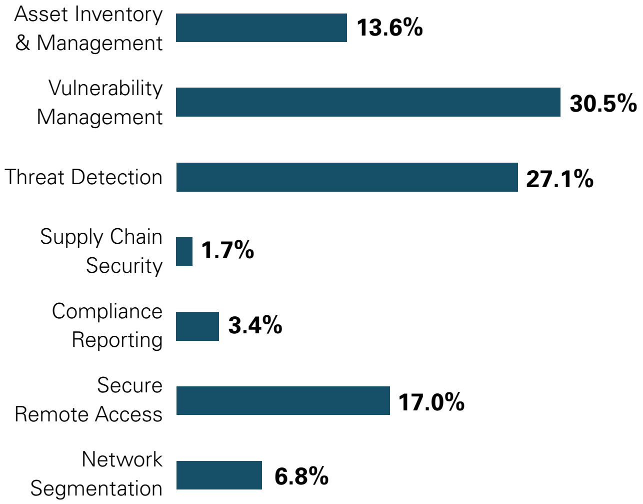
Viewed through a cyber security program maturity lens, it is clear that the less mature programs perceive the need to address basic *Asset Inventory & Management* as well as *Vulnerability Management* (20.6 percent and 30.2 percent, respectively) more than their counterparts in more mature environments (15.4 percent and 15.4 percent, respectively). Both groups intend to address shortcomings in *Threat Detection* (20.6 percent Low Maturity and 23.1 percent High Maturity), and the advanced group is placing an emphasis on implementing *Network Segmentation* (6.4 percent Low Maturity versus 18 percent High Maturity).

> “Despite the growing threats and increasing public pressure,organizations often remain unprepared. As a response, the cybersecurity industry includes a myriad of services, many of which are relatively new and sometimes untested. Confounded by choices, many organizations end up unprotected. Hence, investing in securing OT areas is a prerequisite for future industrial business and building the readiness in culture, process, people and technology. Cybersecurity capabilities need to be implemented to evaluate existing systems for threats and to continually monitor them in the future.”

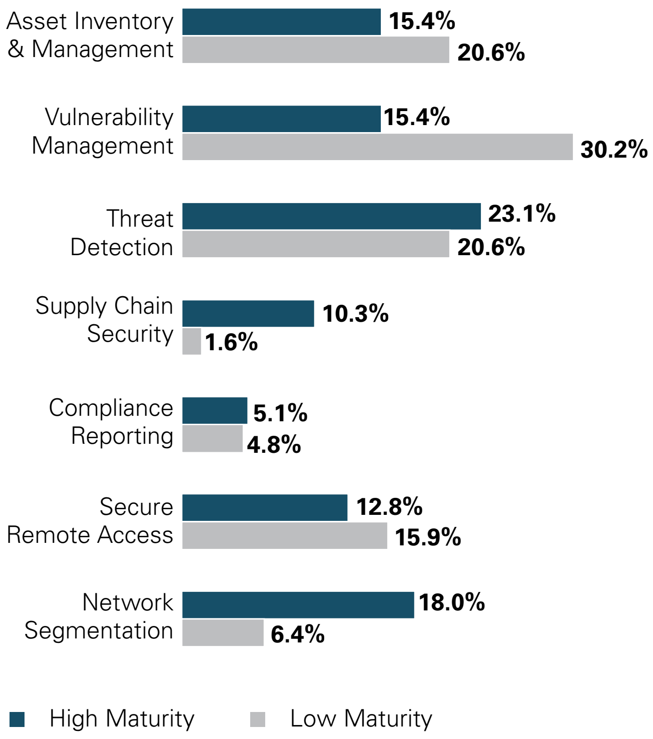
Hossain Alshedoki
Associate Director, IT/OT Cybersecurity & Data Privacy ENR Lead, KPMG in Saudi Arabia

Looking specifically at our financial decision maker and approver respondents, who should have the best knowledge on the matter, we see narrower agreement, with over half targeting just two areas: *Vulnerability Management* (30.5 percent) and *Threat Detection* (27.1 percent).

