(CS)²AI-KPMG Control System Cyber Security Annual Report 2020

(CS)²AI™ CONTROL SYSTEM CYBER SECURITY ASSOCIATION INTERNATIONAL

KPMG

Chairman's message

Dear Industry Colleagues,

Control systems have become vital to ensure that our daily lives run smoothly, supplying power, running refineries, but also running medical, transportation, building control, and logistics technologies. The exposure list is long and stakes are growing higher. As professionals operating and managing cyber security for all types of control systems (CS), you have a tall order with converged OT and IT networks in play. Safeguarding operational assets from persistent threats while also maximizing efficiency, real time intelligence and system uptime is no small task.

That's why we founded (CS)²AI, a not for profit organization we call "See-say". Our mission is to 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 any way we can. Accomplishing this mission also involves coordinating cross community collaborative research. I'm excited to deliver the results of just such an initiative with our inaugural 2020 (CS)²AI-KPMG Annual Control System Cyber Security Report. The report steering committee queried our 17,000+ worldwide membership and the community at large with questions regarding their own direct experiences and observations in the control network trenches.

This first edition and subsequent annual reports are dedicated to one goal: "providing a highly-valued decision support tool to decision-makers and -influencers." Our analysis includes deeper dives into multi-factor correlations and, as our database grows year-over-year, we are committed to providing insights based on longitudinal trend analysis. Even this initial year has surfaced invaluable insights and actionable information for practitioners and leadership responsible for CS, such as mis-matches between security spending priorities and ROI of past allocations, and strong success factors common to the most mature cyber security programs.

An annual research program and report like this is the result of amazing participation from Strategic Alliance Partners (SAP), a dedicated steering committee, additional volunteers (see page 53 of this report) and members like many of you participating in the research for the benefits of other members. We thank many of you for taking our surveys and I'd like to give my most heartfelt thanks to KPMG, our report's Title Sponsor, without whom this report would not exist. I'd also like to specially thank Airbus CyberSecurity, Waterfall Security Solutions, Fortinet, and Palo Alto Networks for their important contributions to this significant project.

I hope this report is valuable to you and please let us know how we can improve it.

Sincerely,

Derek Harp
Founder and Chairman,
Annual Report Chair
(CS)²AI

I urge you to join our *members helping members* efforts by joining the (CS)²AI community as a Global Member, Partner, contributor, committee member, (CS)²AI Fellow and research participant. You can review multiple ways to **GET INVOLVED** on our global website. I look forward to your survey feedback, ideas for future surveys, and community engagement that will bolster this business-critical cause.

For those who prefer not to use embedded links, you can **GET INVOLVED** by directly typing in https://www.cs2ai.org/get-involved-2020

Annual Report Title Sponsor Foreword

We're heading into a new reality for cyber security in industry. The events of this year have disrupted markets and supply chains, forced major change in operating models and exacerbated political tensions. In the midst of this we face a future of relentless and increasingly sophisticated cyber-security threats demanding that businesses raise the bar on their Control Systems security measures while contending with growing cost pressures. But as our new survey findings reveal—perhaps alarmingly—far too many enterprises remain dangerously exposed to costly and potentially debilitating cyber attacks.

The 2020 (CS)²AI-KPMG Control Systems Cyber Security Survey Report offers an in-depth look into the state of Control Systems security practices, measures, threats and risks in today's rapidly changing and endlessly challenging cyber security environment. Our timely analysis is based on input from a representative sample of the more than 16,000 members of the Control System Cyber Security Association International—professionals on the front lines of cyber security for all types of control systems.

Businesses are clearly struggling to resolve cyber-security vulnerabilities in Control Systems and operational technology (OT) environments. Roadblocks include insufficient Control Systems security expertise, cited by 58 percent of respondents, insufficient personnel (48 percent) and operational uptime requirements (44 percent). Lack of financial resources was cited by more that one-third of respondents (37 percent), with a similar number (35 percent) also citing insufficient leadership support.

New threats are emerging

The unfortunate reality is that these perceived obstacles to progress have remained unresolved for several years. Our message to businesses? It's time to focus on immediate solutions that will deliver much needed progress on security and create momentum for change.

Common attack vectors still seem to succeed, including use of USB devices such as memory drives and other portable media, as well as email phishing and ransomware—the commoditization of which has increased throughout the COVID-19 pandemic. And while these attacks continue to inflict costly disruption and collateral damage to Control Systems, the threat is evolving and becoming more targeted as attackers become increasingly 'operational technology savvy' and deliberate in their efforts to disrupt Control Systems.

It seems safe to predict that if businesses don't take appropriate action soon to mitigate such threats, regulators and governments certainly will. In the new reality, many of the baseline assumptions about cyber resilience planning have been challenged. Smart, forward-looking businesses will take steps to reconsider what their worst-case scenarios are, and take decisive action to protect their valuable operations, assets and systems in advance of action being directed by government.

Take action today

Where to start today with fundamental steps in the journey to enhance security amid evolving threats? Begin with network segregation. One of the most powerful but underutilized security controls, network segregation essentially separates segments of the enterprise and OT network, using firewalls to control and police traffic between each segment based on user and device criteria.

For immediate security enhancement, limit and control use of USB devices and scan each for malware. Update malware and virus protection. And create a curated inventory of business assets requiring immediate protection, including hardware and software assets.

Looking beyond these immediate steps, how will you position your business in the longer term to intercept new threats and threat actor behaviors as they inevitably emerge in the Control Systems environment? To enhance security going forward:

— Determine your risk profile and review your assumptions;

— Assess your Control Systems security posture;

— Monitor OT networks for insights into anomalous network traffic activity;

— Segment networks via controls that limit access;

— Secure your supply chain to minimize infiltration.

In addition, don't underestimate today's urgent need for highly skilled OT-security practitioners. The lack of Control Systems security expertise, a key roadblock for so many organizations, has never been greater and continues to limit real progress. Make no mistake—even today's sophisticated cyber-security tools can't replace the need for the skills and insights that security experts can provide in the battle to anticipate trouble and mitigate risk.

Data unlocks critical insights

Becoming data-driven is also indispensable to success. The survey reveals a clear relationship between a failure to focus on the data and metrics needed to enhance security, and poor levels of maturity for OT security programs. Reliance on data is crucial if you hope to optimize security—you can't control and optimize what you can't see. Pursuing a data-driven approach also implies, of course, the need for digitalized solutions and an effective governance regime. And beyond that, data lets you take a tailored, risk-based approach to cyber investment in your OT security; with businesses reviewing their costs during an economic downturn, the need to efficiently apportion resources is more critical than ever.

Ultimately, Control System security is a balancing act between cost control, maintenance of system availability and action to counter a growing threat that businesses will ignore at their own peril. There's less time to prepare for the new reality than ever, with the pandemic unexpectedly accelerating the drive towards digitization and automation as part of efforts to save costs, improve capabilities and reduce dependence on personnel. Take immediate action today, continually build on your security architecture's capabilities, and enable your business to anticipate and intercept tomorrow's emerging threats head on. Success demands appropriate investment, education and awareness in order to act now and, going forward, to ideally embed design principles into the next iteration of infrastructure upgrades and beyond.

Awareness campaigns and a drive toward much-needed cultural change cannot happen soon enough to advance and optimize OT security. We sincerely hope that this in-depth report will encourage today's Control System cyber-security practitioners and their business leaders to pursue strategic, well-informed strategies that can truly enhance the protection of critical assets and position their businesses for a more secure future.

Walter Risi
Global Cyber IoT Leader
KPMG in Argentina

Contents

Executive summary

In 2018 the leaders of the Control System Cyber Security Association International determined that in order to deliver on their core mission of improving professional development opportunities for the Control Systems (CS) cyber security workforce we needed to provide clear and validated information regarding the realities of defending this space, and decision support tools such that OT cyber security practitioners and leaders could make best-informed decisions regarding the protection of their critical assets.

Drawing on decades of Control System (CS) security survey development, research, and analysis led by Founder and Chairman Derek Harp and Co-Founder and President Bengt Gregory-Brown, the (CS)²AI team asked its more than 16,000 worldwide membership critical questions regarding their own experiences in the network trenches, protecting and defending assets and systems worth millions to billions in capital investment and ongoing revenue and affecting the lives and business operations of enterprises spanning the globe. Their answers, undiluted by organizational politics or vendor influence, have enabled us to develop a true picture of the state of the CS/OT threatscape[1] in our rapidly changing environment.

The following Report intends to convey that picture and provide the decision support tools so important to improve our CS/OT cyber security posture and improve our risk management both effectively and efficiently. A number of our questions are designed specifically to gain insight into the ROI of respondents' relevant efforts, and many of our findings establish clear benchmarks and trends.

[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.

Control Systems and Operational Technology

The authors have chosen the overarching terms Control System (CS) and Operational Technology (OT) as an umbrella for all systems that manage, monitor and/or control physical devices and processes. The two terms are used interchangeably in this document and 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.

Project objective

The project team set out to gather data on the current state of CS security practices, measures, threats and risks, in order to foster informed discussions between the key stakeholders in this community: vendors, service providers, practitioners, and leaders; and to educate both the experienced and those newly entering this field.

Our target population consisted of professionals experienced and actively engaged in the cyber security of Control Systems (CS) regardless of whether focused primarily as cyber security practitioners, Operational Technology (OT) engineers, researchers, overseers, or any combination of these. We reached participants from all organizational levels, from entry-level technical staff to senior leadership. Responses came from all over the world.

Survey methodology

The (CS)²AI-KPMG 2019 Control System Security Survey and Report was a collaborative effort of the following entities:

- **(CS)²AI:** As the originator of the project, (CS)²AI bore the primary role in developing the project plan, leading and implementing the project work, and producing the project deliverables.
- **KPMG:** As the Title Strategic Alliance Partner (SAP), KPMG provided support in the form of both its human and organizational resources to augment (CS)²AI's own capabilities.
- **Additional (CS)²AI SAPs:** non-Title SAPs committed to providing support in the form of both human and organizational resources where possible. (see Survey Sponsors).

To accomplish the objectives described above, (CS)²AI and KPMG distributed an online survey to CS/OT security practitioners worldwide for several months of Q3–Q4 2019 to collect key data around Control System security events, trends in attack activities and protective technologies, and how organizations are adapting to changes in the threat landscape. Survey invitations were sent to (CS)²AI associated members, known OT security defenders and researchers, distributed through various social media channels, and promoted on multiple sites serving the CS cyber security workforce, with the intent to collect as wide a sample as possible. Participation was incentivized by a prize drawing for those completing the entire survey. Respondents self-selected by affirming their involvement with the field of CS Cyber Security.

Key highlights

This research had a particular focus on identifying elements key to effective CS security programs. To that end we compared answers of respondents classifying their programs at different levels of maturity. (See CS security program maturity level, page 31, for level definitions)

Several commonalities were identified. Of particular interest, responses from self-identified mature-program participants vs low-maturity-programs showed that the former:

Use Managed CS Security Services much more often: **47%** vs **6%**

Conduct comprehensive, end-to-end security assessments more often: **53%** vs **36%**

Frequently replace vulnerable CS hardware or software following security assessment: **63%** vs **34%**

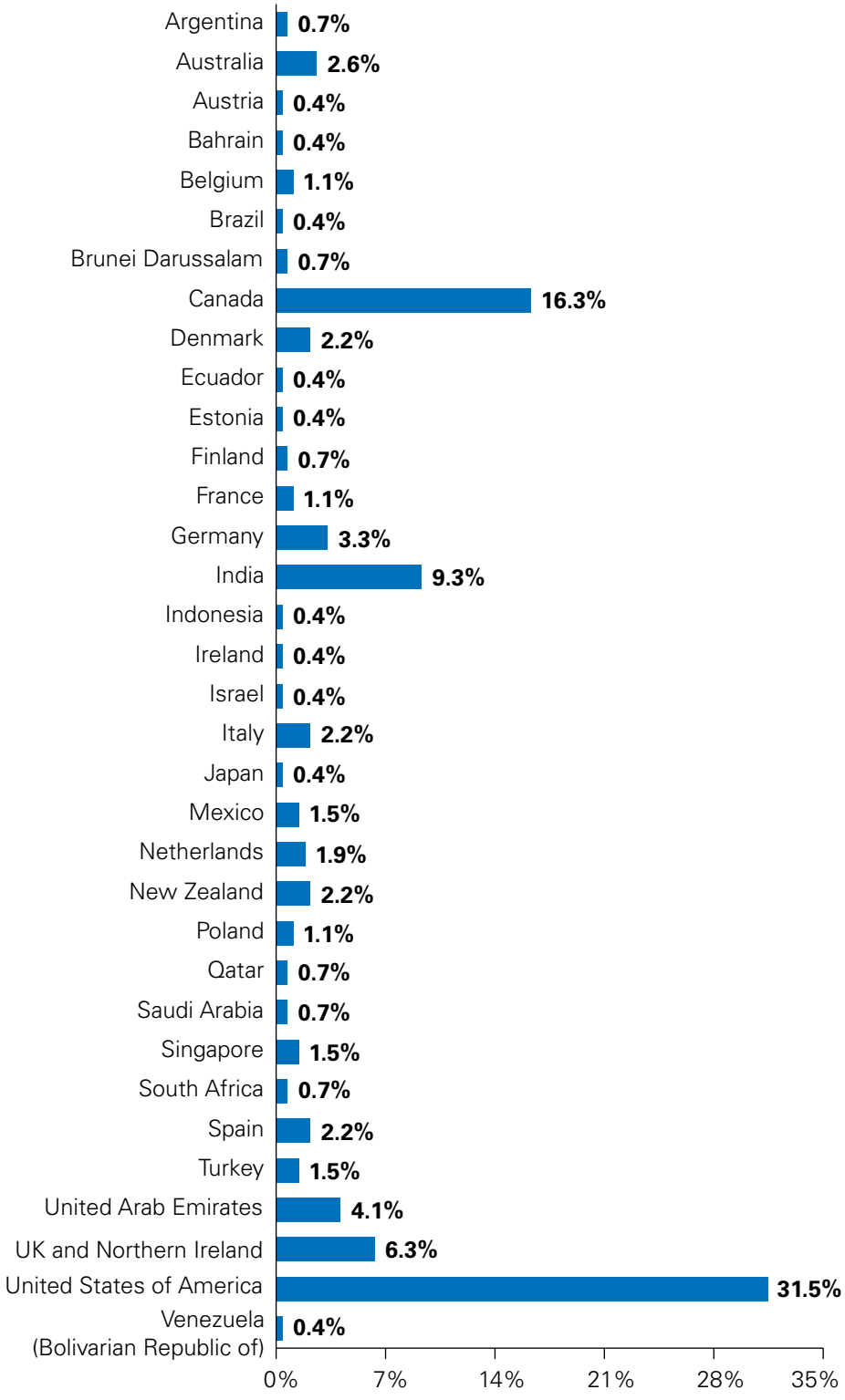
Monitor all CS networks: **53%** vs **16%**

Have implemented NextGen Firewalls: **81%** vs **51%**

Respondent demographics

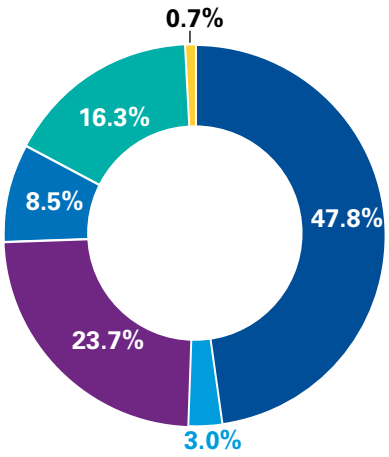
With (CS)²AI's largest concentration of active global members in North America and this inaugural survey being conducted only in English (localizing future surveys for non-English speakers is under discussion) our team was pleased to see that over half of our respondents were located outside of this region. India, the UK and the UAE followed the US and Canada in number of responses and, although individually each fell below the critical numbers needed for nation-by-nation statistical validity, were quite valuable in regional analysis.

Responses by locations



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey

Responses by region



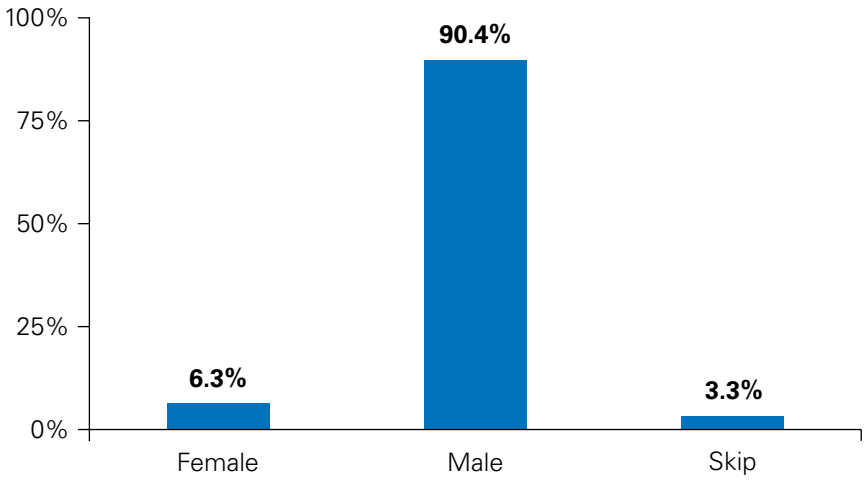
- North America
- South and Central America
- Europe
- Middle East
- ASPAC
- Africa

Answers to survey questions did not generally vary significantly by region, with one exception: respondents in the middle east were much more concerned with Physical Security than other regions, selecting it as their top priority at twice the rate of APAC participants and four times the rate of North Americans and Europeans.

Gender representation

The stereotype stating that the field of OT cyber security is male dominated was born out in our data, with less than one out of fifteen respondents indicating they were female. This was unfortunately too few for statistically valid further analysis of this group, and increased participation by women is hoped for in future surveys.

Gender representation



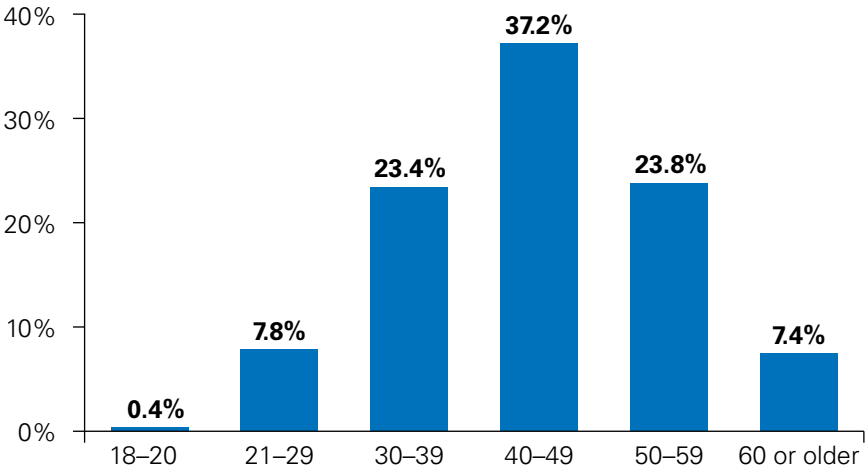
Age representation

It has been recognized (at least in the United States) for some years that the science and engineering workforce, of which OT cyber security practitioners is a subset, is aging.[2] US Census data further indicates that many begin partial retirement even well before reaching the age of 60.[3]

Our respondents confirm that this trend is not solely a North American concern, with over 30 percent within one decade of likely retirement age. With less than 10 percent in the first decade of their careers the available OT cyber security workforce is likely to shrink in the future. This can only worsen the documented shortages found by numerous studies.[4,5]

In light of ongoing and irreversible technological trends towards greater IT/OT integration, the authors recommend any entity with interest in the availability of trained and competent CS/OT cyber security practitioners consider how they might contribute to improving the development of this workforce.

Age representation



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey

Cyber security expertise in short supply

The need for cyber security professionals has never been greater. Insufficient cyber security expertise or personnel stands out as a critical obstacle in mitigating OT security vulnerabilities. Cyber security professionals are in short supply and enterprises are limited in terms of the number of IT security professionals they can hire. With the number and complexity of cyberthreats growing and the comprehensiveness of security architectures increasing, the good news is that there are several options available to support short-term needs while organizations focus on developing long-term solutions.

