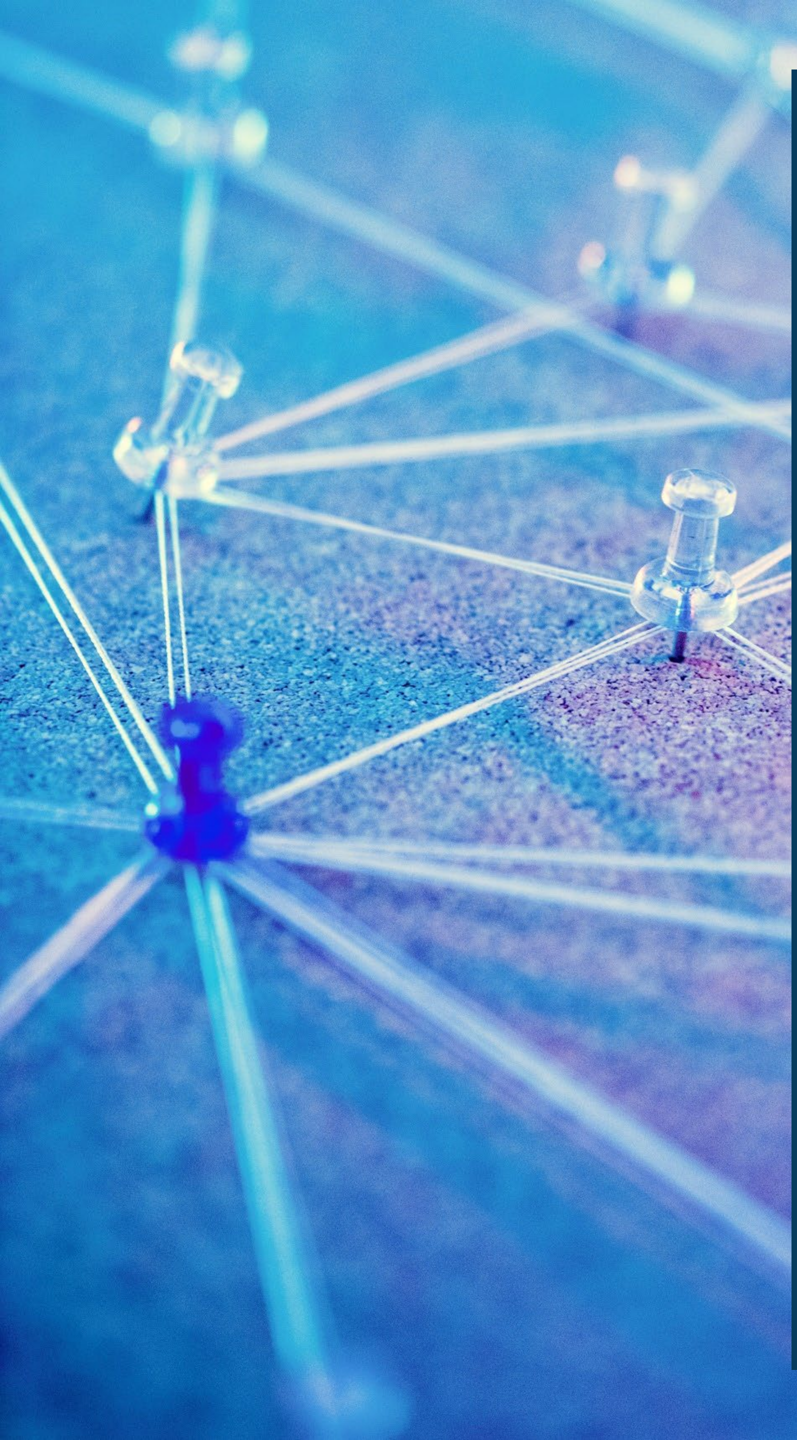
The (CS)^{2}AI-KPMG Control System Cybersecurity Annual Report

2024

Content



Content

The Chairman’s Message

Dear Industry Colleagues,

As we kick-off a new calendar year, it's essential to reflect on the progress we've made in the field of control system security as well as the challenges we continue to face. Though I am certainly an optimist in my core, what I have gathered from the hundreds of personal interactions I have had in the last year is a sense that real progress on a long road is being made. One thing that hasn't changed is the amount of work still ahead of us to ensure secure systems that enable modern ways of life.

I am proud to announce this third edition of the (CS)^{2}AI-KPMG Control System Cybersecurity Annual Report, the product of not only our own analysts and researchers but the growing group of Report Steering Committee contributors.

This year’s report is based on survey results from more than 630 industry members at large and a representative sample of (CS)^{2}AI‘s worldwide membership (approaching 34,000 community members today), with questions regarding their experiences with control system security events, attack patterns, and their responses, and where their organizations are focusing their resources to protect critical systems and assets.

The 2024 report sheds light on several critical trends and challenges in the control system security industry. While the increase in cyberattacks is concerning, organizations have become more proactive in their cybersecurity budgets, focused on prevention, and acknowledging the threat of supply chain attacks. One of the significant issues highlighted in the report is the shortage of skilled workers in the cybersecurity field. With the rise of cyber threats, the demand for cybersecurity professionals has never been higher.

Respondents in the survey report increased difficulty in hiring qualified personnel, and the report highlights the need for organizations to invest in the development of their current employees' cybersecurity skills and training.

This annual publication is the product of a growing group of vital contributors. Our greatest expression of appreciation must go to KPMG International, the report title sponsor, for enabling us to launch this project years ago and for their continued support and collaboration with us on its production. Waterfall Security Solutions and Fortinet have also been with us and providing resources and expertise since our first edition, and we further wish to thank all the other partners whose backing and guidance have helped to make this a valuable decision support tool every year (See Appendix D). Of course, we would be remiss to not include all of those who stepped up and became members of our Annual Report Steering Committee (See Appendix B).

It is our collective aim that this report provides valuable insights into the experiences of colleagues in the field, serving as a tool to support the many difficult decisions being made every day. It's important to use the findings of this report to make informed decisions and prioritize the areas that provide the best ROI in control system security spending. We remain committed to supporting our community in their efforts to ensure secure systems that enable modern ways of life.

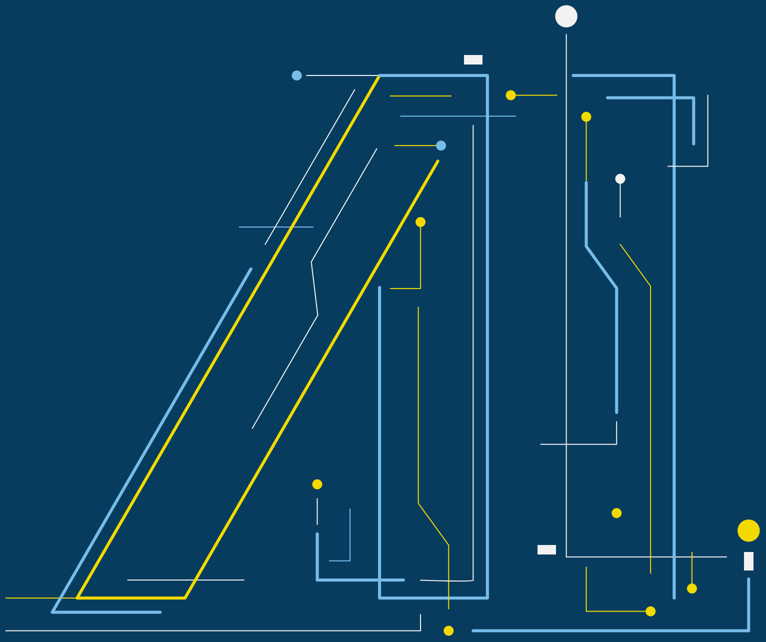
Regards,

Derek R. Harp

Derek Harp

Founder & Chairman, (CS)^{2}AI

Annual Report Title Sponsor Foreword



Walter Risi

Global OT Cybersecurity Leader
KPMG International and
Partner and Head of Consulting
KPMG in Argentina

Pablo Almada

Global OT Cybersecurity Deputy Leader
KPMG International and
Partner and Head of OT Cybersecurity
KPMG in Argentina

While Operational Technology (OT) Cybersecurity has secured its place on the agendas of most industrial Chief Information Security Officers (CISOs), it remains, in many cases, an isolated concern within the broader cybersecurity landscape. Despite significant strides made by numerous companies in recent years, there is an ongoing journey towards greater maturity and integration in this domain. The findings from this year's collaborative effort between (CS)^{2}AI and KPMG International shed light on both the progress we've achieved and the persistent challenges we face.

Regarding maturity, nearly half (49%) of the organizations surveyed continue to operate at maturity levels 1 and 2, which encompass firefighting and basic management, respectively. While the necessity of establishing an OT cybersecurity program is no longer a novel concept, and despite the availability of mature technological solutions, there hasn't been a substantial leap in maturity observable in the survey results. One notable factor likely impeding progress is the scarcity of skilled resources, a well-known challenge with which the field has been struggling for years.

Despite these challenges and the relatively gradual pace of development, our discussions with industry executives reveal a heightened awareness of the risks associated with OT cybersecurity. Whereas it might have been a tough sell in years past, cybersecurity conversations with top-level executives increasingly revolve around OT cybersecurity as a focal point. This signifies a higher level of understanding and recognition of the subject's critical importance. It's not surprising to find that executives are also more willing to engage in crisis simulations and tabletop exercises centered on OT cybersecurity.

We believe that the annual collaboration between KPMG International and (CS)^{2}AI plays a pivotal role in elevating awareness among executive leadership. By drawing from real-world insights provided by practitioners and leaders across the globe, our survey offers an impartial perspective on the global evolution of this field. It aids in informed investment decisions and highlights the growing interest in this area. We believe our joint report serves as a valuable resource for both OT cybersecurity practitioners and leaders, as well as the wider executive community. In this third edition, we reaffirm our commitment to providing an unbiased outlook on the main challenges surrounding OT cybersecurity as perceived by global leaders in the field.

We invite our readers to delve deep into the insights of this year's report, with the hope that our annual endeavor empowers you, whether you're a leader, executive, or practitioner, to make more informed decisions and investments in this domain. We view OT cybersecurity as an ongoing journey with no true ending. This survey, much like cybersecurity itself, is an integral part of this perpetual journey, dedicated to delivering improved insights into this critical field year after year.

Executive Summary

KEY FINDINGS

- Almost half of organizations responding (49%) remain without ICS/OT cybersecurity programs or with only a basic one, lacking established plans, procedures, or capability improvement processes.
- Respondents at different organizational levels revealed quite different priorities for allocation of extra discretionary funds, raising questions of whether their incentives are in alignment and why their goals are different.
- Full monitoring of control system network activity is increasing, with an 80% increase in the past year.
- We assessed the accessibility of many control system components (PLCs, IEDs, RTUs, HMIs, Servers, Workstations & Historians) from business networks, the internet, the cloud, and by integrators/ vendors. There is frequently little difference between organizations with High Maturity programs and those with low ones in this area. In fact, components in High M organizations are often more accessible than in Low Ms.
- Please see page 8 for definitions of High M and Low M.

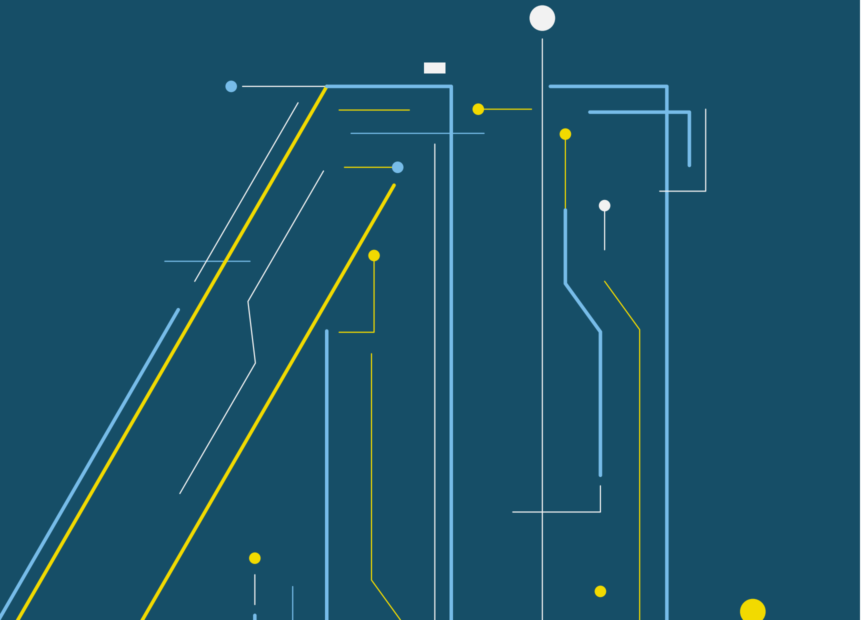
This report is the latest in a series of annual publications, drawn from research by the Control System Cybersecurity Association International (a.k.a (CS)^{2}AI), its community of nearly 34,000 members and dozens of Strategic Alliance Partners (SAPs). Based on decades of cybersecurity survey development, research and analysis led by (CS)^{2}AI Founder and Chairman Derek Harp and Co-Founder and President Bengt Gregory-Brown, the (CS)^{2}AI team invited our global members and thousands of others in our extended community to participate. Asking 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 of individuals and business operations of enterprises worldwide. Over 630 of them responded to our primary survey and many more participated in additional data gathering efforts we run via our ongoing (CS)^2 educational programs.

This pool of data, submitted anonymously to ensure the exclusion of considerations which might otherwise influence participant responses, offers insight into the real-world experiences of individuals and organizations responsible for CS operations and assets beyond what could fit into this report.
We hope the details we have selected to include provide the decision support tool our readers require.

Survey Objective and Methodology

This Report uses the overarching term ‘Control Systems’ (CS) and ‘Operational Technology’ (OT) to refer to any/all systems that manage, monitor and/or control physical devices and processes. CS, (CS), and OT should therefore be understood 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 Cybersecurity field, profession, programs and workforce.



The (CS)^{2}AI-KPMG Control System Cybersecurity Annual Report series was launched in 2019 to produce informative decision-making tools for all parties involved with the work of securing control system assets and operations, whether end-users or vendors, executives, managers or operational resources, anywhere in the world.

This report is a collaborative effort of these entities:

- (CS)^{2}AI: As the project originator, (CS)^{2}AI held the primary role in planning, leading and implementing the project, including data collection and analysis and authoring this report.
- KPMG International: As the Title Report Sponsor, KPMG provided primary funding and organization resources support to augment (CS)^{2}AI’s own capabilities.
- Additional sponsors: non-Title Sponsors Fortinet, Waterfall Security Solutions and Opscura provided additional funding and other resources. (See Appendix D: Report sponsors.)

Pursuant to the objectives stated above, (CS)^{2}AI and our sponsors distributed online surveys to members of the CS/OT cybersecurity community working in the field, collecting key data around CS events, activities and technologies, and details on how organizations are responding to the changing threatscape[1].

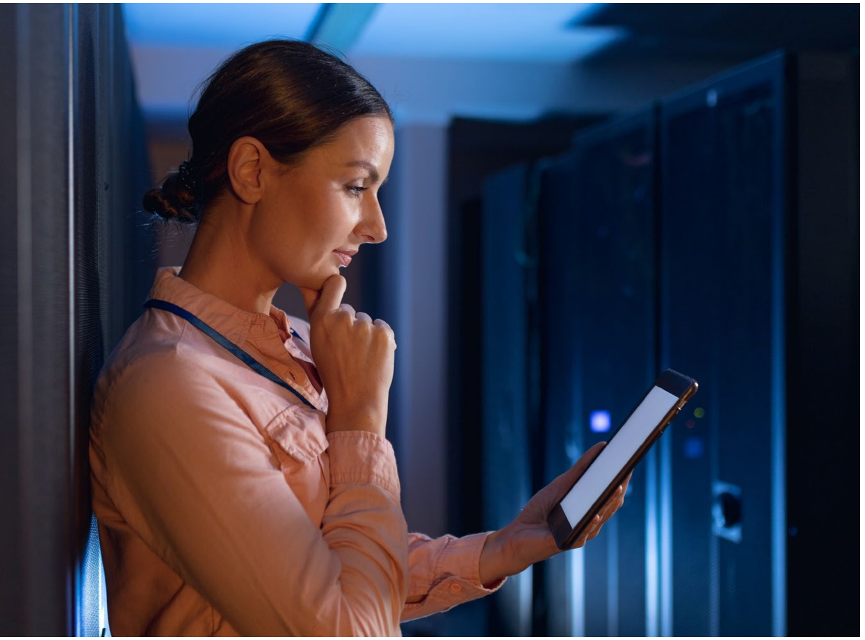
(CS)^{2}AI invited participation from its associated members, known OT security defenders and researchers, distributed the survey through direct invitations and various broadcast media channels, and promoted it on sites serving the CS cybersecurity workforce, with the intent to collect as wide a sample as possible. Respondents self-selected by affirming their current or recent involvement with the (CS)^2 field. They include professionals at all organizational levels: cybersecurity 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.

The ability to parse our participants into different groups and compare their inputs across these groupings associations is key to the insights derived from this annual research project. While we consider survey participants’ (CS)^{2}AI program maturity the most important dimension, we also considered their organizational levels, their regions, and their relationship with (CS)^2 assets (vendors, users, owners, or operators). Of course, we also performed longitudinal analysis and, where we found interesting trends, we share those as well.

[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.

(CS)² Programs

A measure of respondent organizations' (CS)² program maturity is key to much of our annual analysis, providing a metric to evaluate much of the other data they provide. What are organizations with more mature programs[2] doing differently or more often than others? Where we find significant differences between the responses of these groups we bring these to our reader's attention. We asked each participant to choose which of the following descriptors best fit the situation in their organization.



Levels of Control System Cybersecurity Program Maturity

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.

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 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 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 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.

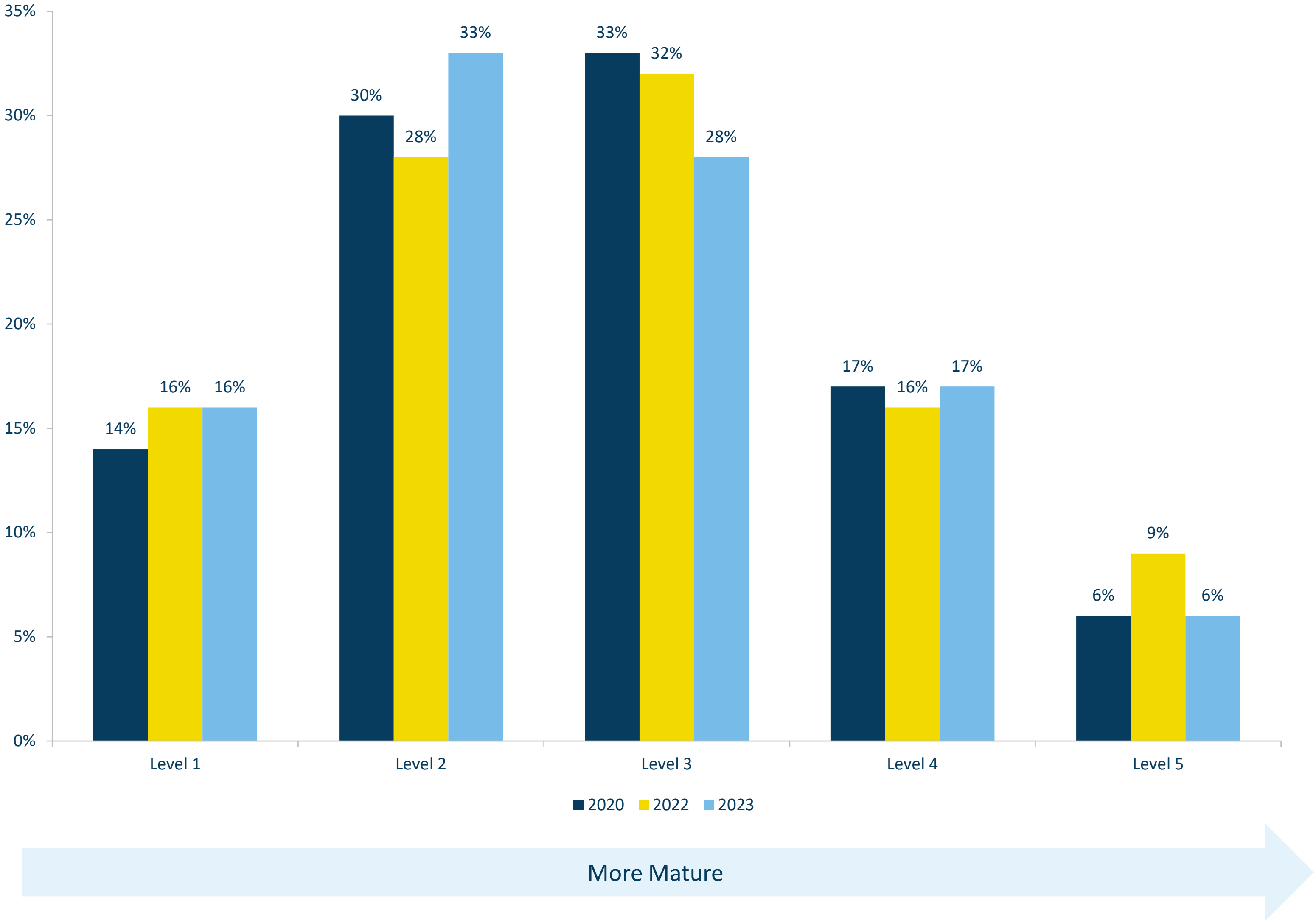
Passive Defense.

[2] The High M group includes all respondents self-rated at Level 4 or 5; the Low M group those identifying as Level 1 or 2.

(CS)² Program Maturity – Longitudinal Analysis

The number of participants in each ranking has shifted over (Note the rise of Level 2 responses this year) but we found little change in the sizes of the aggregated High M/Low M groups over the years. Participants continue to rate their own (CS)² programs consistently. Our team considers this supportive of the validity of this self-evaluation. We use this extensively in our analyses of contrasts and similarities between the High Maturity (Levels 4 and 5) and Low Maturity (Levels 1 and 2) groups to base recommendations to base recommendations on.

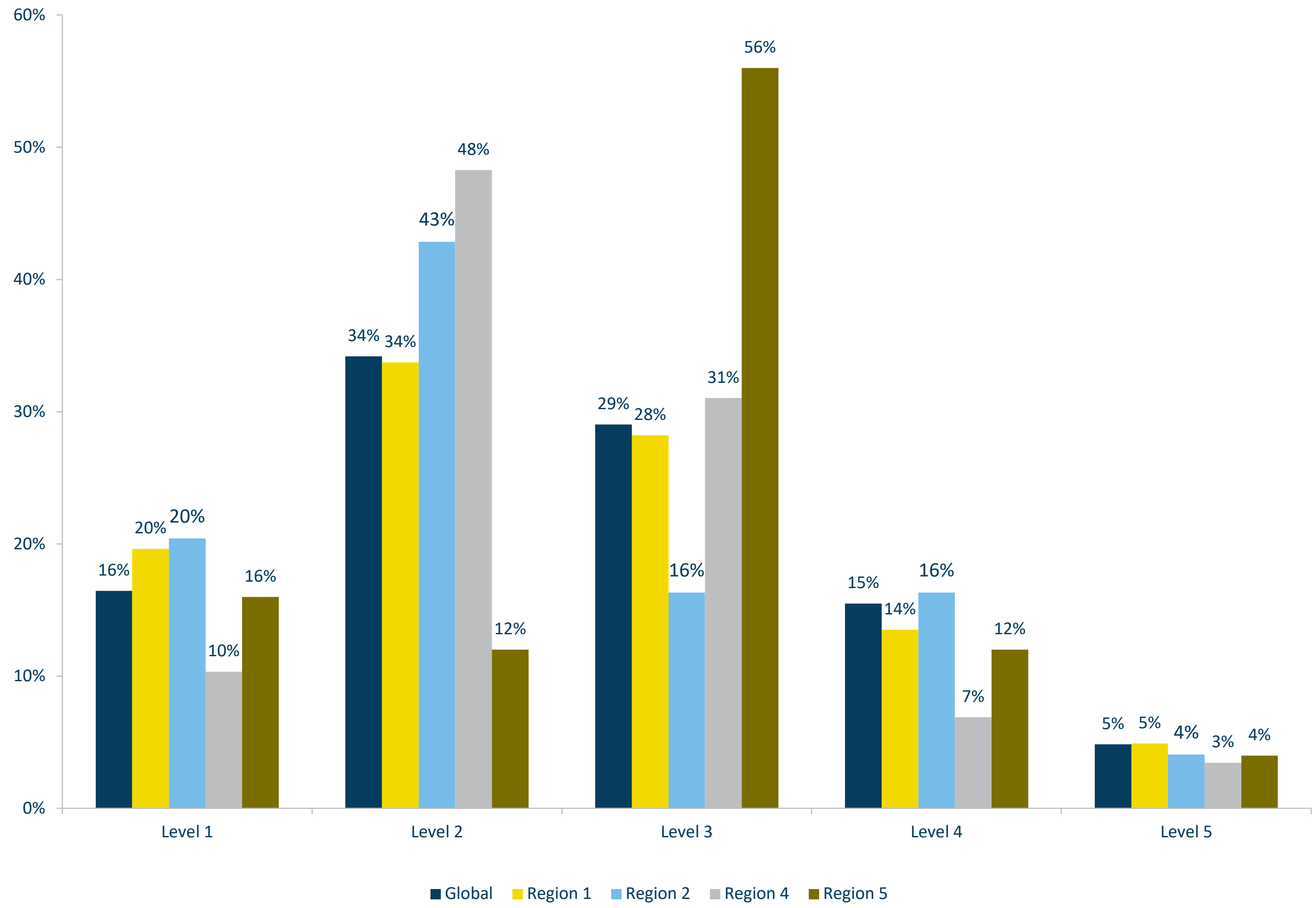
Which of these best describes your control system cybersecurity program?