Which element of OT cybersecurity will you invest most in during the coming year? (Financial Decision Makers & Approvers)



Which element of OT cybersecurity will you invest most in during the coming year? (High M vs Low M)

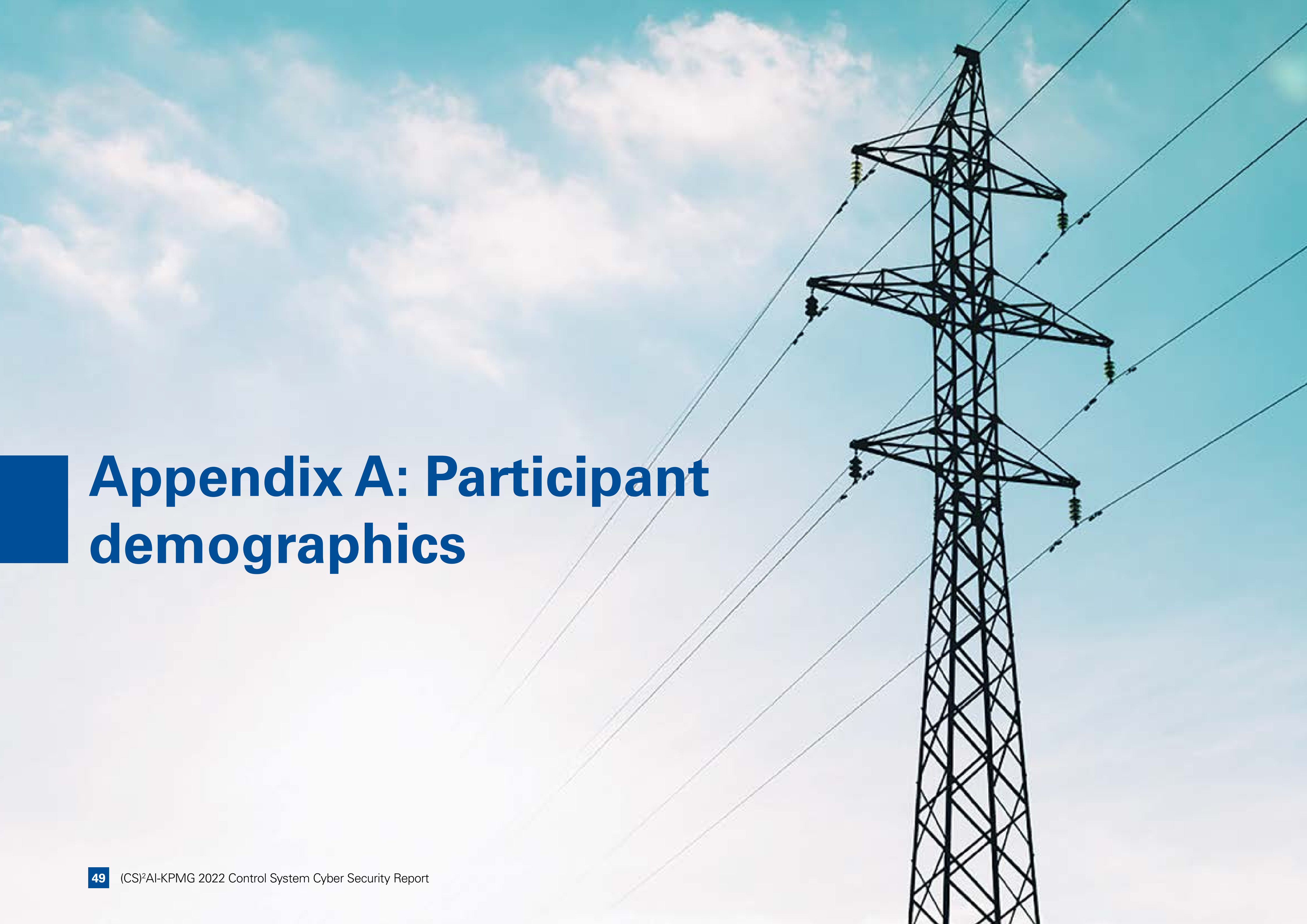


Chief recommendations

There are a few key concepts underlying our suggested approach to securing your CS environment. Firstly, security is an ongoing pursuit rather than a destination. The ideal state of being completely secure is a hypothetical only and likely not achievable in today's world. Deriving from that, we take as given the core mission of security is to manage risk, i.e., reduce it to acceptable levels. The parameters of this mission are established by organizational leaders, who define risk tolerance and must provide resources needed to bring risks into alignment with that appetite.

The absence of a 'one size-fits all' solution limits the specificity of recommendations to guide those leaders, but we can and do suggest that each organization pursue some basic objectives to the extent possible for them:

- Develop your workforce, through training, education, and creation/improvement of a security culture within your organization. This will reduce risk of incident occurrence, impacts and recovery time.
- Increase your insight into your control system environments by improving asset inventory and network traffic activity monitoring. This will reduce the likelihood and duration of disruptions.
- Segment your control systems, both from non-operational networks and where feasible, from each other. This will reduce the scope of incidents by limiting their ability to spread.
- Investigate your supply chain security and implement controls around entry points into your environments. This will reduce the potential of attacks on your suppliers impacting you.