[2] https://nsf.gov/statistics/2018/nsb20181/report/sections/science-and-engineering-labor-force/age-and-retirement-of-the-s-e-workforce

[3] Ibid

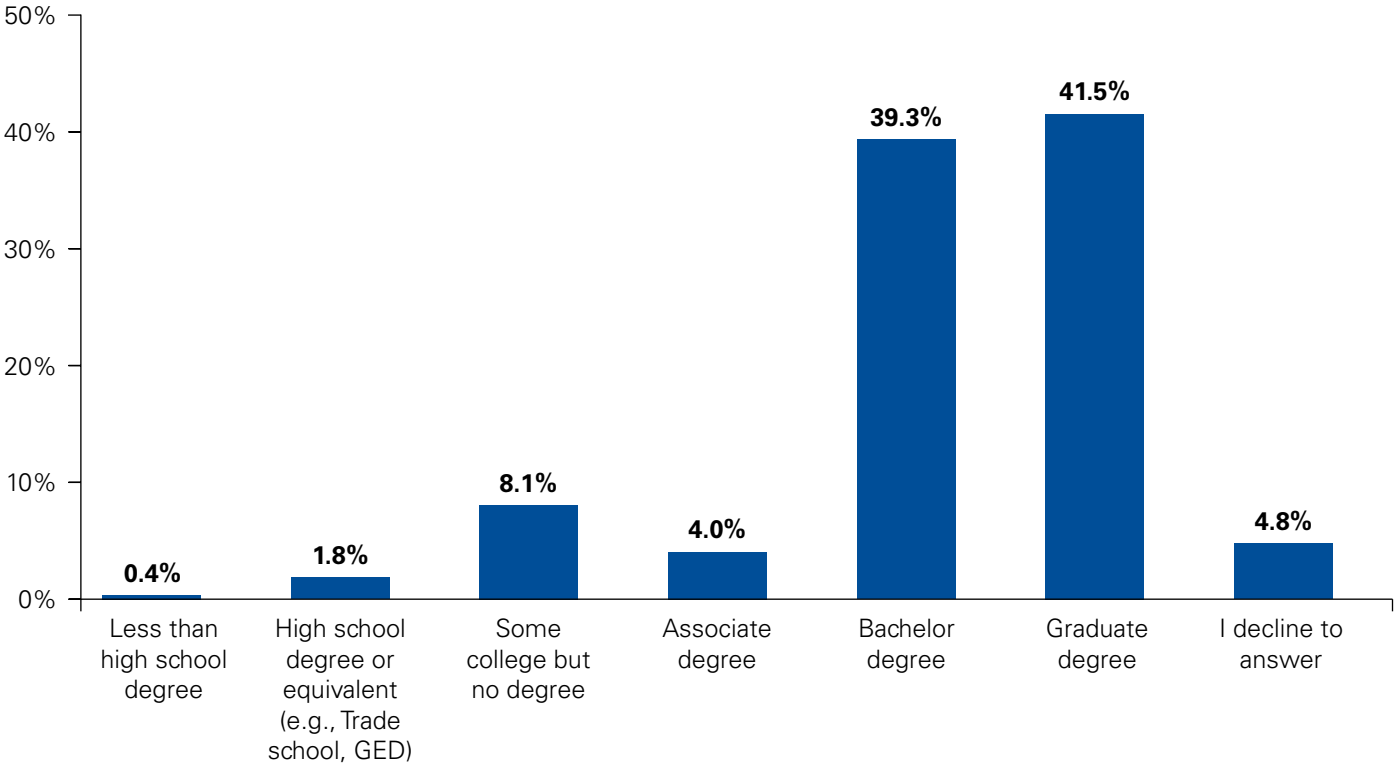
[4] https://www.csis.org/analysis/cyber security-workforce-gap

[5] https://www.isc2.org/News-and-Events/Press-Room/Posts/2018/10/17/ISC2-Report-Finds-Cyber security-Workforce-Gap-Has-Increased-to-More-Than-2-9-Million-Globally

Respondent educational level

Controls System work is frequently technical and requires significant personal investment in education and training, and Control Systems cyber security work calls for additional learning beyond that. Over 80 percent of respondents indicated their completion of a 4-year or more higher education degree.

Education level

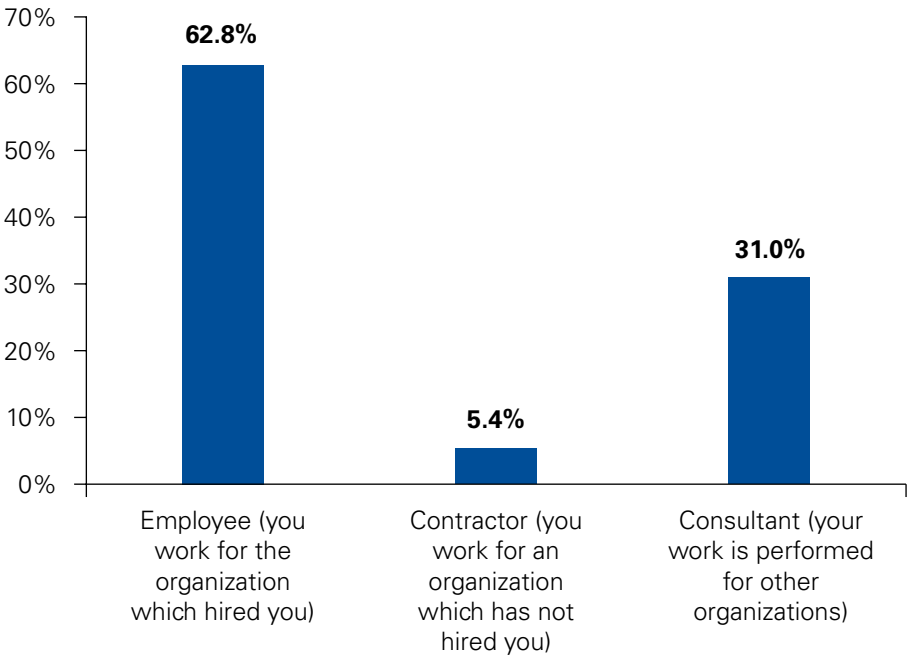


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Respondent employment type

A large majority of individuals develop their expertise working directly for critical asset owner/operators. With the continually high demand/supply ratio of skilled CS cyber security practitioners, of course, opportunities abound for capable freelancers. Further research into career paths is an area for future projects.

Employment type

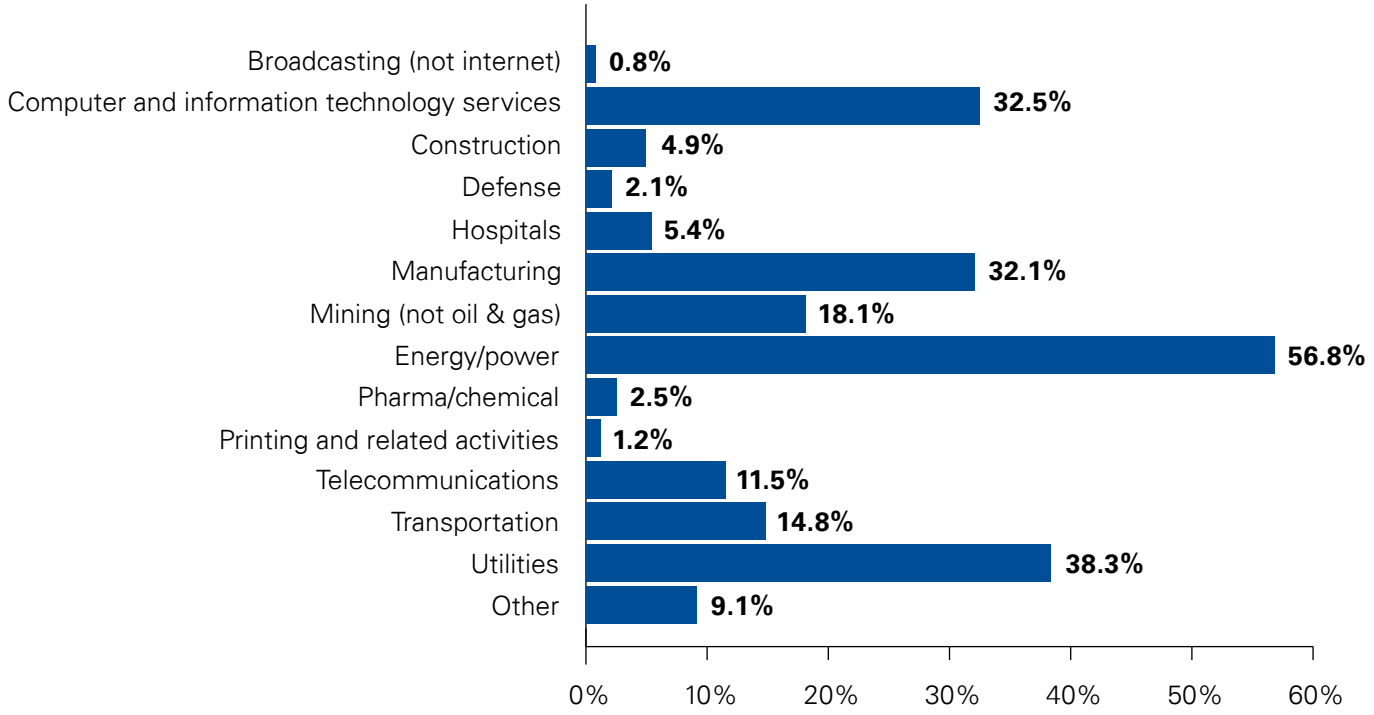


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Industry representation

Note that the sum of industry representation is much greater than 100 percent. This is to a degree because some organizations have physical operations in multiple industries. Most of this effect though, is because many respondents are consultants and serving multiple end user enterprises in multiple industries.

Industries represented

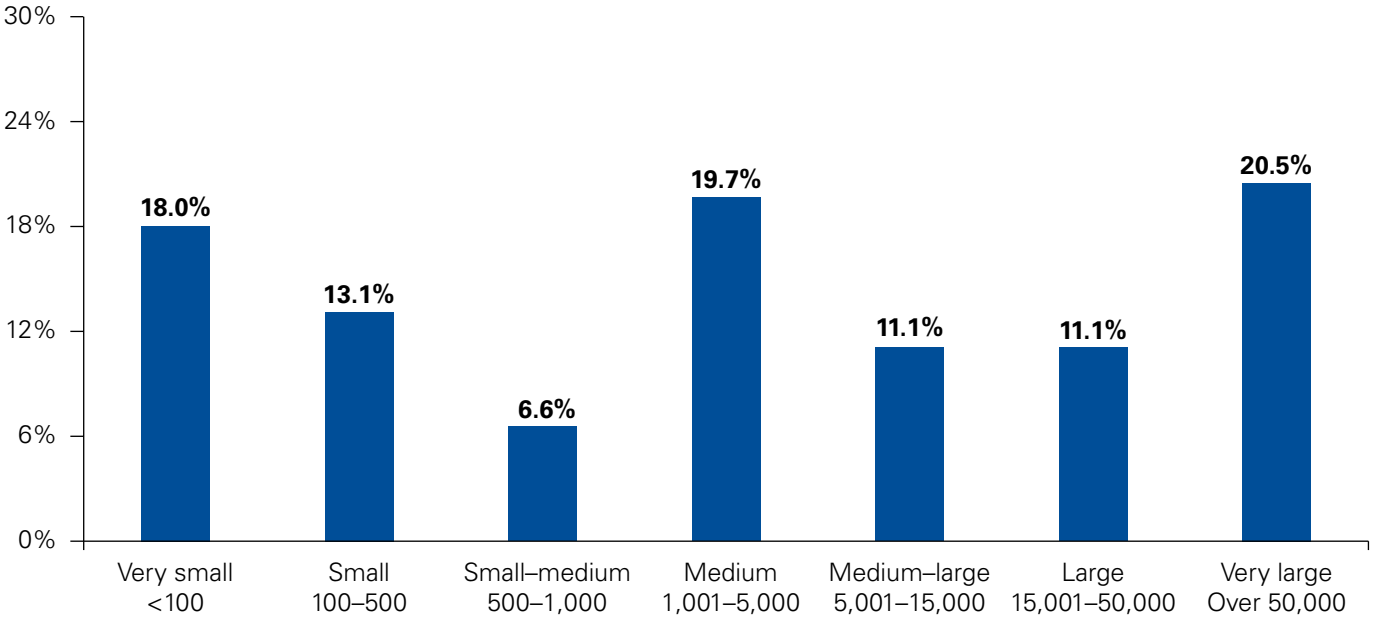


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Organization workforce size

Participants came from organizations of all sizes, reinforcing the awareness that industrial control systems appear in the full range of companies, from smallest to largest.

Organization workforce

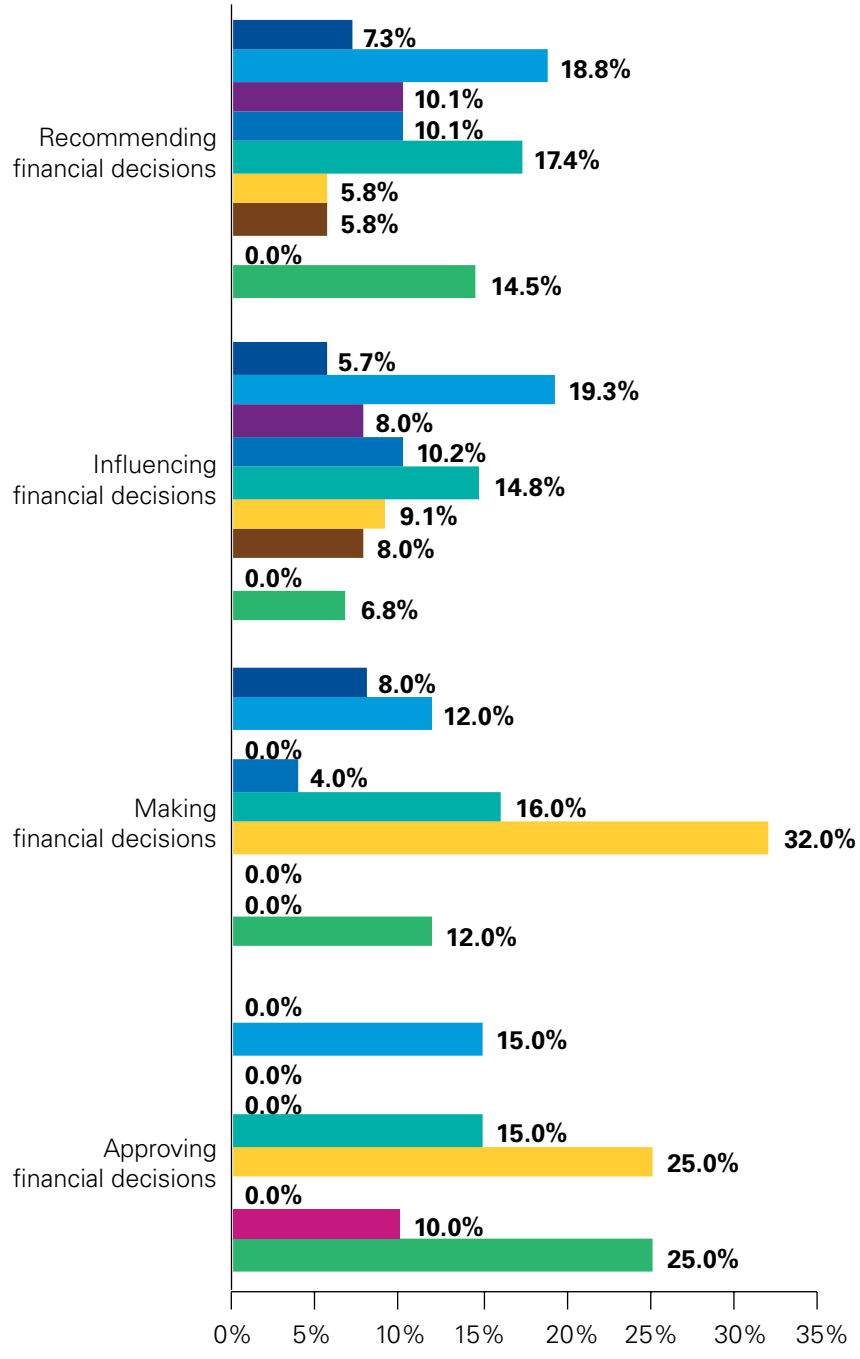


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Respondent decision making role

With over 80 percent of our respondents having some role in OT security expenditure decision making, we decided to take a deeper look into which positions in their organizations were most influential. As the table below shows, Security Directors far and away lead this process, with 32 percent of SDs making financial decisions and matching CISOs at 25 percent approving the OT security expenditures.

Decision role by title

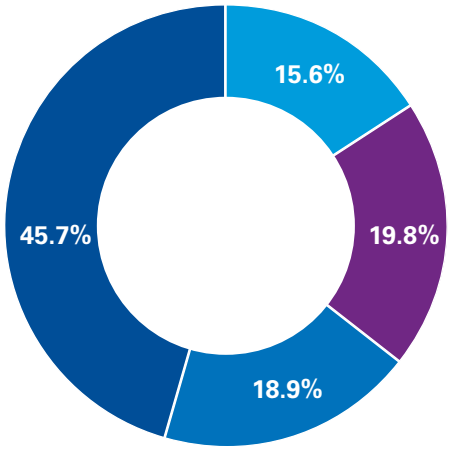


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Respondent organizational level

We were fortunate to have statistically useful numbers of participants at all levels of organizations, giving us not only good data on those directly involved with the implementation and impacts of CS Cyber Security work (46 percent in Operations) but an even larger pool of management and leadership respondents.

Respondents by organization level



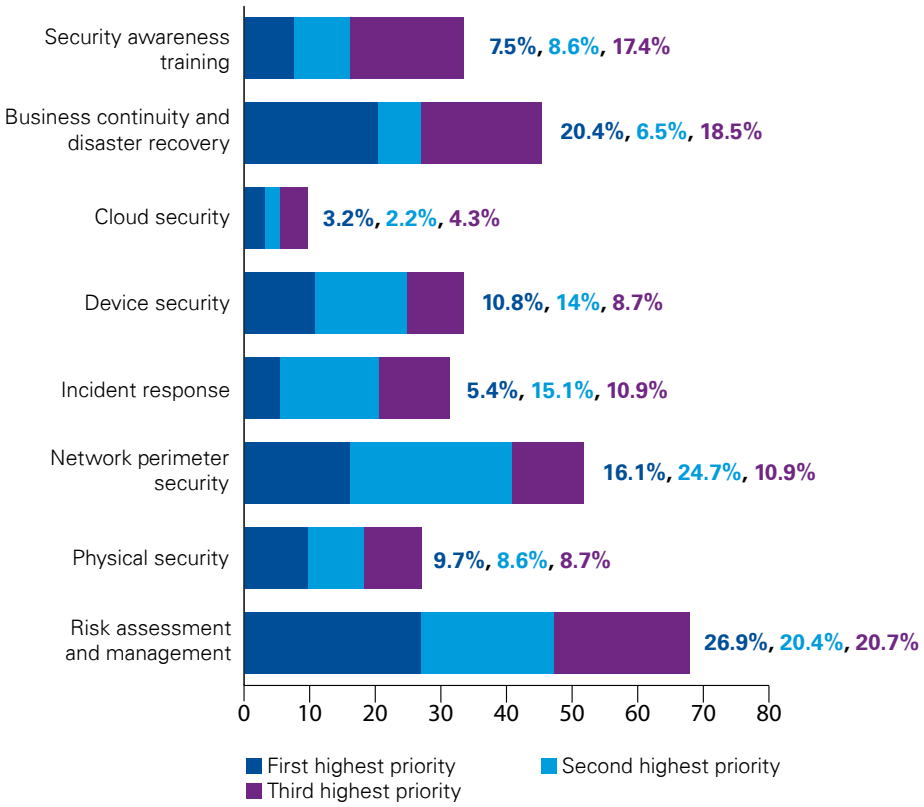
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS cyber security prioritization

Security prioritization responses suggested that many organizations continue to struggle for greater understanding of the actual risks to and from their OT systems, with *Risk Assessment and Management* chosen most often as the highest priority and (by nearly 20 points) the overall top choice.

It is noteworthy that, despite increasing use of cloud services by OT systems, few respondents at any organizational level indicated this area as a top three security priority (see table below for prioritization by executive participants). This bears further investigation to determine whether this response pattern is due to insufficient awareness of CS/OT-cloud connectivity, assumptions that cloud services are highly secure and have no potential as a Control Systems attack vector, or terminology – terms like "predictive maintenance" and "vendor monitoring and diagnostics" have been used by many industries for a long time. Modern usage identifies most such offerings as cloud services, since connections from many sites are funneled into one Internet-resident site. This is a topic under discussion for future research.

Top three CS security priorities (All respondents)



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

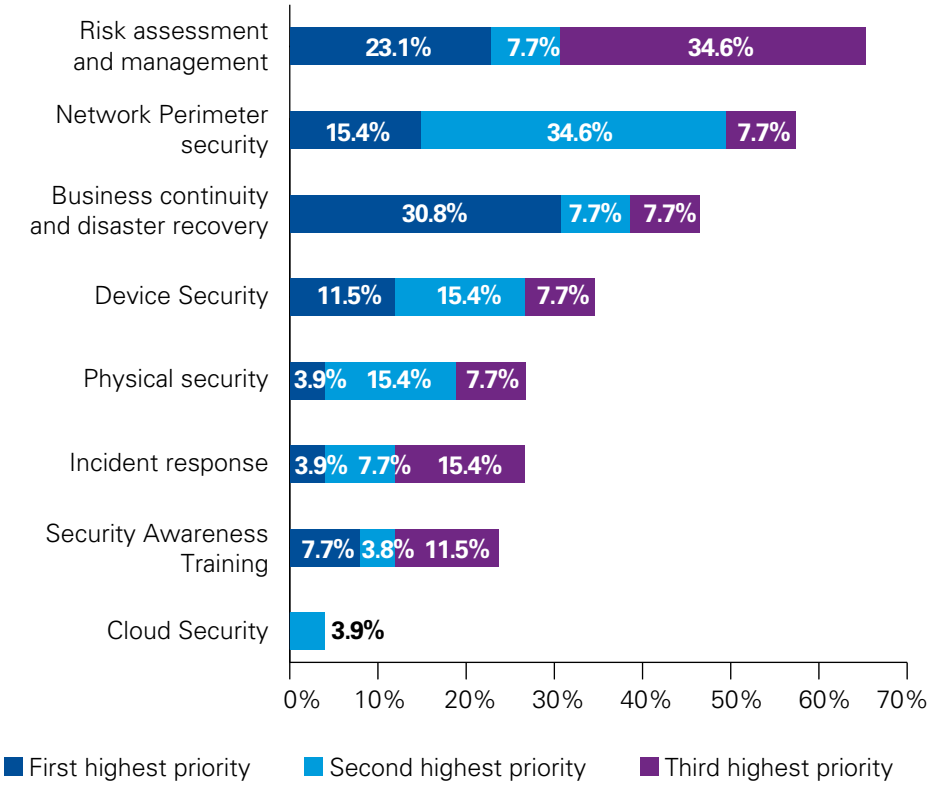
Zero trust

Zero Trust moves the network security focus from the perimeter to defending individual or small groups of resources. No trust is implicitly granted based on physical or network location. Access to digital assets is granted and only for validated business requirements, only with proper authentication (user and device), using role-based access controls and granting least privilege.

Looking exclusively at our executive-level responders, we see that beyond their primary focus on risk they are significantly more concerned with *Network Perimeter Security* than the overall pool, with 35 percent rating it as second highest priority versus 25 percent of all respondents.

There was general agreement between the groups that the top three CS security priorities were Risk *Assessment and Management, Network Perimeter Security* and *Business Continuity/Disaster Recovery*, but views diverged beyond that point, with *Security Awareness Training* a lower priority among executives and *Device Security and Incident Response* greater ones.