Client (CS)^2 Program Maturity – Regions[3]

Consultants (vendors, service providers, integrators) around the world do not share the same view of the maturity of their client's (CS)^2 programs. Different regions have different views with respect to maturity. Region 2 self-scores lower, with 63% in Levels 1 and 2, Region 4 centers around Level 2 (48%), and Region 5 centers around level 3 (56%). Regions 3, 6 and 7 lacked sufficient participation to include in this analysis (see footnote[3]).

Which of these best describes the control system cybersecurity programs of your clients?



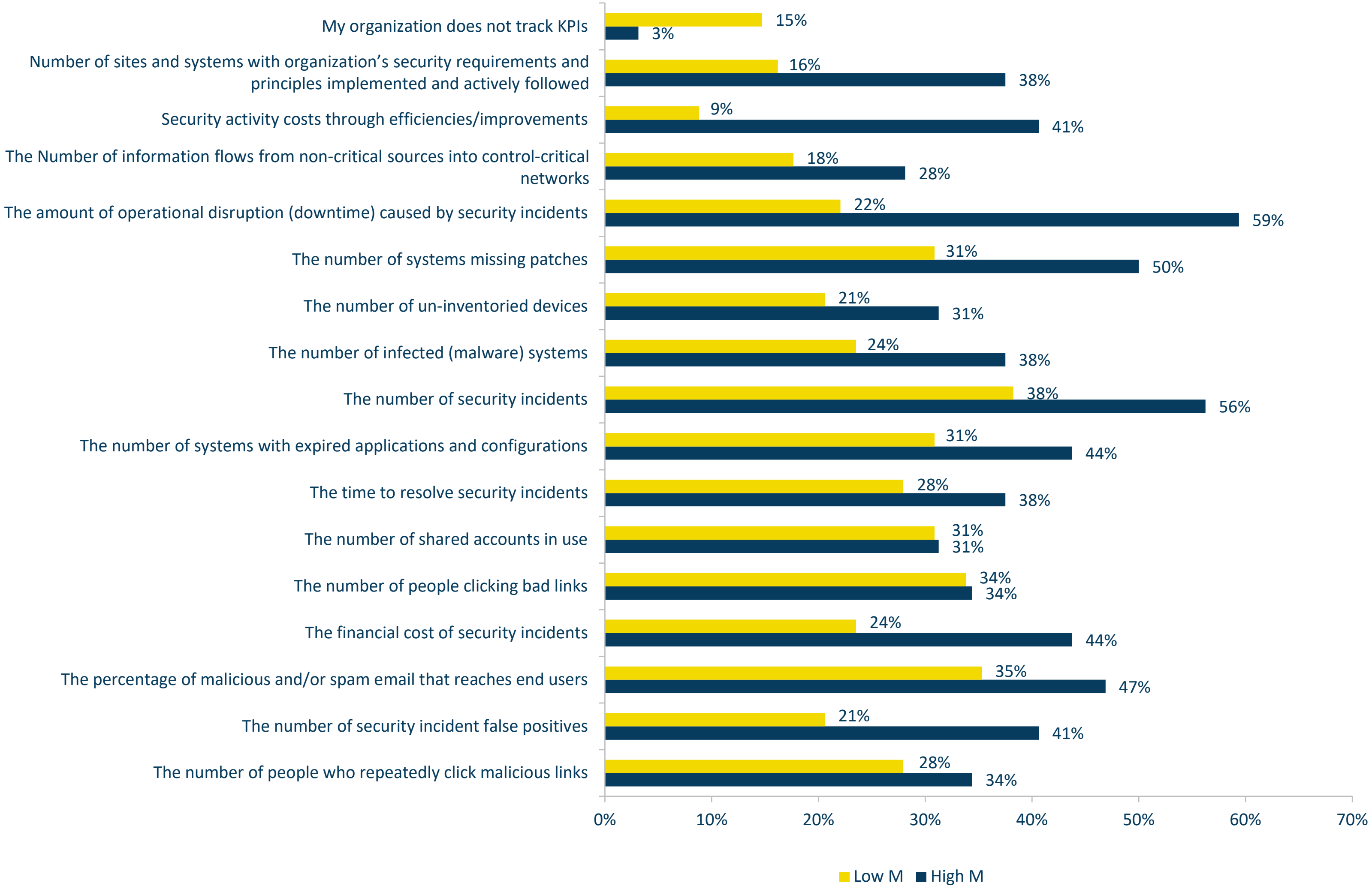
[3](CS)^{2}AI is organized into seven Regions.

1) North America;
2) Europe (Central, Western, Northern and Southern);
3) Eurasia;
4) Indo-Pacific;
5) Middle East-North Africa;
6) Southern Africa;
7) Latin America-Caribbean

(CS)^2 Key Performance Indicators (KPIs) – High M vs Low M

While the greater tracking of some Key Performance Indicators (KPIs) by more mature programs is unsurprising (e.g., the nearly five-fold increase in *Security Activity Costs Through Efficiencies/Improvements* at 8% Low M vs 40% High M is expected since this is a core activity used to improve any program over time), we consider it concerning that so many programs track so little. We had approximately twice as many Low M respondents as High M this year, and although an encouraging 85.3% of those track some KPIs, most only track a few. We highly recommend these organizations expand their metrics to gain greater visibility into the effectiveness of their security program efforts.

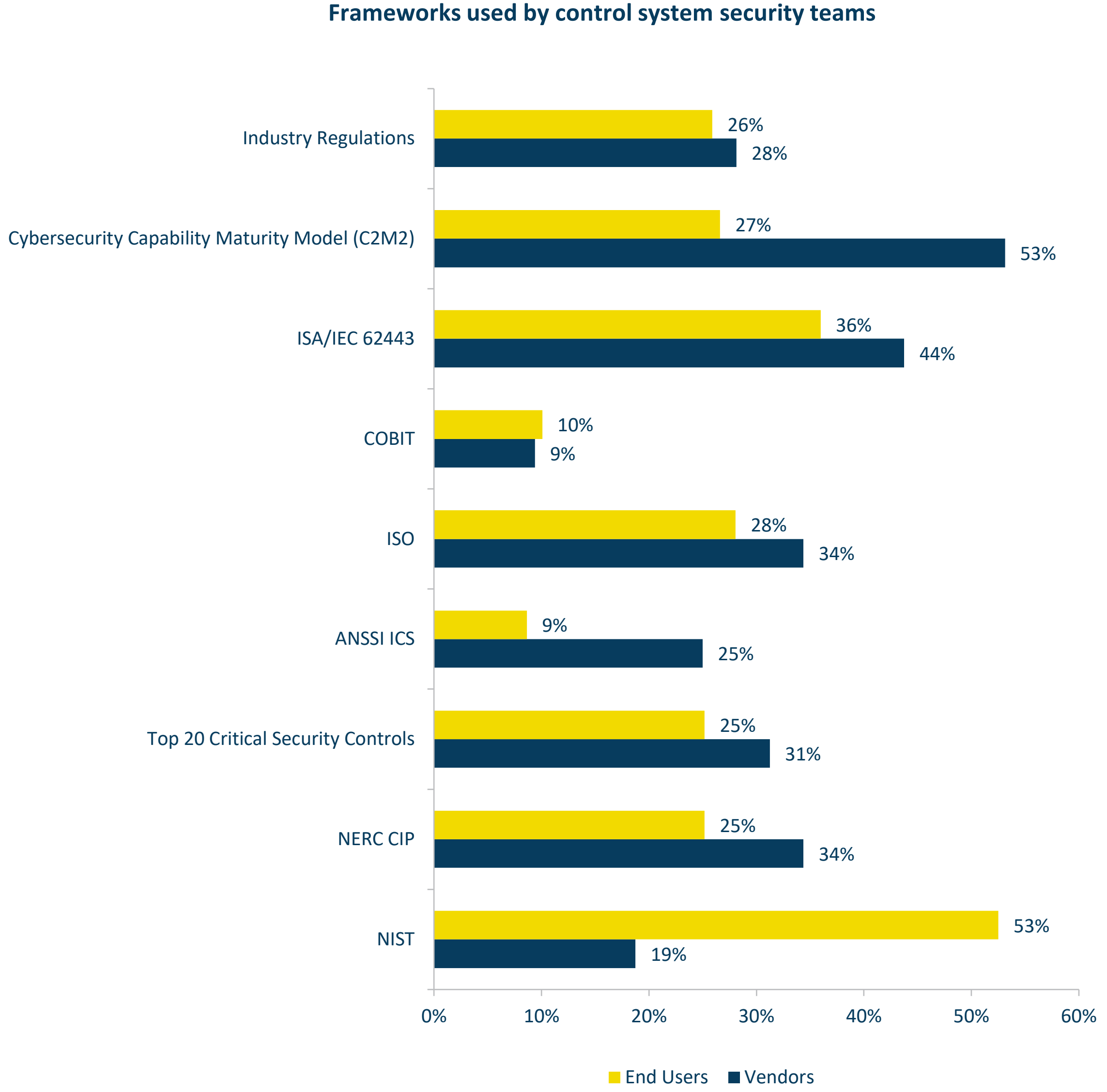
Typical (CS)^2 KPIs monitored by organizations



Security Frameworks in use – End Users vs Vendors

Comparing the views of disparate groups has its detractors, but we consider viewing the perspectives of these two side-by-side useful as they both have responsibility for the security of controls systems, and we see here that while the standouts are the *C2M2* and *NIST*, the former for Vendors and the latter for End Users. Reported use of the *C2M2* by End Users is effectively matched with last year's overall data (2022-*C2M2* 26.3%) but that report did not differentiate between End Users and Vendors.

In the latest iteration of our survey, Vendors responded separately and report using the *C2M2* almost exactly twice as often (End Users *C2M2* 26.6% vs Vendors *C2M2* 53.1%). *NIST* usage does not appear to have changed as much, with last year's All-Participants response of 45.7% (2022), as an averaging of the two groups falls into that range.

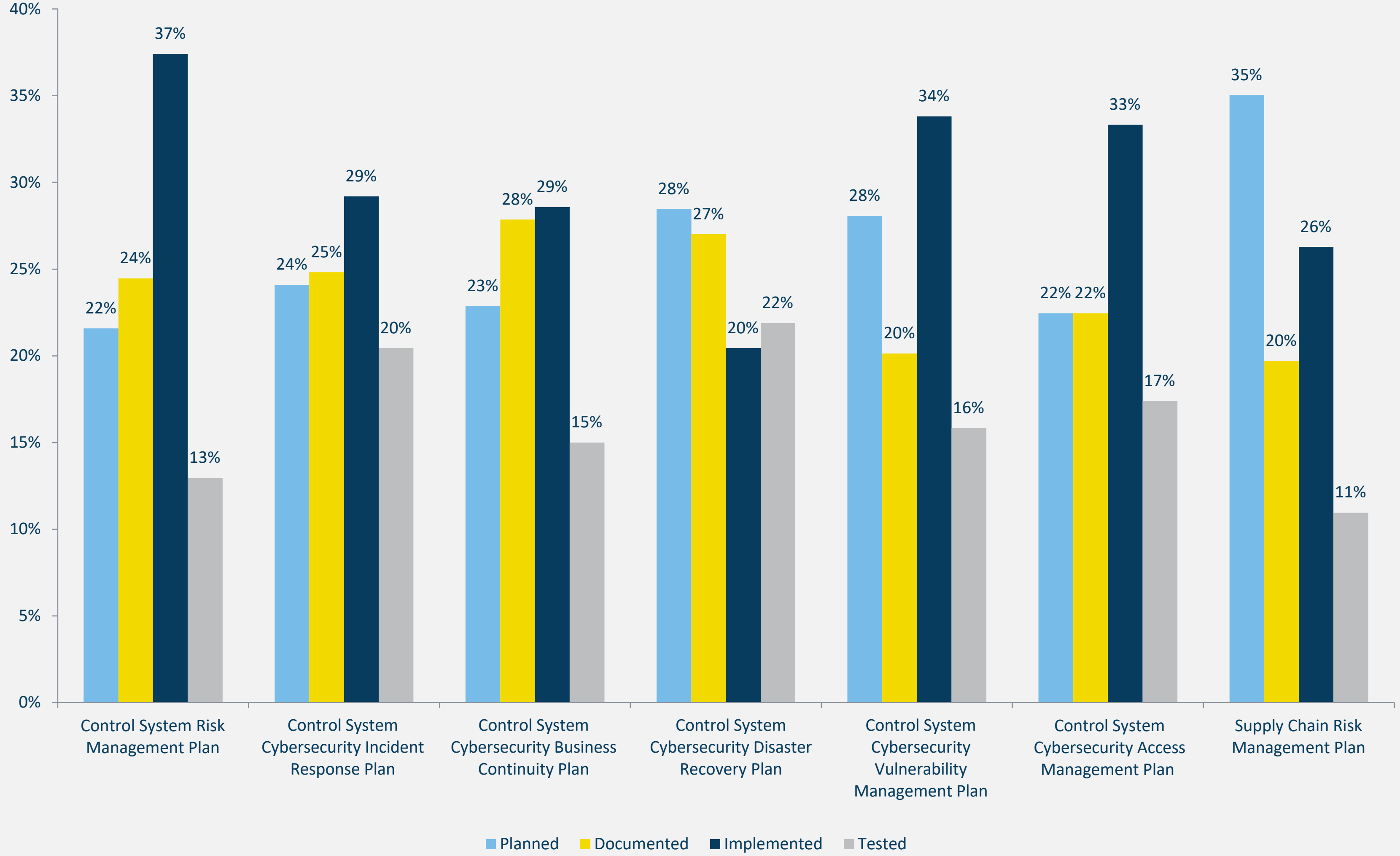

Frameworks used by control system security teams
Industry Regulations 26% 28%
Cybersecurity Capability Maturity Model (C2M2) 27% 53%
ISA/IEC 62443 36% 44%
COBIT 10% 9%
ISO 28% 34%
ANSSI ICS 9% 25%
Top 20 Critical Security Controls 25% 31%
NERC CIP 25% 34%
NIST 53% 19%
0% 10% 20% 30% 40% 50% 60%
End Users
Vendors

Framework	End Users	Vendors
Industry Regulations	26%	28%
Cybersecurity Capability Maturity Model (C2M2)	27%	53%
ISA/IEC 62443	36%	44%
COBIT	10%	9%
ISO	28%	34%
ANSSI ICS	9%	25%
Top 20 Critical Security Controls	25%	31%
NERC CIP	25%	34%
NIST	53%	19%

Organizational Plans – End Users

It is our team's view that every organization with (CS)^2 responsibilities should manage its risks comprehensively, with documented, implemented and tested plans and procedures to reduce incidents and minimize impacts on their company, employees, and clients. With plans fully *Implemented* and *Tested* being the gold standard, the large numbers of respondent companies with plans mostly only *Documented* or *Planned* is concerning as they are not procedurally prepared to manage and respond to the types of events these plans are intended for.

Current state of organizational plans



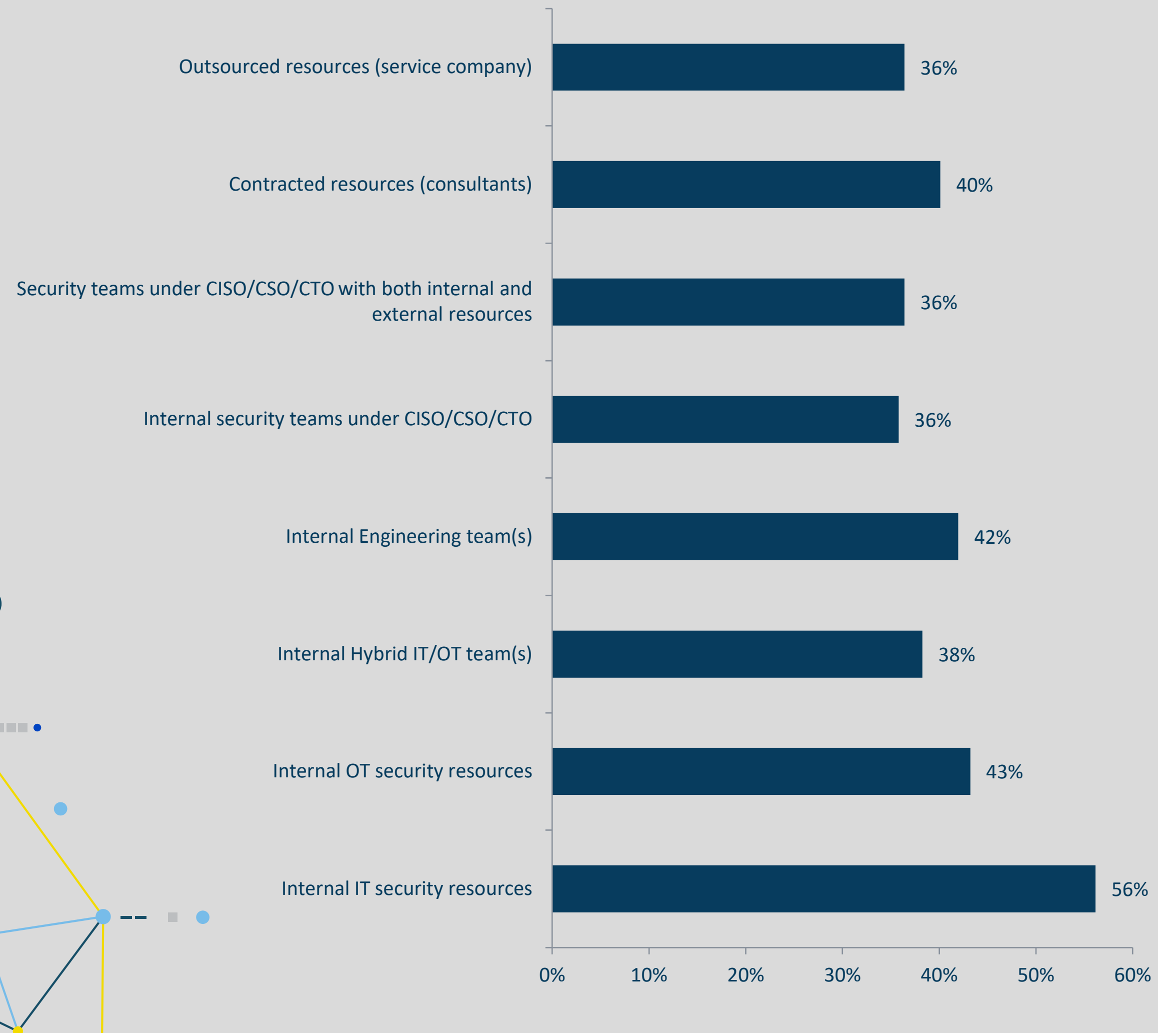
(CS)² Services – End Users

Where do organizations go to find the aid they need to protect their (CS)² assets, people, and operations? Everywhere they can, according to our respondents. The standout response of *Internal IT Security Resources* (56.2%) suggests that OT cybersecurity is being driven by IT groups in most organizations, with the concomitant likelihood that IT security methods and technologies are being applied in these environments.

> *Many CISOs are intimidated by OT security projects because the cure for cybersecurity in plants is worse than the disease. I used to be a CISO, so I understand. OT requires prioritization for the process whereas IT prioritizes security over downtime.*
>
> *We are losing the war against bad actors largely due to inaction. Securing OT using traditional IT tools is costly not just because of the consulting, planning, and equipment, but most of all, the debilitating amount of downtime.*
>
> *Operators have to make painful decisions to reconfigure their networks, replace working (but end of life) assets, and to deploy security teams - all while shutting down their plant for days if not weeks. We are forcing them to make the hard decision to NOT move forward with cybersecurity for their operating lines and facilities. The downtime in many cases is more expensive than the whole security project itself.*
>
> *Let's partner to make securing and maintaining our plants and factories less time-intensive, more affordable and, most importantly, with far less (if not zero) downtime.*
>
> *Together, we can remove the traditional IT barriers and join together to secure our world's infrastructure.*

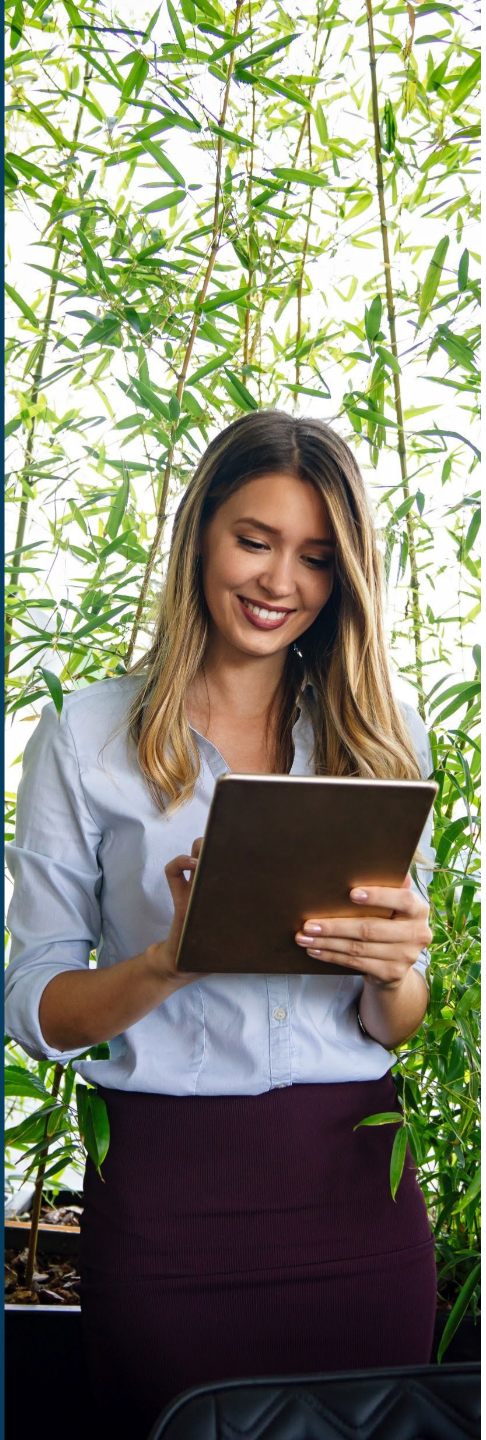
Brian Brammeier,
CEO of Opscura

Sources of control system security services used by organizations

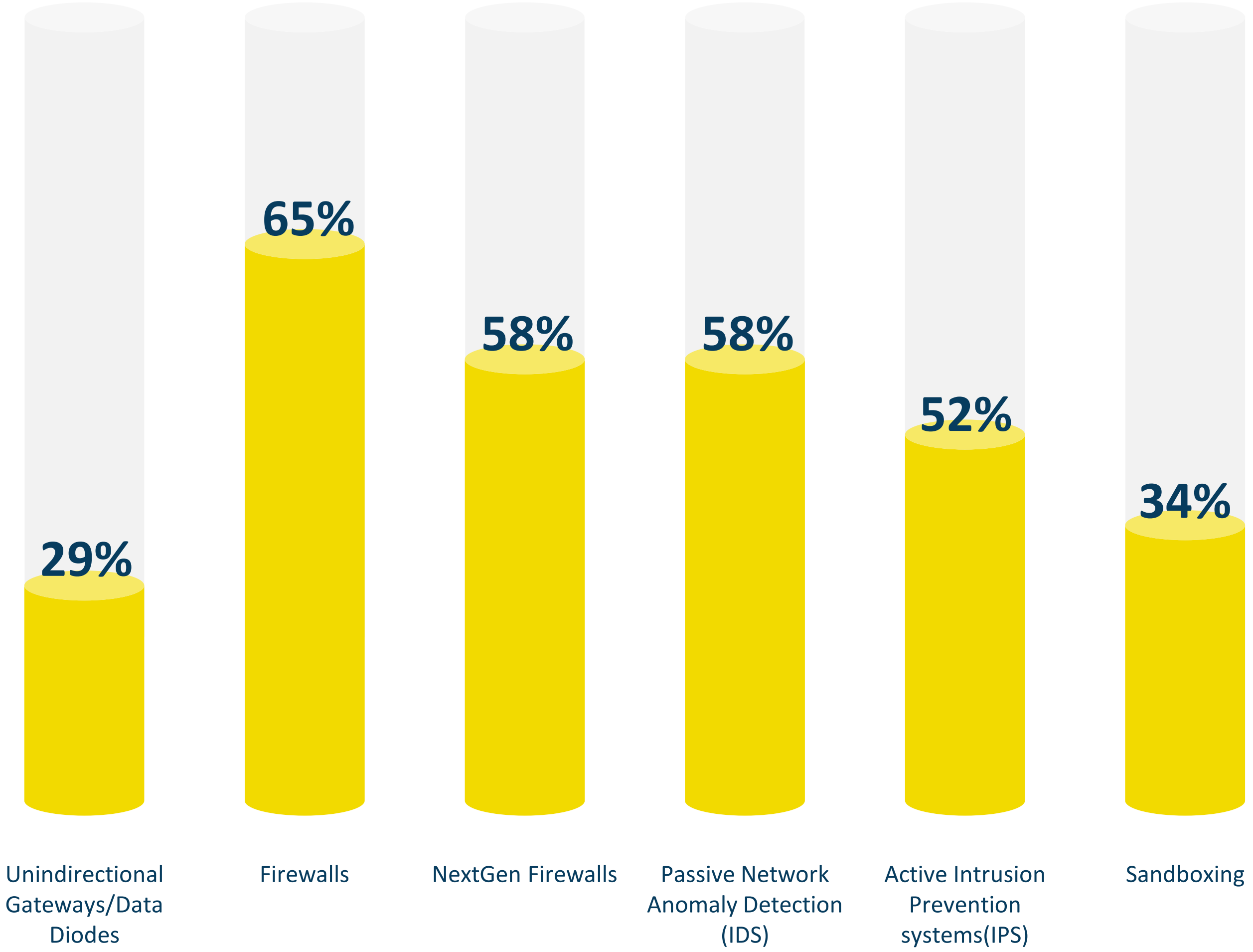


(CS)² Technologies – End Users

Not all technologies fit the needs and requirements of all environments. That said, we consider it likely that the organizations owning and/or operating ICS/OT assets who indicated they have *Passive Network Anomaly Detection* (58% IDS) would be well served by implementing *Active Intrusion Prevention Systems (IPS)* into use. NextGen Firewalls have similarly wide utility and should be protecting more ICS environments from threats originating on their enterprise or other external networks. *Unidirectional Gateways/Data Diodes* have had a reputation for complexity and cost due to their use primarily in the highest security environments (e.g. nuclear power plants), but we have recently seen both of those factors diminish and expect to see more deployment in the future.