Appendix A: Participant demographics

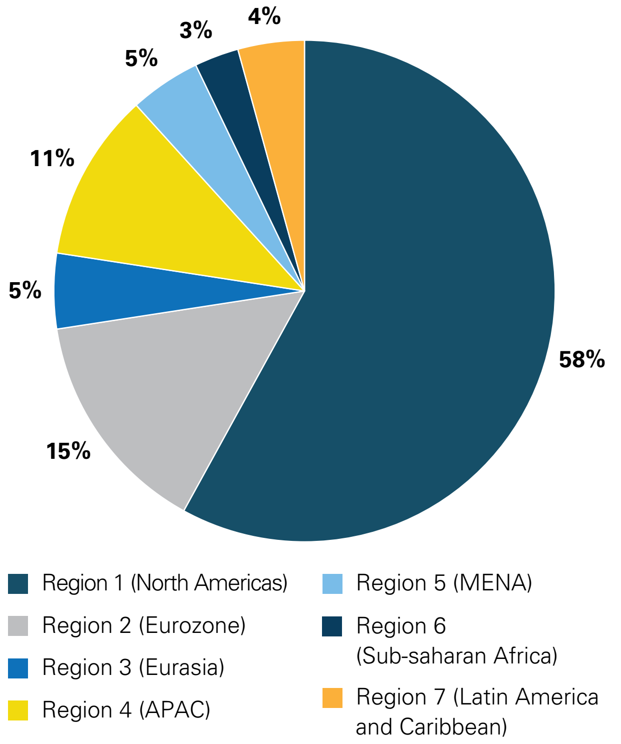
Respondent demographics

Location

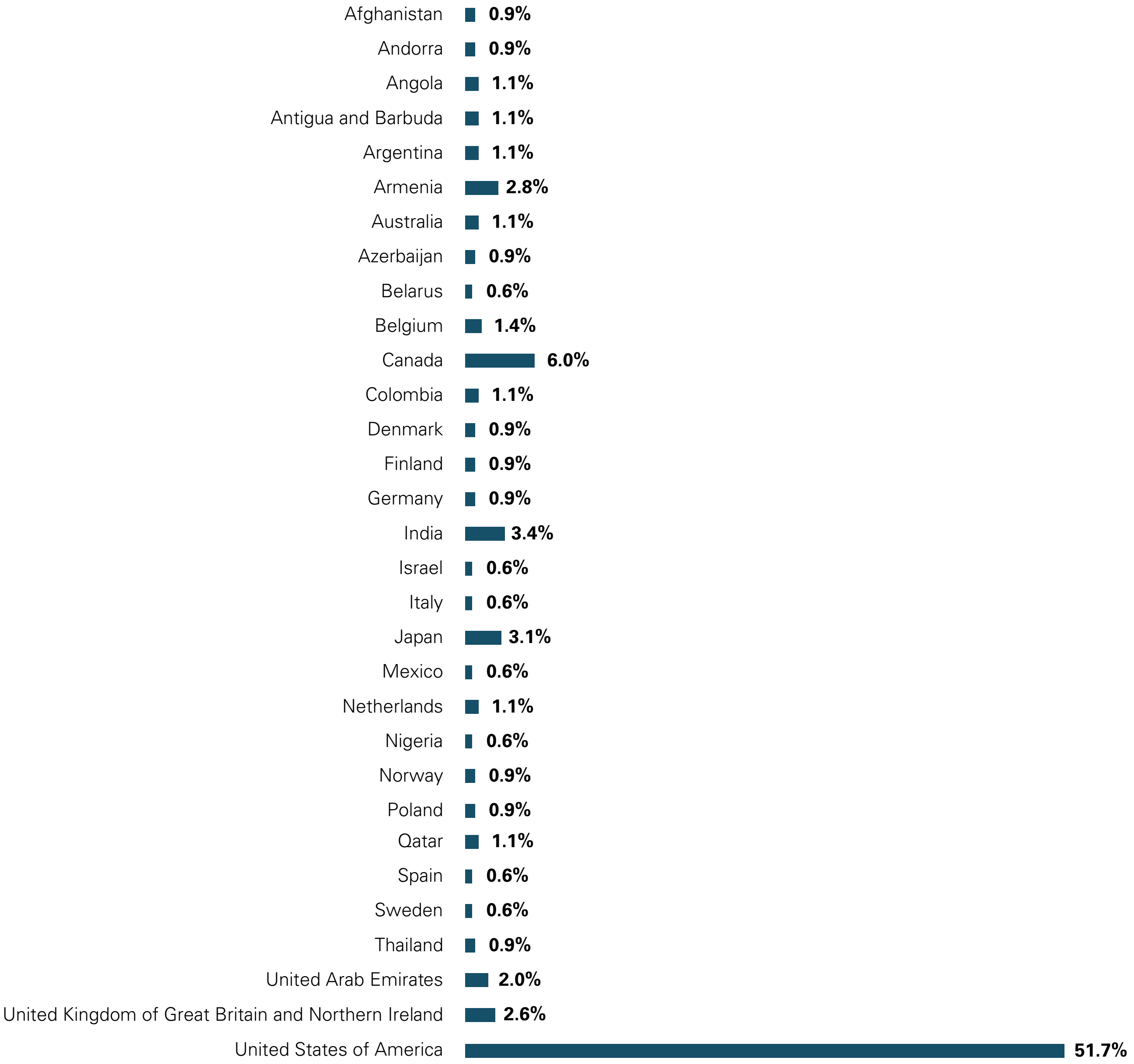
(CS)²AI has seen its membership grow by over 20 percent in the past year, but the pool of participants engaging with our research projects extends far beyond that group, and it is clear this larger body has grown most rapidly in North America. In absolute numbers, international response to our survey invitations increased significantly, as was our goal. However, participation from US and Canada grew so much more that, on a percentage basis, this region now represents more than half of our participants.

Please note the list of countries is partial; many have been excluded for legibility purposes.