Top three CS security priorities (Executive respondents)



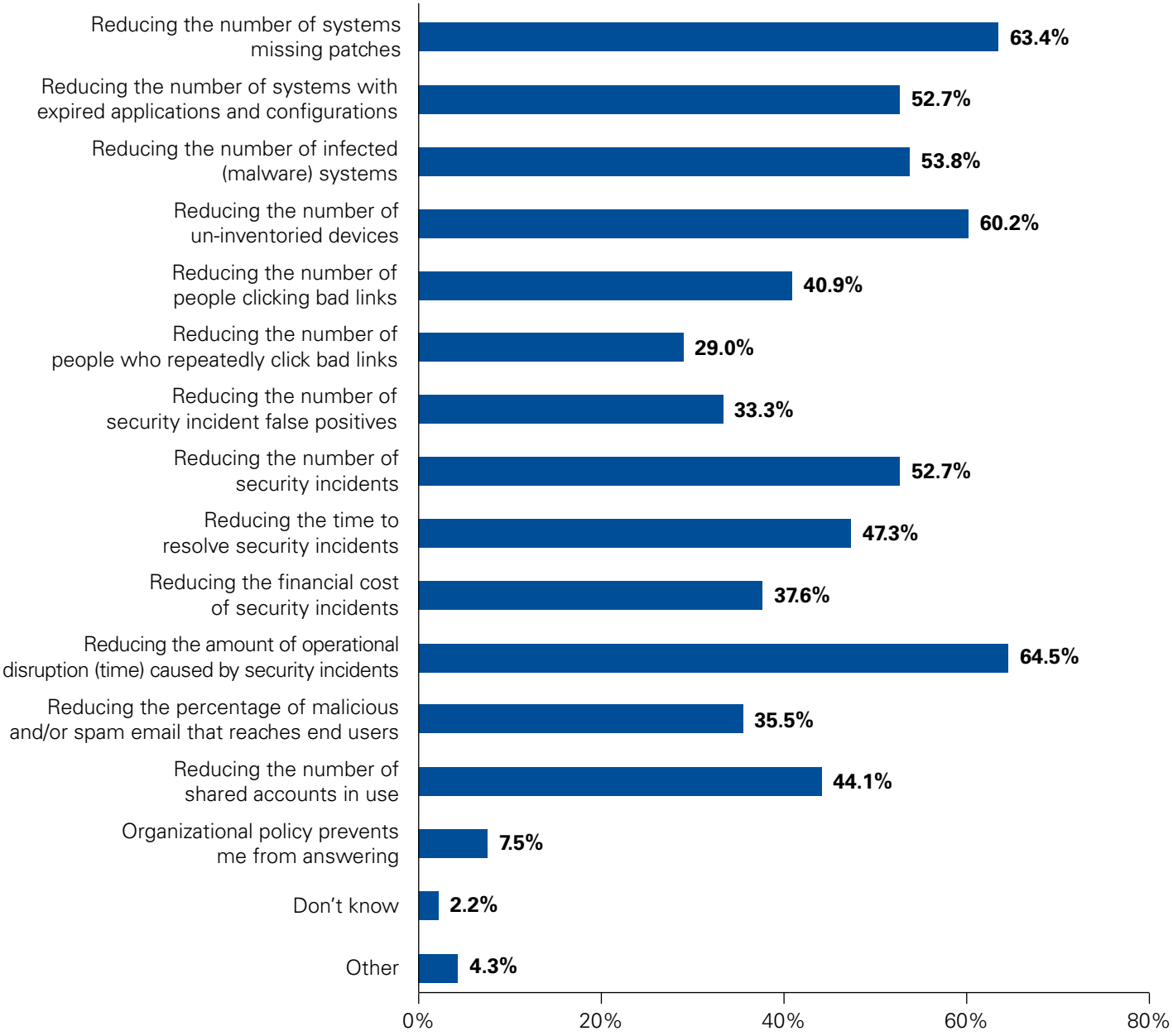
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Zero trust

The high prioritization of Network Perimeter Security highlight participants' awareness for the need to better segment OT networks. CS and SCADA systems have traditionally been implemented as large, flat networks with weak, often easily penetrable perimeters. Inside, attackers can freely pivot to access any assets/systems they wish. Zero Trust coupled with other standards-based approaches (e.g. ISA 62443 Zones and Conduits) can greatly improve these organizations' OT protection. NIST has recently published draft SP 800-207 to educate security teams on this approach and its merits.

Del Rodillas, Dir. CS/OT Industries Marketing, Palo Alto Networks

CS security KPIs



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

There were few surprises in participants' answers regarding their security KPIs. That *Reducing Operational Disruptions* was selected more often than any other metric is interesting, however, possibly signaling that disruptions stemming from or related to a cyber security incidents have become frequent enough to appear on a lot of peoples' radar, despite the continued rarity of such events being reported.[6]

The authors observed some differences between the key performance indicators chosen by respondents of different industries. Specifically, those in Transportation or Energy placed importance on their CS security programs reducing the number of systems missing patches, while those in Telecommunications indicated a greater concern with reducing the financial costs of those security incidents which do occur.

Reducing Operational Disruptions is the most commonly chosen KPI, so it follows that responding organizations would carefully assess the risks of introducing new

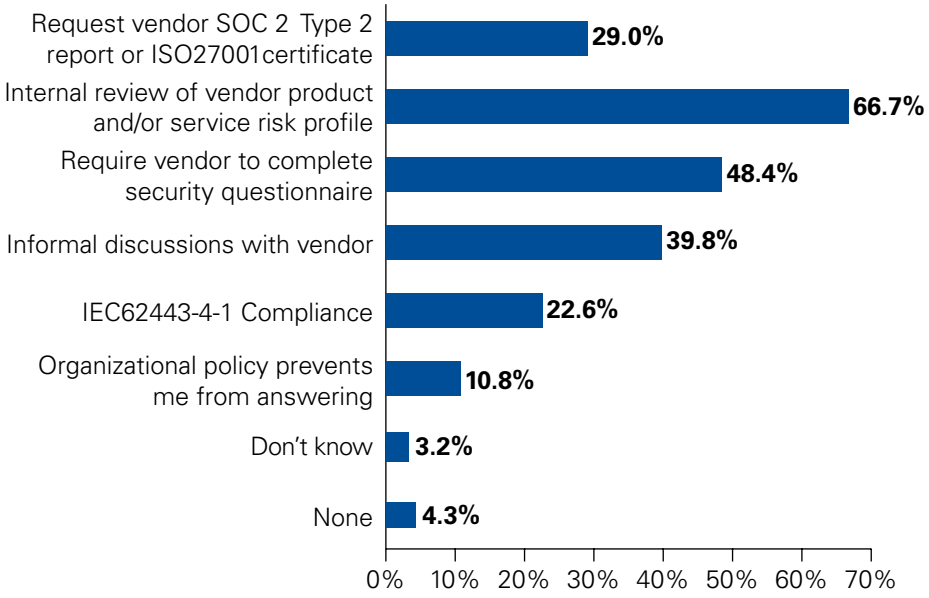
[6] https://ics.kaspersky.com/media/2018-Kaspersky-CS-Whitepaper.pdf, Pg 17

equipment, services or workers into their OT environments. The authors are glad to see that at least two-thirds (67 percent) do carry out reviews of the product/service profile, although this optimally would be done by every organization. More concerning is that less than one third request either ISO certificates (29 percent) or IEC62443-4-1[7] (23 percent), and we recommend that OT-dependent organizations consider adding these steps to improve their pre-acquisition risk assessments.

A perennial topic of debate, the collection of hurdles to resolving cyber security vulnerabilities in our OT environments remains broad and challenging. Many discussions center around the key issue of operational uptime requirements, and almost half (44 percent) of our participants stated that this is one of their greatest obstacles. That issues of insufficient personnel and CS security expertise (problems already widely reported in cyber security publications for some years) were even more frequently selected suggests that those two obstacles are preventing remediation/mitigation even beyond uptime constraints.

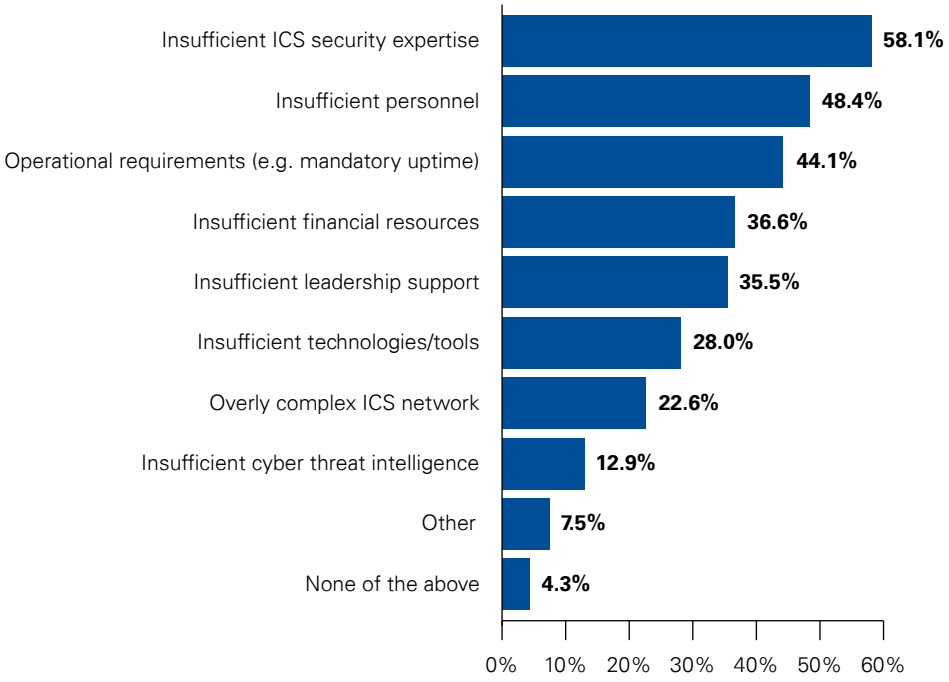
A relationship was found between *Greatest Obstacles* and the *Maturity Level of CS Cyber Security Programs.* More than half (53 percent) of respondents rating their organizations at higher levels (4 or 5 on a 5 point scale — See CS Cyber Security Program Maturity Level, below) listed *Operational Requirements* as the greatest problem, and nearly half (47 percent) of that group cited *Insufficient Financial Resources,* diverging significantly from organizations at lower Maturity Levels. Of those stating their CS Cyber Security Programs were at Level 1 or 2, the top obstacles identified were *Insufficient CS Security Expertise* (68 percent) and *Insufficient Personnel* (63 percent). All respondents agreed that *Insufficient Cyber Threat Intelligence*[8] and the *Complexity of their CS Networks* were their lowest concerns.

Pre-CS acquisition risk assessments



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Greatest obstacles to resolving CS security vulnerabilities (All respondents)

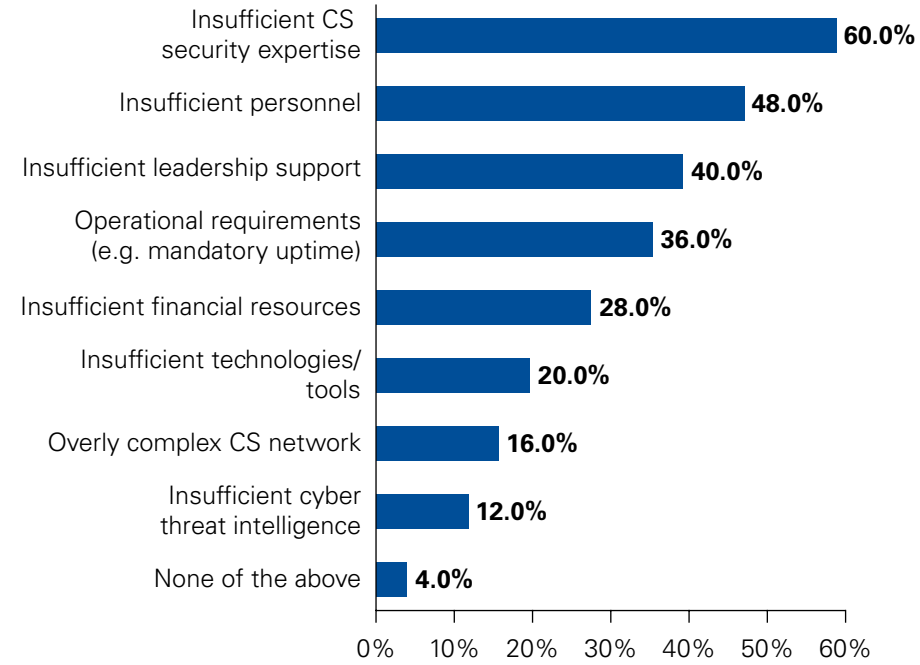


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

[7] Not all types of equipment or software systems can be IEC62443-4-1certified.

[8] Threat Intelligence: evidence-based, actionable knowledge regarding existing and potential hazards. It is the product of data collection, evaluation and analysis, and includes guidance on protecting against threats.

Greatest obstacles to resolving vulnerabilities (Executive respondents)



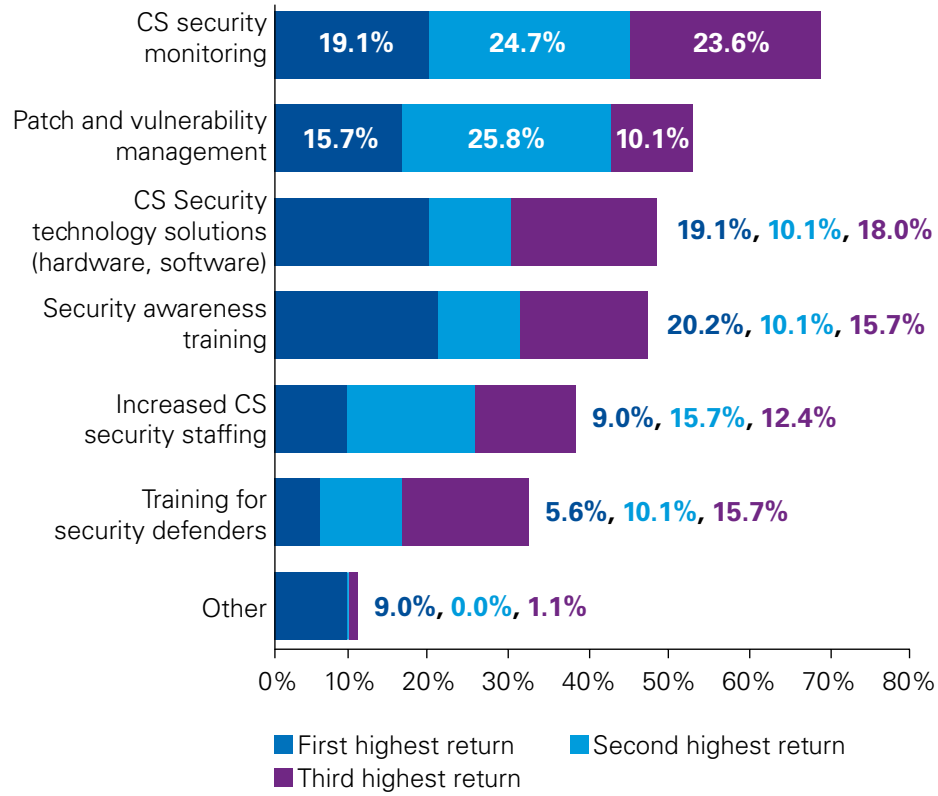
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

The authors noted that, while broadly similar, respondents at the Executive level of organizations consider *Insufficient Leadership Support* a greater obstacle than the overall pool (40 percent vs 36 percent) and *Operational Requirements* a lesser one (36 percent vs 44 percent).

CS security budgets

The topic of Return on Investment (ROI), much like prioritization, is one on which views often differ depending on a respondent's levels of an organization. With this in mind the authors searched for correlations between top ROI selection, job roles and titles but found no significant relationships.

Top CS security ROI

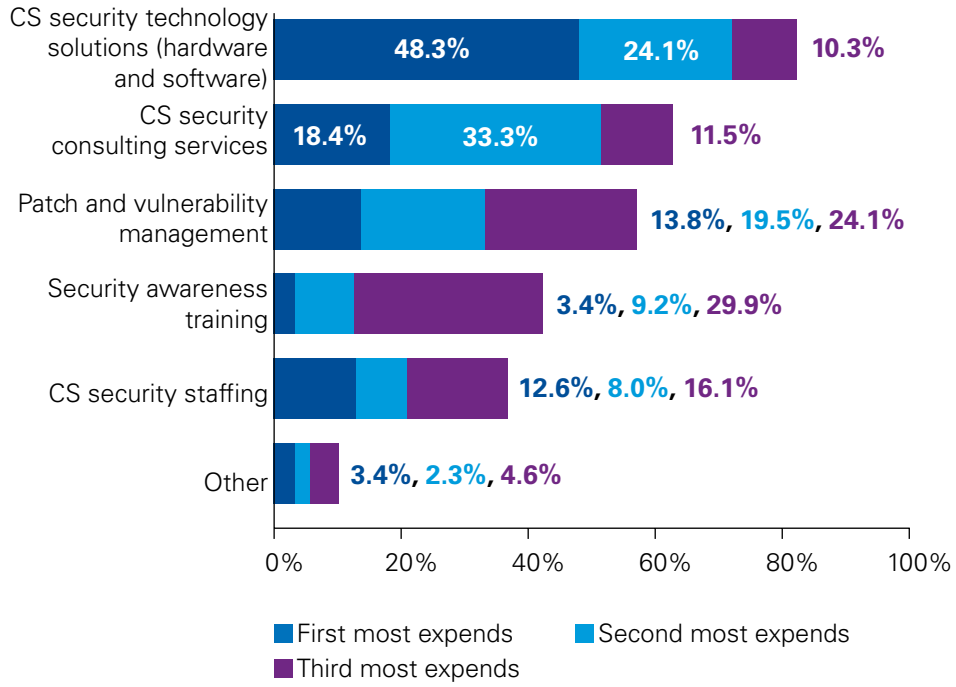


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

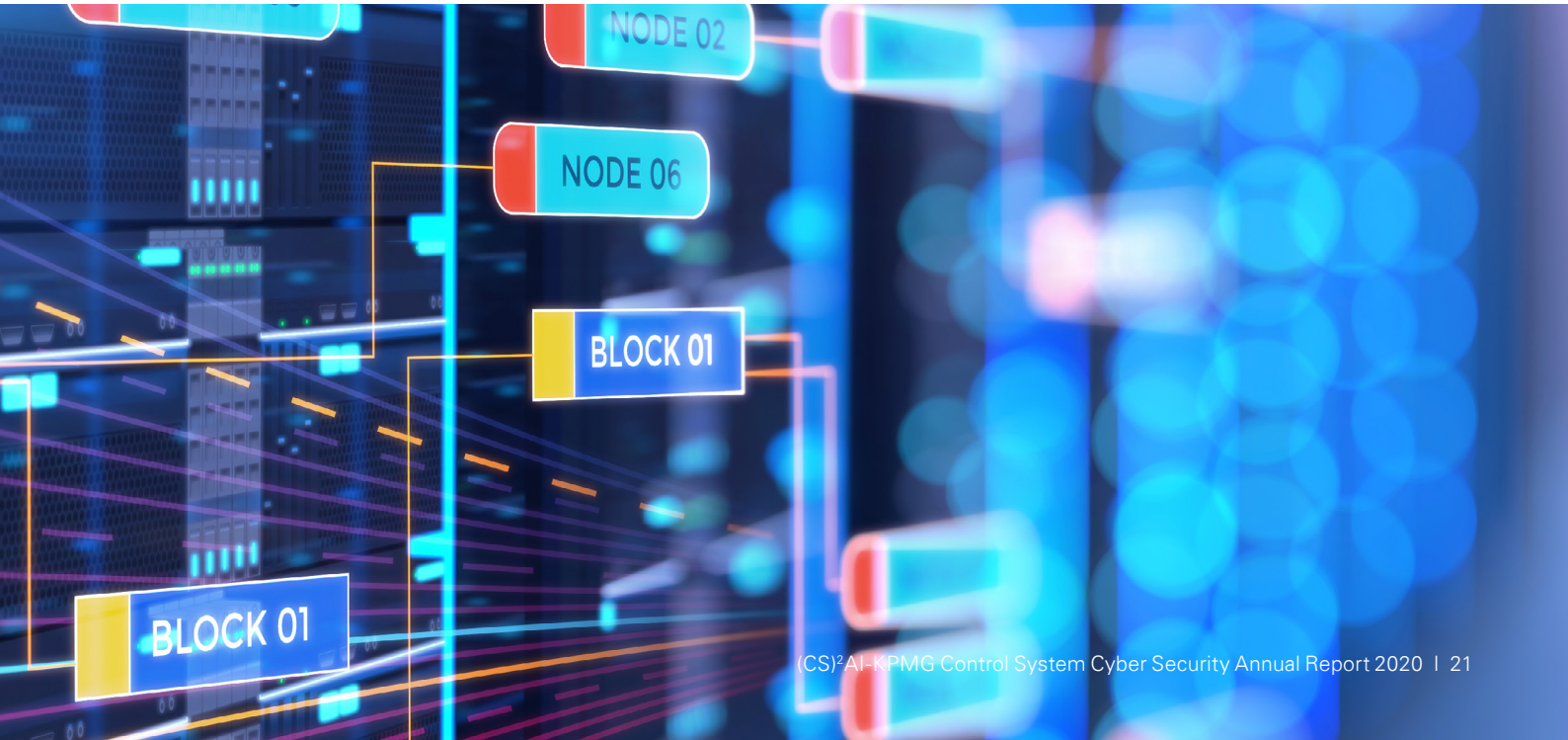
Training for security defenders is ranked the least worthwhile investment (31.5 percent), with *Increased CS Security Staffing* only slightly higher (37 percent). At the same time, *Insufficient CS Security Expertise* and *Insufficient Personnel* are cited as the greatest obstacles to resolving CS vulnerabilities (Greatest Obstacles to resolving CS security vulnerabilities, page 17). It is not clear at this time what methods of addressing these vulnerabilities remain other than increasing CS Security Consulting Services.