Security technologies used by organizations to protect controls system assets against cyber threats

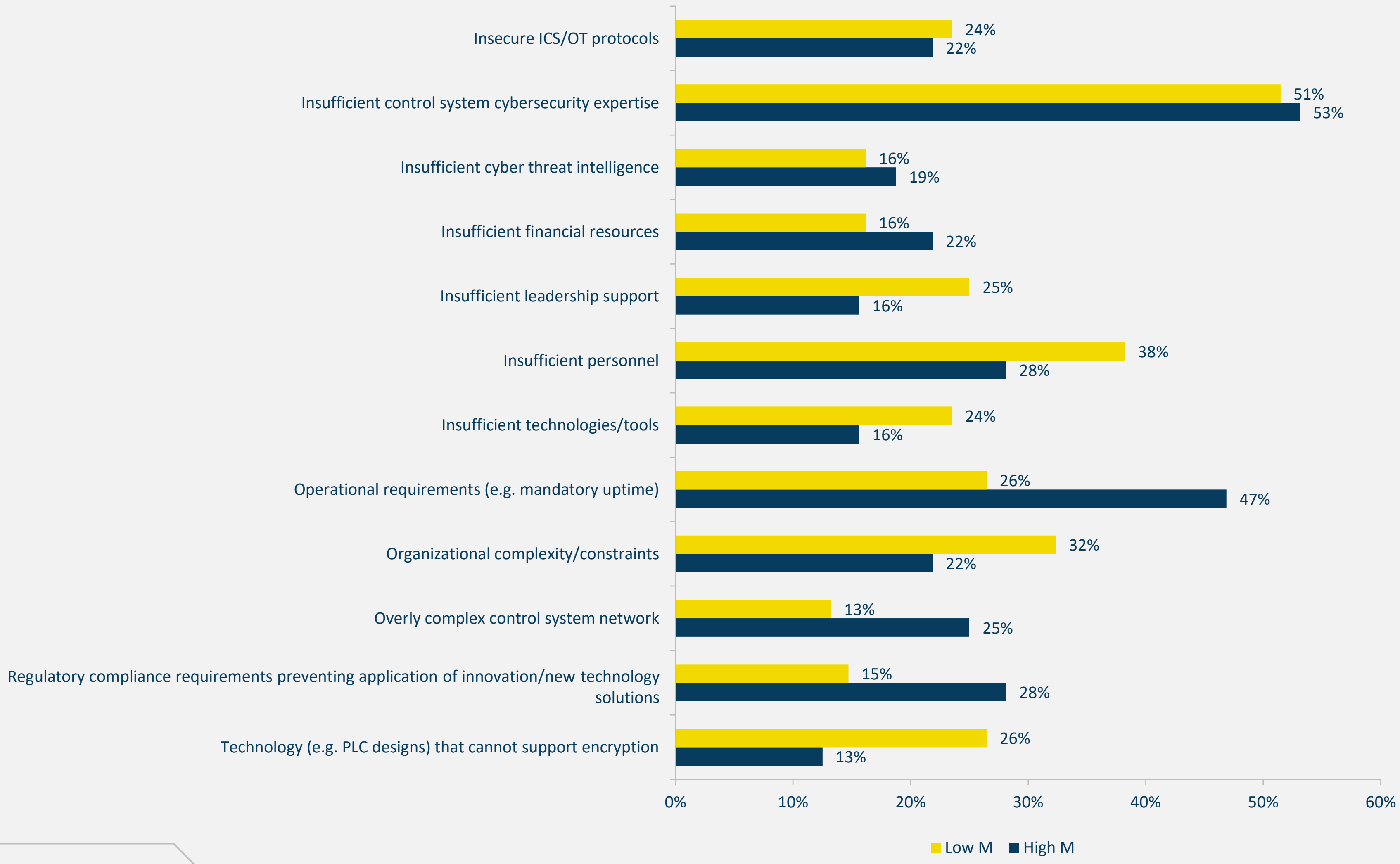


Obstacles to Reducing the (CS)^2 Attack Surface

(CS)^2 Obstacles – High M vs Low M

We annually compare conditions and perspectives between distinct groups; here we consider what they consider their greatest obstacles through the lens of respondent organizations' control system cybersecurity programs relative maturity (High M vs Low M) to identify what is working, what isn't, and how things change as organizations progress on their journeys of improving their security. In the table above we see that some obstacles are widely agreed upon, such as *Insufficient Control System Cybersecurity Expertise* (Low M 51.5%, High M 53.1%) and *Insecure ICS/OT Protocols* (Low M 23.5% vs High M 21.9%), while others differ widely, such as *Technology That Cannot Support Encryption* (Low M 26.5% vs High M 12.5%) and *Insufficient Leadership Support* (Low M of 25.0% vs High M 15.6%). These suggest that more mature programs have overcome some of the hurdles that less mature programs are still struggling with.

What are the greatest obstacles to reducing the (CS)^2 attack surface?

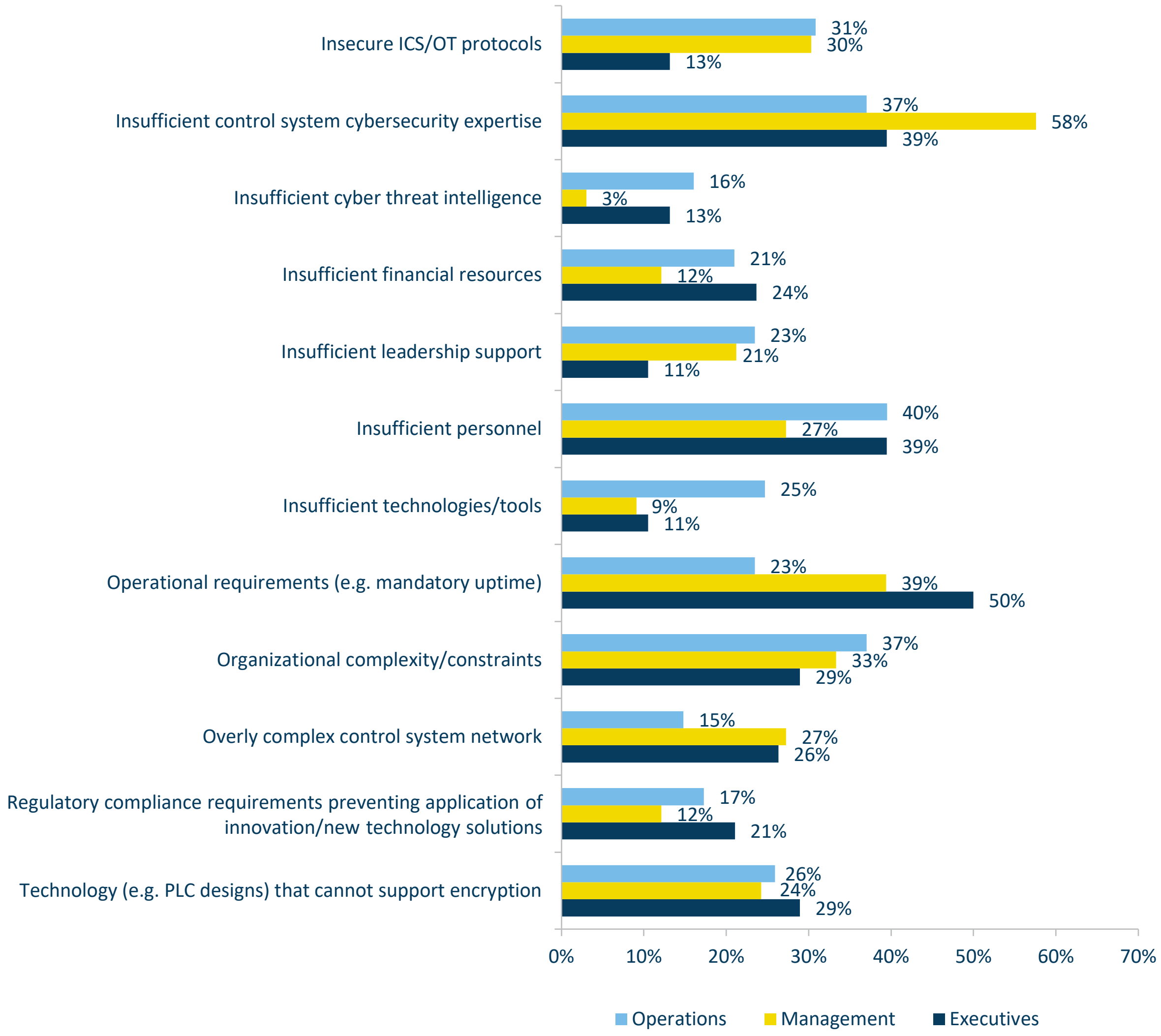


$(CS)^2$ Obstacles – Organizational Level[4]

It is very unlikely that any one individual could have both a complete overview and all details of a modern control system environment, and differences in individuals' views inevitably lead to differences in their perceptions of what needs to be done. Here we see the Executive consensus that *Operational Requirements* (50.0%), *Insufficient Personnel* (39.5%) and *Insufficient $(CS)^2$ Expertise* (39.5%) are the largest obstacles partly aligns with Operations personnel (this group's highest being *Insufficient Personnel* 39.5% and *Insufficient $(CS)^2$ Expertise* 37.0%), but Ops believes *Operational Requirements* much less of a hurdle (6th on Operations list at 23.5%). Management disagrees with one or both parties frequently, highlighting the importance of knowing the role of end users within their organization when we support them with addressing their issues.

[4] The number of participants responding to each question in our surveys varies. At times this results in insufficient representation from a particular subset of participants for valid statistical analysis. In the case of breaking down our data by participation from different levels of their organizations, we received too few Leadership-level respondents to include them in some charts.

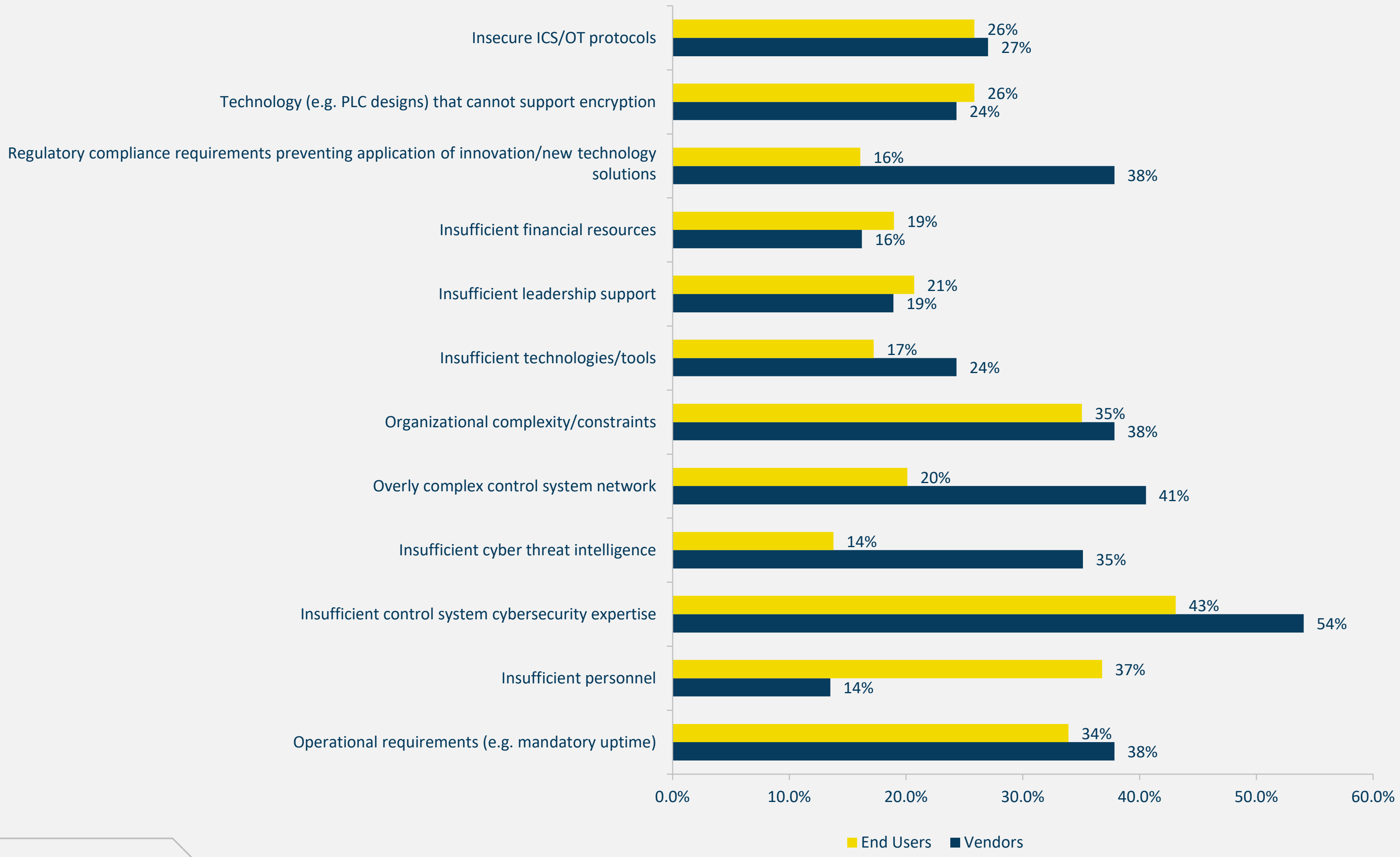
What are the greatest obstacles to reducing the $(CS)^2$ attack surface?



(CS)² Obstacles – End Users & Vendors

Our team found many of the differences in the perspectives of End User and Vendor respondents interesting. Do these derive from their ownership/operation of the control systems versus production/monitoring of OT assets, distinct resources available to them, varied fiscal responsibilities, or some combination of factors? That vendors identified *Regulatory Compliance Requirements, Overly Complex Control System Networks,* and *Insufficient Cyber Threat Intelligence* as top obstacles at two to three times the rate that end users did is noteworthy. The only similar ratio from the end users is their view of *Insufficient Personnel* (End Users 36.8% vs Vendors 13.5%). We advise Vendors to note what their End User clients identified as the greatest obstacles in order to best help them overcoming those barriers.

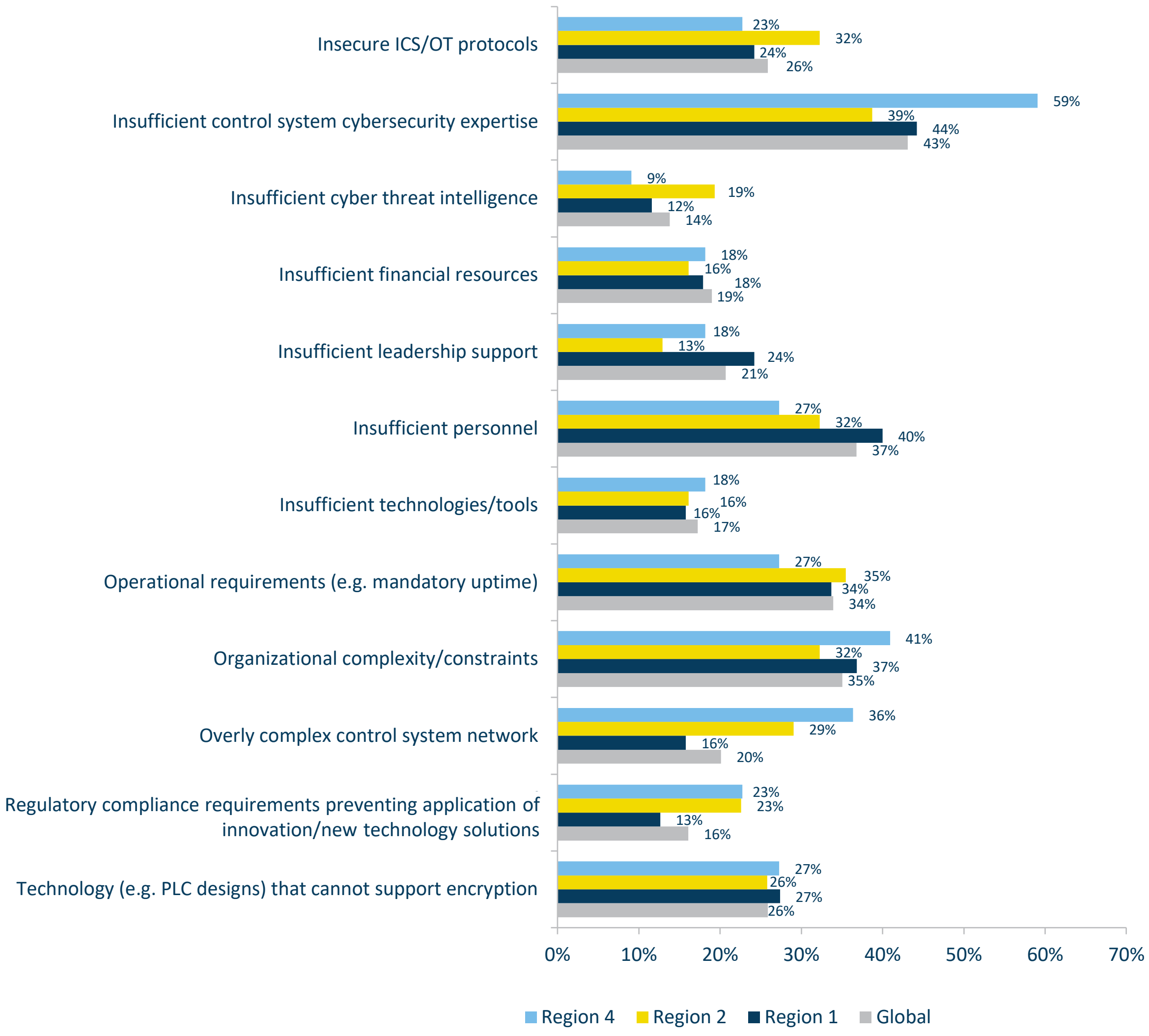
What are the greatest obstacles to reducing the (CS)² attack surface?



(CS)^2 Obstacles – Regional Analysis[5] [6]

For our final look at security obstacles we searched for differences between respondents from different regions of the globe. Control Systems worldwide are largely built upon common technologies, so we expected some degree of uniformity of responses to this question regardless of geographic location and, in fact, this chart shows less differentiation than many in this report. One notable distinction is the Region 4 (APAC) identification of *Insufficient Control System Cybersecurity Expertise* (59.1%) 15 points higher than Region 2, 1, or Global. Respondents in Regions 2 (Europe, Central, Western and Northern) and 4 (APAC) are also more concerned with *Overly Complex Control System Networks* than the rest of the world (R2 29.0%, R4 36.4%, vs Global 20.1%)

What are the greatest obstacles to reducing the (CS)^2 attack surface?



[5] Just as in our analysis of responses by participant organizational level, some regions lacked sufficient representation for valid analysis. The tables below show only those regions with sufficient participation to include, as well as the Global (All respondents) for comparison.

[6] (CS)^{2}AI is organized into seven Regions. 1) North America; 2) Europe (Central, Western, Northern and Southern); 3) Eurasia; 4) Indo-Pacific; 5) Middle East-North Africa; 6) Southern Africa; 7) Latin America-Caribbean

(CS)^2 Spending and Budgets

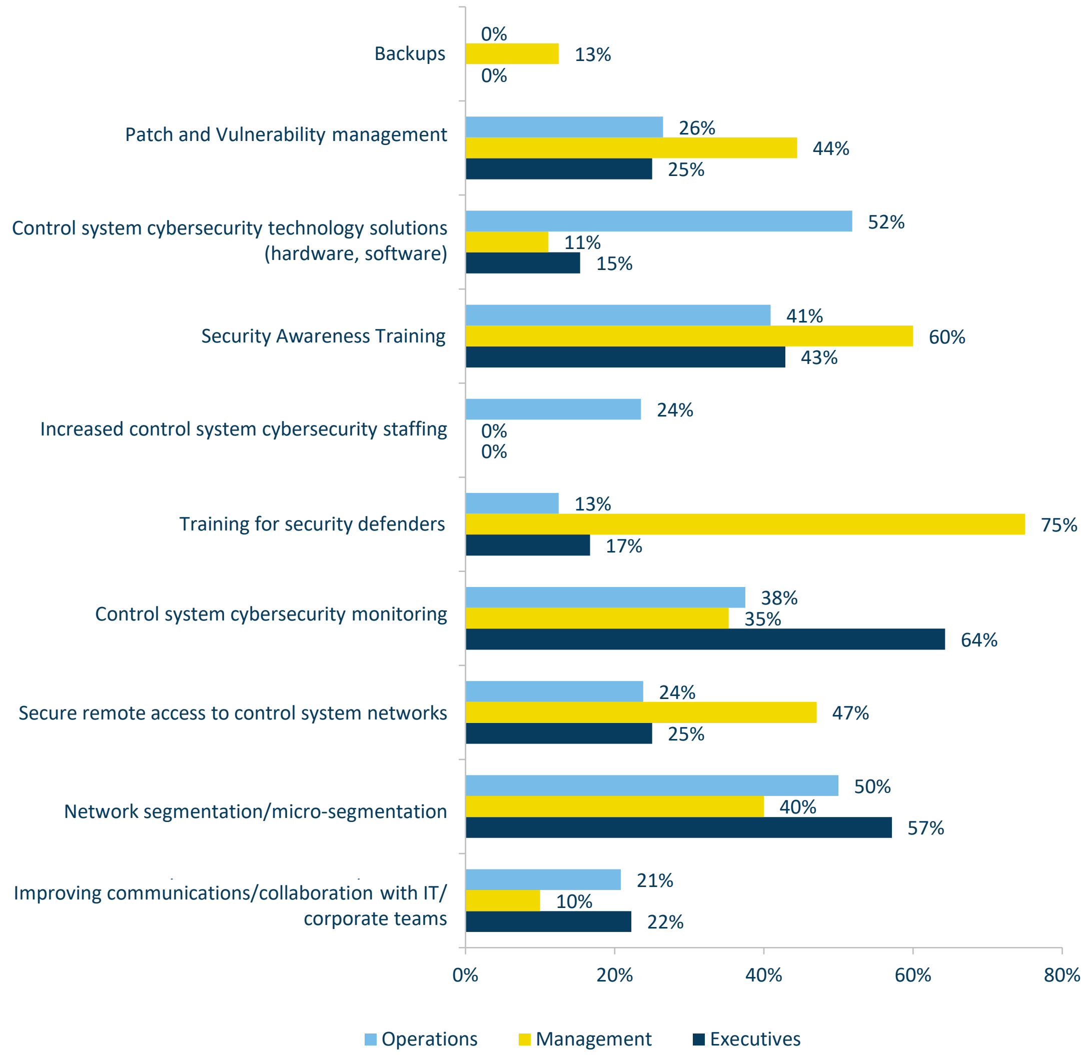
Top (CS)^2 ROI – Organizational Level[7]

The (CS)^{2}AI team and our many speakers are familiar with questions of how to get executive backing for security needs, particularly segmentation projects, which require impact analysis and, in some cases, significant network re-architecture work, so it is good to see that most participant Executives recognize the ROI of implementing this in their organizations (57.1%), fundamental to both security and resiliency. We see as even more positive their support for (CS)^2 monitoring (64.3%) after years of SME arguments that visibility is step 1 in any security improvement program. Respondents in Management, on the other hand, have found their best ROI in Training, whether for *Security Awareness* (60.0%) or *Security Defenders* (75%).

Our team believes it important to draw attention to the fact that none of the Executives or Management participants consider *Increased Control System Cybersecurity Staffing* a top ROI (0% for both groups) despite 27-39% of them identifying *Insufficient Personnel* (See Chart (CS)^2 Obstacles – Organizational Level) among their greatest obstacles to improving their (CS)^2 situations.

[7] Too few Leadership-level respondents answered to include them in this analysis.