Responses by region



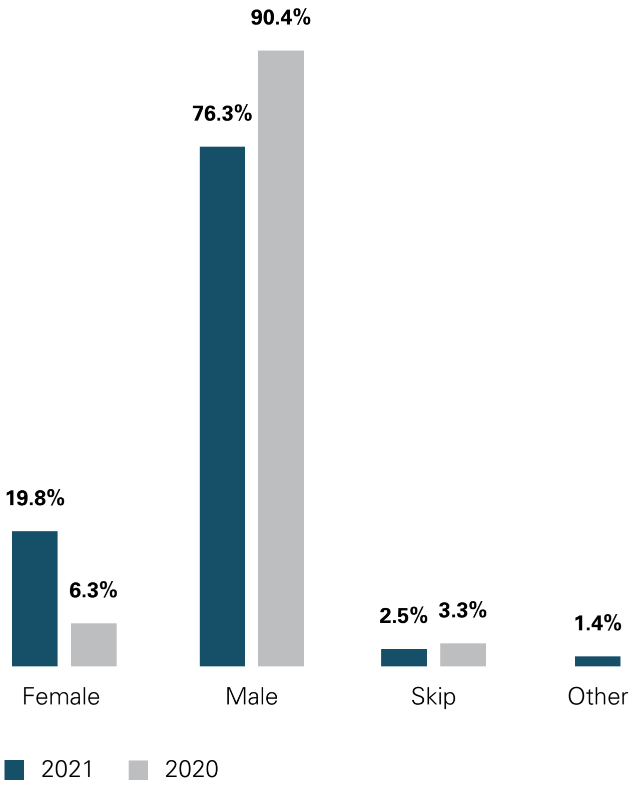
Please identify the country in which you primarily work



Gender participation

It is taken as a given that addressing the shortages in this workforce will require drawing from all populations. We were gratified to have reached a much greater number of women in the CS cyber security field this year, with significantly more participating in the survey than previously. This offers us the opportunity to consider differences in perspectives between these groups. One interesting note on representation here: We found the women roughly 50 percent more likely to work for organizations with workforce sizes between 100 and 1,000.