We found a significant correlation between rising CS Security budgets and where those funds are allocated. The organizations who increased budgets the most (increases of 30 percent or more, 50 percent or more) spent the most on *CS Security Technology Solutions*, while those with budget increases of less than 30 percent focused more on *Patch and Vulnerability Management*.

Top 3 CS security expenditures



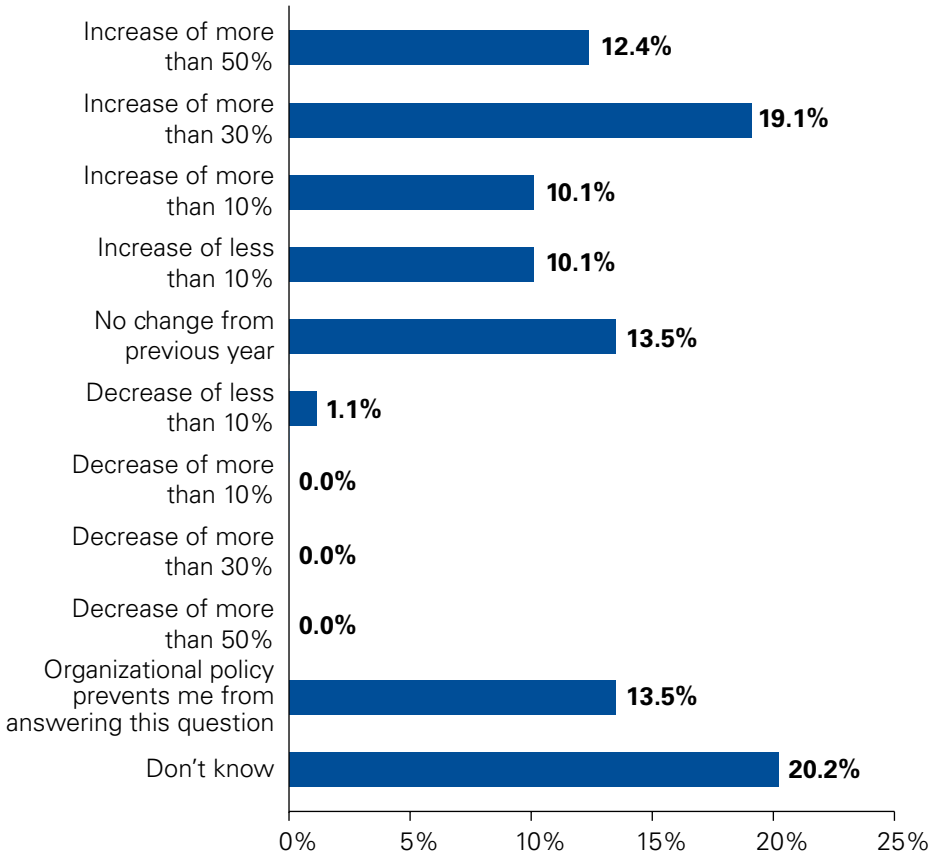
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.



Overall, Control System security budgets are stable or rising, with 51 percent indicating an increase, only 1 percent stating any reduction at all, and the largest group of respondents (19 percent) showing funding growing by more than 30 percent from the previous year.

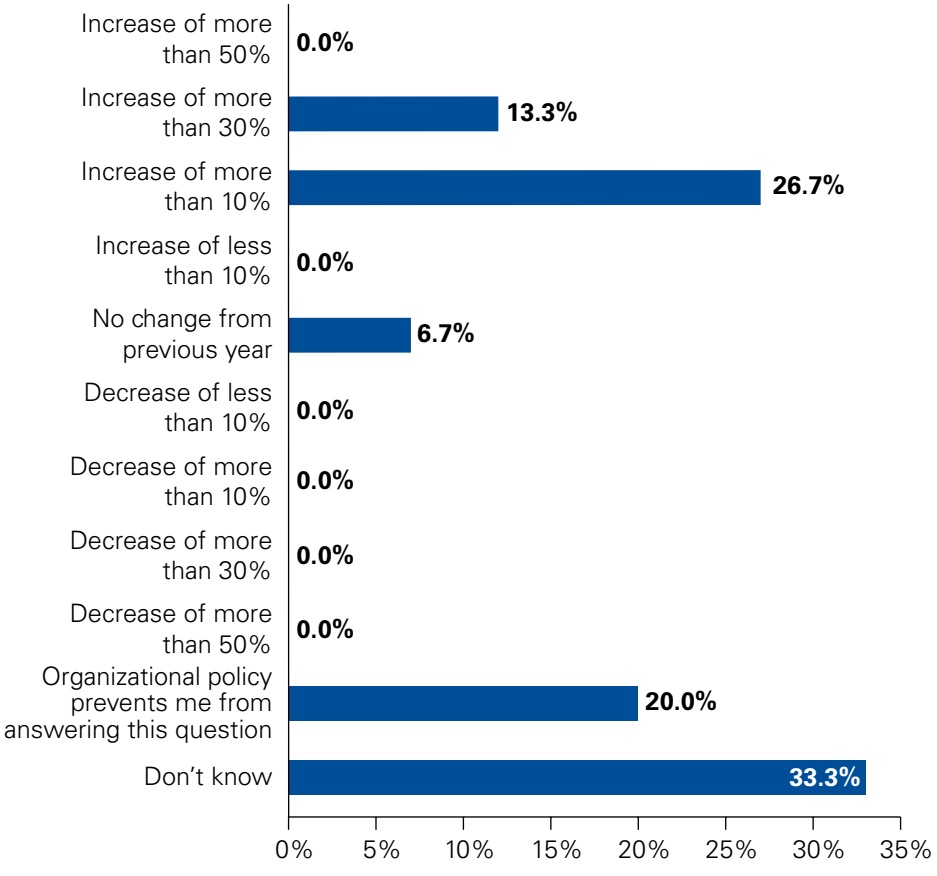
Two industries stood out because of how little they increased CS security budgets, Mining and Utilities. Setting aside the unusually high percentage of Mining respondents who lacked information to answer (33 percent), both industries diverged from the overall group, with increased budgets falling primarily in the 10 percent or greater/30 percent or greater increase categories and few (Utilities 3 percent) or none (Mining 0 percent) in the 50 percent or greater increase category.

CS security annual budget change (all industries)



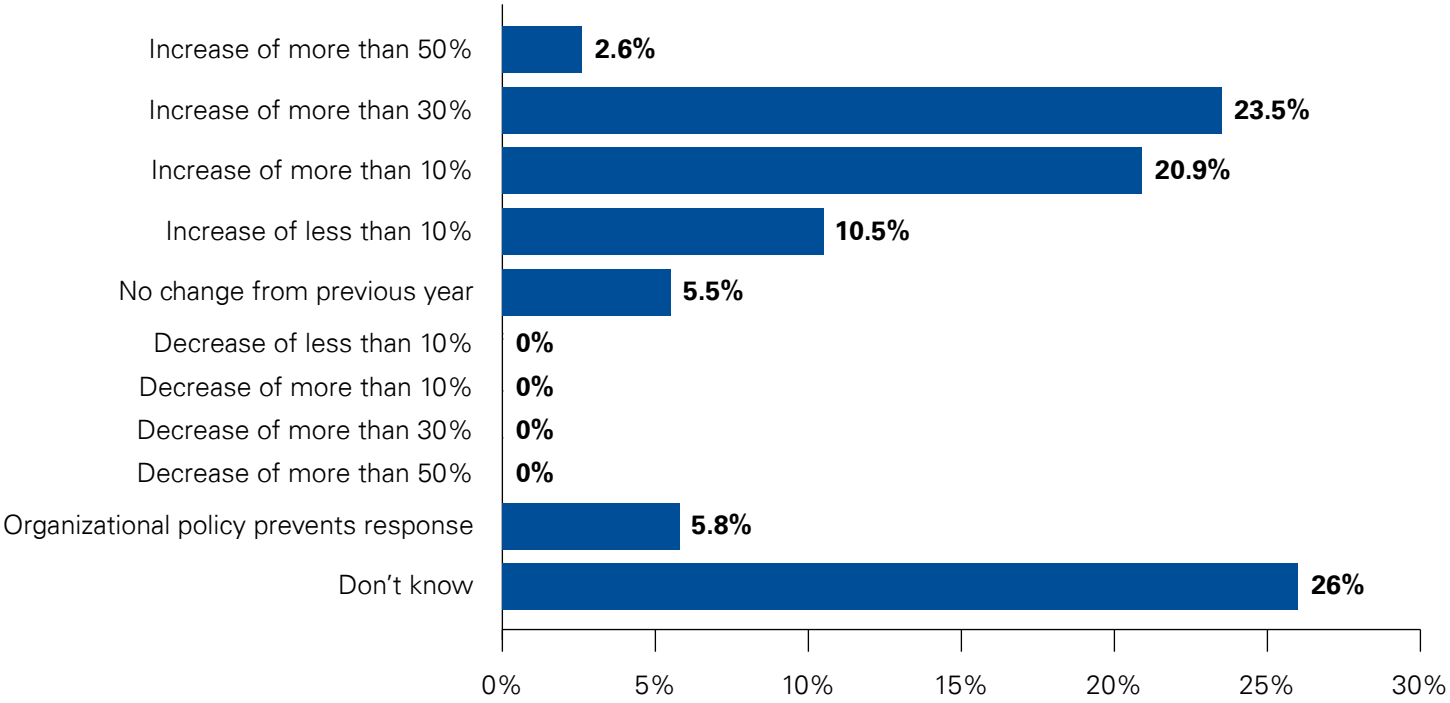
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS security annual budget change (Mining only)

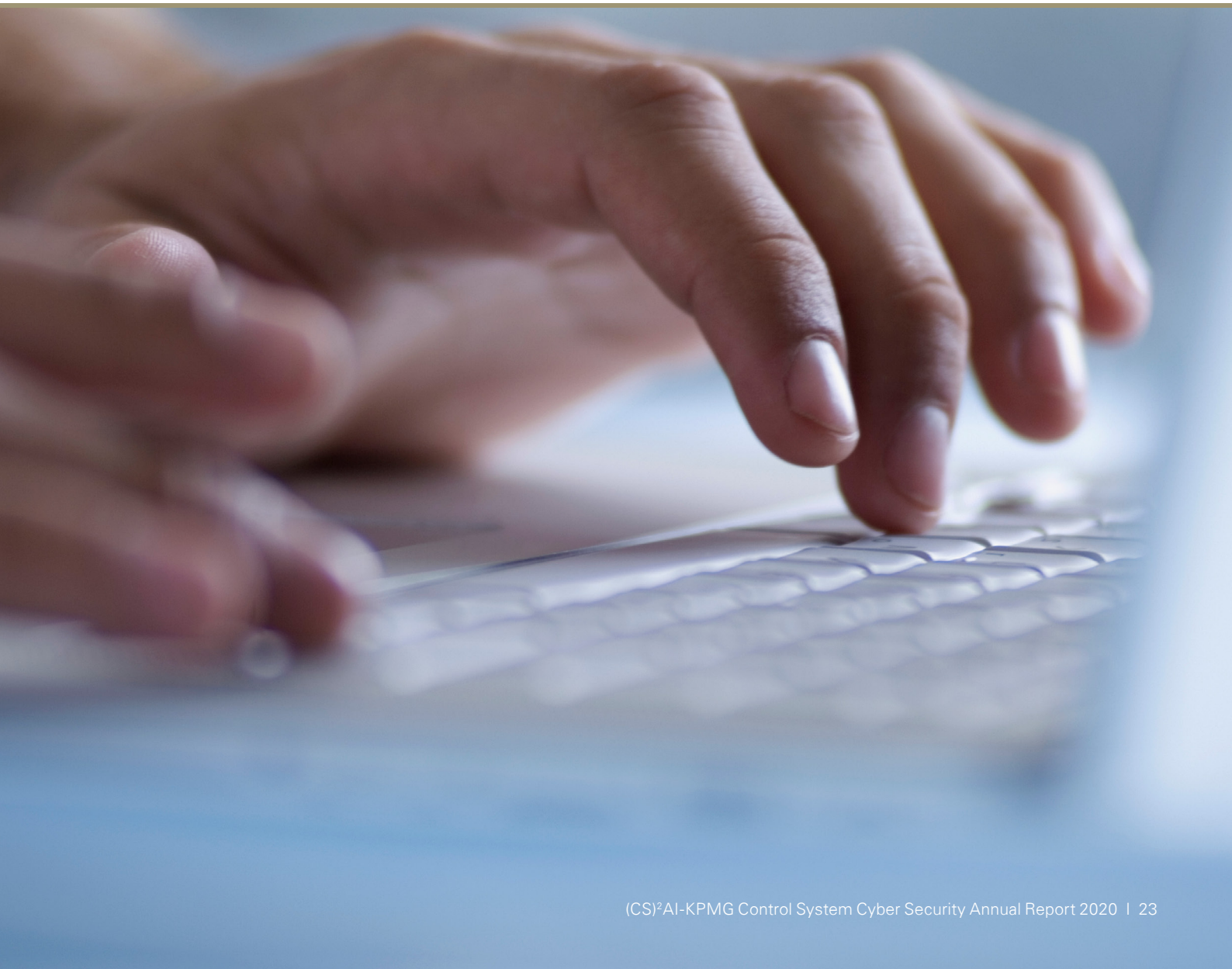


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS security annual budget change (Utilities only)



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.



CS cyber security staffing

Although staffing was low on the list of CS Security spending for most respondents, it is often one of the most closely examined budget areas, and the need for skilled personnel can vary significantly over time as cyber security projects ramp up, complete and roll over to operations. How are organizations to balance resource demands for both temporary CS security *projects* and ongoing CS *security programs?*

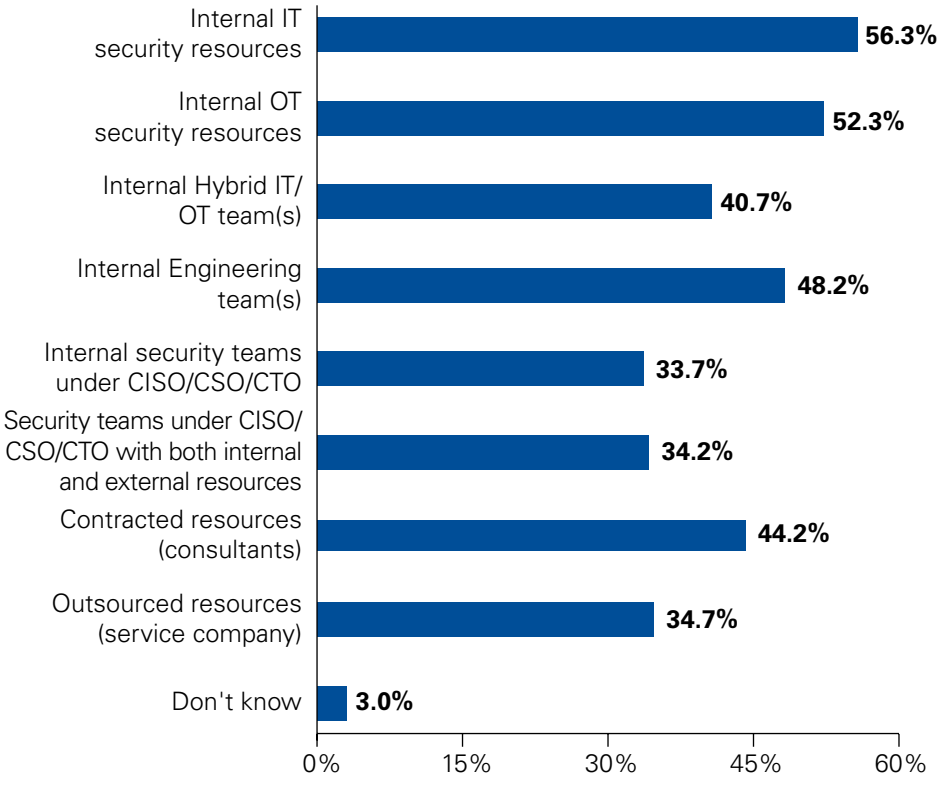
Participants' answers to these questions indicate that the majority use internal resources primarily, with a fairly even split between IT security, OT security and engineering personnel. That Internal OT Security specialists appear so frequently in survey responses is positive, as resources in this category are scarce and generally have the best combination of skills, expertise and business process comprehension for these environments. Even in organizations with Internal Hybrid IT/ OT teams, these are most often made up of specialists in one or the other area of technology, and best practices calls for the presence of cross-trained individuals to reduce introducing incompatibilities in security projects.

Addressing cyber security expertise shortages

Automation. Process automation can leverage technology to take on some of the work and offload overburdened OT security teams. The labor-saving benefits from a security fabric with integrated and automated solutions is a compelling alternative to point solutions that require cyber security staff to manually correlate detection, identification, protection, and response. Specifically, in a security fabric all aspects of security can be combined for a centralized and transparent view. This helps enterprises scale in their support of an ever-growing and evolving security landscape.

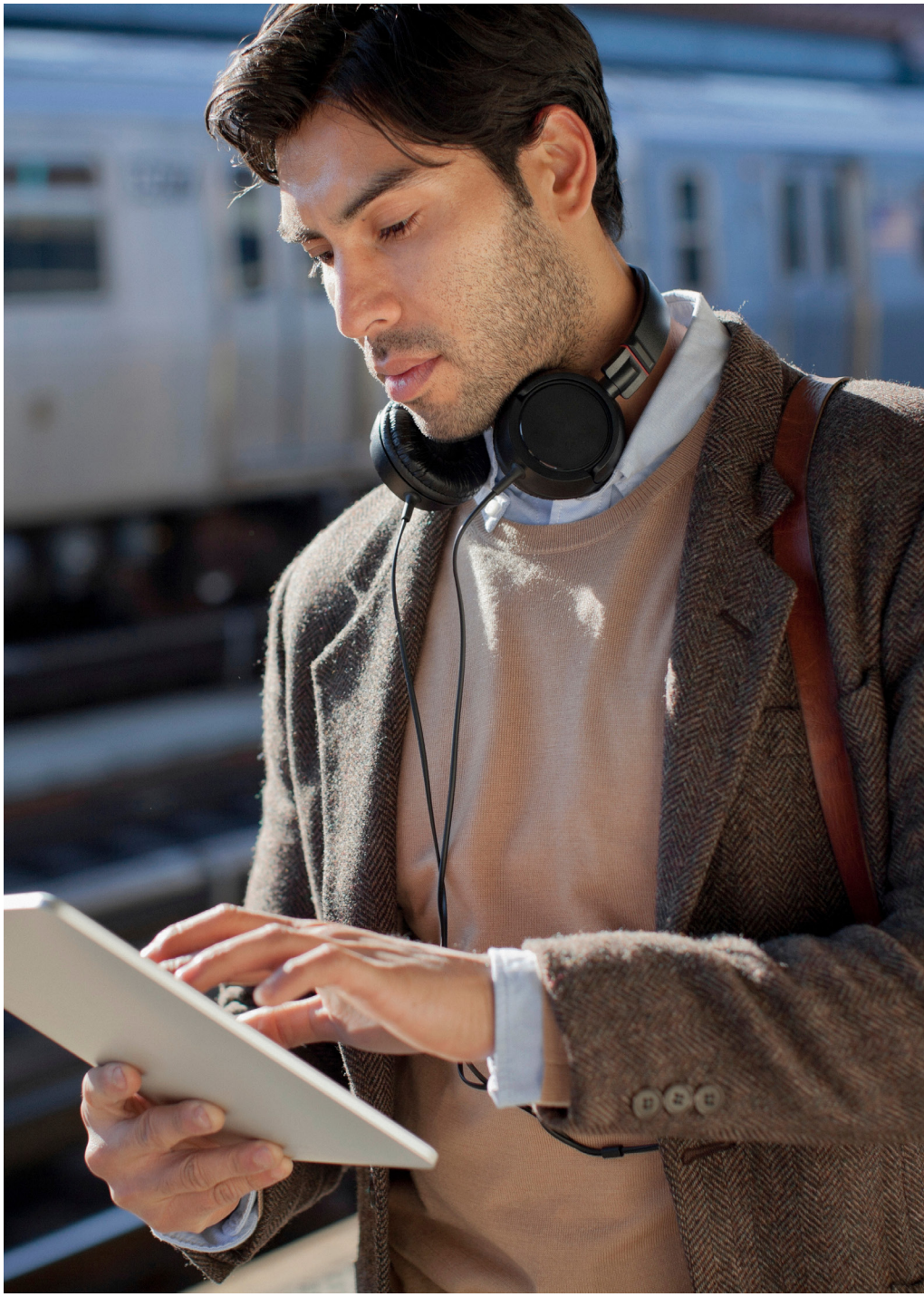
Peter Newton, Sr. Dir IoT Security Product Marketing, Fortinet

CS security services in use



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Many different approaches to staffing OT cyber security work exist, with proponents and arguments for (and against) each. Our respondents showed that, on the question of who is actually carrying out the work of securing and defending OT assets, every possible model is in use, from fully outsourced to fully internal and from wholly OT-led to wholly IT. The authors are encouraged to see the strong numbers indicating the use of internal resources. While there will likely always be an important supplemental role for external resources, the long-term gains deriving from developing internal personnel, who are already the most familiar with business processes and constraints, are substantial and clear when compared with offloading such important responsibilities to resources who take their knowledge and experience with them when projects end.



CS security awareness training

Training on security generally falls into one of two categories, Security Training and Security Awareness Training. The former intends to enhance the capabilities of actual security practitioners, those in charge of protecting an organization's assets. The latter aims to raise the awareness or knowledge of all personnel, in order to reduce security breaches resulting from accidental or unaware actions. IT security being a relatively mature field, there are many quality sources and providers of both types of training.