Top ROI area for (CS)^2 investments



Top (CS)² ROI
High M vs Low M

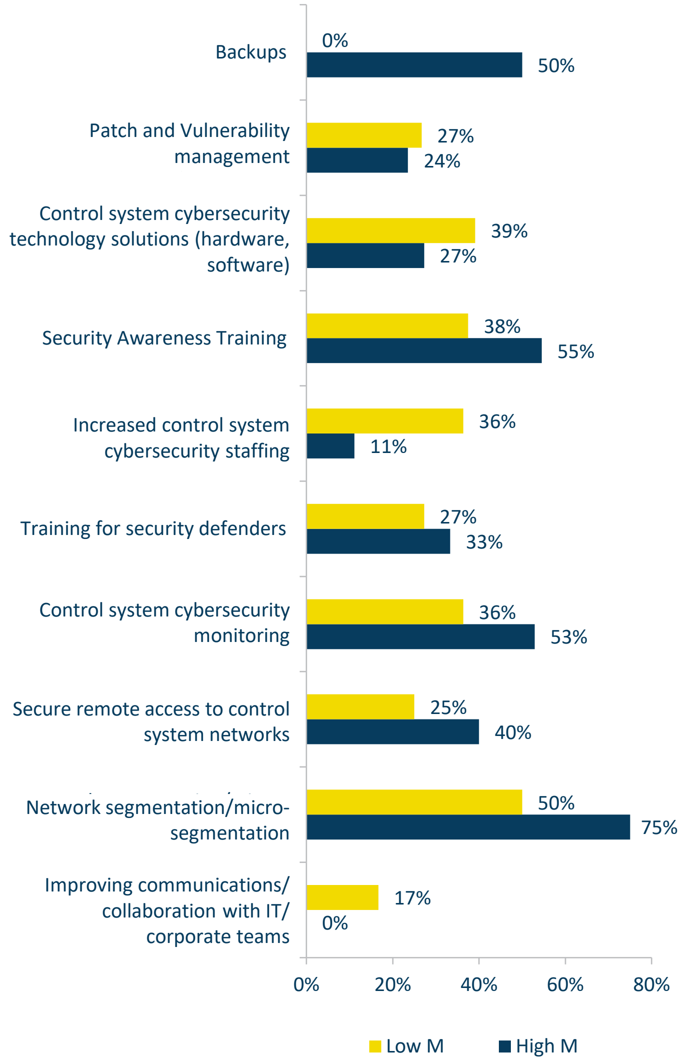
Compared to their perspectives on security obstacles to overcome, there is more agreement between security programs on where they are finding the greatest Return on Investment (ROI) in their (CS)² expenditures. There are some obvious outliers to note, particularly the Low M emphasis on *Improving Communications/Collaboration with IT/Corporate Teams* (Low M 16.7%, High M 0%) and *Backups*[8] (Low M 0%, High M 50%).

One possibility this suggests is that the most mature programs have already integrated teams and implemented solid backup systems and procedures, of course. The agreement between all groups that their highest ROI is in *Network Segmentation/Micro-Segmentation* is in line with years of research and recommendations to implement this to both improve overall security and reduce impacts of cyber incidents.

[8] A possible indication of the more mature program's experiences during the recent rise in ransomware attacks.

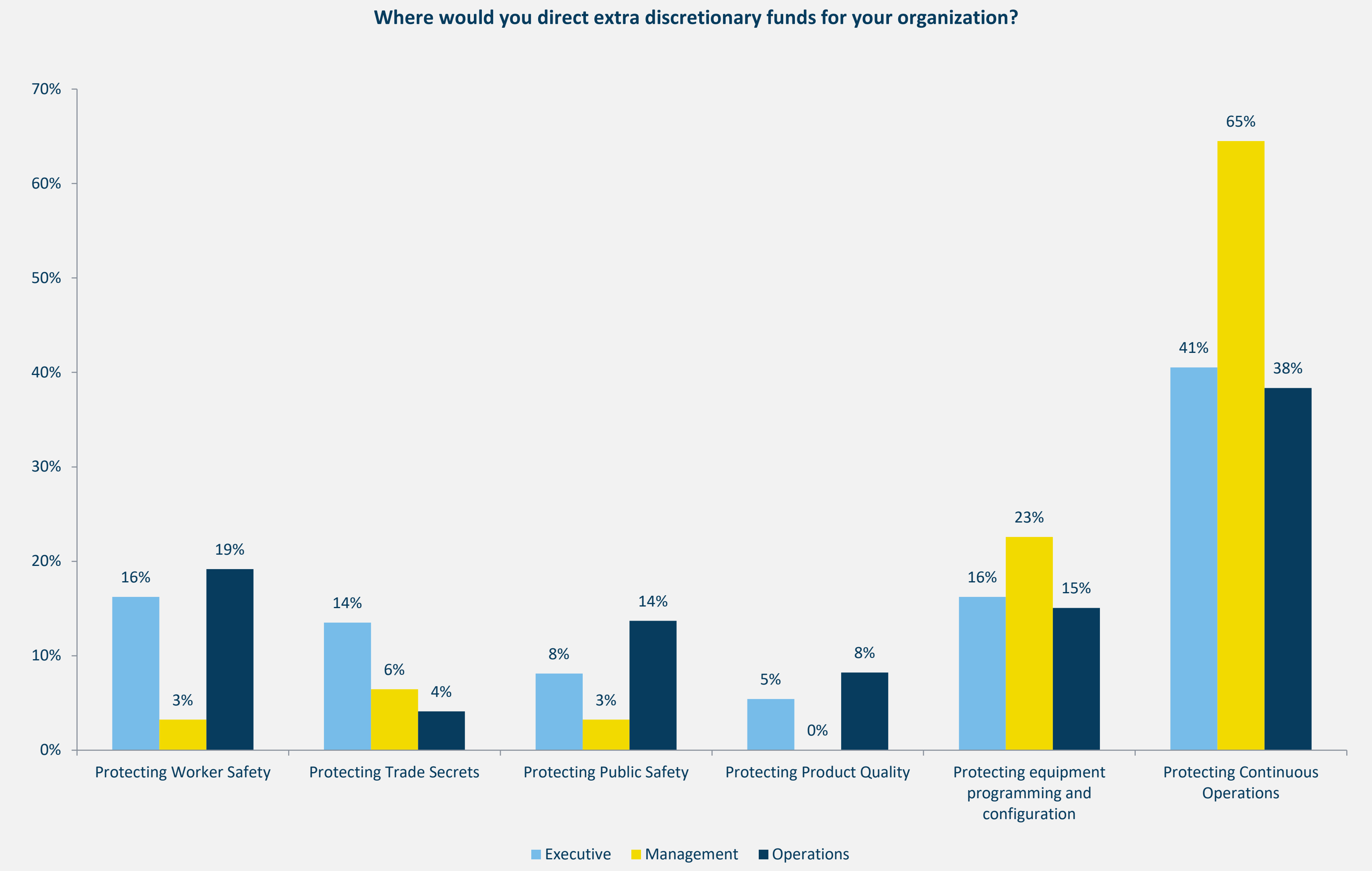
> *50% of respondents believe that network segmentation is the top area for cybersecurity program ROI. The latest thinking in network engineering is that, at consequence boundaries, it is most beneficial to deploy any of several* ***engineering-grade network segmentation*** *approaches. Consequence boundaries include the IT/OT interface, any OT/Internet interface, and any other connection between networks whose worst-case consequences of compromise differ sharply. Results of attack tree analyses show that engineering-grade segmentation at such boundaries reduces a critical network's attack surface by up to 3 orders of magnitude.*
>
> ***Andrew Ginter***
>
> *VP Industrial Security,*
> *Waterfall Security Solutions*

Top ROI on (CS)2 investments (High VS Low M)



Spending Priorities – Organizational Level

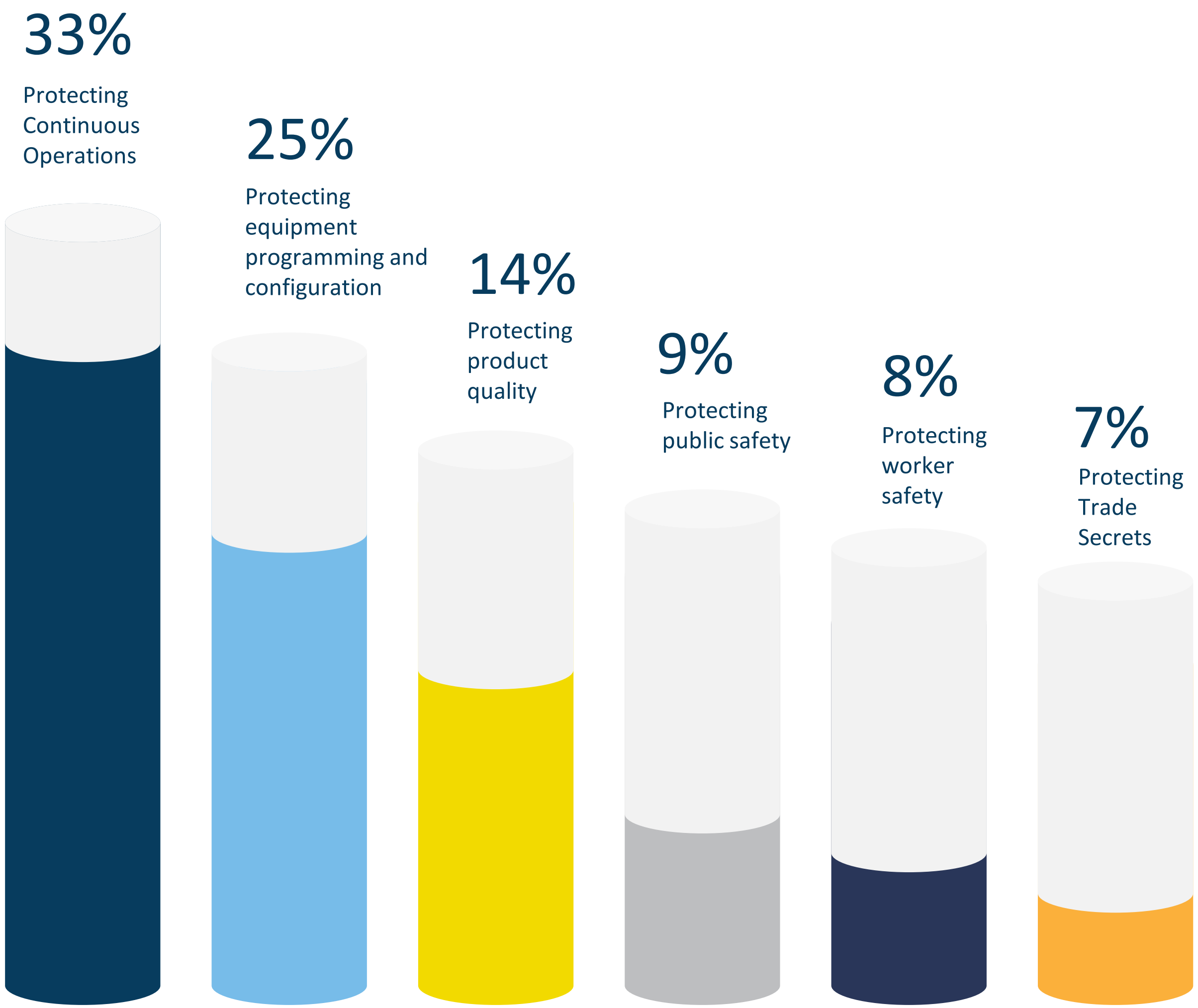
A new question this year, our team found participant responses interesting. Some general agreement aside (such as all levels identifying *Protecting Continuous Operations* as their top target for spending extra funds), the differences do stand out. Note the very low emphasis participants in Management put on *Protecting Public Safety* and *Protecting Worker Safety* (3.2% in both), and none on *Protecting Product Quality*. Given these differences, organizations are encouraged to foster discussions on aligning business priorities.



Vendor Budget Guidance to Clients – Vendors

Many asset owners/operators depend on SME advice from their trusted vendors, so we looked this year at vendor advice regarding resource allocation. Comparing this and the preceding chart, we see the highest emphasis remains on *Protecting Continuous Operations*.

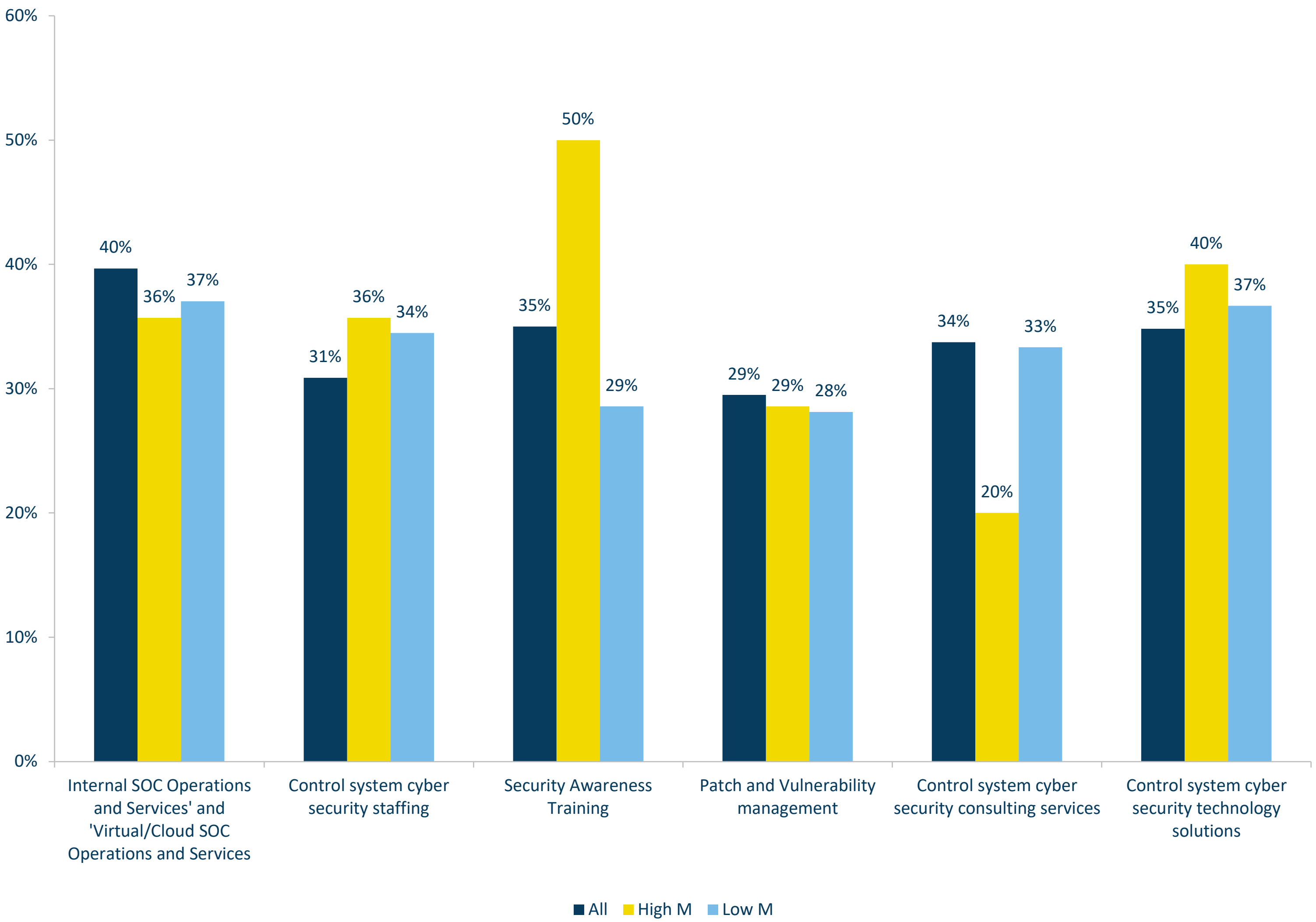
Where would you advise most of your clients to direct more resources in the coming year?



Top $(CS)^2$ Expenditures – High M vs Low M vs All

We have included responses from all participants in these tables for ease of comparison. This allows us to show that the High M group spends significantly more on *Security Awareness Training* (50.0% High M vs 28.6% Low M and 35.0% All) as well as how relatively few of them focus on *Control System Cybersecurity Consulting Services* (20.0% High M vs 33.3% Low M and 33.8% All).

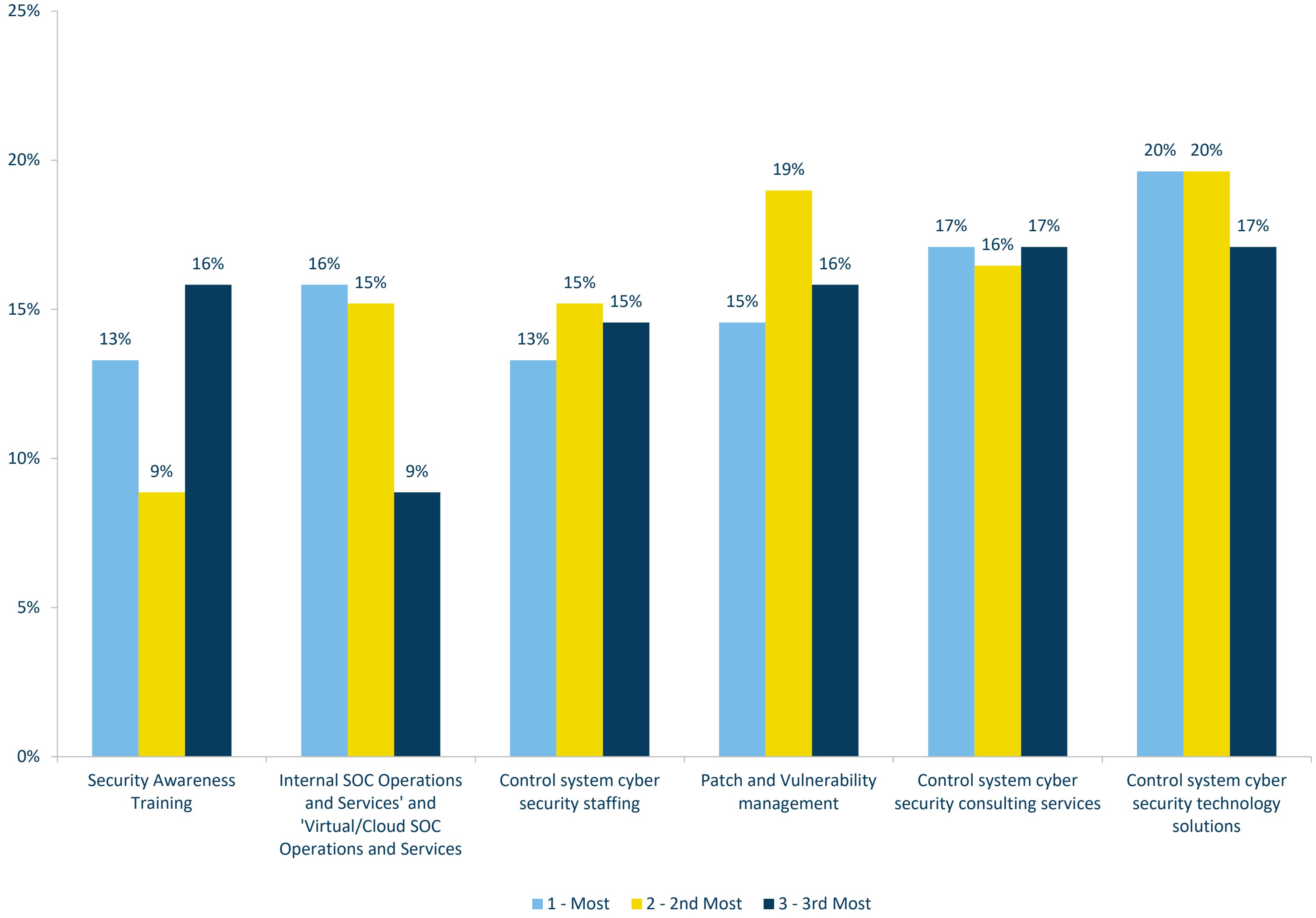
Top $(CS)^2$ expenditure area (High M VS Low M and All)



Top $(CS)^2$ Expenditures – End Users

An additional view into $(CS)^2$ budget priorities beyond the top spend for High and Low M groups, we also asked our End Users to identify the three areas their organizations put their resources into. *Security Technology* and *Security Consulting Services* get the largest slices of the budget pie (totaling 56.3% and 50.6%, respectively). Our team considers it worth investigating whether the relatively low investment in *Control System Cybersecurity Staffing* is a contributing factor to the ongoing demand for workers in this field outstripping the supply.

Top three areas organizations expend the most resources for control system cybersecurity

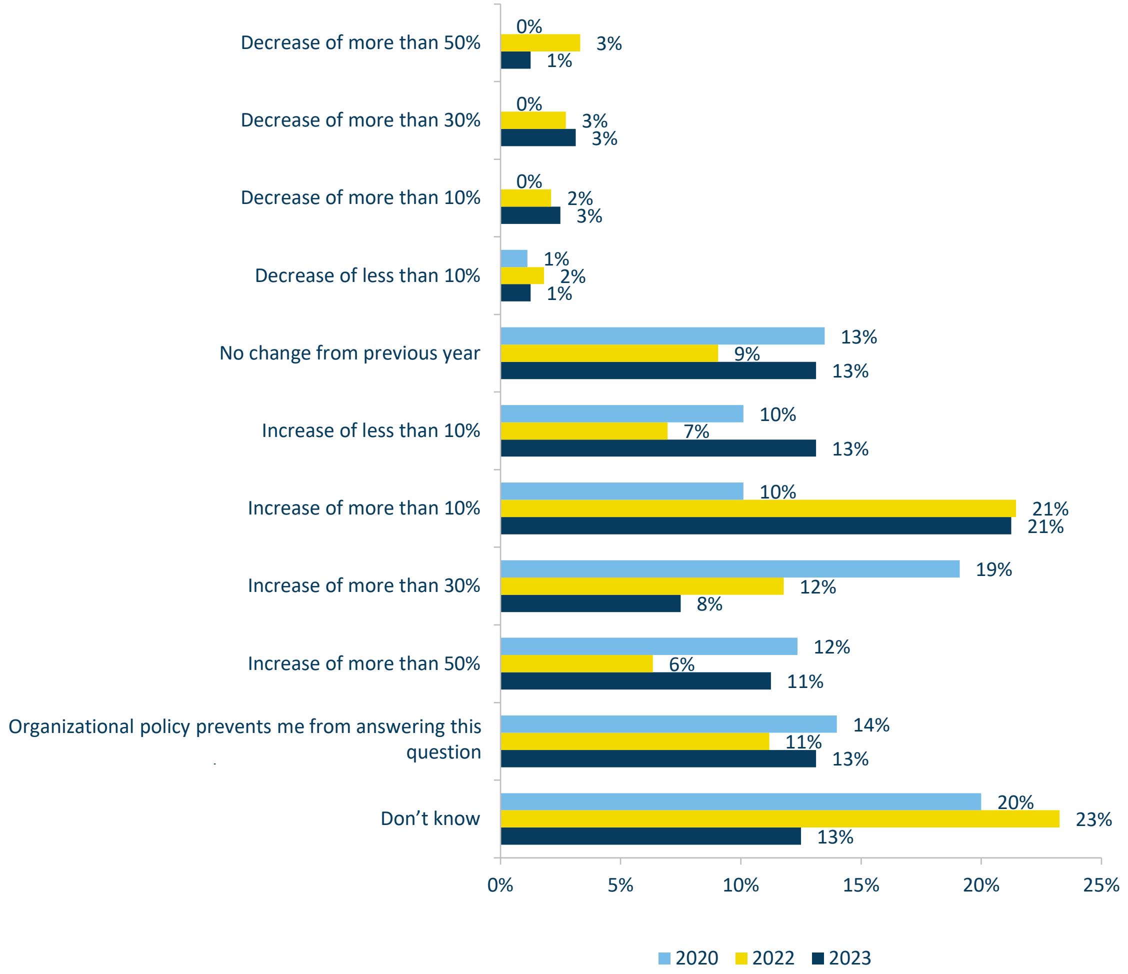


(CS)² Budget Change – Longitudinal Analysis

A slim majority of organizations continue to increase their (CS)² budgets (53%), with this response rate hovering close to the midpoint for several years (47% 2022, 52% 2020). There is a pattern of steady increase in the slow growth group, those with (CS)² budget increases of below 30%, rising from 20% of respondents in 2020 to 34% this year. The higher growth group, those with increases above 30%, has correspondingly shrunk from 31% of 2020 respondents to 19% now. Members of our analysis team pointed out certain slowdowns in the (CS)² vendor/solution provider sector, possibly a response to increased competition, or overshooting market appetite.