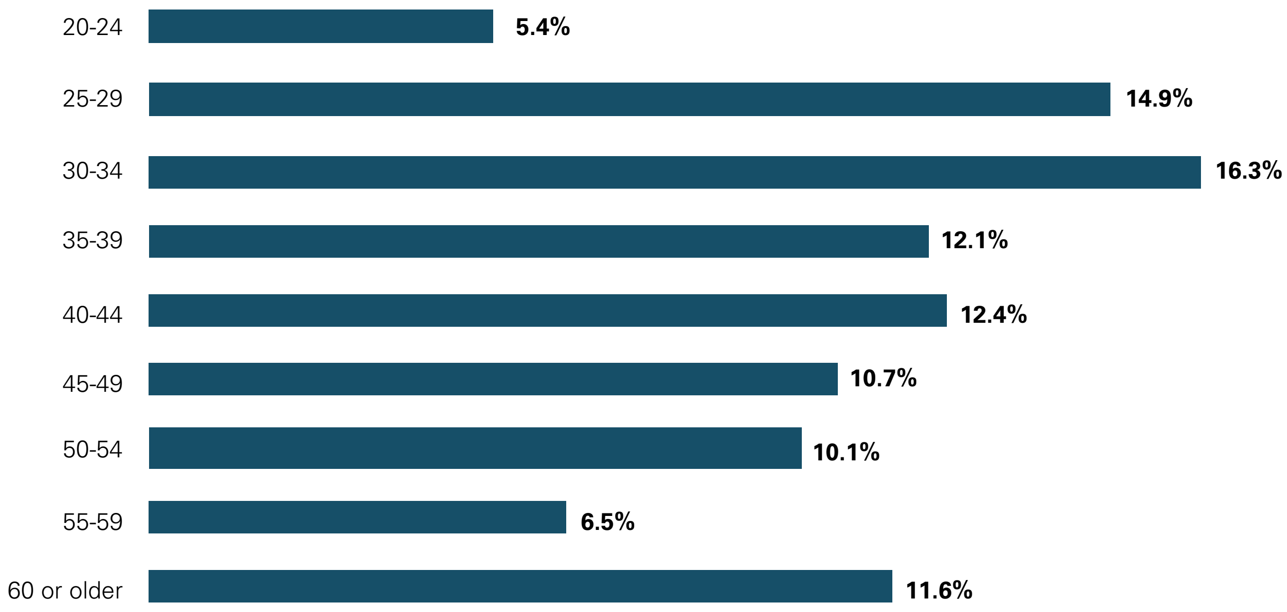
Please select your gender



Age distribution

We take as a positive sign that the number of respondents in the younger age brackets rose sharply this year. The aging out of the science and engineering workforce, of which CS cyber security practitioners is a part, has been frequently reported on and presents concerns both because of the loss of institutional knowledge and the reductive effect on available human resources in the face of growing demand. The effect is particularly pronounced in highly developed nations such as the United States, where we are seeing the combination of rapidly increasing levels of interconnected infrastructure and supply chains with generational turnover among professional engineers. With all of this in mind, we are very glad to see that most (61.1 percent) of our participants are in the first half of their careers, with decades remaining to contribute to our shared mission.

Select your age range



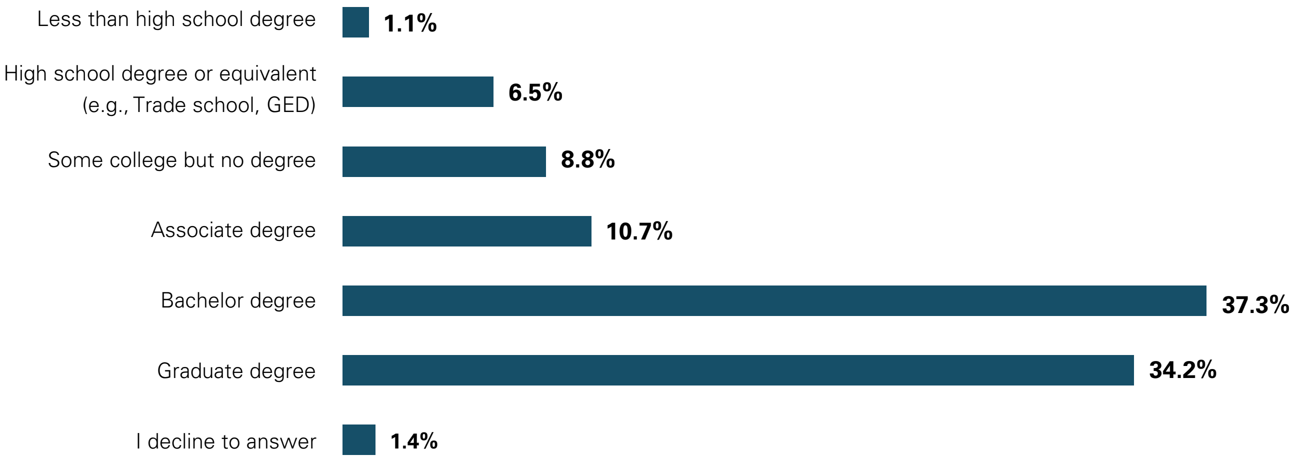
Respondent employment type

With access to learn on expensive OT systems constrained and the costs of technical training high, most practitioners gain these through their employers, for whom these are part of the costs of doing business. We continue to see the great majority (59.8 percent) of respondents working as employees of the organization for whom they perform their cyber security duties.