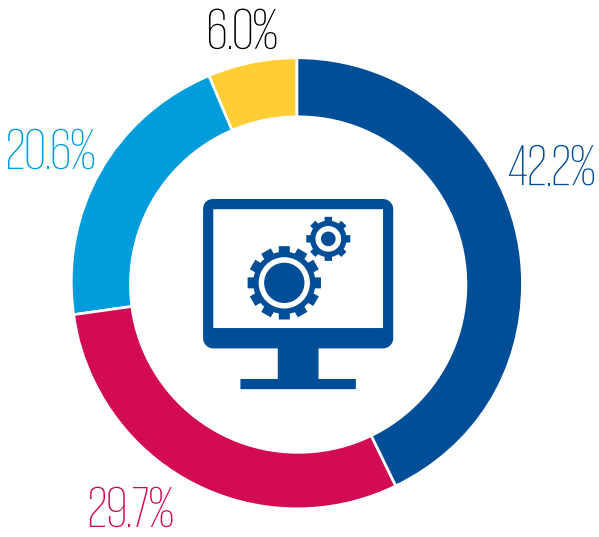
OT security is newer and very much still developing. In addition, those working in Control Systems were historically able to rely on the isolation of their equipment and networks from the internet, business networks, and common protocols (such as the otherwise ubiquitous TCP/IP). This isolation has been disappearing at an ever increasing rate for the past two decades (or more, in some instances) as a result of the ongoing introduction of IT technologies into OT environments, frequently termed IT/OT Convergence[9]. The resulting exposure of Control Systems to network-based threats obviously demands training specific to these environments, both to increase the knowledge of threats among all individuals with access (CS Security Awareness Training) and the capabilities of those charged with protecting them from cyber threats (CS Security Training).

Addressing cyber security expertise shortages

Online and external course offerings Universities globally recognize the opportunity to develop the next-generation workforce skilled in CS cyber security capabilities. There are more than 80 universities around the world offering network security programs to provide certification curricula preparing students for a careers in cyber security. In addition, there are online offerings through various resources designed for professionals who are interested in independent validation of their security skills and experience. Most offer a wide range of self-paced and instructor-led courses with certification testing to demonstrate mastery of network security concepts

Peter Newton, Sr. Dir IoT Security Product Marketing, Fortinet

CS security awareness training program



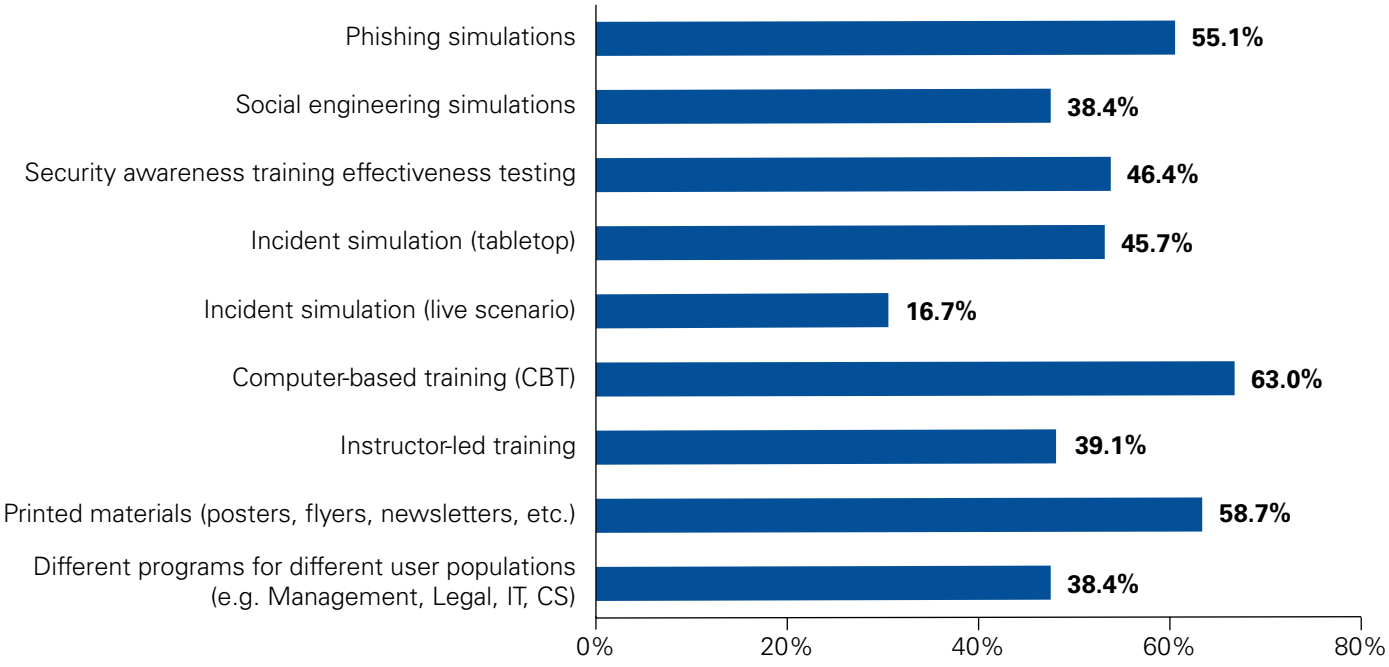
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

[9] See also: Digital Transformation, Industrial Internet of Things (IIoT), Industry 4.0, Smart Grids/Cities/Factories, etc.

CS Security Awareness Training is required for a larger group within an organization and generally less mature than practitioner training. It is also more targeted than that for IT, and we were glad to see that nearly one third (30 percent, *Separate from the IT security Awareness Training)* have developed training specific for this audience. That more than one out of five (21 percent, *Nonexistent)* have no CS Security Awareness Training, on the other hand, is quite concerning. We strongly recommend those organizations address this shortcoming with all possible speed.

Among those respondents from organizations which do have CS-specific Security Awareness Training, a broad range of teaching components are in use. We see some correlation between component cost and frequency of its use, with *Computer-Based Training* (63 percent), *Printed Materials* (59 percent), and *Phishing Simulations* (55 percent) the most common, and live Incident Simulation (17 percent) the least. The authors were encouraged to see that nearly half (46 percent) do test the effectiveness of their training; this is key to the ongoing improvement of programs as well as to identifying personnel requiring additional support.

CS security awareness training inclusions



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS component vulnerability

Too many respondents (10-20 percent) indicated that they did not know whether any given component was remotely accessible. Experience and best practices suggest it best to assume remote accessibility exists until confirmed otherwise. With two decades of ongoing IT/OT convergence connecting Control System assets to all categories of external networks, it has become expected among CS security practitioners that investigations will routinely discover external connections unknown to organizations. SMEs strongly recommend segmentation both of and within Control System networks to reduce the risks of undesired and unintended connectivity.

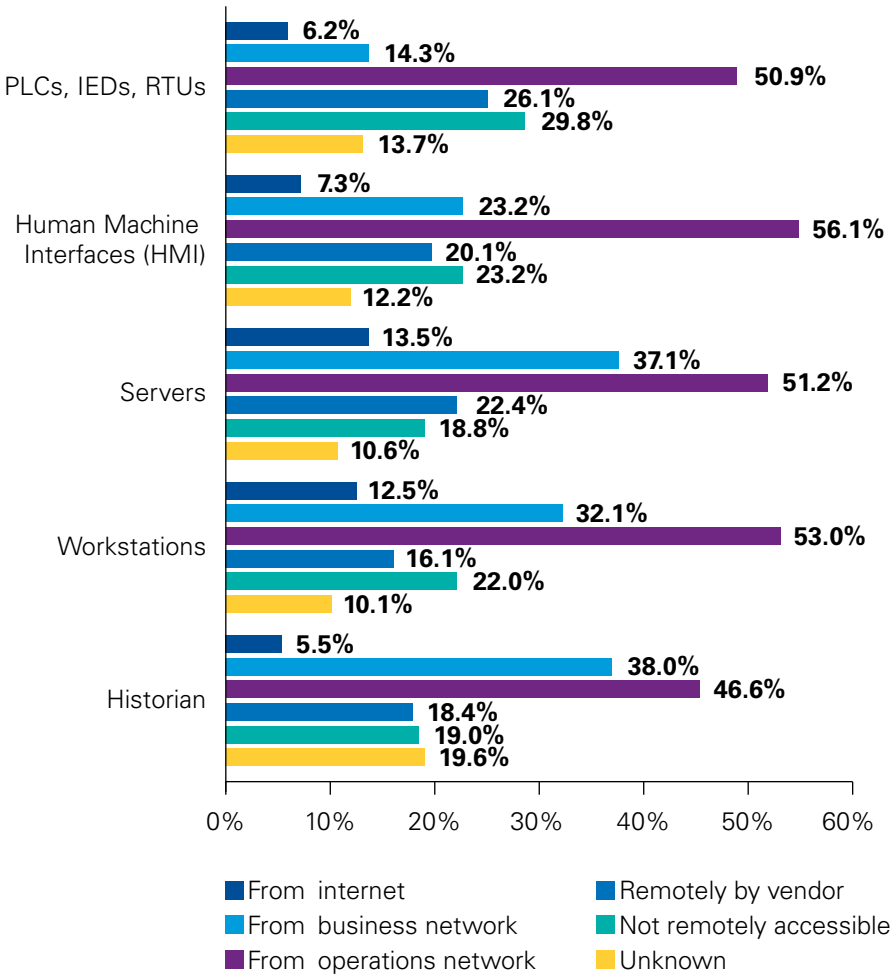
IT/OT Convergence trends have made it increasingly likely that most OT components can be accessed from business networks unless significant segmentation both between and within networks has been carried out. Connections between business systems and Operational networks are routinely identified as a common vector for attacks into those Operational networks.[10] The authors strongly recommend all organizations dependent on the performance and reliability of their Control Systems environments enlist expertise in this field to architect and implement micro-segmentation solutions to protect their assets without negative impact to their businesses.

Zero trust

The accelerating pace of OT Digital Transformation ensures there will be valid reasons for remote access to OT assets by, for example, remote workers and 3rd party vendors. A Zero Trust approach with NGFWs technology could help to safely resolve these remote access requirements.

Del Rodillas, Dir. CS/OT Industries Marketing, Palo Alto Networks

Remotely accessible CS components



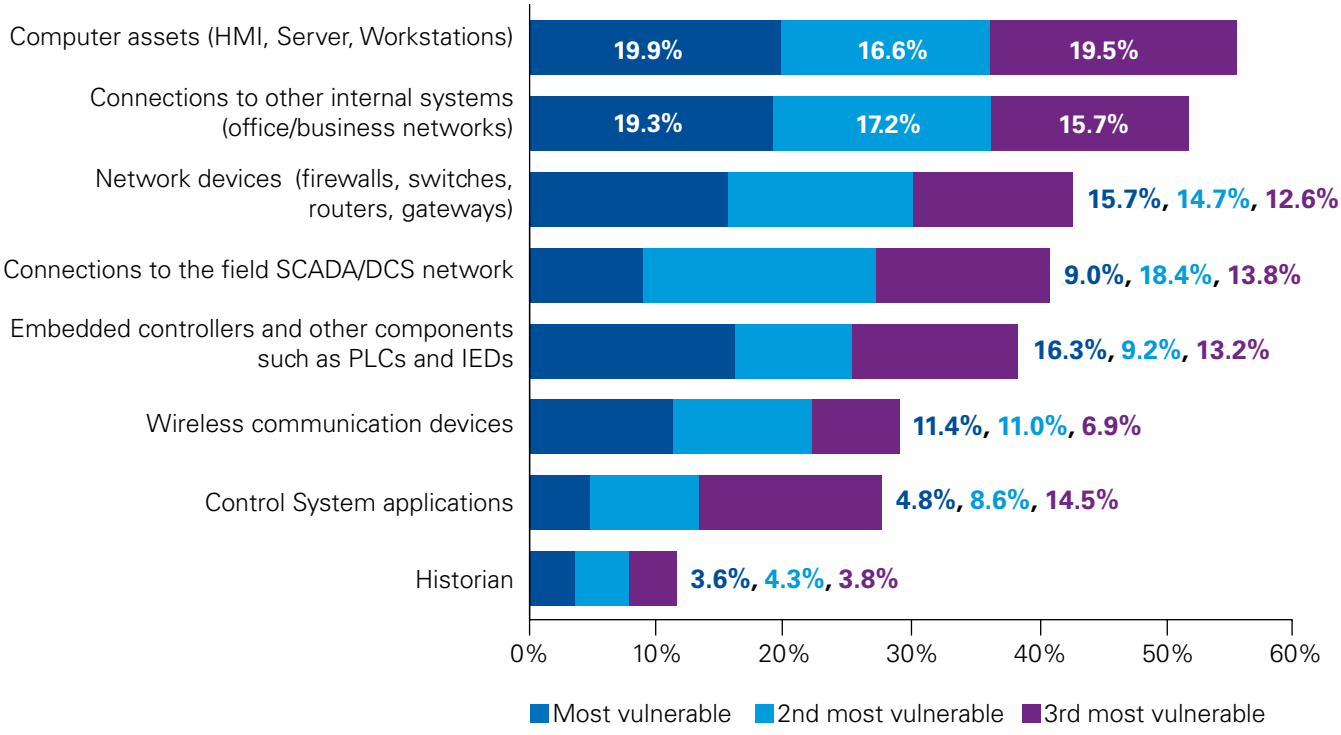
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

[10] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=3 Pg 2.

Remote Access

Given that targeted remote-control attacks routinely pivot from one compromised asset to another, the question is not whether individual assets are remotely accessible, but whether any asset on the network is remotely accessible.
(Lior Frenkel, Co-Founder & CEO, Waterfall Security Solutions)

Most vulnerable CS systems



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

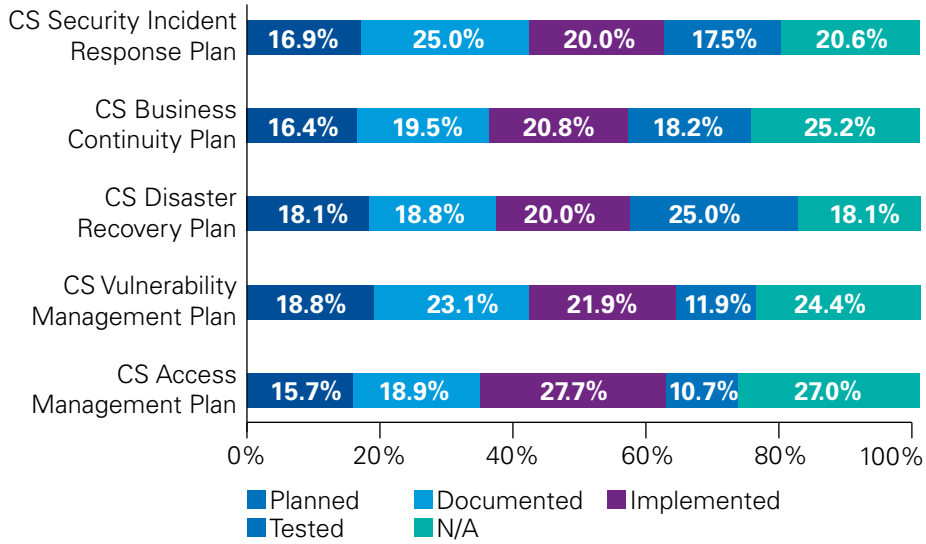
The authors consider it worth pointing out that *Connections to Other Internal Systems* was only slightly less frequently identified as the MOST vulnerable than *Computer Assets* (51 percent vs 55 percent) in light of the approximately half (47–51 percent) of respondents stating that all of their CS components are connected to those systems (previous chart). This emphasizes the high importance of greatly improving the security of those connections.

CS cyber security organizational plans (Including adjacent plans)

Organizational plans for Business Continuity and Disaster Recovery may not be, strictly considered, security plans in the same way that CS Access Management, CS Vulnerability and CS Incident plans are, but the potential always exists that the circumstances of a Control System cyber security incident may trigger the activation of one of these adjacent plans, hence they were included in our survey.

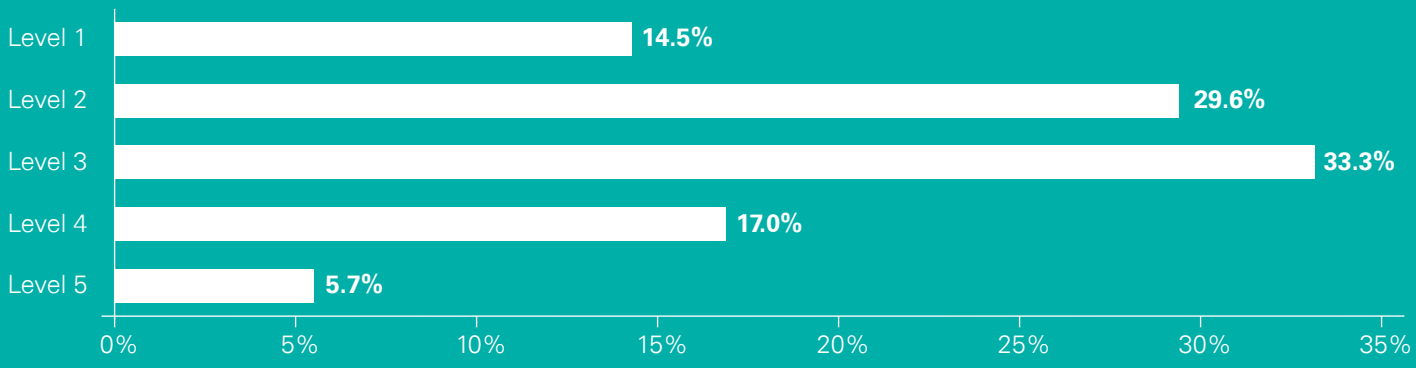
Optimally all Organizational Plans would have reached the fully mature state of not only being *Implemented* but actually *Tested* to evaluate their completeness and effectiveness. Our respondent pool drew from organizations at all stages of development. The authors did note that participants clustered in their answers to this question in correlation with their overall CS Security Program Maturity Level, with those in Levels 1 and 2 much more likely to have no plan (*N/A* response) or in *Planned* phase and those in Levels 4 and 5 leaning heavily towards plans being Implemented and/or Tested. As these two groups diverged from each other in multiple areas, several other correlations were identified and merited secondary analysis and charting, as will be seen on the next page.

Organizational plans



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS security program maturity level



Level 1 — Fire fighting. Cybersecurity processes are unorganized and undocumented, not organized in a "program." Success depends on individual efforts; 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 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 CS security duties have training and experience.
- Program is Managed, Proactive, tracks metrics, some automation.
- Active Defense, SIEM, Anomaly and Breach Detection.

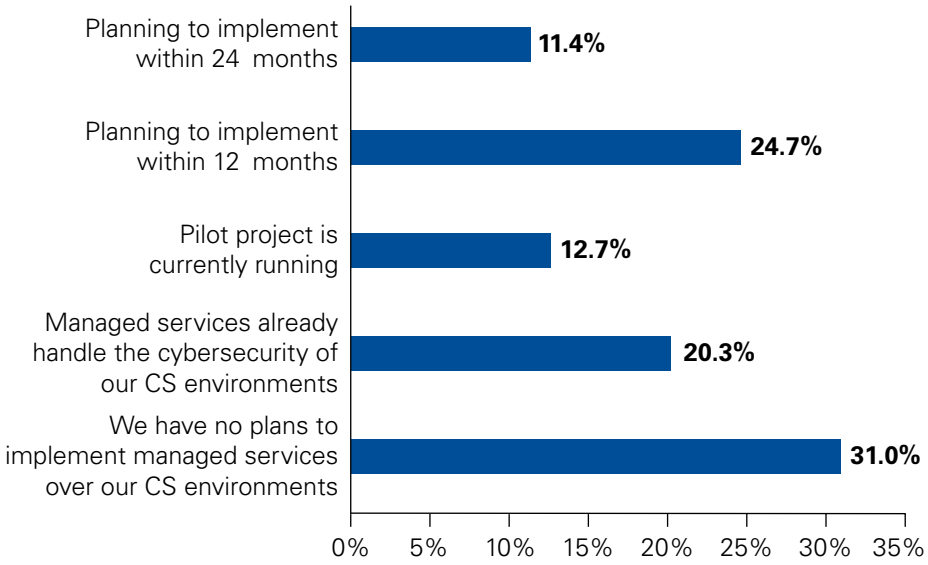
Level 5 — Cybersecurity processes continually improved via feedback from existing processes and adapting to better serve organizational needs. Personnel performing the processes have adequate skills and knowledge. Optimizing, automated, integrated, predictable active defense, threat intelligence, incident management.

Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Managed CS security services

The use of Managed CS Security Services revealed perhaps the greatest distinction between the most mature CS Security Programs (Levels 4 and 5) and least mature ones (Levels 1 and 2), with nearly half (47 percent) of the former already having managed services handling CS cyber security versus only 6 percent of the latter, and the least mature organizations being six times as likely to have no plans to implement managed services in this area (36 percent in Levels 1 and 2 vs 6 percent in Levels 4 and 5).

State of managed CS security services



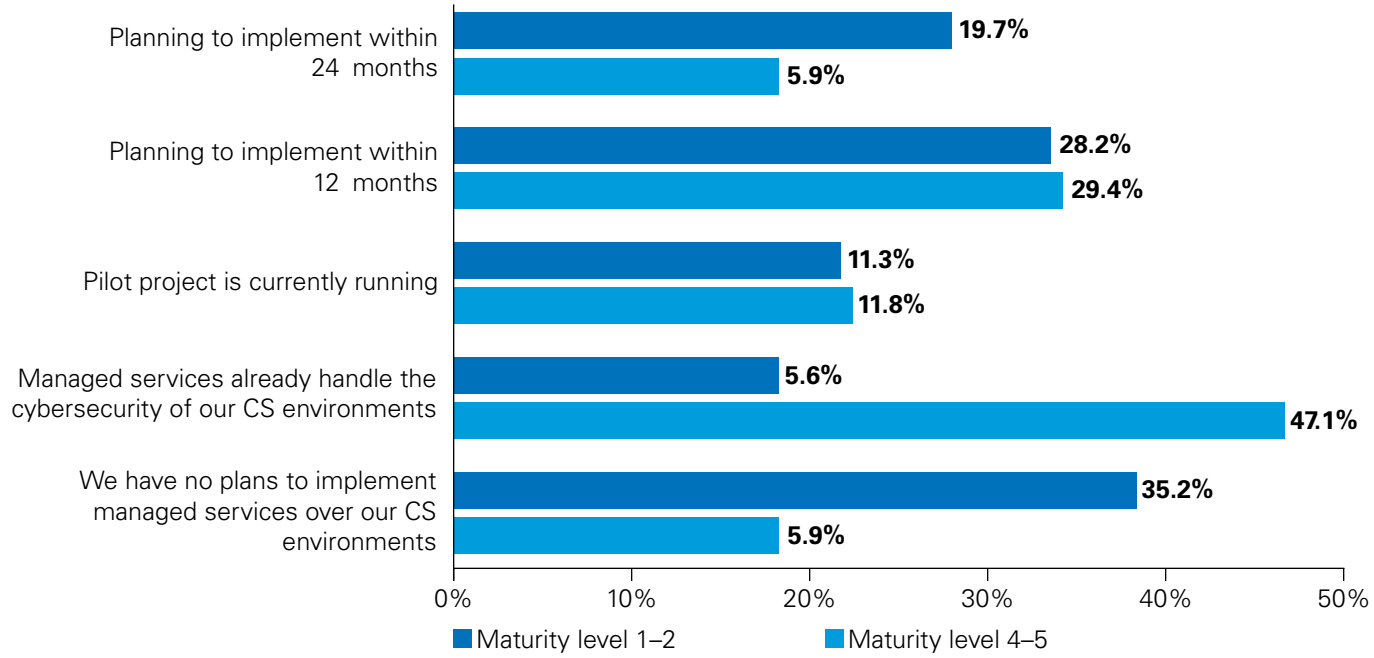
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Managed security services

This result confirms Airbus CyberSecurity's view of when Managed Security Services (MSS) generates the most added value. The higher the maturity of CS security, the better the ROI: customers gradually benefit from cost reductions and better management of scarce CS expertise.