> *The continued commitment to increase spending YOY shows that organizations are coming to better understand the threat landscape in which they operate and some degree of the exposure they face. Recent (CS) cyber incident headlines have increased awareness of both the cyber risks present and the necessary actions to prevent a similar event from occurring.*
>
> ***Brad Raiford***
>
> *Director, National IoT & OT Cyber Services*
>
> *KPMG in the US*

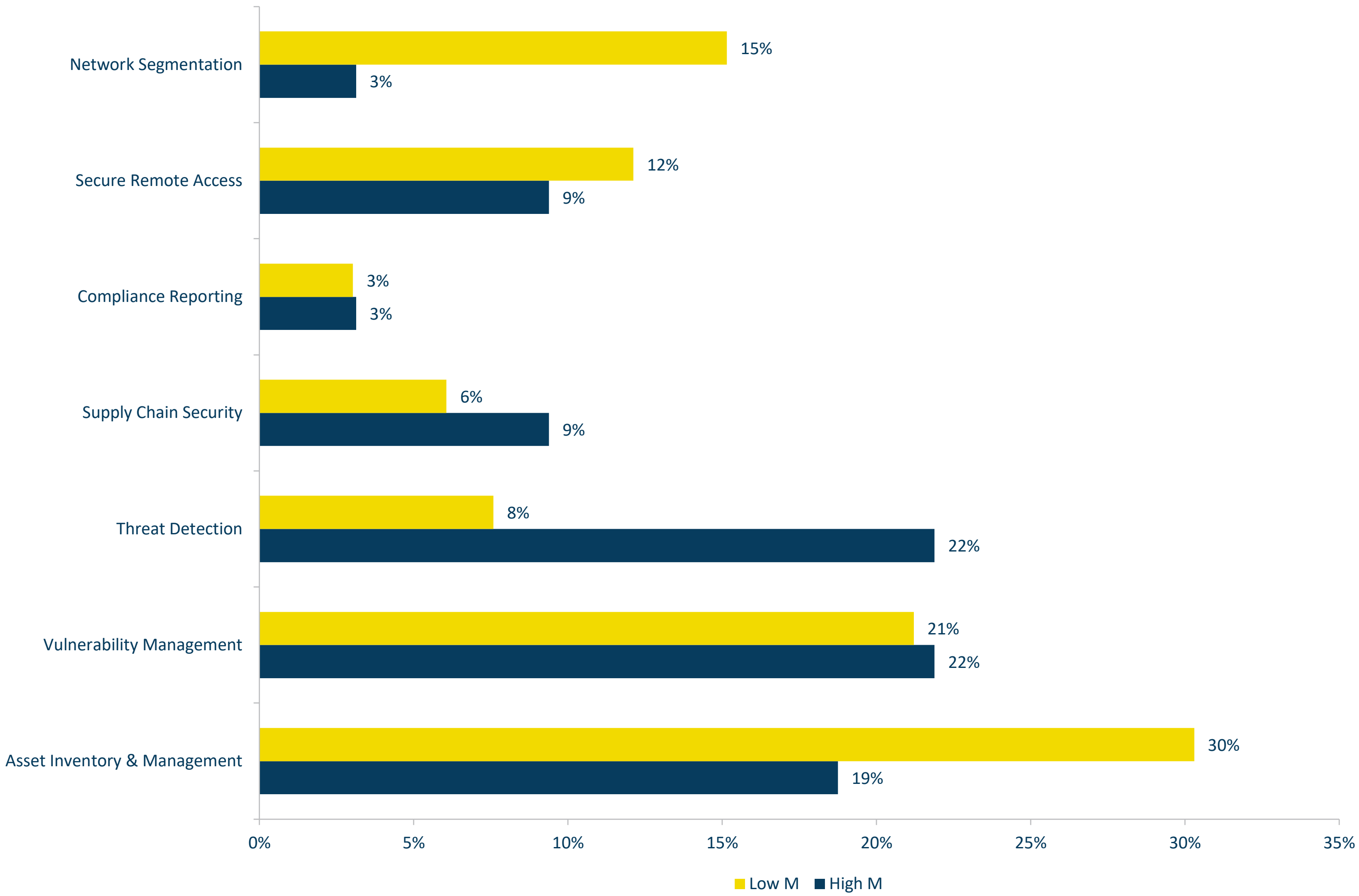
Estimations of how this year's organizational controls system security budget compares to prior year's



Planned $(CS)^2$ Investments – High vs Low M

With the strong support for the value of *Network Segmentation* (see charts on Top ROI) we consider it notable few organizations plan to focus their upcoming security spend in that area. The explanation may be that High M organizations may have already significantly segmented their network, so they are now spending much less (3%) than the Low Ms (15%). A similar factor may be behind the difference in their planned expenditures on *Asset Inventory & Management* and *Threat Detection.*

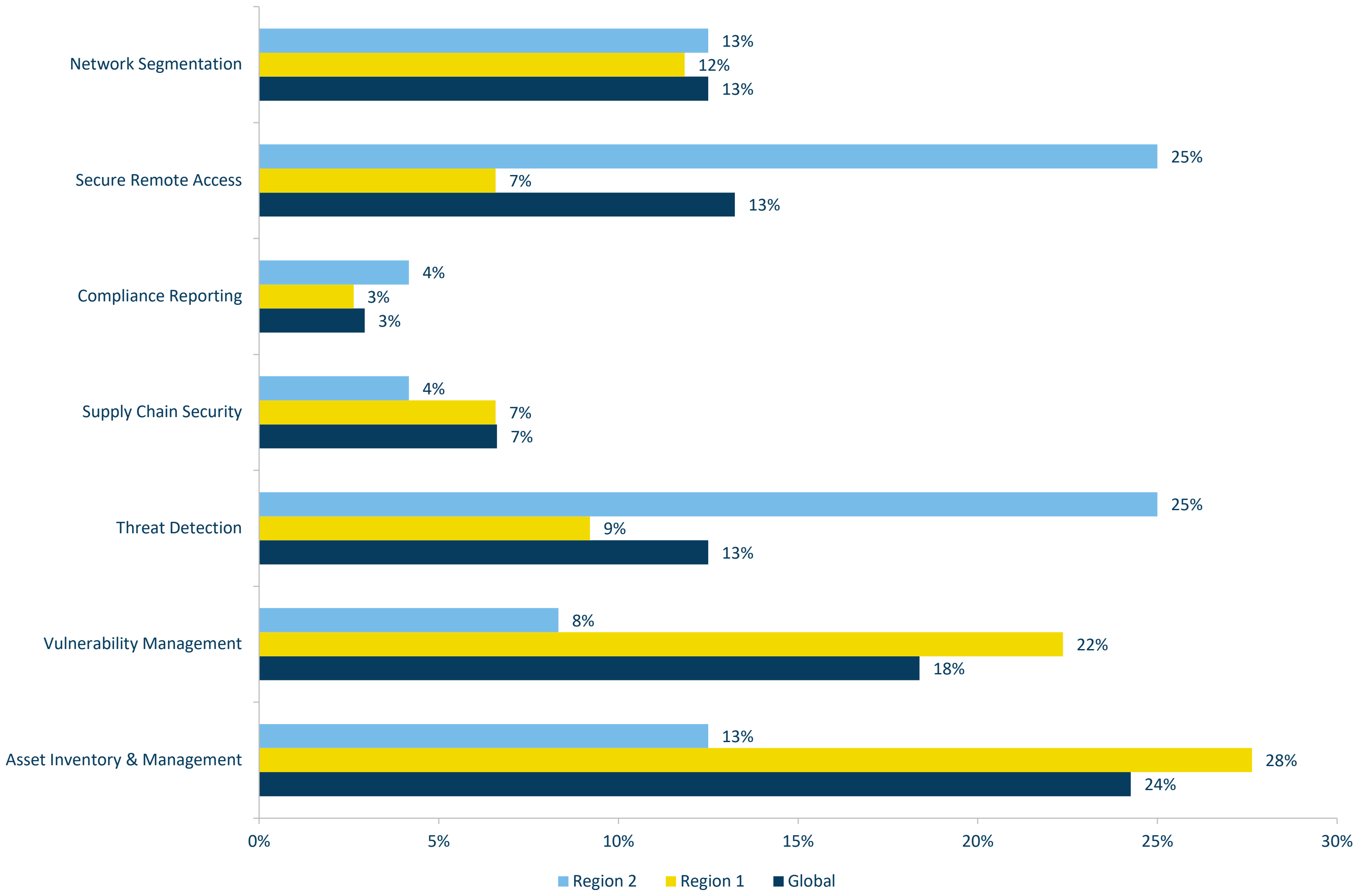
Highest investment areas for $(CS)^2$ for the year ahead



Planned (CS)^2 Investments – Regions

Response to this question was insufficient in Regions 3-7[9] to include, but plans are quite different between respondents in Regions 1 and 2. Region 2 participants are focused currently on *Secure Remote Access* and *Threat Detection*[10] (25% on both) while their North American colleagues seem to consider *Vulnerability Management* and *Asset Inventory & Management* more pressing matters (18.4% and 24.3%, respectively). One possibility raised in our review is that Region 2 organizations have resolved these *Management* concerns to a degree not yet accomplished in Region 1.

Highest OT cybersecurity investment areas for the year ahead



[9] (CS)^{2}AI is organized into seven Regions. 1) North America; 2) Europe (Central, Western, Northern and Southern); 3) Eurasia; 4) Indo-Pacific; 5) Middle East-North Africa; 6) Southern Africa; 7) Latin America-Caribbean

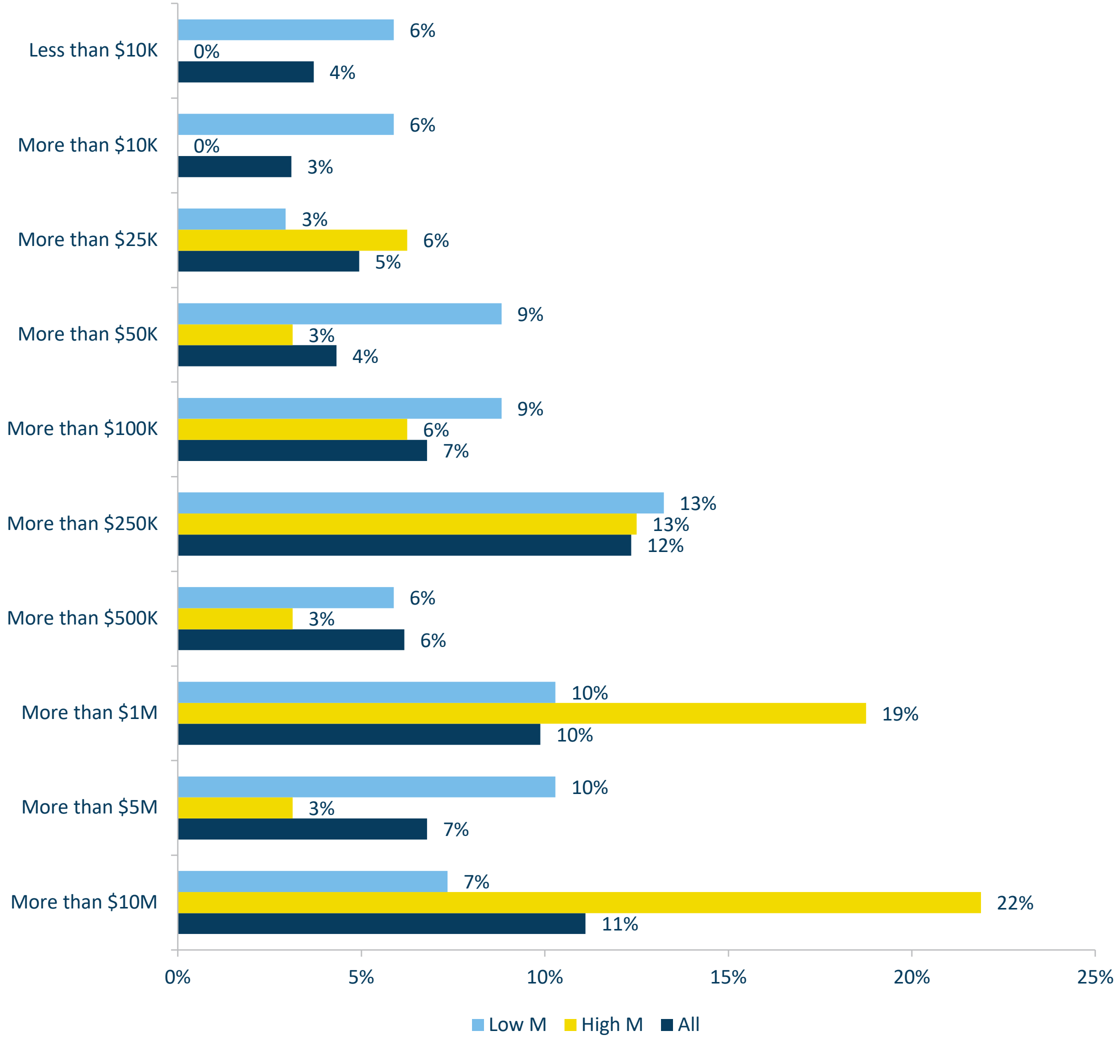
[10] One possible factor here is that regulatory bodies in Europe (both national and international) have been advancing/issuing legislation requiring threat detection in multiple industries and infrastructure sectors.

(CS)^2 Budgets – High M vs Low M

We have seen that High M organizations tend to have the highest Control System Cybersecurity budgets. One theory is that the larger organizations (i.e., those with the greater resources) are generally further along in their security journey than smaller ones. While recognizing that the financial challenges to smaller companies allocating sufficient resources to improving their security are often greater, we also wish to point out that those same fiscal limitations may mean they have less capability to weather and recover from the impacts of damaging cyber incidents. The threat of a cyber attack shutting down their operations for an extended time may be more existential to them, and their risk management processes need to take this into consideration.

> *This correlation also highlights the need for the (CS)^2 space to better serve smaller customers with solutions and services that scale down to their budgets.*
>
> ***Rod Locke***
>
> *Director, Product Management*
>
> *Fortinet*

Total (CS)^2 budget estimations by organizations for the previous Fiscal Year

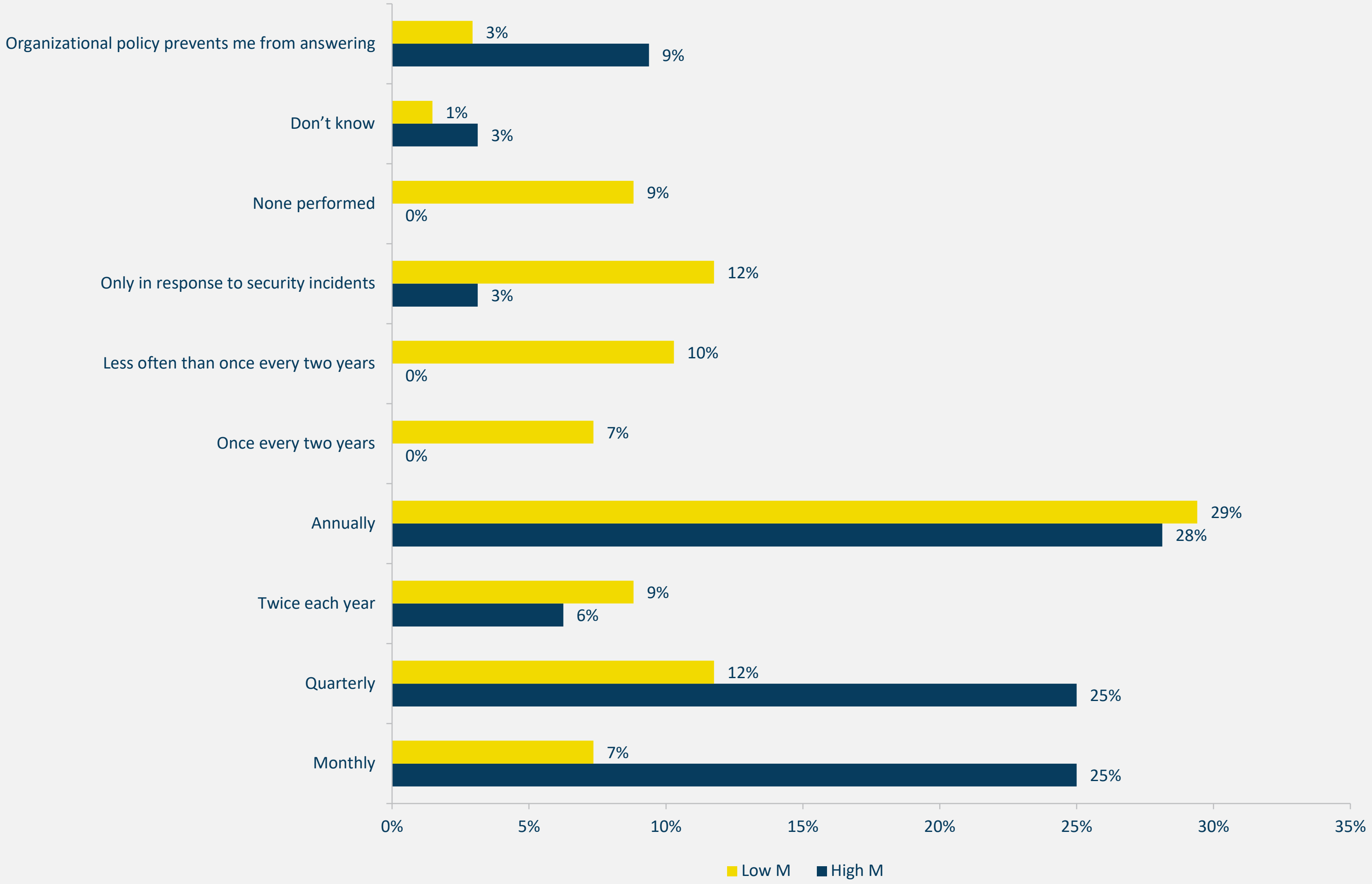


(CS)^2 Assessments

(CS)² Assessment Frequency – High M vs Low M

One of the clearest differences between programs of varied maturity levels is the frequency of their control system cybersecurity assessments, with fully half of the High M programs conducting these at least quarterly while over half of Low M programs carrying these out only annually or less. That 9% of Low M programs do not or have not performed security assessments speaks for itself.

Frequency of (CS)² assessments by organizations (Low M VS High M)



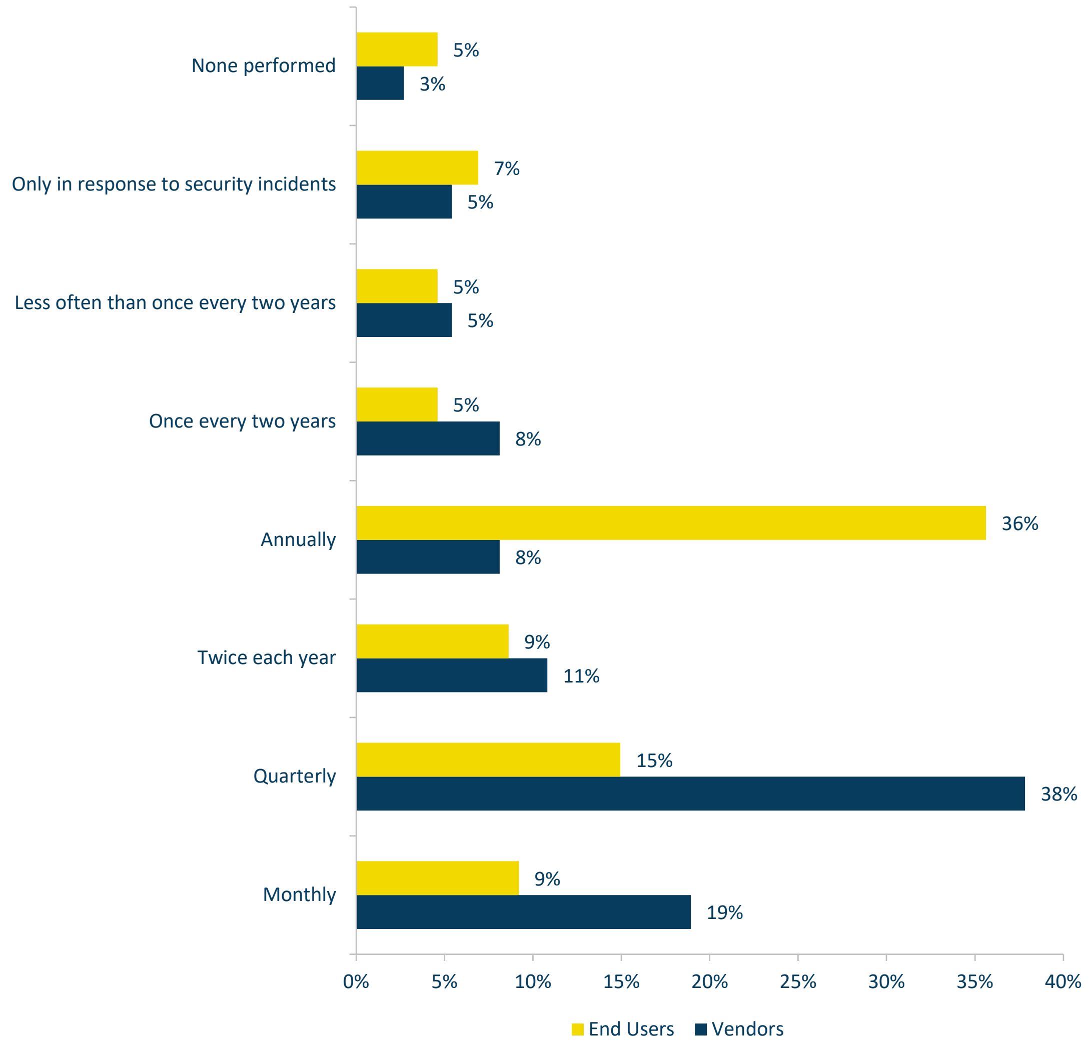
(CS)^2 Assessment Frequency – End Users & Vendors

Vendors bear different responsibility for their security from End Users because they must protect not only themselves but their clients, who often grant privileged access for ongoing monitoring, maintenance, and updates. Our team was glad to see that Vendors are carrying out (CS)^2 assessments so frequently, with over two-thirds (67.6%) at least *Twice* Each Year. Their position in the End Users' supply chains makes them a very valuable target to attackers[11]. That the End User organizations do so less often, with their single largest group assessing only *Annually* (35.6%) is less encouraging.

Technology, privileged personnel, attack methods and capabilities, changes occur in all of these continually and, even with IPS/IDS (Intrusion Prevention/Detection Systems) some victims only discover malefactors have accessed their networks during assessment activity. More frequent assessments can greatly reduce this dwell time and thereby potential harm of all sorts. We recommend all organizations, End User and Vendor alike, assess their (CS)^2 networks and assets at least quarterly.

[11] See any of many articles reporting on the Solar Winds supply chain attacks of 2021.

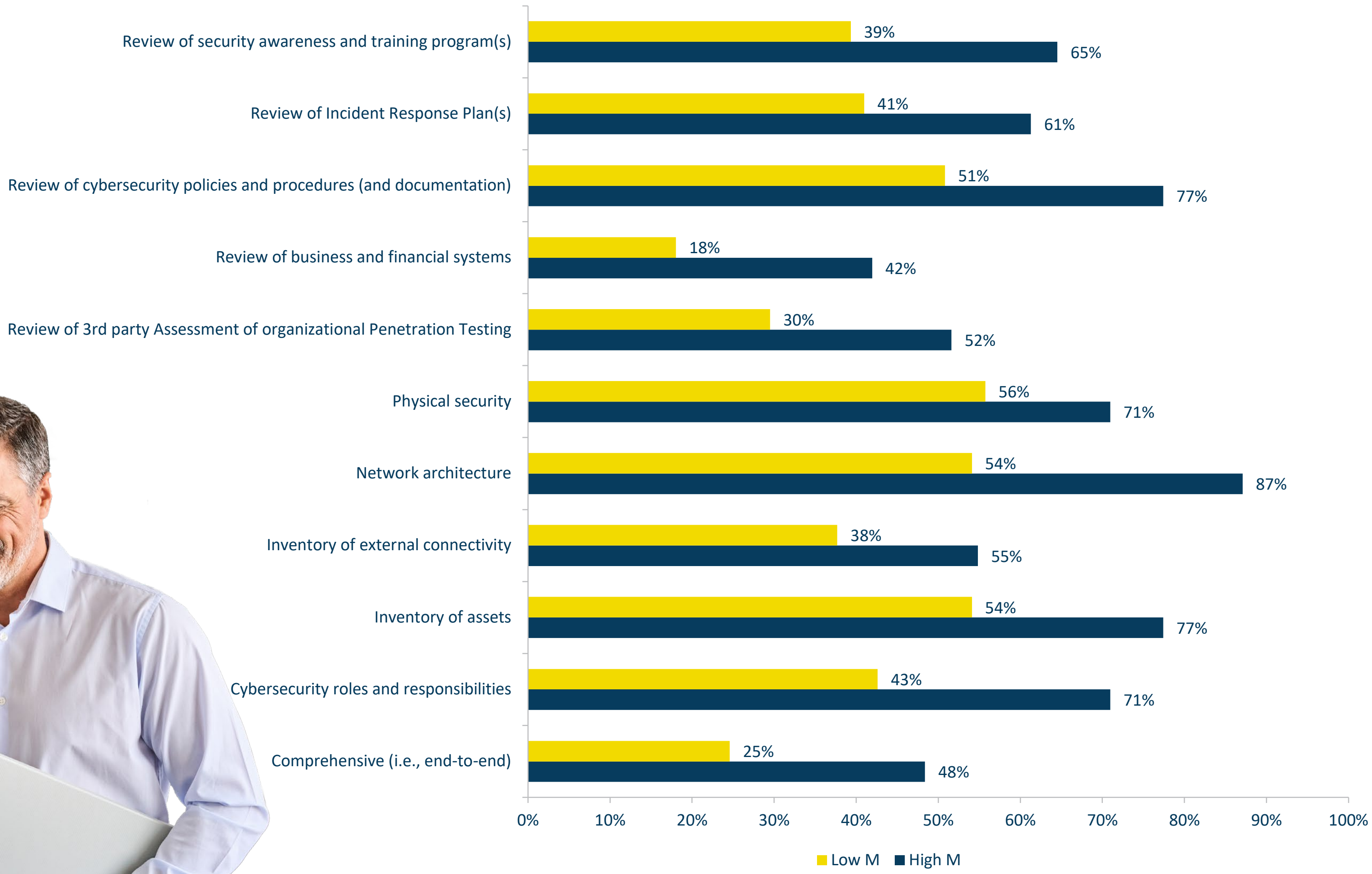
Frequency of (CS)^2 assessments by organizations



(CS)² Assessment Inclusions – High M vs Low M

Of no less importance than the frequency of security assessments is their thoroughness and, as this table indicates, High M programs conduct more complete assessments than Low M ones on every metric we use, by at least 50% in almost every category.