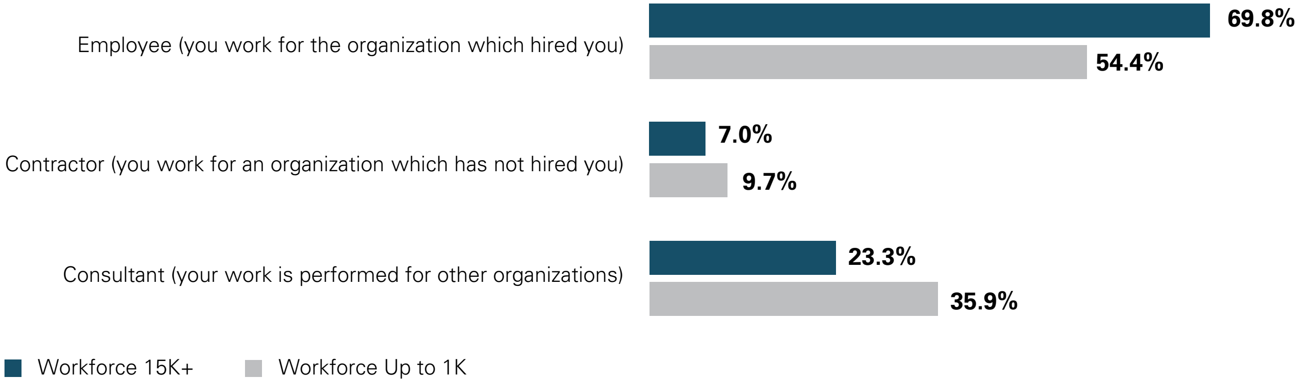
We did observe some difference between organizations based on their size, however, showing an increased use of *Consultants* and *Contractors* among entities with workforces below 1,000. This may reflect the effect of tighter financial constraints reducing the capacity of these organizations to dedicate permanent resources to cyber security duties.

Respondent educational level

Please select the highest level of education you have completed or the highest degree you have received



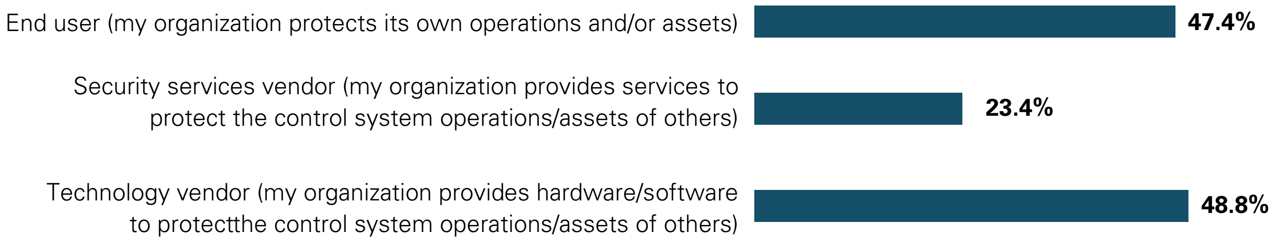
Please select the description which best fits your work position



Organization category

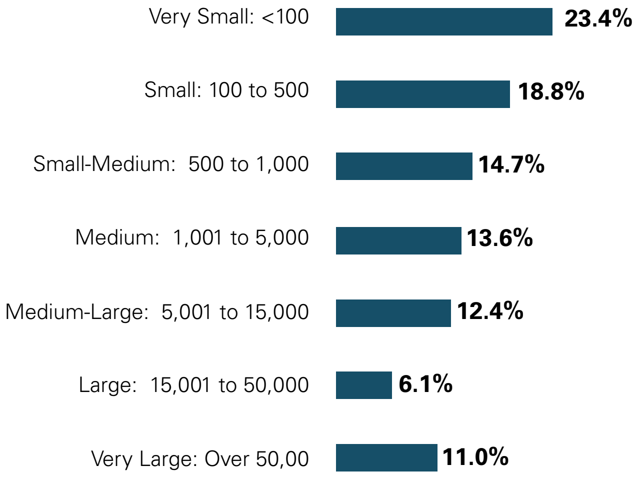
Please note that respondents were able to choose more than one category. While few did, the responses in this table do sum to more than 100 percent due to this.