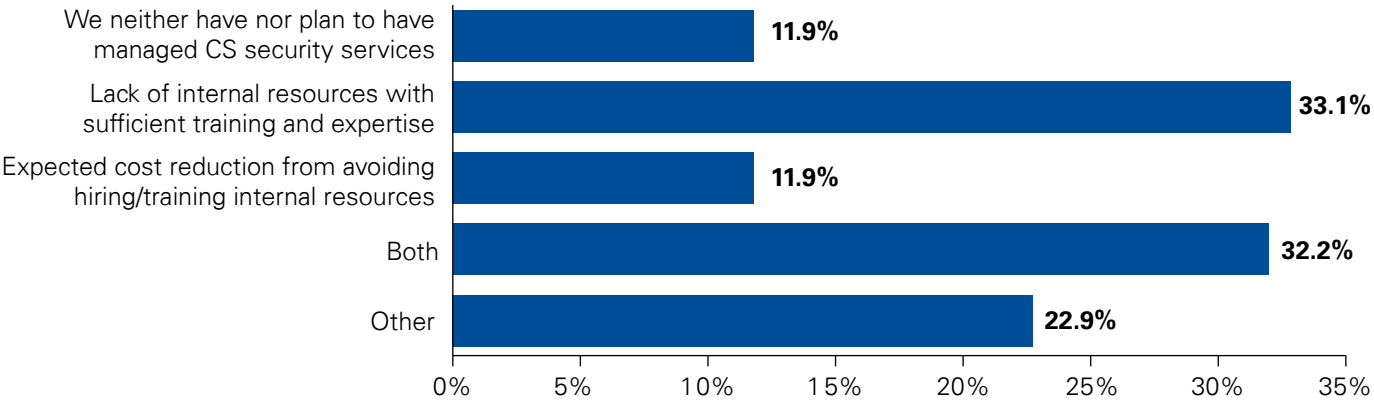
Joerg Schuler, OT Security Portfolio & Partnerships Manager, Airbus CyberSecurity

State of managed CS security services (by program maturity level) ρ



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Reason for using/planning to use managed CS security services



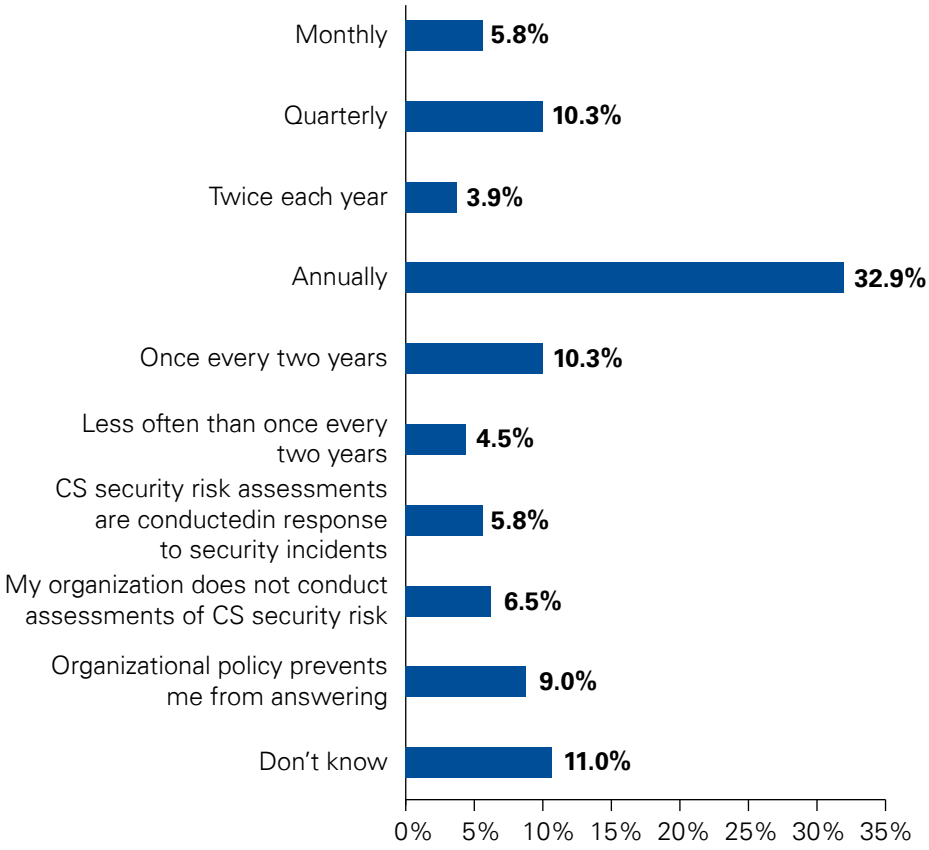
Among those organizations currently or planning to utilize CS Security Managed Services, both financial savings and the previously mentioned shortage of personnel with sufficient training and resources were widely cited as causes.

Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS cyber security assessments

The growth of Advanced Persistent Threats[11] (APTs)[12] has increased the importance of frequent CS Cyber Security Assessments, with many threat actors enjoying months of dwell time[13] within a target network before being discovered. We see that more mature CS cyber security programs recognize this and conduct assessments more frequently, with more than one out of four of the most mature (17 percent and 9 percent of Levels 4 and 5) completing assessments two to four times each year and an equal number annually (26 percent of Levels 4 and 5).

CS security assessment frequency



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

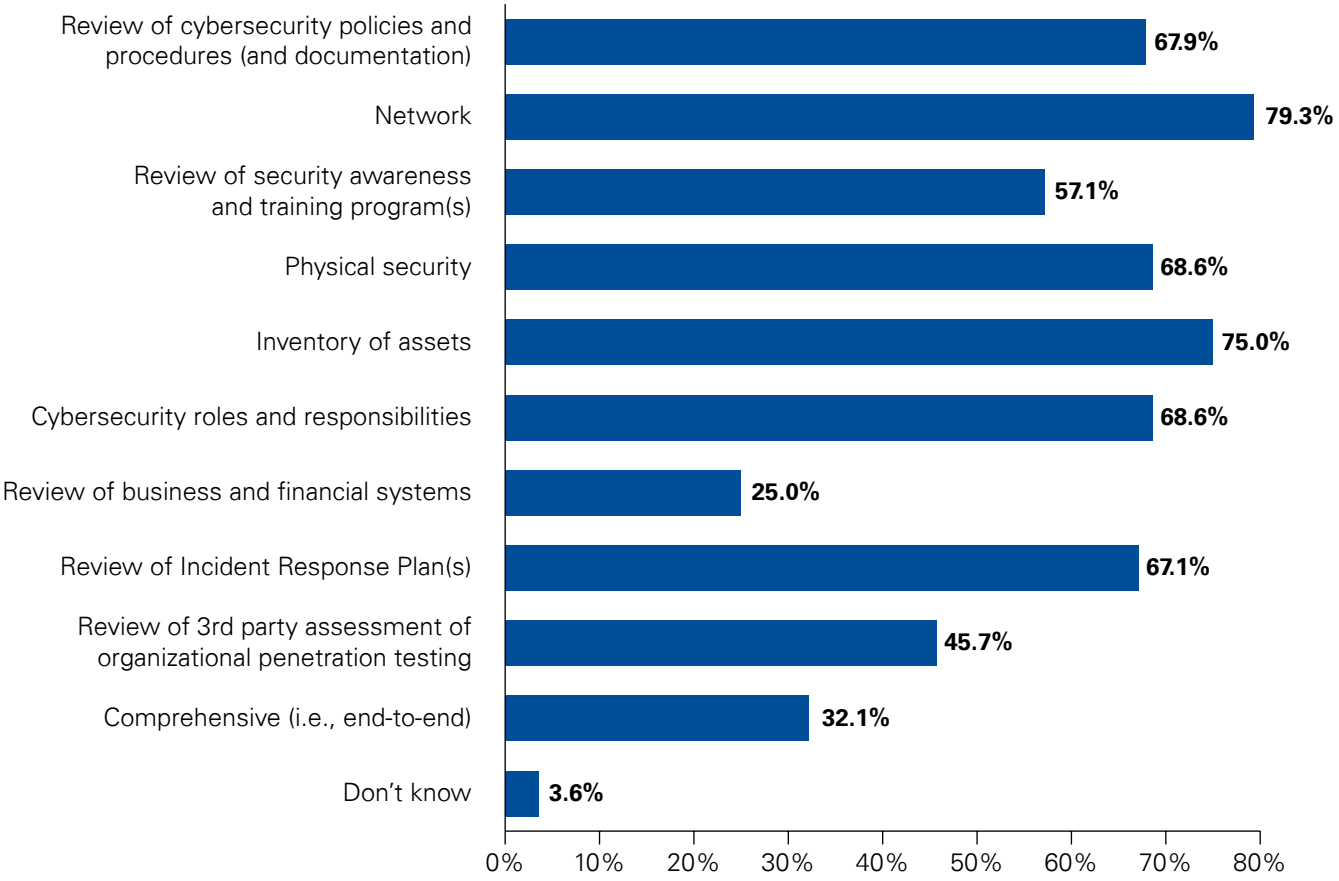
[11] Advanced Persistent Threat: an attack in which attackers gain access to networked systems and assets but remain undetected for an extended period of time to steal data, infiltrate other connected systems (often referred to as "pivoting") and/or increase their level of access and control.
[12] https://techerati.com/features-hub/interviews/the-inexorable-rise-of-advanced-persistent-threats/
[13] Dwell Time: period beginning with an attacker gaining undetected access to a target system or network and ending with owners/defenders of that system or network detecting the breach.

No matter how frequently an organization assesses their CS cyber security program, the thoroughness of that assessment process itself makes the difference between a compliance or 'check the box' approach and a security effectiveness-minded one. There are innumerable potential points to measure, of course, but we selected a set of common components we would hope to see included in every assessment process.

CS security assessment frequency (by program maturity level) ρ

Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

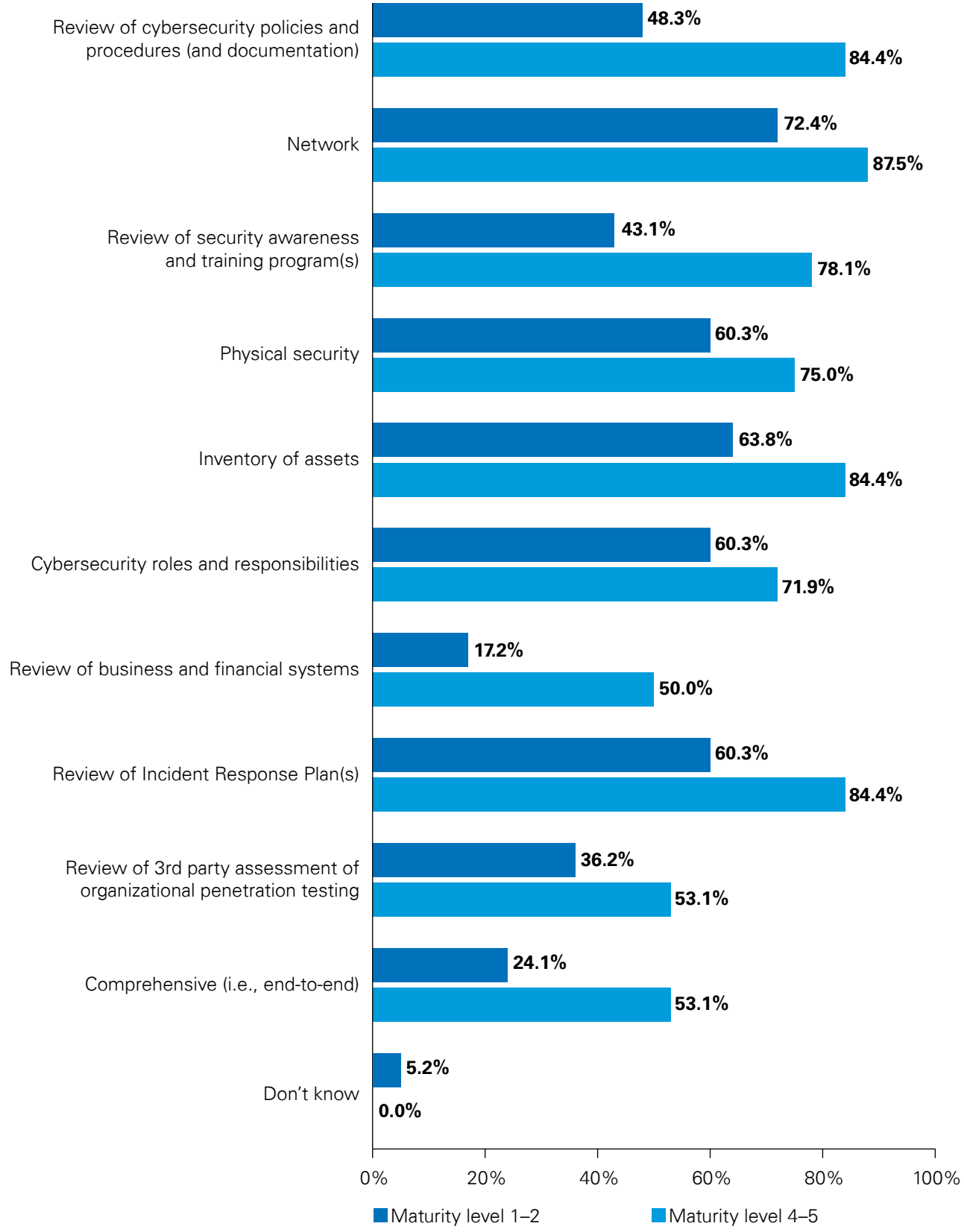
CS security assessment components



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Once again, the differences between the most mature CS cyber security programs (Levels 4 and 5) and least mature (levels 1 and 2) stood out clearly, with the former's assessments more likely to evaluate every area of exposure, often quite significantly.

CS security assessment components (by program maturity level) ρ



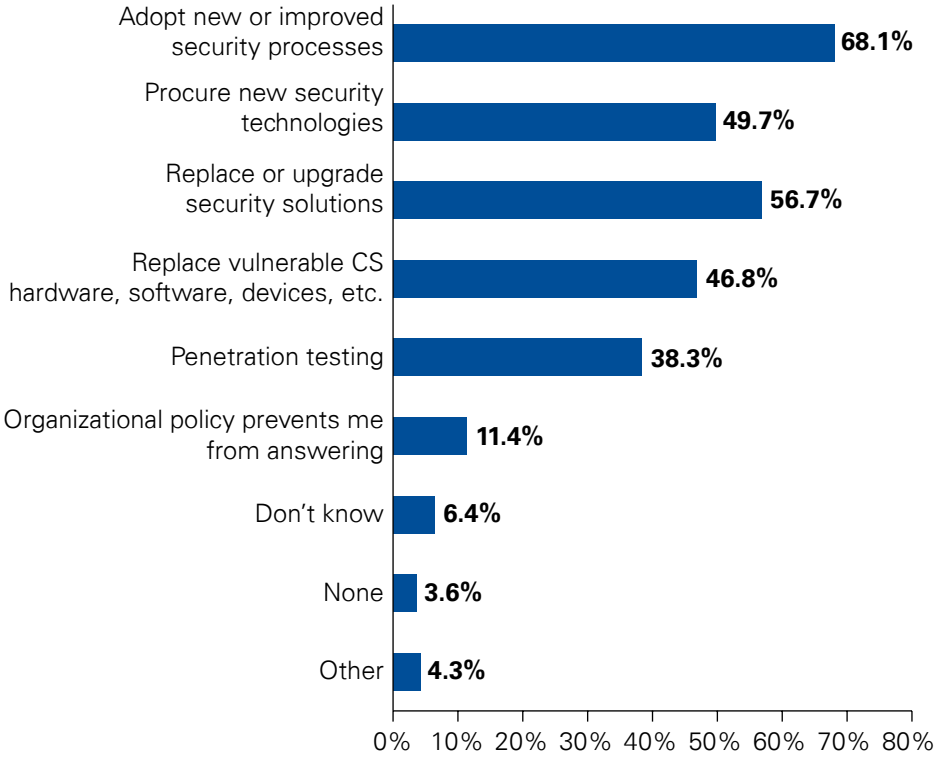
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Even the best assessment is only the first part of the picture, and follow-up action is required to address shortcomings and gaps in protective controls. We consider it highly concerning that any respondents indicated either that they did not carry out corrective action after assessments (4 percent, *None*) or were not aware whether their organizations did so (6 percent, *Don't Know*).

Participants with lower CS Security Program Maturity Levels were less likely to have the knowledge necessary to answer regarding follow-up activities (9 percent *Don't Know,* vs 0 percent of Levels 4 and 5). On the topic of follow-up activities to CS Security Assessments they are also less likely to carry out any follow-ups to assessment findings (In Levels 1–2, 9 percent answered *None* vs 0 percent in Levels 4—5).

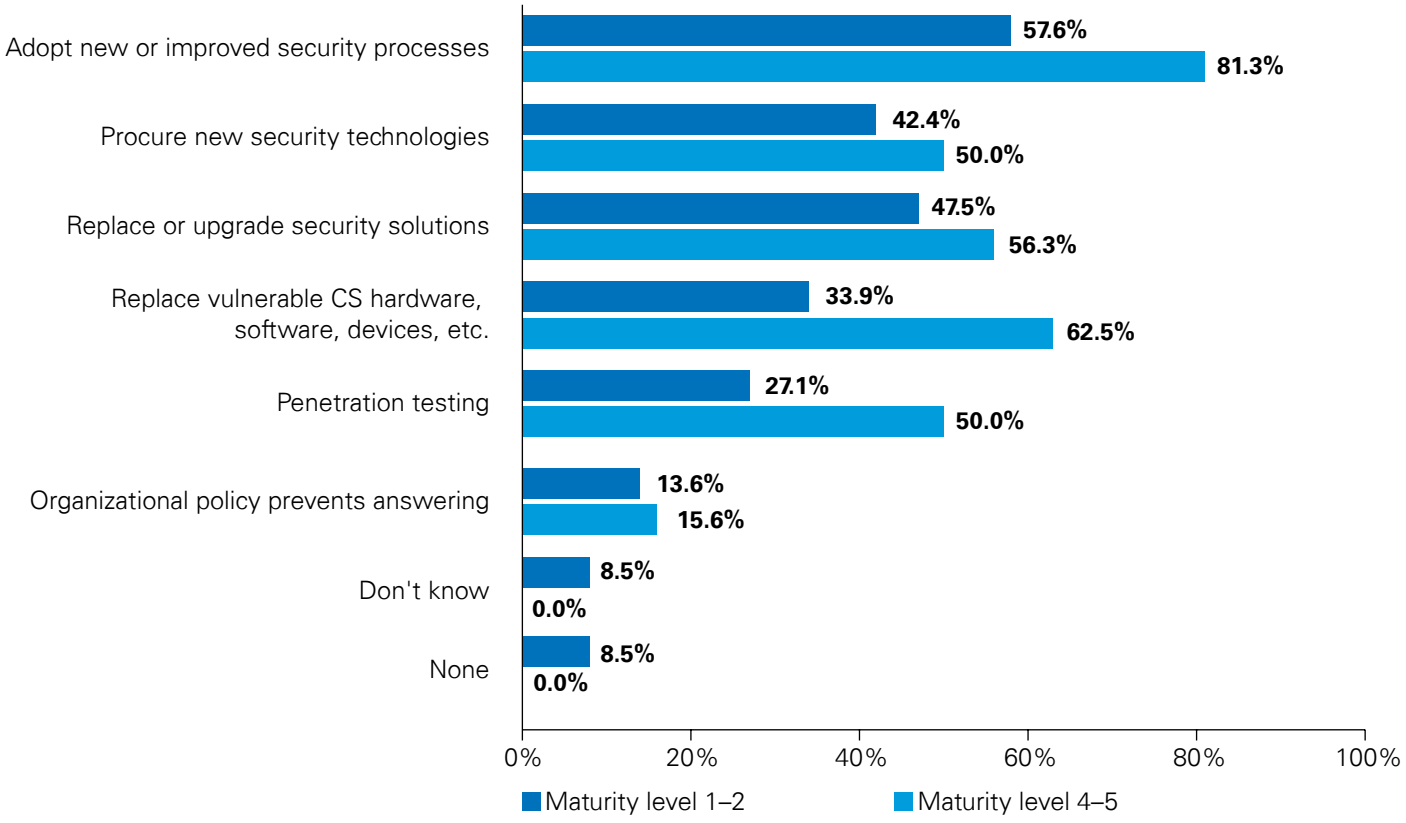
Overall, organizations with more mature programs were more likely to conduct all types of follow-up activities, with the strongest deltas in *Adopting New or Improved Security Processes* (81 percent vs 58 percent), *Replace Vulnerable Hardware, Software*, etc. (63 percent vs 34 percent), and Penetration Testing (50 percent vs 27 percent)

CS security assessment follow-up activity



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS security assessment follow-up activity (by program maturity level) ρ



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.