Components included in organization's (CS)² assessments

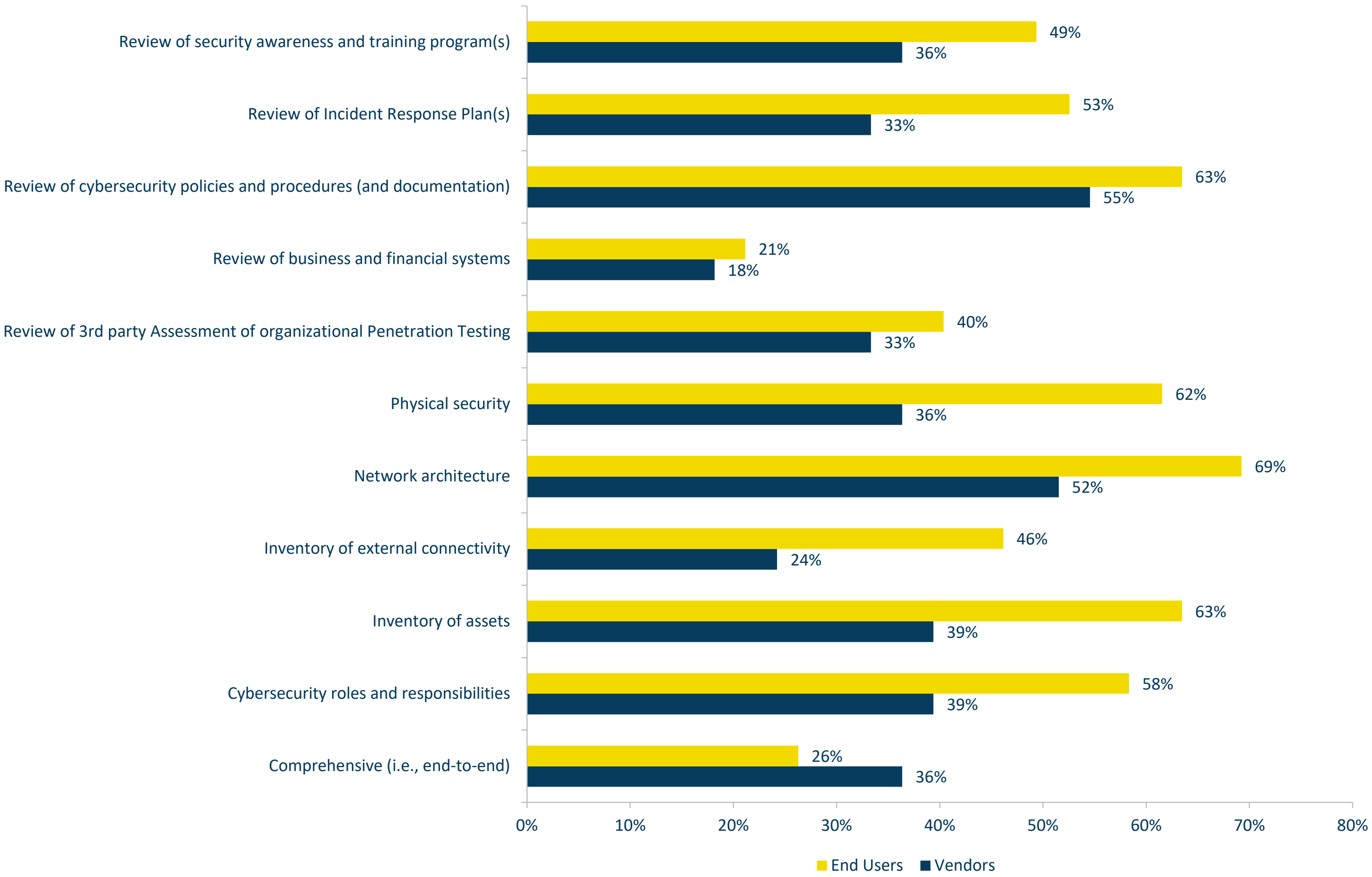


(CS)² Assessment Inclusions – End Users & Vendors

There's an interesting observation to be made here in that End Users appear to carry out all these security checks more than Vendors do except for *Comprehensive Assessments* (End Users 26% vs Vendors 36%). This suggests that End Users assessments, while including multiple important activities (End Users: *Physical Security* 62%, *Network Architecture* 69%, *Inventory of Assets* 63%, etc.) are less often complete than those of Vendors or Vendor clients. It is possible that End Users lack the end-to-end visibility needed here. It is also important to keep in mind that Vendors are often mid-stream and must consider security of their own supply chain and application security as well as what they provide their clients/customers.

Every item listed in this chart addresses critical points in preventing bad actors progressing along their kill chains (or catching them as they do). We recommend developing plans including all these components, each with defined assessment and remediation cycles.

Components included in organization's (CS)² assessments



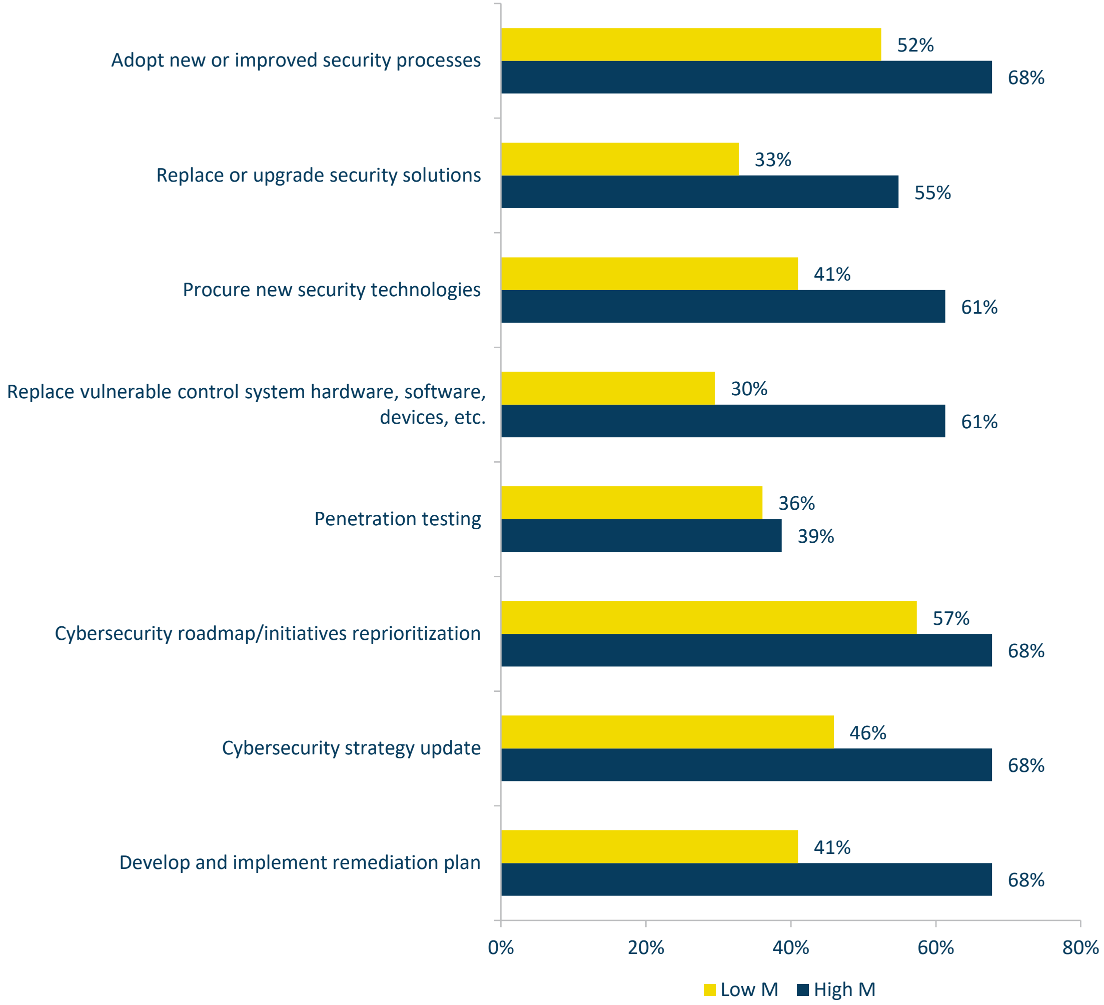
(CS)^2 Assessment Responses – High M vs Low M

To complete the triumvirate of organization's (CS)^2 assessment factors we investigated what they do after their analyses. Again, we see that High M programs follow through on assessment findings more often than Low M programs on every metric. Particularly notable are their actions to *Develop and implement*.

Remediation Plans (41.0% Low M vs 67.7% High M) and *Replace Vulnerable Control System Hardware, Software, Devices*, Etc. (29.5% vs 61.3%).

> *While investments on cyber hygiene activities (e.g. network segmentation, training and vulnerability patching) are key to prevent potential compromise to an industrial network, it will be tough to prevent a highly motivated and technically sophisticated threat actor from accessing the network. The ability to recover fast from a cyber incident will be critical to minimize disruption to operation or supply of essentials such as electricity or water to consumers.*
>
> *Routine backup and recovery assessments should be reviewed to improve the cyber resiliency of critical or industrial systems.*
>
> ***Eddie Toh***
>
> *Partner, KPMG in Singapore and Head of Forensic Technology, KPMG in Asia Pacific*

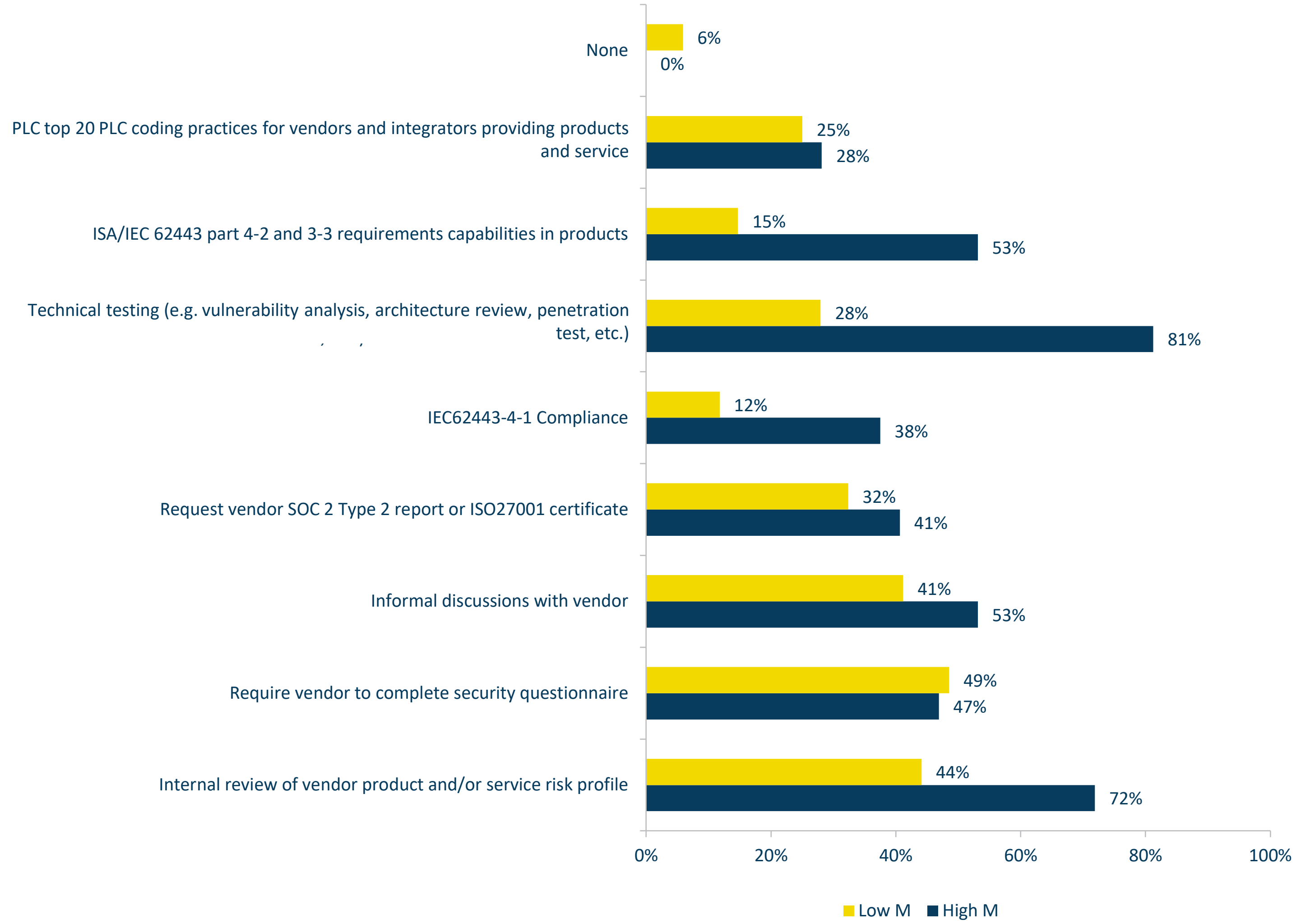
Activities carried out/planned in response to findings of (CS)^2 assessments completed by organizations within the last 12 months



Pre-Acquisition (CS)^2 Risk Assessments – High M vs Low M

Risk evaluation on new devices and/or software is not the same as cyclical security assessments and must be considered separately. Just as we saw that organizations with High M (CS)^2 programs carry out overall security assessments more frequently, we note that they are more likely to conduct almost all types of pre-acquisition risk assessment (*Security Questionnaire* being the exception). Increased US regulatory activity is likely a factor in deltas touching on compliance for many of our respondents, but we see the high rate of *Technical Testing* among High M (27.9% Low M vs 81.3% High M) as positive and, since it provides only snapshots, complementary to periodic security assessments.

Risk assessments performed by organizations before acquiring control system products or services (High M vs Low M)

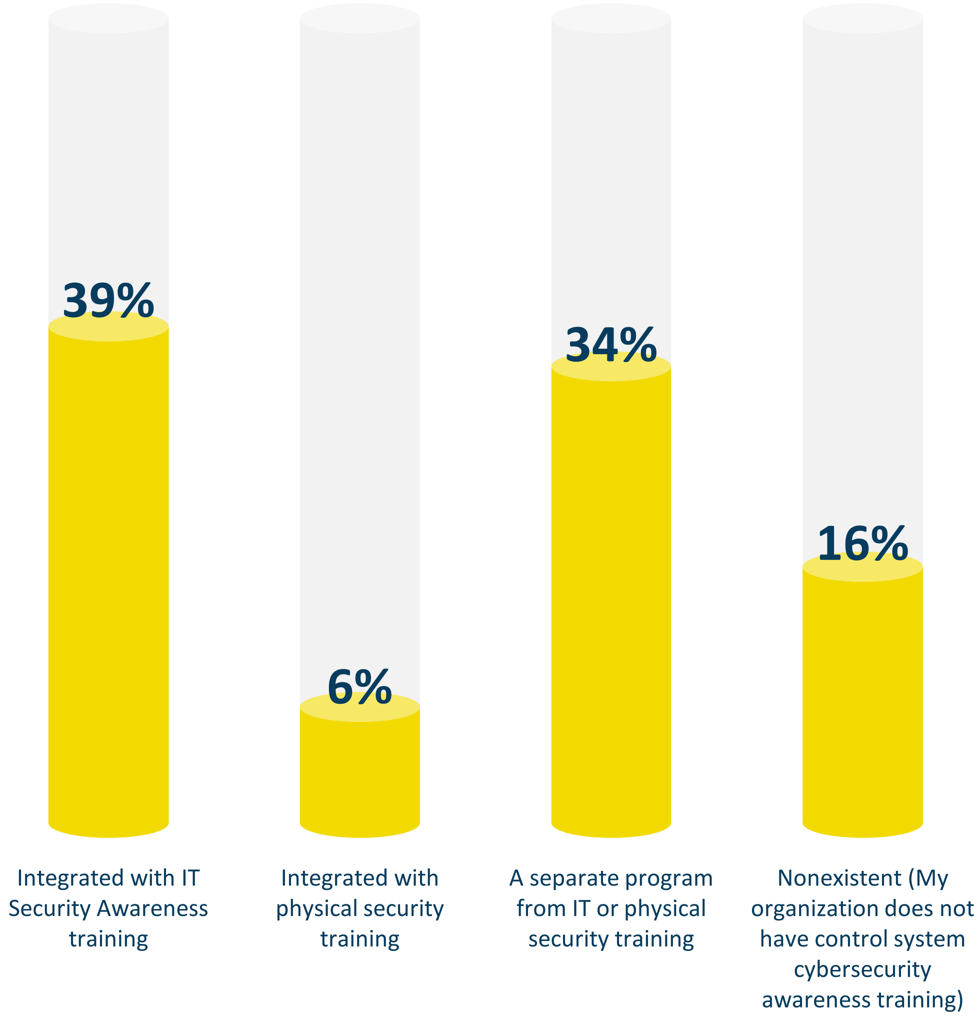


Security Training

$(CS)^2$ Awareness Training Integration – End Users

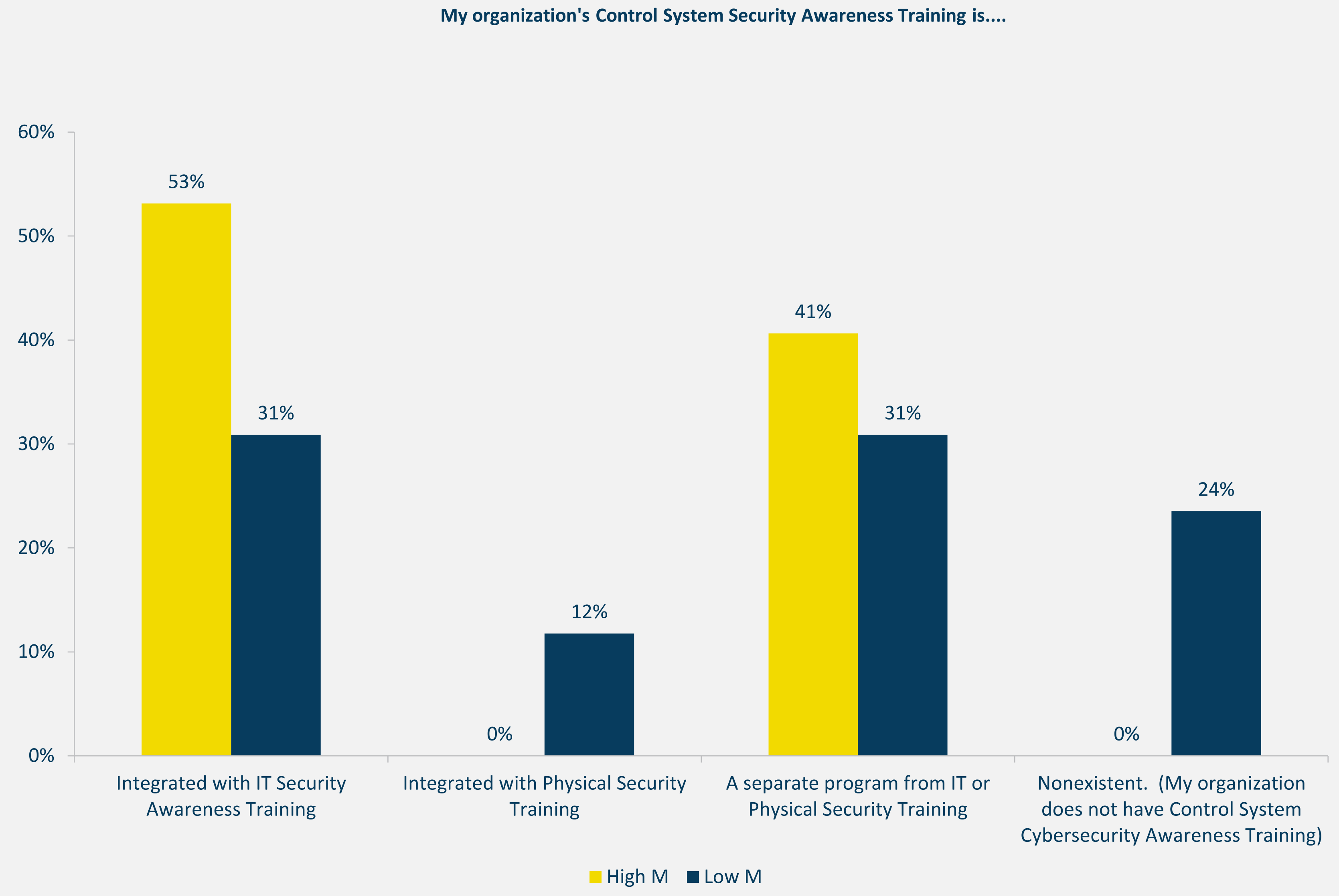
The obvious concern here is that so many End User organizations lack any $(CS)^2$ Awareness Training (16.1% *Nonexistent*). Whether driven by IT departments, Risk Management programs, wholly within Operations or some other design, achieving and maintaining high awareness of $(CS)^2$ threats, attack methods, vulnerabilities, and procedures is essential to managing the risks inherent in any ICS/OT operational environment. We cannot recommend highly enough that every organization with responsibilities for assets/operations implement such programs.

My organization's Control System Security Awareness Training is....



$(CS)^2$ Awareness Training Integration – High M vs Low M

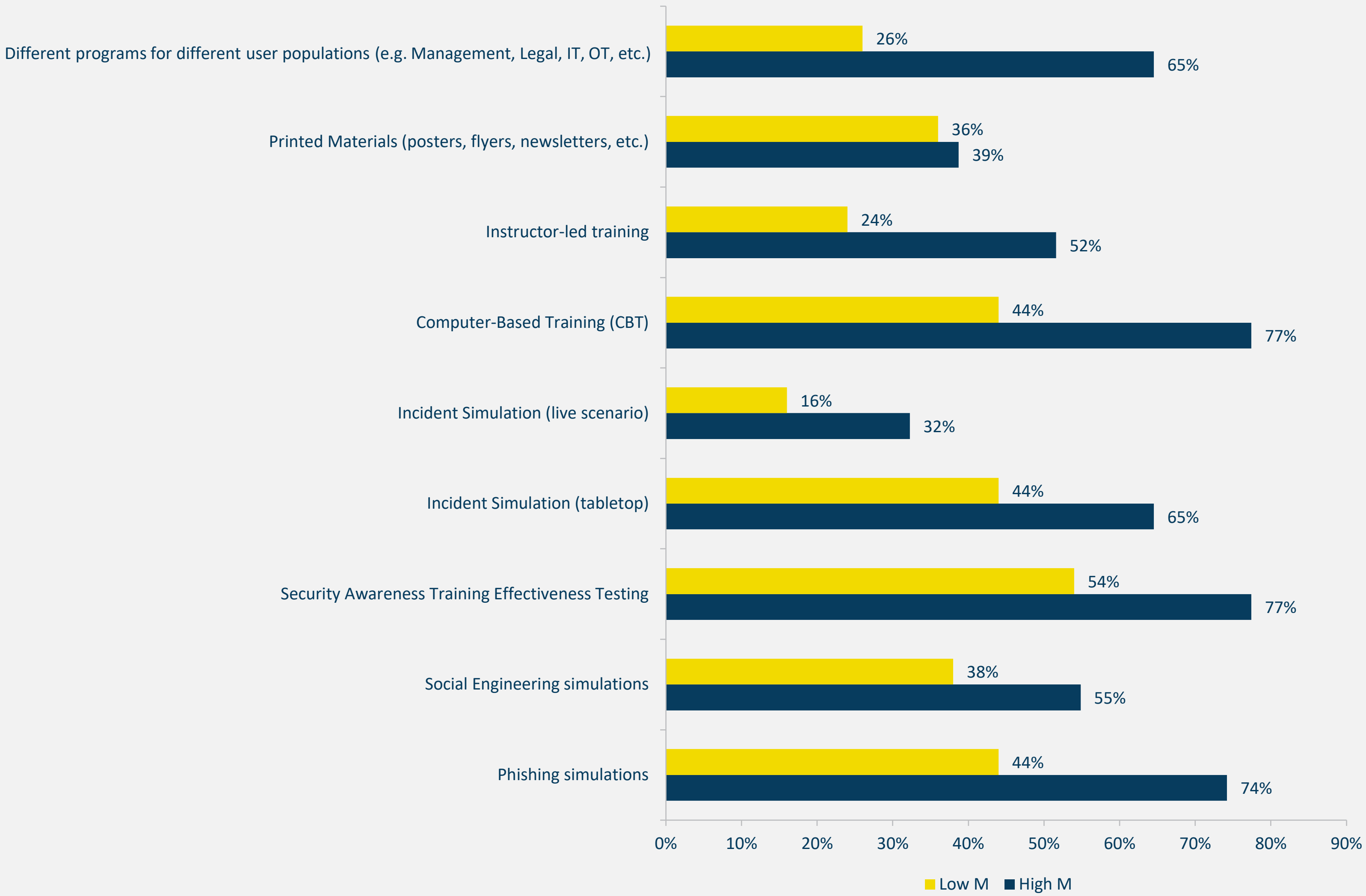
Breaking out our data by maturity level groups reveals that it is exclusively organizations with Low Maturity $(CS)^2$ security programs lacking the relevant *Awareness Training* (24% *Nonexistent* vs 0% High M), while most of their colleagues in the High M group have *Integrated IT Security* and *Control System Cybersecurity Awareness* trainings.



(CS)² Training Inclusions – High M vs Low M

Although we did not include security training in our descriptions of the various security program maturity levels, it is clear from this chart that the High M organizations invest more into ensuring a trained workforce. The only component in which the two groups are even close to one another is in the use of printed materials, which is often considered less effective than any of the others. In fact, it is in the most effective areas such as *Simulations* (any) and *Instructor-Led Training* that we see some of the largest deltas. The greater use of *Security Awareness Training Effectiveness Testing* (High M 77% vs Low M of 54%) should enable these companies to focus on what works best and continually improve their training programs.