Identify your organization’s category in relations to control system cyber security



Organization workforce size

Please provide your best estimate of your organization's workforce



Appendix B: Annual report steering committee

Derek Harp

(CS)^{2}AI Founder and Chairman: Annual Survey & Report Chair, Co-Author

Bengt Gregory-Brown

(CS)^{2}AI Co-Founder and President: Annual Survey & Report Director, Lead Designer & Analyst, Co-Author

John Merkel

(CS)^{2}AI Lead Data Analyst, Annual Survey & Report Lead Data Scientist

Walter Risi

(CS)^{2}AI Strategic Alliance Partner Liaison, Survey Design and Report Analysis Teams
Global Cyber IoT Leader
KPMG in Argentina

(CS)^{2}AI MEMBERS HELPING MEMBERS

On behalf of the entire community, (CS)^{2}AI would like to extend a sincere **Thank You** to the 2022 annual report steering committee. From reviewing questions, helping publish the survey tool, studying results, providing or editing content, and distributing the final report, this group of professionals makes this annual effort possible. It is one of the best examples of (CS)^{2}AI **Members Helping Members**.

Brad Raiford
Survey Design and Report Analysis Teams
KPMG in the US

Hossain Alshedoki
Report Analysis Team
KPMG in Saudi Arabia

Eddie Toh
Report Analysis Team
KPMG in Singapore

Jaco Benadie
Report Analysis Team
KPMG in Malaysia

Sandra Cusato
Report Production Lead
KPMG International

Andrew Ginter
(CS)^{2}AI Strategic Alliance Partner Liaison, Survey Design and Report Analysis Teams
Waterfall Security Solutions

Bryan Singer
Report Analysis Team
Accenture

William Noto
Report Analysis Team
Fortinet

George Kalavantis
Report Analysis Team
Industrial Defender

Robin Berthier
Report Analysis Team
Network Perception

William Malik
Report Analysis Team
Trend Micro

Ron Indeck
Report Analysis Team
Q-Net Security

Keith Beeman
Report Analysis Team
Tempered

Rick Kaun
Report Analysis Team
Verve Industrial

Richard Springer
Report Analysis Team
Tripwire

Appendix C: About (CS)^{2}AI

VISION

Strengthen global critical infrastructure by fostering Control System Cyber Security peer-to-peer networking and development.

MISSION

An international organizaton enabling peer-to-peer organizations and supporting their grassroots efforts.

GOALS

- Professional networking
- Global alliances
- Professional development
- Community outreach
- Leadership opportunities

(CS)^{2}AI ("See-Say" for short) is a rapidly growing global nonprofit association approaching 24,000 members worldwide, the premier global not-for-profit workforce development organization supporting professionals of all levels charged with securing control systems. We provide the platform for members to help members, foster meaningful peer-to-peer exchange, continue professional education and directly support cyber security professional development in every way.

Peer-to-peer networking on a global scale

As a member of (CS)^{2}AI, you join a global community of Control System Cyber Security practitioners who are motivated to improve and develop both personally and professionally in this highly critical and consequential field. (CS)^{2}AI delivers a venue for peer-to-peer connections, small-group interactions with leading industry experts, the sharing of experiences, challenges and best practices, and resources you need to develop and grow. Explore the growing range of exclusive (CS)^{2}AI member opportunities designed to help you reach the next level in your career journey.

If you are not already an active member of the Control System Cyber Security Association International, we invite you to join our members-helping-members efforts by GETTING INVOLVED today. Our association has many ways to contribute as a global member, speaker, teacher, mentor, partner, contributor, committee member, (CS)^{2}AI Fellow or research participant.

Appendix D: Report sponsors

(CS)²AI wishes to extend our heartfelt thanks to the following Strategic Alliance Partners for their continued contributions to this annual report and most importantly, their support of cyber security professionals around the globe who are striving to protect the critical systems we all rely on.

Title Sponsor	Editor Sponsor	Sponsors		
KPMG	Fortinet	Applied Risk	Network Perception	Trend Micro
	Waterfall Security	GBQ Partners	Q-Net Security	Tripwire
	Sable Lion Cyber	Industrial Defender	Tempered	Verve Industrial

(CS)^{2}AI Web/Media Links

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

Designed by Evalueserve.
Publication name: (CS)^{2}AI — KPMG Control System Cyber Security Annual Report 2022
Publication number: 137866-G
Publication date: April 2022