2.01E+03
1.00E+00
2.00E+00
3.00E+00
4.00E+00
5.00E+00
5.00E+00
6.00E+00
8.00E+00
8.00E+00
1.30E+01
9.00E+00
1.60E+01
1.10E+01
1.80E+01
1.20E+01
2.00E+01
Last:
Open:
High:
Low:
Jun 15
$600.00
Jun 15
$600.00
Jun 15
$600.00
Reset Parameters
Date 7/15/12

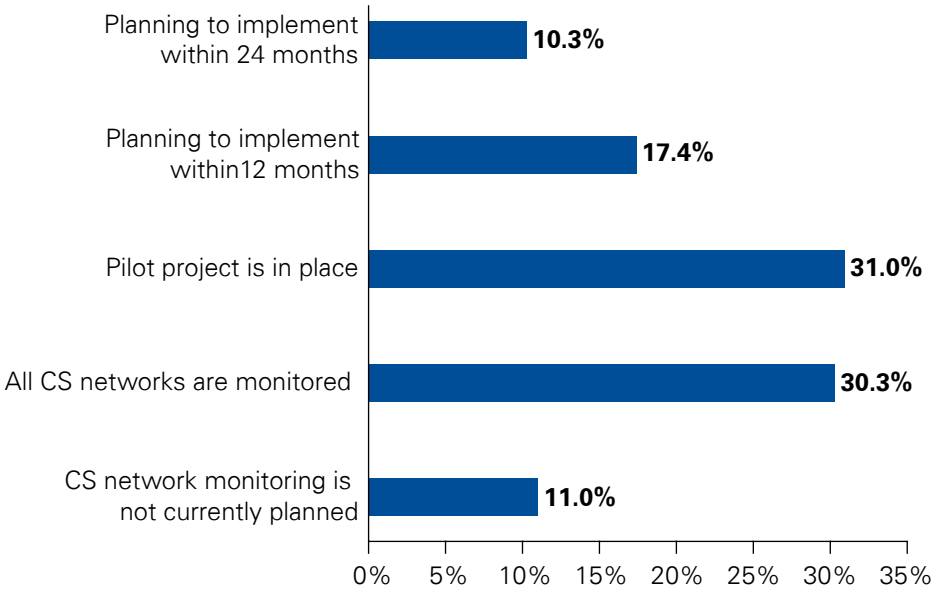
CS network security monitoring

IT network monitoring technologies have been well-known since the last century. These were largely active-scanning systems, however, and early use of them in OT environments was found to directly cause operational process disruption at times. The highly deterministic networks in operational settings, in combination with the significantly greater potential for negative outcomes of OT disruptions (relative to IT network disturbances) created a resistance among many to the use of network scanners.

Control System network-specific network monitoring tools are much more recent developments. The first generation, referred to by terms such as 'non-intrusive anomaly detection' or 'passive network listening' solutions, emphasizing the safety of their use within critical network settings, began to reach the market around 2013. Numerous vendors now exist in this space, and a second generation of tools has become available, the Control System-specific Intrusion Detection/ Prevention System (ID/PS or IPS).

Driving this tool development is awareness that the rapidly increasing exposure of Operational networks and assets to attack through ongoing convergence trends has completely outpaced operators' and defenders' ability to observe OT network activity. Without visibility into this activity, it has too often been the case that the first indications of security breaches have been operational disruptions occurring months after attackers[14] gained illicit access to target networks.

CS network monitoring



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Cyber security monitoring

Effective CS monitoring means first getting and maintaining visibility of critical assets, then using risk-based methods when planning and implementing protective security monitoring. CS/ OT specific sensors help to get visibility over and to monitor CS assets. The real added value however comes from combining data from those sensors with CS threat intelligence in a SIEM solution, introducing automated SOC rules and relying on IT/OT SOC analysts who can take protective actions.

Joerg Schuler, OT Security Portfolio & Partnerships Manager, Airbus CyberSecurity

[14] https://www.chaossearch.io/advanced-persistent-threat

Initially encouraged by the number of respondents indicating their use of OT network monitoring (31 percent in pilot and 30 percent fully implemented), we remain highly concerned that over 10 percent even yet have no plans to implement this basic security practice.

The authors believe they cannot overstress the importance of understanding network monitoring as the inseparable companion of network security assessments. However thorough and insightful an assessment is, it can only exist as a snapshot in time. Assessments can and do find issues missed by network monitoring because they use different tools and methodologies but, without monitoring, organizations can be blind to intrusions and other issues that develop in the gap between assessments. Further, monitoring also serves as a check on the effectiveness of measures introduced after a security assessment. For the same reason that entry points into restricted access facilities are alarmed in addition to periodic eyes-on checks, monitoring provides a crucial piece of OT network security knowledge.

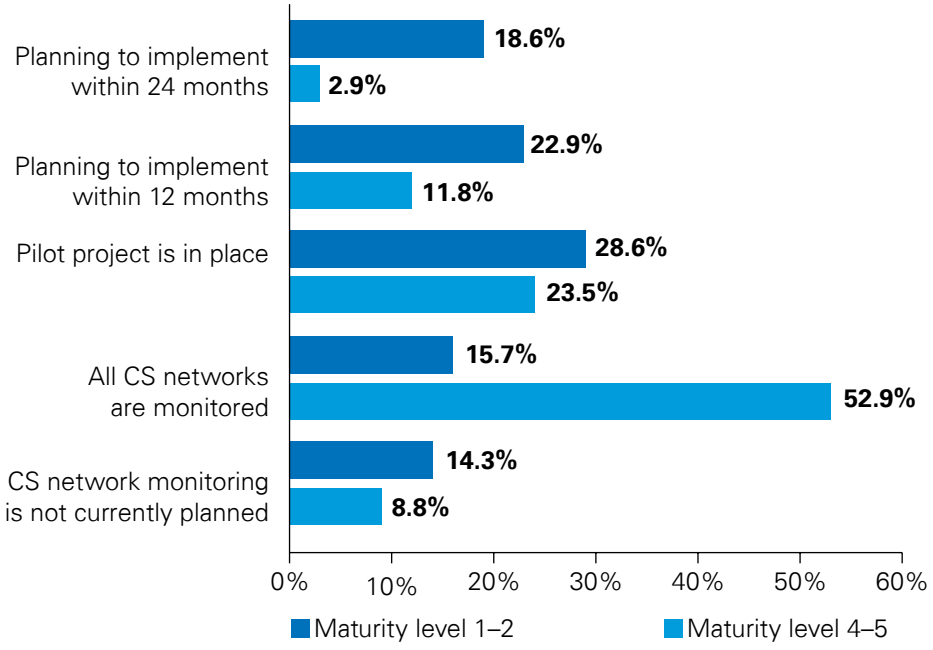
We found that the most mature CS cyber security programs were more than three times as likely to have fully implemented CS network monitoring than the least mature (53 percent at Levels 4–5 vs 16 percent for Levels 1–2), and the least mature approximately half-again as likely to have not yet even planned for monitoring (14 percent at Levels 1–2 vs 9 percent for Levels 4–5).

Safe Security Monitoring — Where to manage OT IDS sensors?

Connecting IDS management ports to CS networks requires SOC analysts to remote into CS networks routinely. Connecting IDS sensor management ports to IT networks makes the sensors dual-homed hosts with a management port on the IT network and monitoring ports connected to OT SPAN and mirror ports. The safest OT sensors are deployed on and managed from IT networks with hardware-enforced unidirectional connections to OT SPAN/ mirror ports.

Lior Frenkel, Co-Founder & CEO, Waterfall Security Solutions

CS security services (by program maturity level) ρ

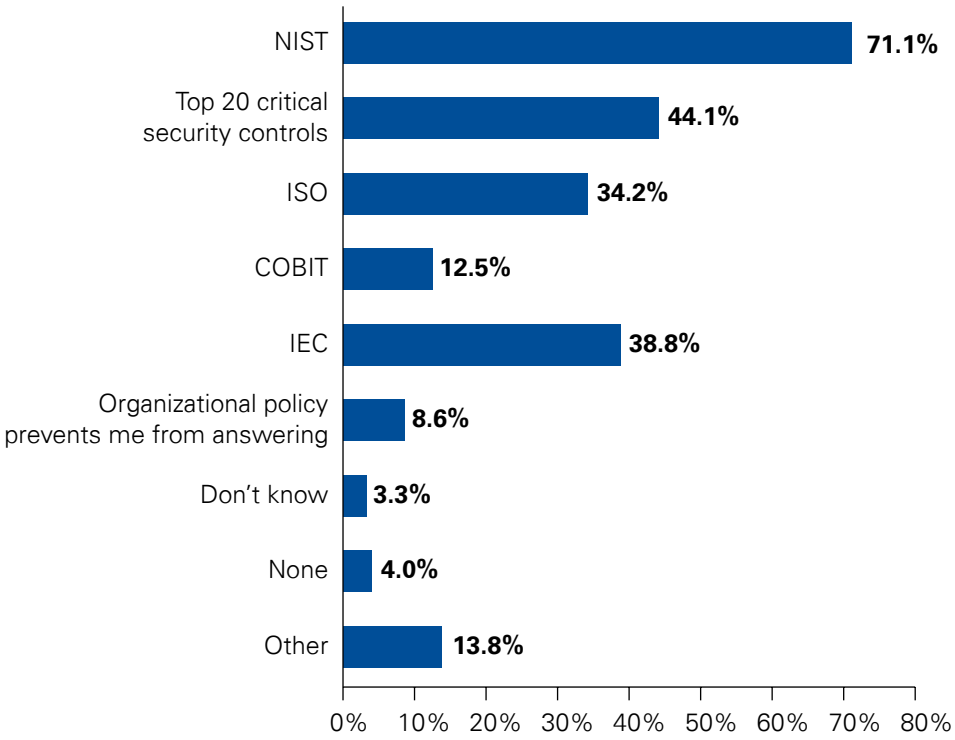


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS security frameworks

Security frameworks are important tools, providing tested methodologies and enabling security practitioners to develop their programs with guidance from subject matter experts. By viewing threats and security objectives through a shared lens, organizations are more able to objectively evaluate and manage their risks. Numerous Control System cyber security-relevant frameworks exist, some more widely applicable than others. NIST is by far the most used framework among our respondents, continuing trends noted in multiple publicly available reports.

CS security frameworks



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Cyber security monitoring

For business critical industrial processes, monitoring of the entire value chain should be handled by a Security Operations Center keeping an eye on all critical IT and OT assets. NIST is the reference framework but, when it comes to the protection of CS, other relevant frameworks have to be taken into account as well to define the right security measures.

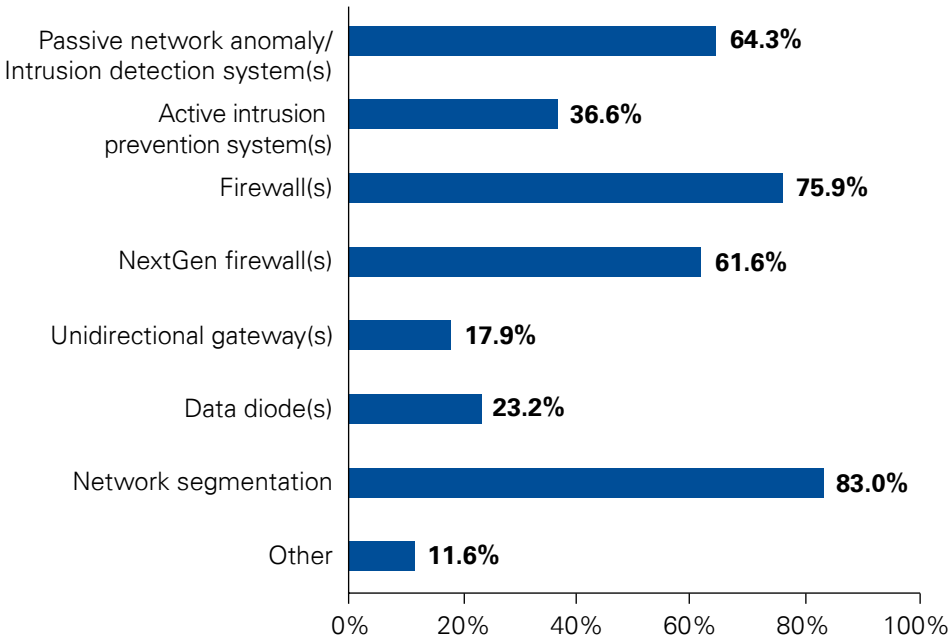
Joerg Schuler, OT Security Portfolio & Partnerships Manager, Airbus CyberSecurity

CS security technologies

Segmentation is fundamental to network security and, when done well, is one of the most effective means of controlling OT networks , reducing threats from both in- and outside organizational structures.[15] In a segmented network environment, whether attackers (external threat actors) initial access is gained via emails with malicious links, stolen credentials, or infected removable media, their ability to travel across networks is constrained by the controls at segmentation points. At an absolute minimum this increases the amount of time required for reconnaissance of an organization's networked environment, thereby increasing defenders' opportunities to detect an adversary's access. At best segmentation limits their access to a single network zone and thereby the potential for theft or damage. It also reduces potential damage from insiders, widely thought to be the greatest source of threat to OT networks (see *Negligent Insider* in CS security incident threat actors table, below).

While some Security Technologies were used in similar numbers by all participants, CS Security Program Maturity Level 4 and 5 respondents were much more likely to have implemented *NextGen Firewalls* (81 percent vs 50 percent in Maturity Levels 1–2), which we recommend highly.[16] It is arguable that a similar level of protection is achievable by using a number of different technologies in combination, but simplifying a solution decreases potential misconfigurations and incompatibilities.

CS security technologies



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Unidirectional Gateways

Thoroughly-secured industrial networks use at least one layer of unidirectional gateway technology in their defense-in-depth architectures. While there are roles for firewalls, zero-trust, and security monitoring in such architectures, unidirectional protection is essential to robust security. Modern gateways replicate servers unidirectionally, enabling safe IT/OT integration, seamless OT visibility and disciplined control.

Lior Frenkel, Co-Founder & CEO, Waterfall Security Solutions

[15] https://www.securityweek.com/reducing-pain-ot-network-segmentation
[16] https://www.cisoplatform.com/profiles/blogs/9-top-features-to-look-for-in-next-generation-firewall

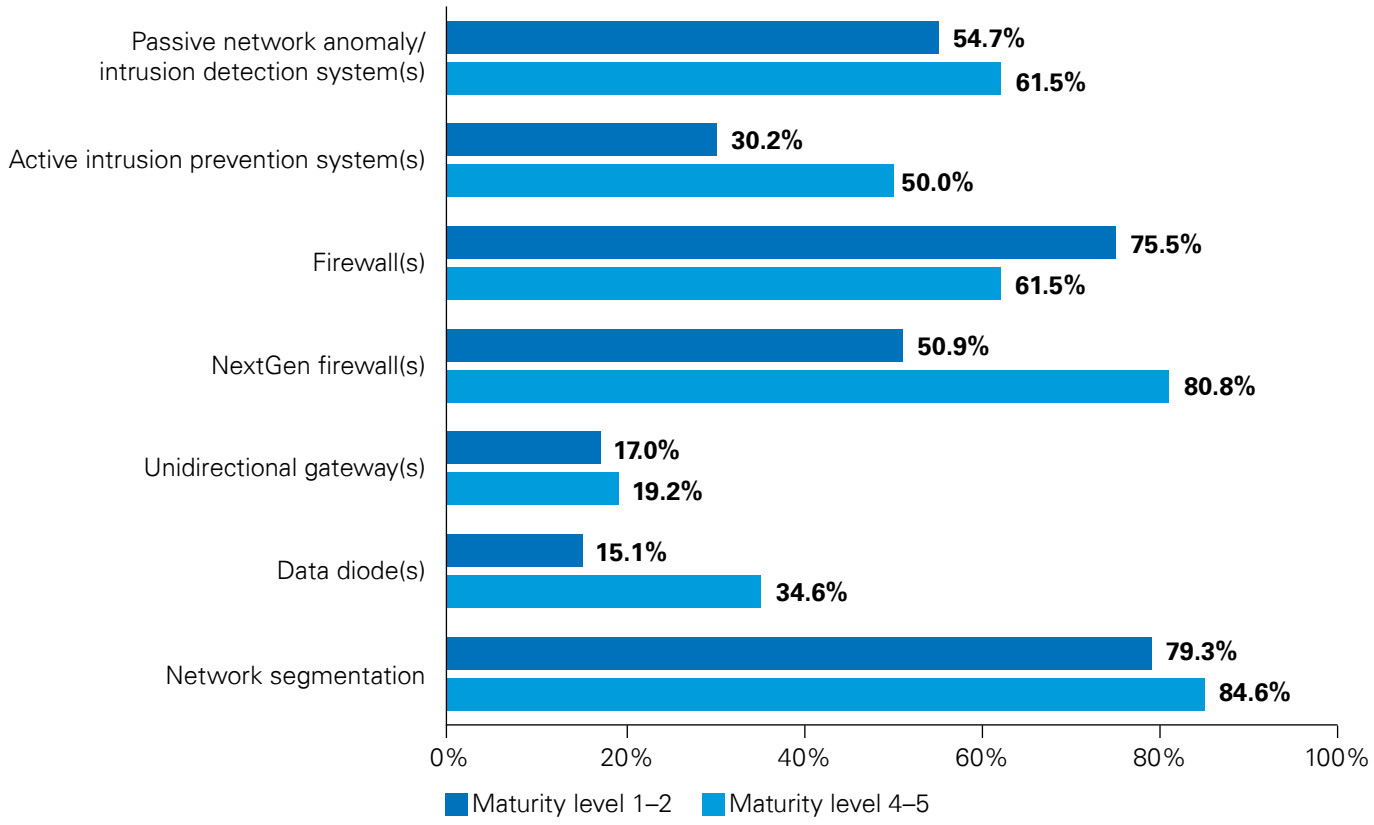
Maturity Level 4 and 5 respondents also indicated greater adoption of *Data Diodes* (35 percent vs 15 percent of Level 1 and 2) and *Active Intrusion Prevention Systems* (50 percent vs 31 percent of Level 1 and 2) to protect their OT networks. These technologies are newer in the OT space than others, and their acceptance by highly disruption-averse OT professionals is an ongoing process. We look forward to the continued expansion of their use.

Nextgen firewalls

Next-generation Firewalls play a key role in realizing Zero-trust architectures with their ability to easily implement zones and conduits with granular layer-7 policies based on application, user and content. Strong authentication systems are easily coupled to conduits to fortify defenses. Further, NGFWs natively integrate IDS/IPS functions enabling simultaneous detection and prevention of exploits and malware.

Del Rodillas, Dir. CS/OT Industries Marketing, Palo Alto Networks

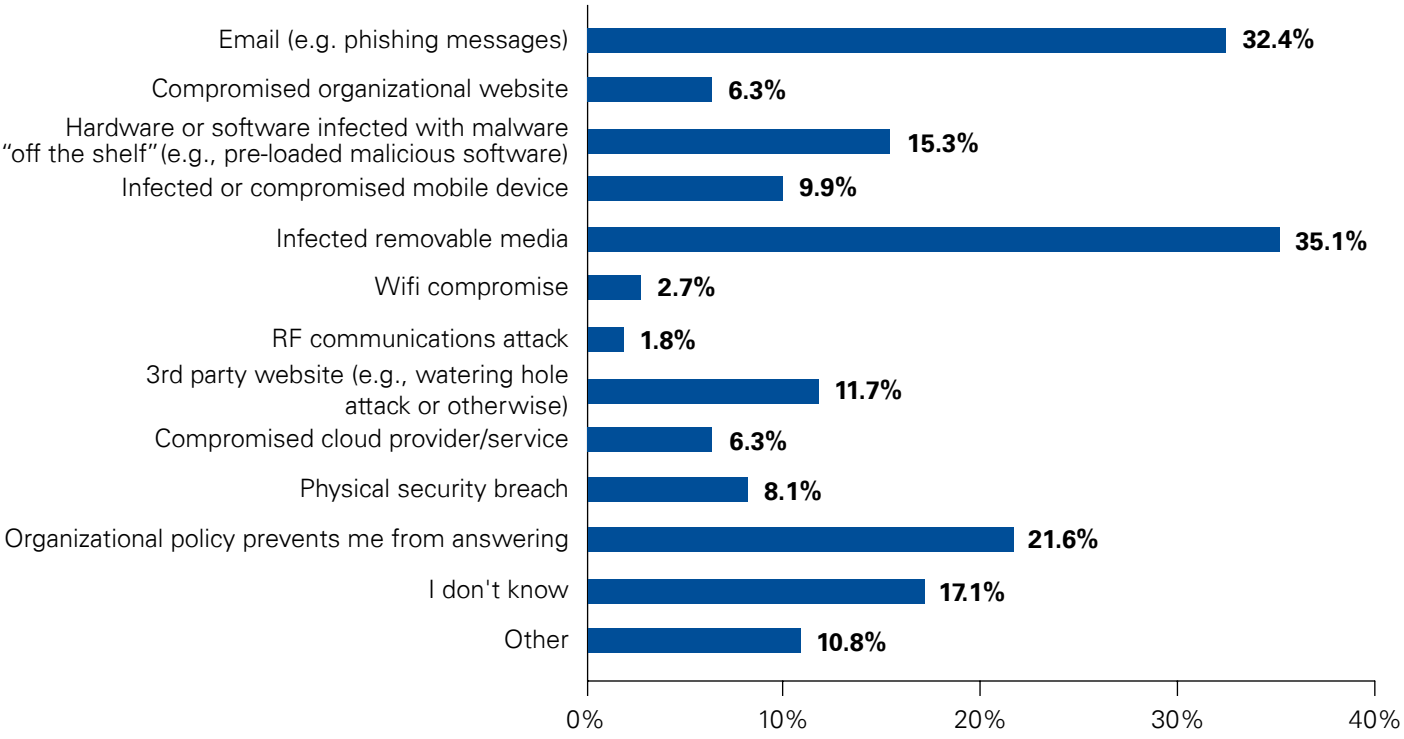
CS security technologies (by program maturity level) ρ