Components included in organization's control system security related training



$(CS)^2$ Networks

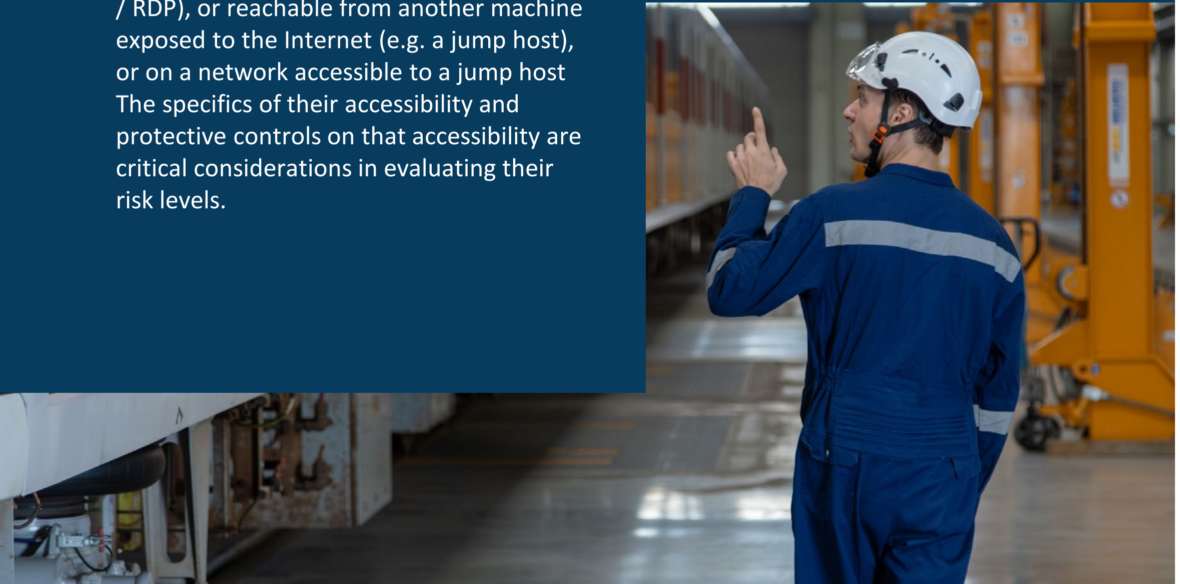
Control System Component Accessibility

Overall, this chart and those following are quite concerning. To have so many elements of control systems accessible, even controllable, from the internet (from 15% of Low M PLCs to 39% of Low M Historians) indicates attackers have a very large attack surface and the potential for high impacts on these companies.

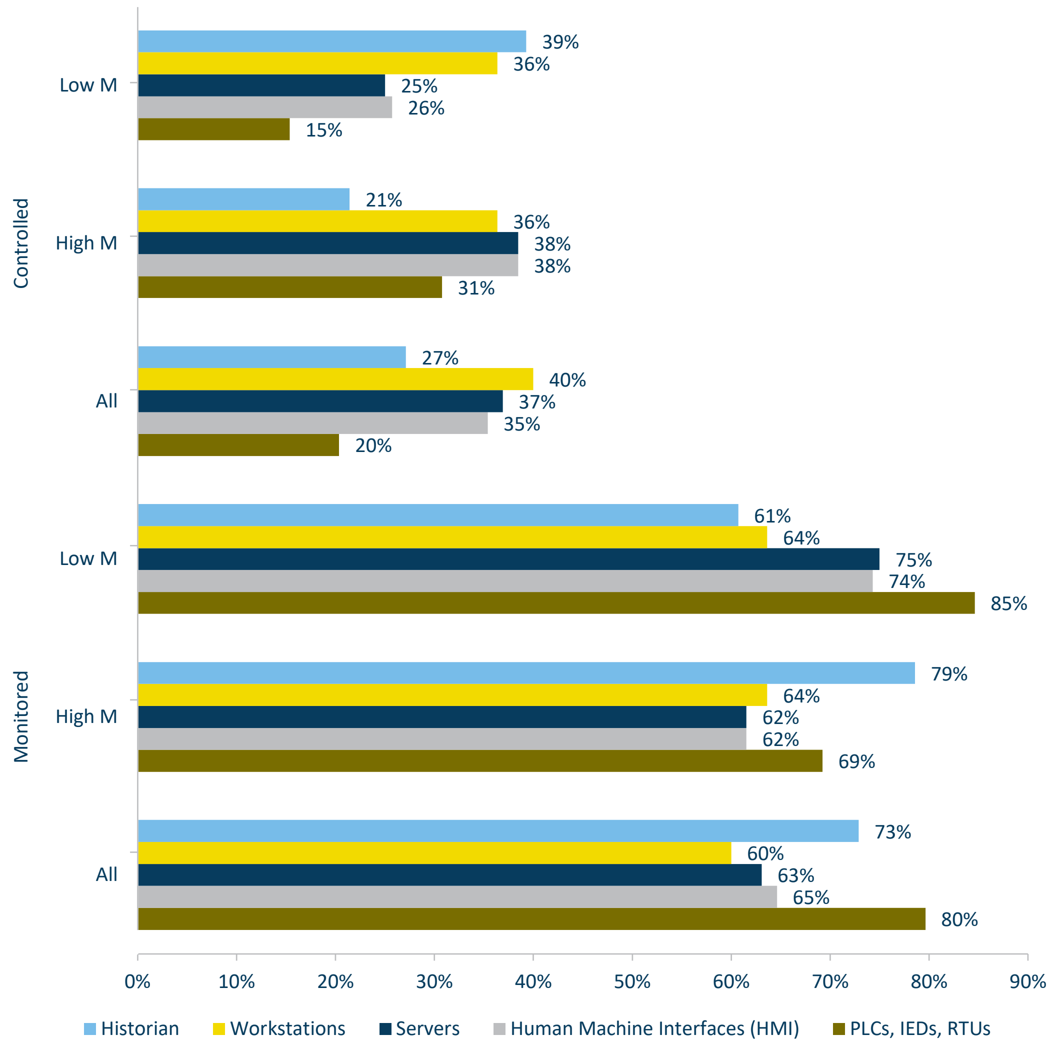
Some of our SME contributors pointed out the importance of keeping in mind that "accessible" does reveal the *controls on* or *method of* that accessibility. These could be systems with ports open to the Internet (e.g. HMI login screen?), with remote access enabled from the Internet (e.g. VPN / RDP), or reachable from another machine exposed to the Internet (e.g. a jump host), or on a network accessible to a jump host The specifics of their accessibility and protective controls on that accessibility are critical considerations in evaluating their risk levels.

We do consider it curious that so many components are as frequently controllable via internet in High M organizations as in Low M ones. Indeed, Servers, HMIs and PLCs/IEDs/RTUs are more often accessible this way in the former[12]. This pattern continues in the following charts showing component accessibility from Business Networks, Vendors/Integrators, and the Cloud.

[12] The high ROI placed on network segmentation by the more mature group (75%, see chart on Top ROI – High M vs Low M) may be an influence here.



Components Accessible from the Internet



Control System Component Accessibility (cont.)

These responses indicate that outside access to control systems is prevalent today—including from business networks, vendors, and the cloud. Because of this increasing IT/OT convergence, it is imperative that organizations consider control system security as part of their overall security program, rather than as a separate domain. This applies both to security management programs (under standards such as IEC 62443 and ISO 27001) and to the controls used to secure and monitor these systems.

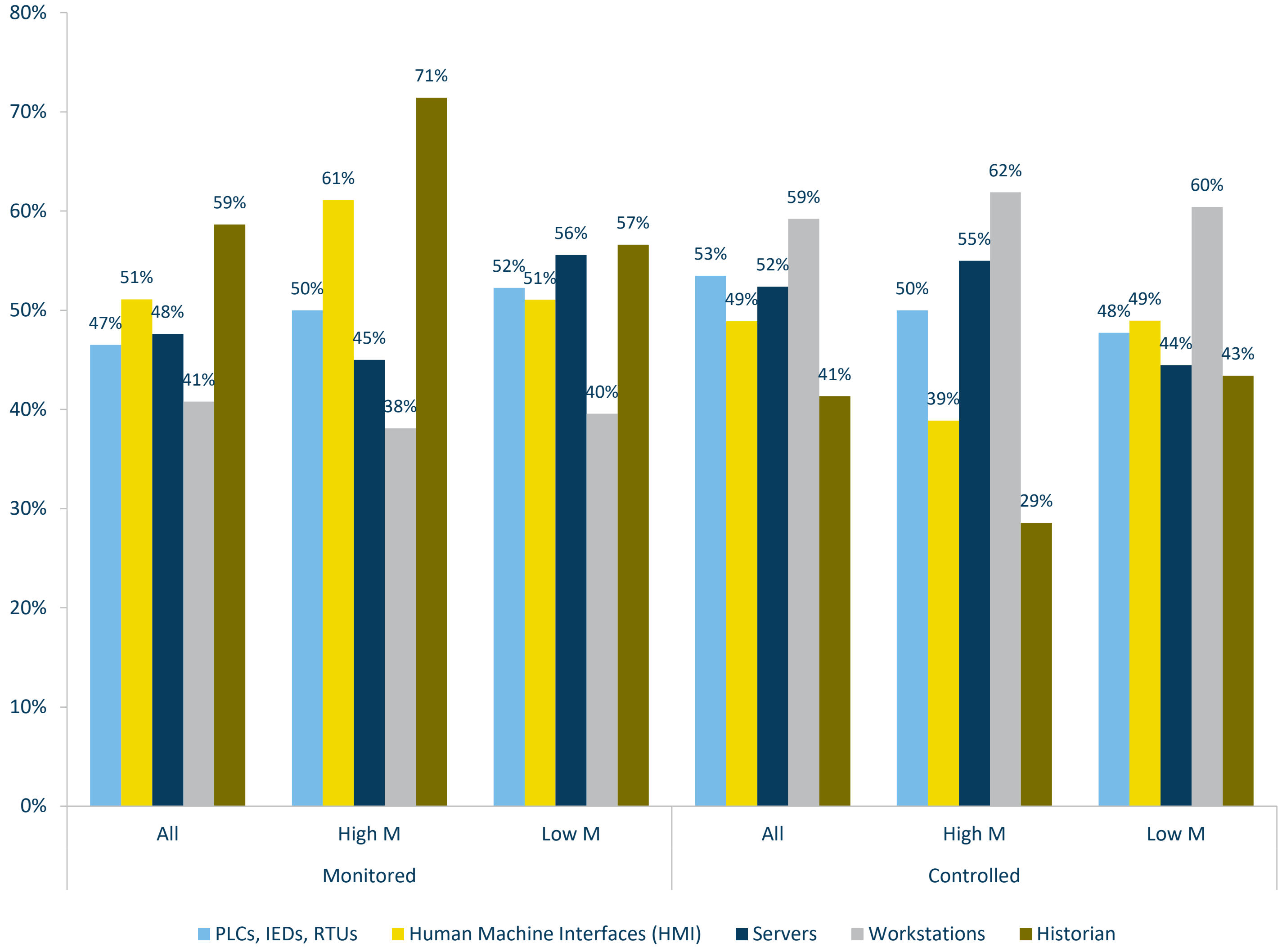
In Fortinet's 2023 State of Operational Technology and Cybersecurity Report, respondents indicated that OT security is part of the CISO's responsibilities in almost all organizations (95%). The reality of IT/OT convergence was also reflected in organizations' view of the threat landscape—where a strong majority of organizations (77%) viewed ransomware as a larger concern than other threats to the OT environment.

Rod Locke

Director Product Management

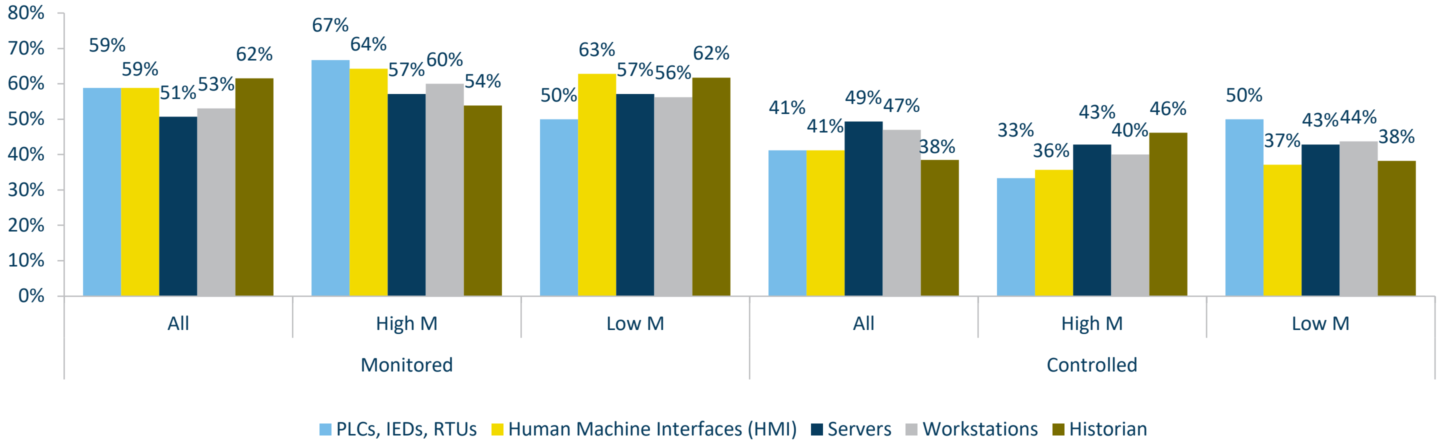
Fortinet

Components Accessible From Business Network

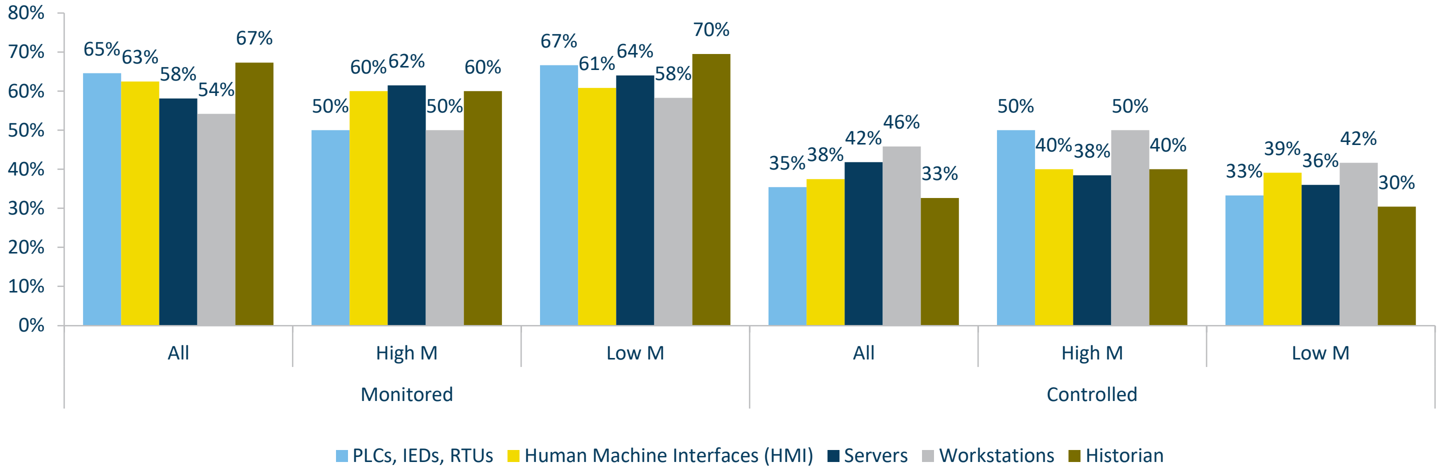


Control System Component Accessibility (cont.)

Components Accessible Remotely by vendor/integrator

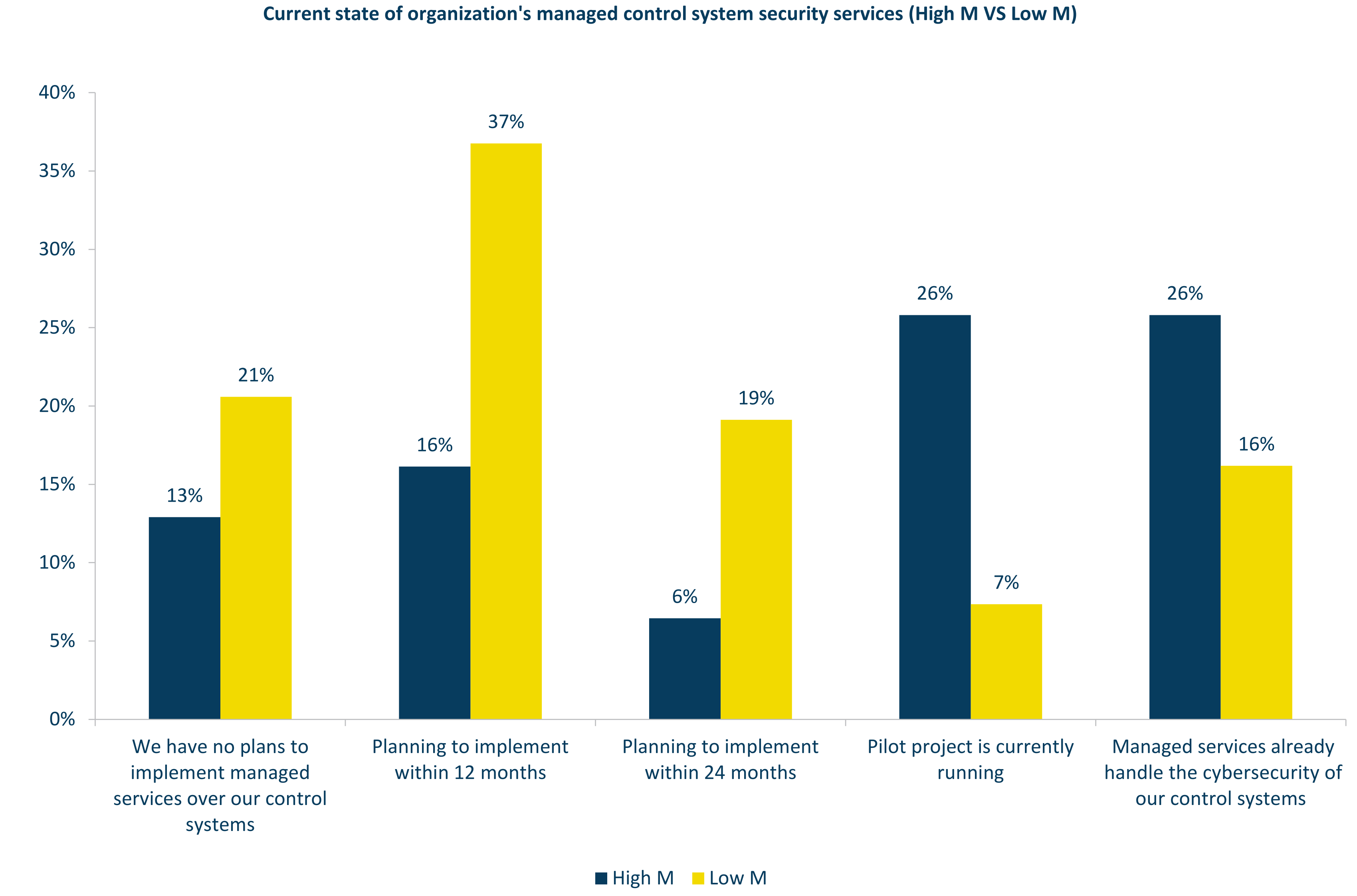


Components Accessible from Cloud



Current Managed $(CS)^2$ Services – High M vs Low M

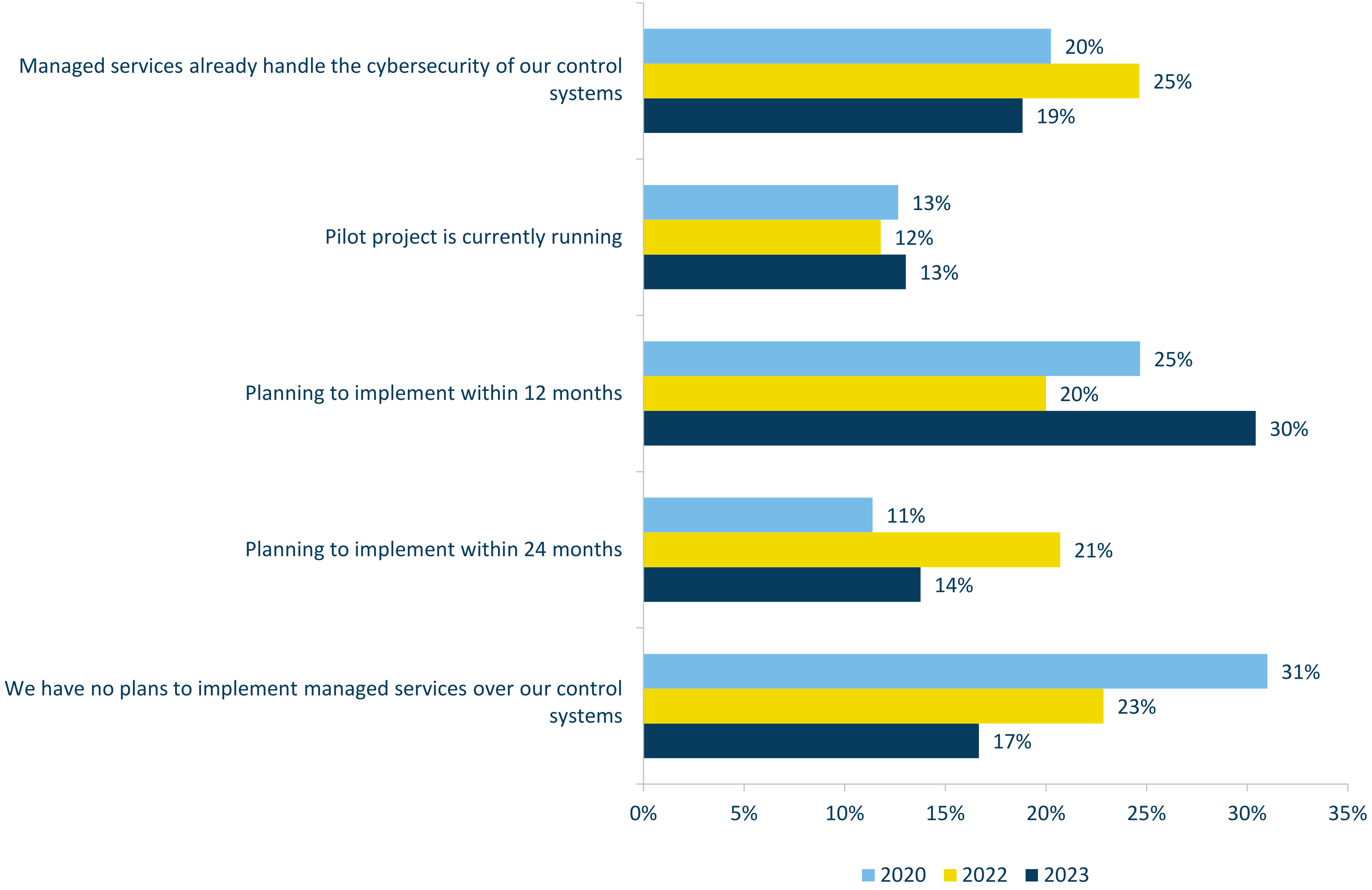
This year's participants have again indicated that the High M organizations are more likely to either have managed services already handling their cybersecurity (25.8% High M vs 16% Low M) or be in the process of doing so with *Pilot Projects* (25.8% High M vs 7% Low M).


Current state of organization's managed control system security services (High M VS Low M)
40%
35%
30%
25%
20%
15%
10%
5%
0%
13%
21%
16%
37%
6%
19%
26%
7%
26%
16%
We have no plans to implement managed services over our control systems
Planning to implement within 12 months
Planning to implement within 24 months
Pilot project is currently running
Managed services already handle the cybersecurity of our control systems
■ High M
■ Low M

Use of Managed $(CS)^2$ Services – Longitudinal Analysis

The shift towards use of managed $(CS)^2$ services is in line with many years of our advice to readers. Training and education of internal resources has inarguable points but these are longer (and possibly less certain in the short term) investments. The $(CS)^2$ workforce supply of knowledgeable and experienced practitioners has long been insufficient to meet the demands of the rapidly changing technology, practices, and growing hyperconnectivity of control system devices. That this feeds an expanding market for $(CS)^2$ services is inevitable. Our recommendation for those companies with sufficient resources is to pursue both internal resource development programs and use outside expertise to address the immediate needs of protecting their assets and operations. We believe this is the best approach to improve the long-term outlook for their organizations.

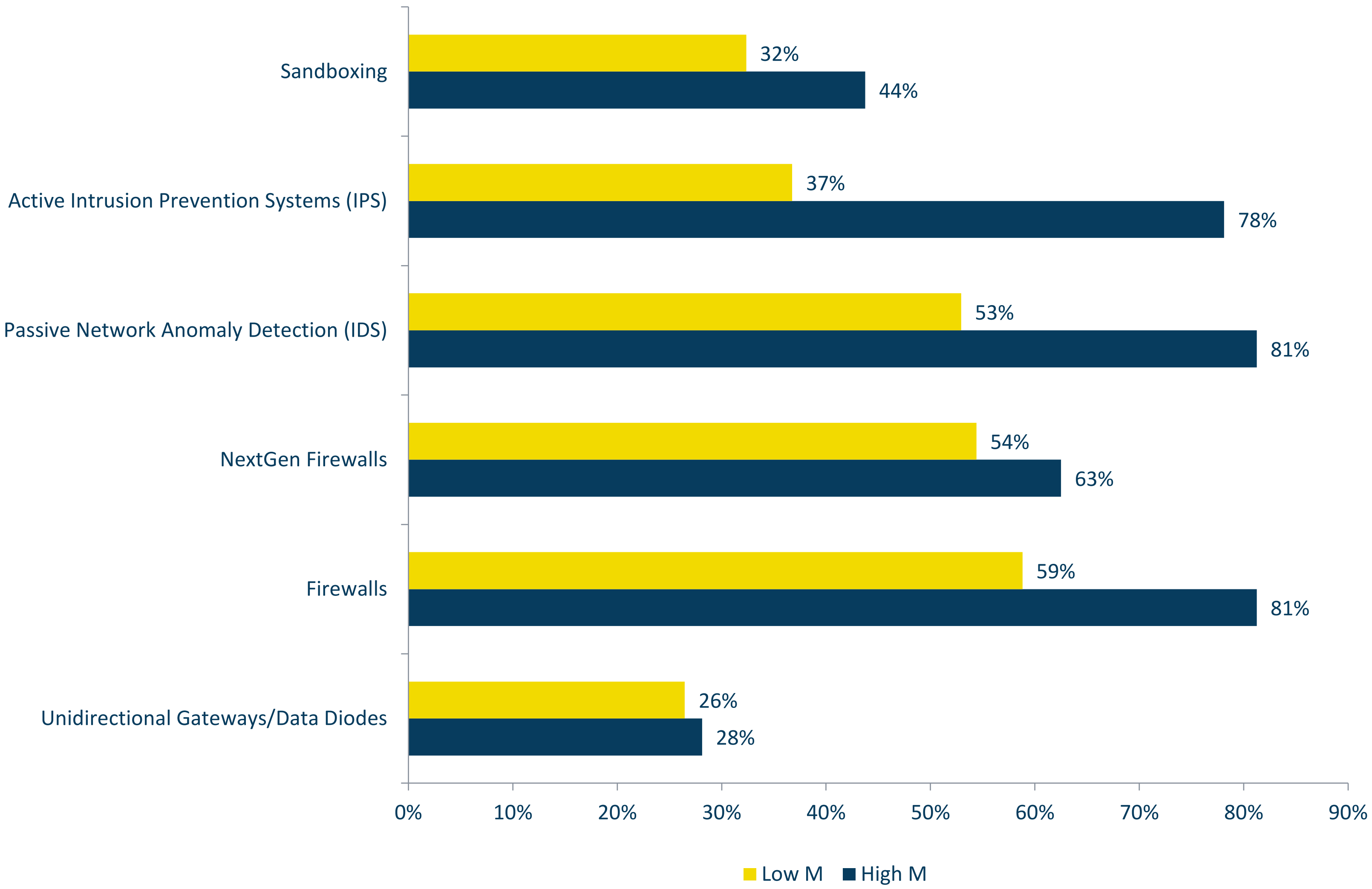
Current state of organization's managed control system security services (Longitudinal)



Current (CS)^2 Technologies – High M vs Low M

Other than the overall trend of High M organizations using every security technology more often than the Low M group, the large deltas between the use both of *Active Intrusion Prevention Systems* (High M 78.1% vs Low M 36.8%) and *Passive Network Anomaly Detection* (High M 81.3% vs Low M 36.8%) indicate a much greater likelihood that these companies will identify and block attempted incursions in shorter timespans, thus reducing potential impact on their systems.