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

CS cyber security incidents

CS incident attack vectors encountered within past 12 months

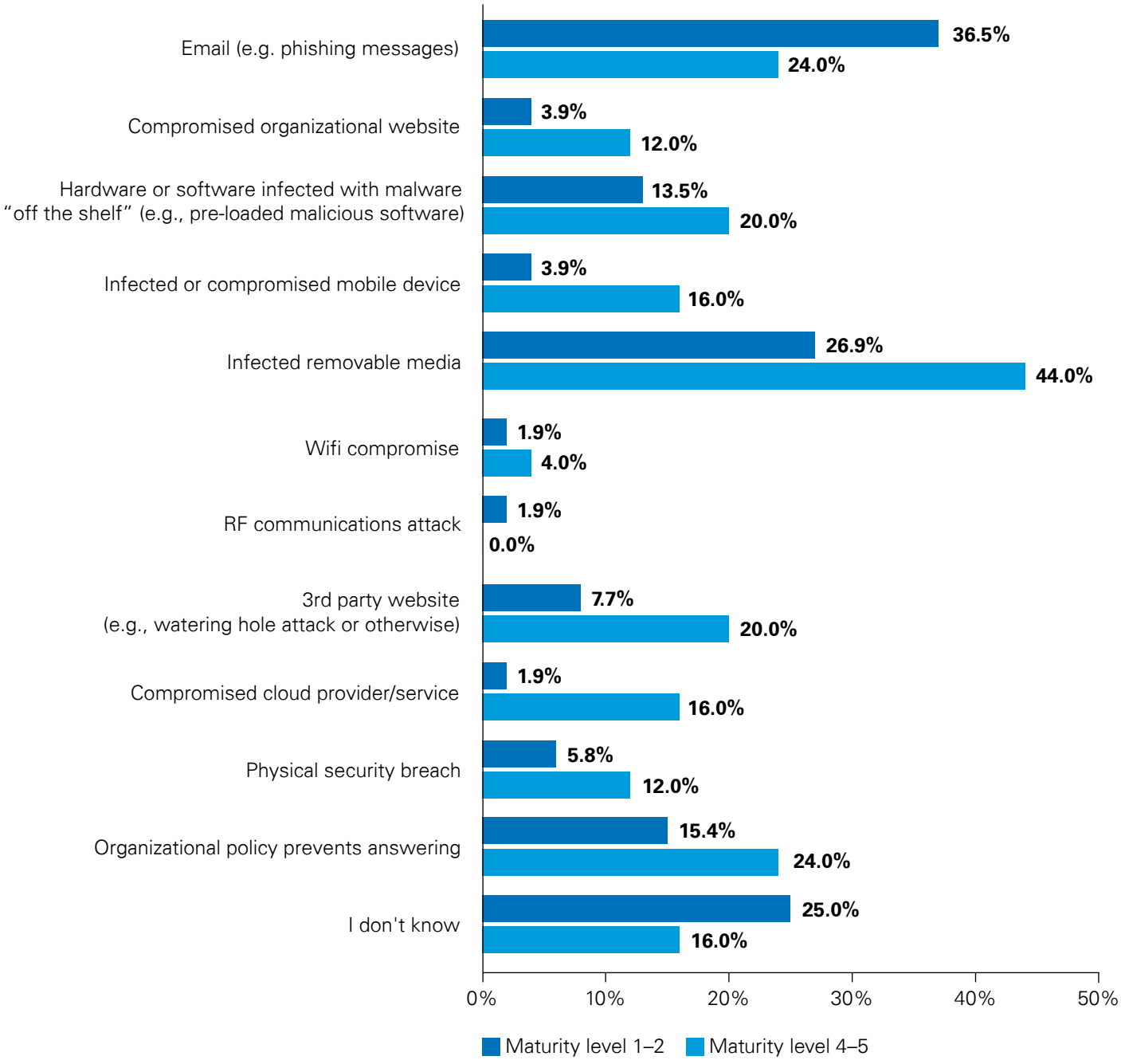


Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

While respondents were in consensus that the most common attack vectors were *Infected Removable Media* and *Phishing,* we observed a split between the most and least mature ICs cyber security programs, with 44 percent of Levels 4 and 5 citing *Infected Removable Media* to 27 percent of Levels 1 and 2, and 35 percent of Levels 1 and 2 citing *Phishing* versus only 24 percent of Levels 4 and 5.

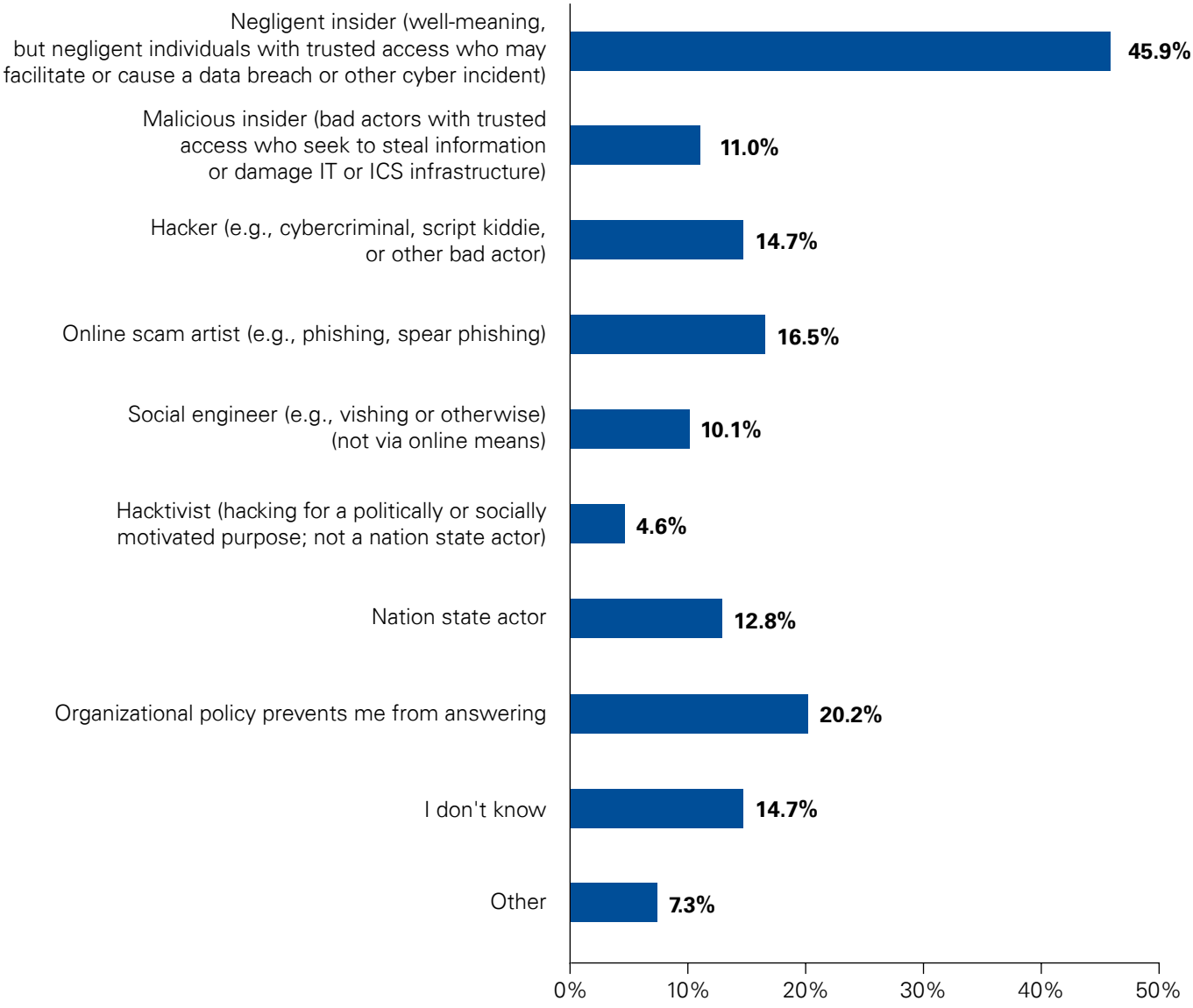
We noted one interesting pattern; the Levels 4 and 5 group chose *every* attack vector more often than the Levels 1 and 2 group with the exception of the aforementioned Phishing and "*I don't Know*." Whether this is due to greater awareness on the part of those with more mature security programs or not remains an open question at this time.

CS incident attack vectors encountered within past 12 months (by program maturity level) ρ



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

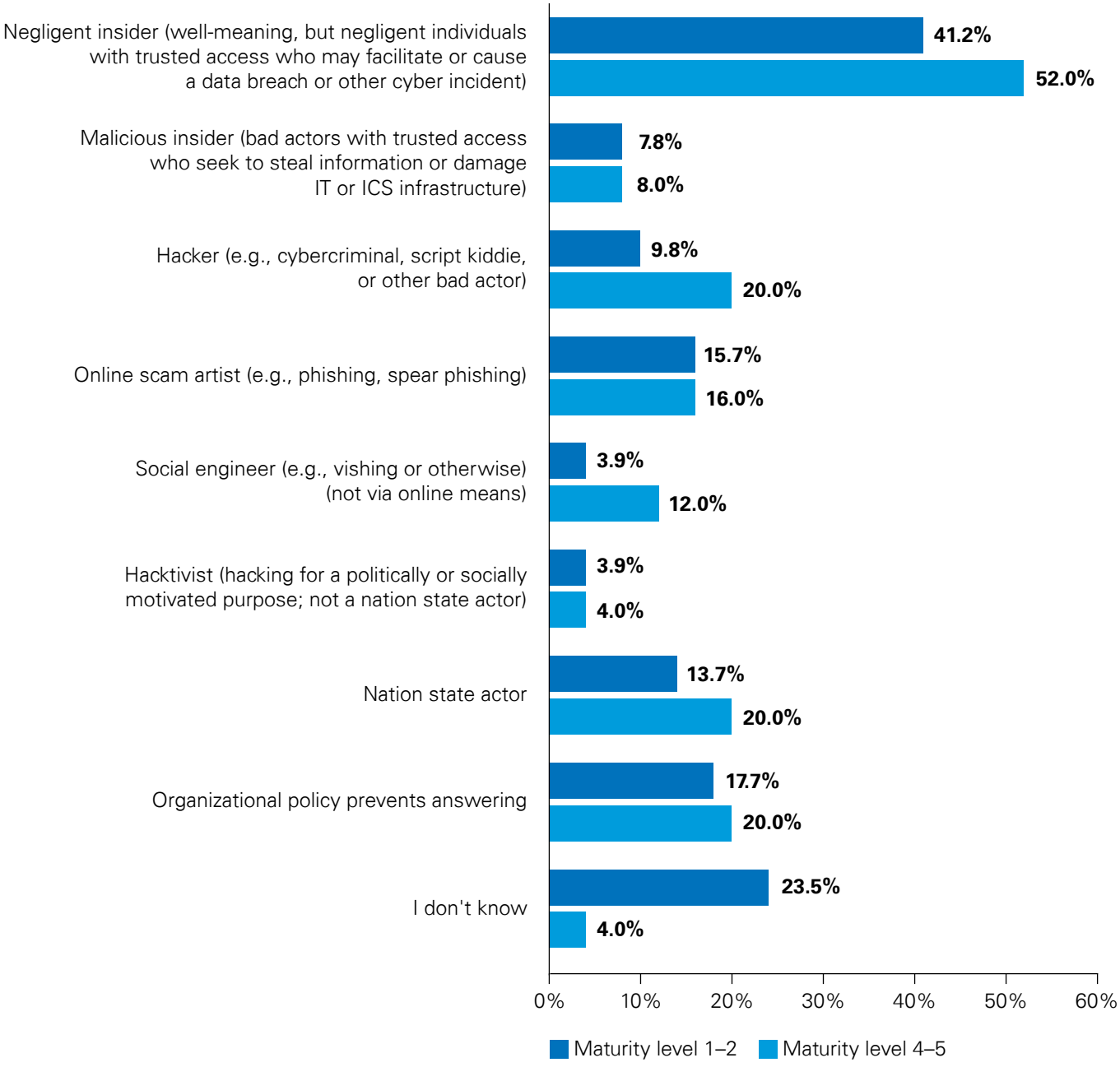
CS security incident threat actors encountered within past 12 months



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

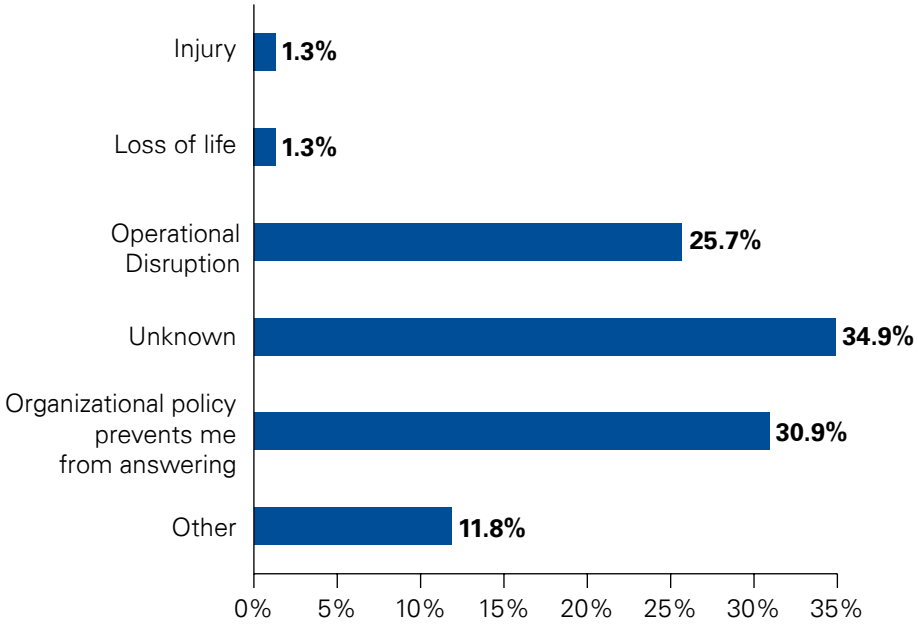
Respondents overwhelmingly chose *Negligent Insiders* as the most common "Threat Actor" of their recent OT Security Compromises. Beyond that, it is worth noting that the less mature CS Security Programs were again more likely to indicate that they lacked information to answer the question (24 percent *"I Don't Know"* in the Level 1-2 group vs 4 percent in the Level 4-5 group). Organizations with the most mature Programs (Levels 4-5) were much more likely to identify the involvement of *Social Engineering* (level 4-5 group 12% vs Level 1-2 group 3.9%), *Hacker* (Level 4-5 group 20% vs Level 1-2 group 9.8%), and *Nation State Actors* (level 4-5 group 20% vs Level 1-2 group 13.7%).

CS security incident threat actors encountered within past 12 months (by program maturity level) ρ



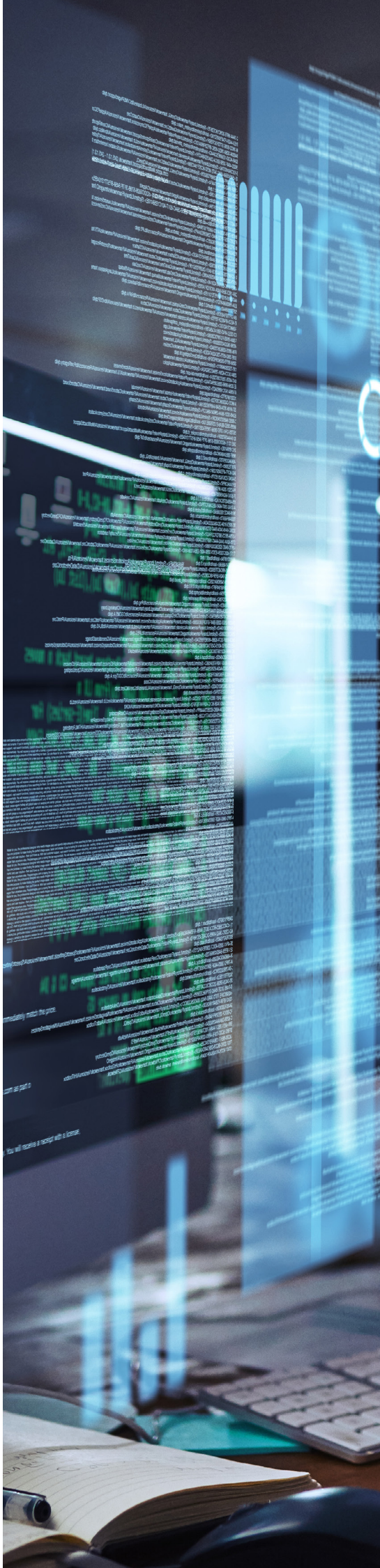
Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Impacts of CS security incidents



Source: (CS)²AI-KPMG 2019 Control System Cyber Security Survey.

Having not been aware of any CS security incidents within the past year that resulted in *Loss of Life,* we did not anticipate reports of any. This result caused us to examine our data particularly closely on this question. Respondents' answers were submitted anonymously, so requesting confirmation or additional information from the relevant individuals was not possible. In lieu of this we analyzed the sets of answers of which these were part, including the length of time spent on the survey and, to the best of our ability to ascertain, this response is valid.



Chief Recommendations

Determine your risk profile
Evaluate quantifiable risks to your Control Systems environment and your business considering evolving threats and vulnerabilities. Engage resources with the greatest level of expertise available, as everything else depends on the thoroughness and accuracy of this work.

Assess your security posture
What are you currently doing to secure your CS environment? How effective are these security efforts? Based on your risk profile and appetite, what should you invest to protect your systems, assets, and people? What technologies, services, and/or processes would improve your security the most, and what would they cost? Re-assess regularly.

Communicate your security posture
Business decision-makers need clear information to fulfill their role, and may comprehend attack scenarios and consequences better than abstract risk scores. What is the simplest attack with serious consequences that your current security posture does not defeat reliably? No security posture is perfect, so there is always a possibility of attack.

Monitor your CS networks
At the minimum, implement an Intrusion Detection System to gain basic insight into network traffic activity in your OT environment. This will greatly increase your ability to successfully plan and implement network segmentation.

Segment your networks
Implement controls limiting access to and between networks. These inhibit the spread of malware infections, malefactors who gain access to your network, and accidental damage from unaware insiders.

Develop your defense team
There are not enough skilled and experienced CS cyber security practitioners in the workforce. Train the people already familiar with your operational systems to give them the skills needed to protect your systems and assets.

Raise the roof on cyber security awareness
Insiders continue to be involved in the majority of security incidents, often unintentionally. Ensure that everyone knows their role in security and understands the harmful potential their access could be used for by malefactors.

Secure your supply chain
With integration, infiltration of your suppliers' systems can easily become infiltration of yours. Implement access controls around all connections into your OT environment from partner networks and require your suppliers to verify their own cyber security.

Addressing cyber security expertise shortages

Cross-training internal team members Many organizations can leverage cyber security expertise from the IT team. Their knowledge sharing with the OT team of the IT network, environment, and experience can help build a foundation of cyber security practices across the CS environment. It also creates an opportunity to bridge the differences between IT and OT environments as an organization evolves its cyber security strategy.

Peter Newton, Sr. Dir IoT Security Product Marketing, Fortinet

Annual

Report Steering Committee

Name	Company	Role
Derek Harp	(CS)²AI	Annual Survey & Report Chair, Co-Author
Bengt Gregory-Brown	(CS)²AI	Annual Survey & Report Director, Lead Designer, Co-Author
Dani Michaux	KPMG in Ireland	(CS)²AI Strategic Alliance Partner Liaison, Survey Design Team
Brad Raiford	KPMG in the U.S.	CS²AI Strategic Alliance Partner Liaison, Survey Design Team
David Ferbrache	KPMG in the UK	Survey Design Team Member
Jaco Benadie	KPMG in Malaysia	Survey Design Team Member
Walter Risi	KPMG in Argentina	Survey Design Team Member
Manish Tembhurkar	KPMG in India	Survey Design Team Member
Ninad Purohit	KPMG in Canada	Survey Design Team Member
Martin Ignacio Cafferata	KPMG in Argentina	Survey Design Team Member
Andrew Ginter	Waterfall Security Solutions	Survey Design Team Member, Analysis Contributor
Bryan Singer	Accenture	Survey Design Team Member
Del Rodillas	Palo Alto Networks	Analysis Contributor
Peter Newton	Fortinet	Analysis Contributor
Michael Chipley	PMC Group	Survey Design Team Member
Cherise Gutierrez	Security Gate	Survey Design Team Member
Raheem Beyah	Georgia Institute of Technology	Survey Design Team Member
Samara Moore	Amazon Web Services	Survey Design Team Member
Markus Braendle	Airbus CyberSecurity	Survey Design Team Member
Joerg Schuler	Airbus CyberSecurity	Survey Design Team Member, Analysis Contributor
Christopher Blask	Unisys	Survey Design Team Member
Ernest Wohnig	System 1, Inc	Survey Design Team Member
Najo Ifield	Canadian Cyber Security Alliance	Survey Design Team Member

About (CS)²AI

Peer-to-Peer Networking on a Global Scale
As a member of (CS)²AI, 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)²AI 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)²AI member opportunities designed to help you reach the next level in your career journey.

Vision	Mission	Goals
Strengthen global critical infrastructure by fostering Control System Cyber Security peer-to-peer networking and development.	An International organization enabling peer-to-peer organizations and supporting their grass roots efforts.	Professional networking Global alliances Professional Development Community Outreach Leadership Opportunities

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)²AI Fellow or research participant.

Our Strategic

Alliance Partners (SAPs)

(CS)²AI wishes to extend our heartfelt thanks to the following companies for their continued contributions toward our ability to directly support cyber security professional development.

Learn more about becoming a (CS)2AI Strategic Alliance Partner by clicking here.

Notes

Notes

(CS)2AI Social Media Links

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: (CS)²AI-KPMG Control System Cyber Security Annual Report 2020

Publication number: 136868-G

Publication date: September 2020