Security technologies in use to protect organization control system assets against cyber threats

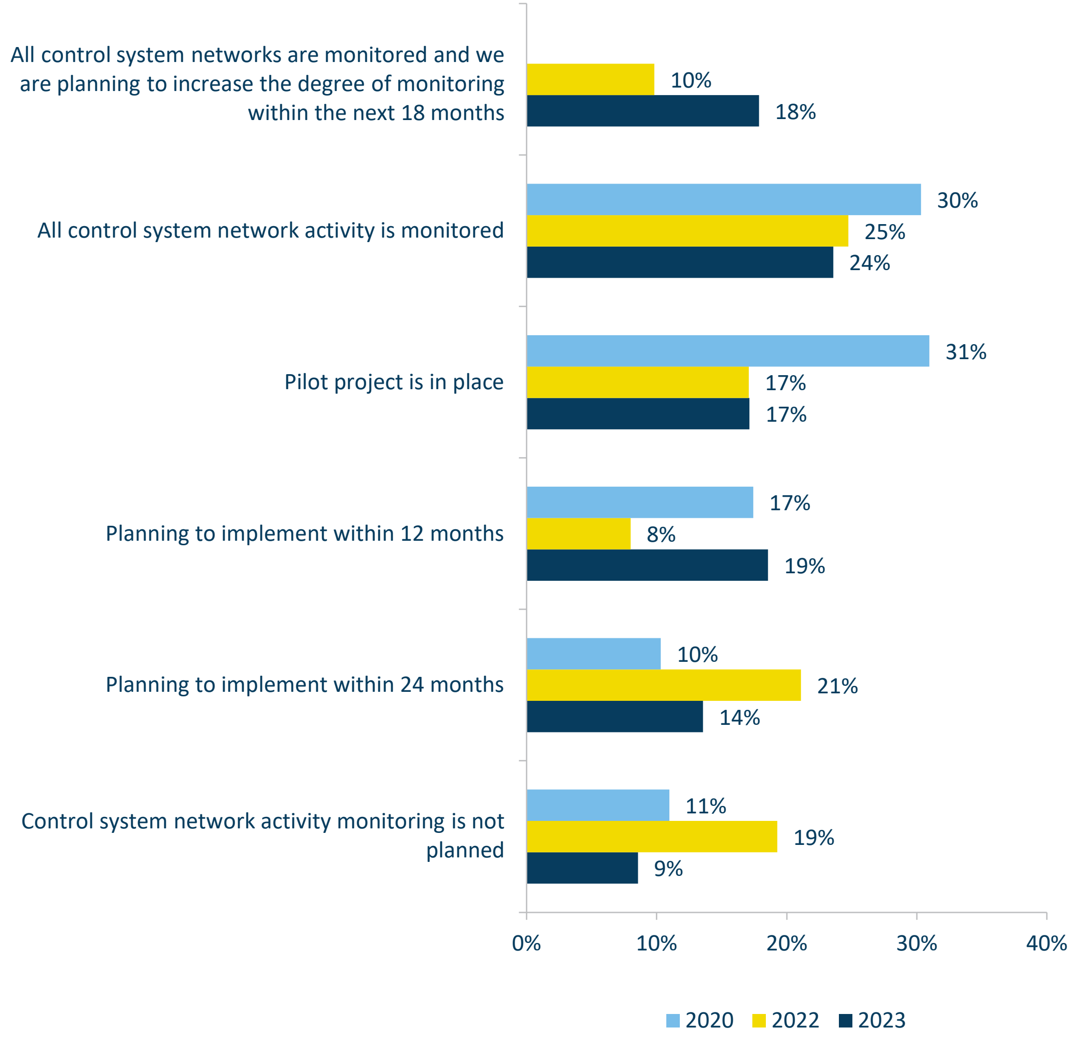


(CS)² Network Monitoring – Longitudinal Analysis

Visibility into our control system networks is crucial to protecting those networks and connected assets. Whereas OT culture was historically resistant to introducing network monitoring technologies (understandably, due to some cases of operational disruption occurring from doing so) into their environments, the tools and techniques providing this insight have continued to mature and improve, with acceptance of their risk/benefit ratio increasing. It is encouraging to see the year-over-year growth of organizations who have implemented (CS)² network monitoring and plan to strengthen it, increasing from none a few years ago to 17.9% today. Organizations not planning to implement any network activity monitoring has dropped to a single digit percentage (9%) for the first time. The results show that organizations will continue to deploy and strengthen network activity monitoring into the future. The spike of organizations with no plans to implement monitoring in 2022 (19%) was originally thought to be an indication of many moving into the 'All is monitored' state; that is called into question by this year's results. We will continue to pursue this puzzle.

> *As operational technology modernizes, the attack surface continues to expand when OT systems increasingly connect to IT systems. Threat actors will continue to employ sophisticated "Tactics, Techniques, and Procedures" and exploit it against any weak links to disrupt such systems. For example, given the breath of its functionality, Pipedream is an example of increased sophistication and capability of threat actors in disrupting industrial systems.*
>
> *To detect malicious activities and respond timely to such events, it will be imperative to have visibility and continuous monitoring on the OT/IT/IIOT network.*
>
> ***Eddie Toh***
>
> *Partner, KPMG in Singapore and Head of Forensic Technology, KPMG in Asia Pacific*

Current state of organization's Control System Network Activity Monitoring

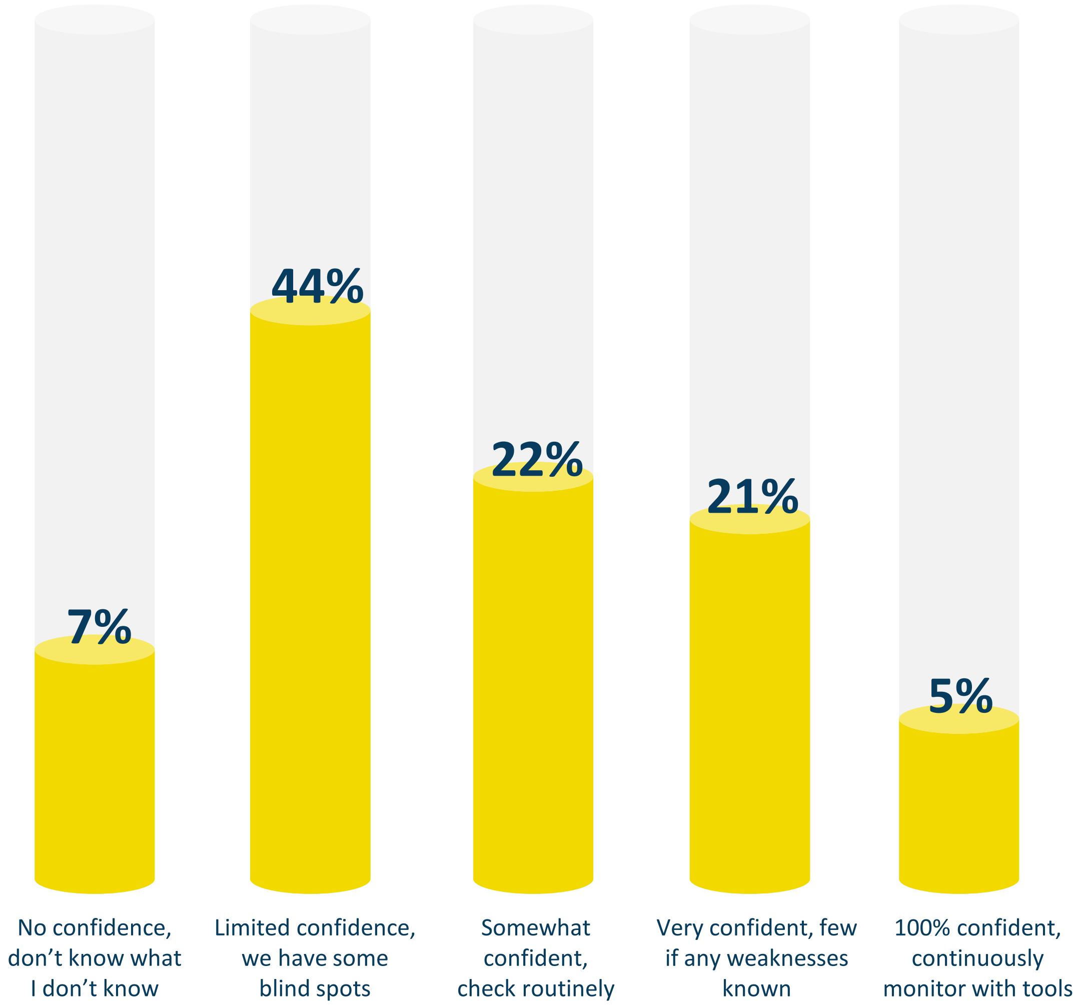


(CS)^2 Visibility – End Users

Our team considers the confidence level of our largest End User respondent group (*Limited Confidence, We Have Some Blind Spots* 43.7%) quite realistic. Visibility into control system networks has always been an issue, and it is only in recent years that the tools to gain this important capability have become widespread. We recommend that our reader, if they have not already done so, make use of these tools to overcome the blind spots and provide your (CS)^2 defenders with the essential knowledge they need to perform their roles.

> *Offline network modeling serves as the fastest and most effective method of providing comprehensive network visibility in a non-intrusive manner. It helps build an accurate understanding of the network environments that we are committed to protecting without disrupting operations. By analyzing network configurations, topologies, and security policies in an offline setting, we gain deep insights into critical communication paths and coverage gaps that might otherwise remain hidden during a live network analysis session. This method preserves the integrity and performance of the network while quickly identifying and addressing areas lacking visibility, thereby bolstering the network's defense against potential cyber threats.*
>
> ***Robin Berthier***
>
> *CEO and Co-Founder,*
> *Network Perception*

Confidence in the visibility of devices, users and applications on organization networks

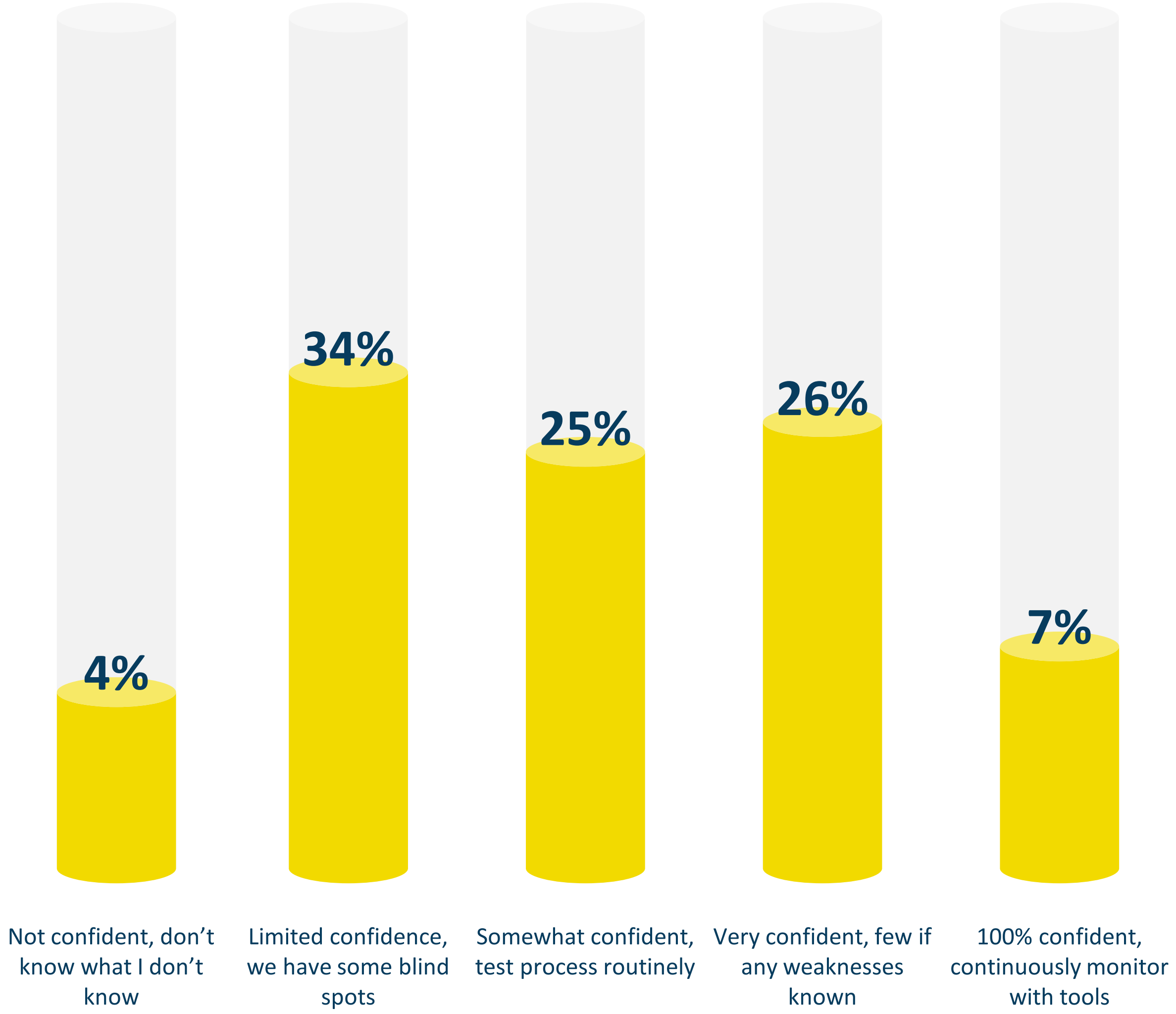


(CS)^2 Incidents

(CS)² Attack Responses – End Users

Our team was glad to see the level of confidence in cyberattack incident response processes among asset owner/operators (End Users), with 58% at least *Somewhat Confident* and most of those *Very or 100% Confident*. This is greater confidence than this group had in their visibility into their own networks (See previous table on Visibility).

Confidence in organization's response processes in the event of a cyberattack



Recent (CS)^2 Incidents – Longitudinal

While a very slight rise in respondents involved with *More than 50* (CS)^2 incident in the past year (from 5.2% last report to 5.8% now) the obvious standout results are the large increase in answers of *None* (2022 14.8% vs 2023 25.4%) and decrease in 26-50 (2022 19.4% vs 2023 10.1%). It is hoped that this shows results of ongoing protection and resiliency efforts rather than ignorance or error.

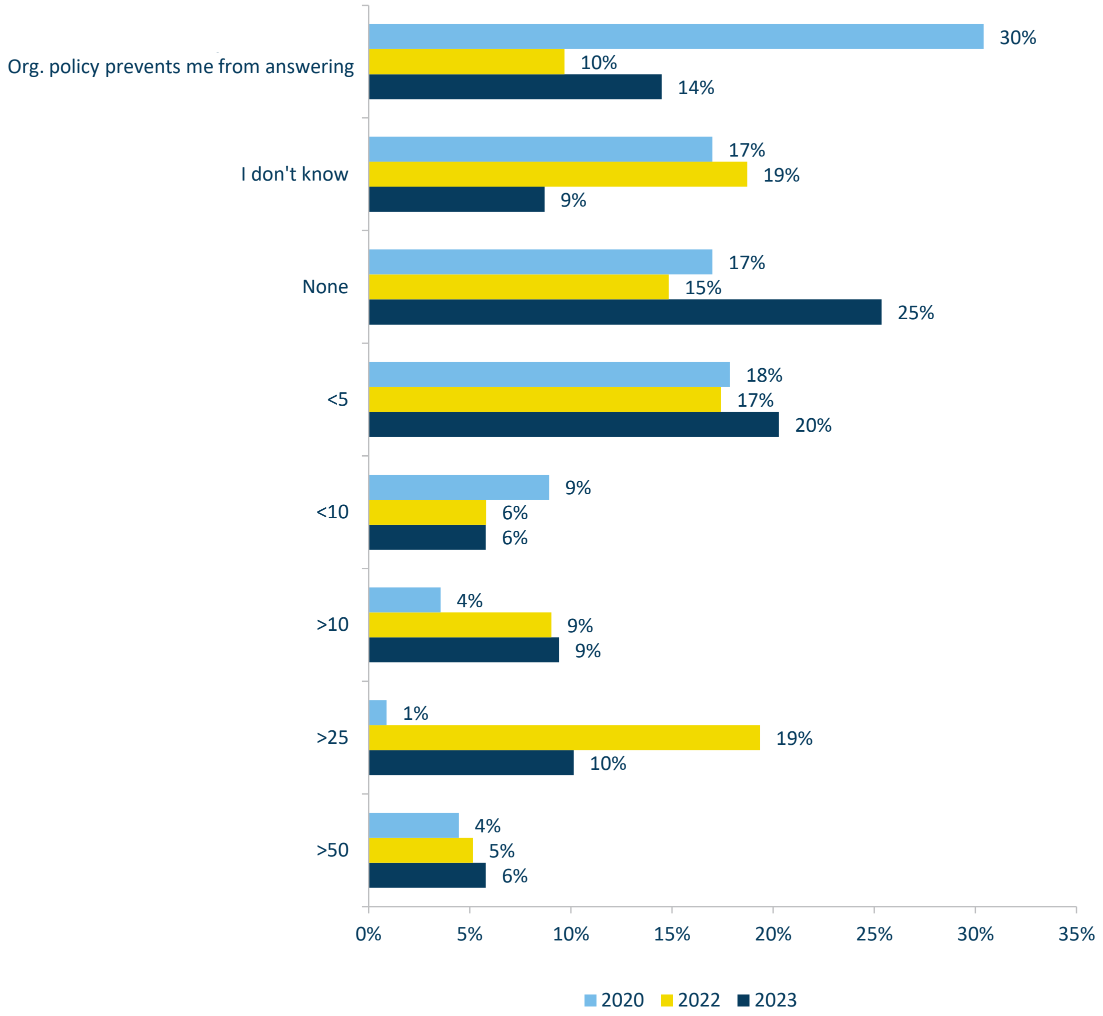
> *Cyber attacks are only expected to increase - this is the downside of the digitalization of industrial production. There is an increasing number of interfaces within an organization, but also with external partners that unfortunately increases the attack vectors.*
>
> *Therefore, a prioritized and focused approach is important to protect production systems and processes. A sound OT security approach does not only cover technical aspects, but also security processes, governance, and the human factor.*
>
> *Key for the prevention, detection and defense is to stay up to date. Because OT cybersecurity is characterized by two crucial features: Change and Speed.*

Marko Vogel

Partner and Head of OT Cybersecurity

KPMG in Germany

Estimates of how many control system cybersecurity incidents have occurred in your organization within the past 12 months

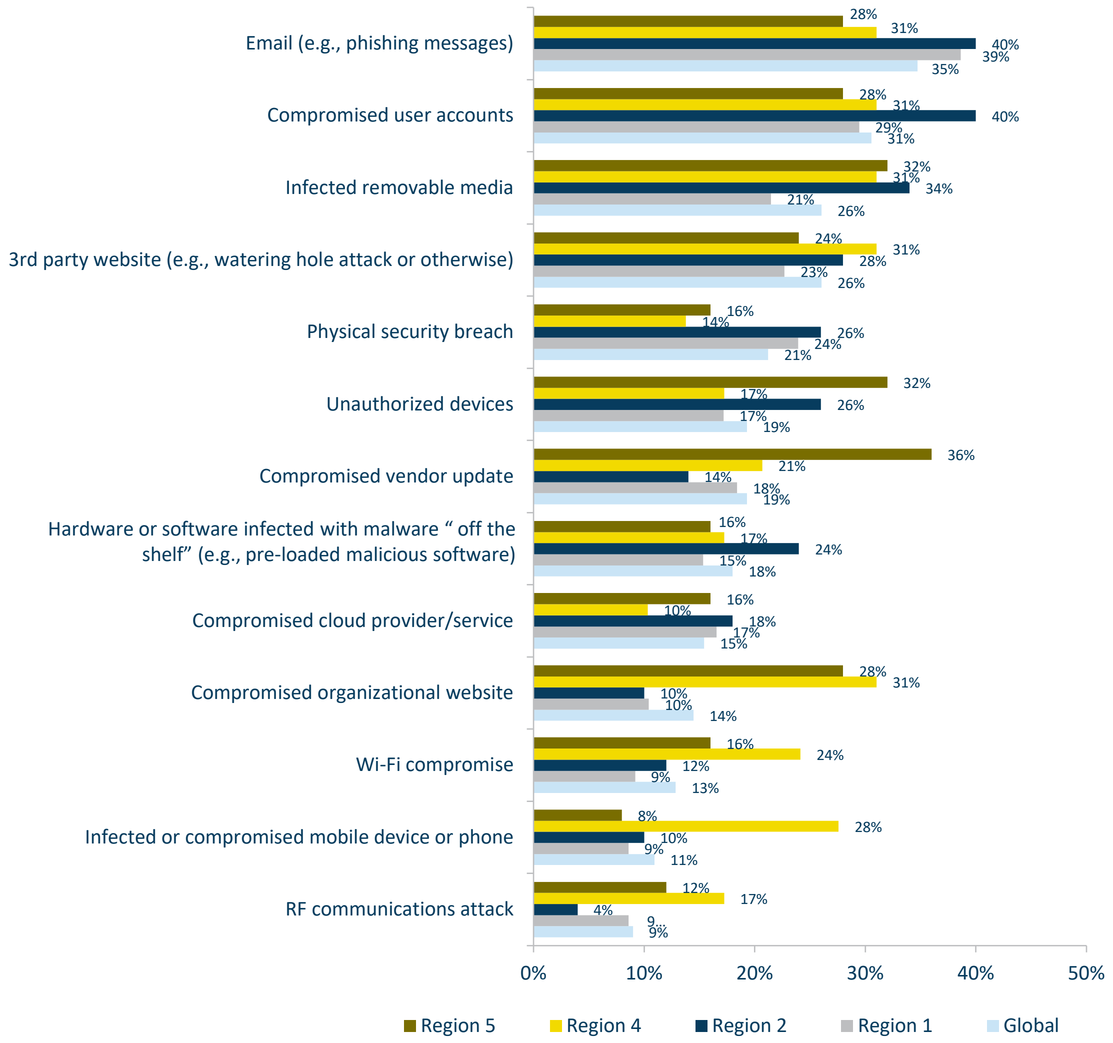


Client (CS)^2 Incident Attack Vectors – Regions[13]

Email (35% Globally) and *Compromised User Accounts* (31% Globally), potentially overlapping concerns, are the top two attack vectors this year, barely pushing *Infected Removable Media* out of second place even though it was encountered more frequently as well (24% last year, 26% this year). Region 5 (MENA) saw more *Compromised Vendor Update* incidents (36%) than any other by over 70%, while experiencing nearly the same level of *Compromised Organizational Website* activity as Region 4 (APAC) (28% and 31% respectively). Region 4 stands out for the frequency of *Wi-Fi Compromise* (24%) and *Infected or Compromised Mobile Device or Phone* (28%), both numbers well above all others.

> *In many organizations the IT Security maturity posture is greater than the OT Security posture for various compelling reasons, yet there is a great opportunity for organizations to uplift the OT security posture, enhance security operational efficiency, and elevate business innovations by applying the IT/OT cyber convergence which shall help organizations to have unified security posture, reduce attack surface, enable IIoT to facilitate digital transformation and support advanced technologies to improve decision making for many businesses.*
>
> ***Hossain Alshedoki***
>
> *Cybersecurity & Privacy Energy and Natural Resources Lead*
>
> *KPMG in Saudi Arabia*

Attack vectors in clients' (CS)^2 incidents responded to in the past 12 months



[13](CS)^{2}AI is organized into seven Regions. 1) North America; 2) Europe (Central, Western, Northern and Southern); 3) Eurasia; 4) Indo-Pacific; 5) Middle East-North Africa; 6) Sub-Saharan Africa; 7) Latin America-Caribbean

(CS)² Incident Impacts – Longitudinal Analysis

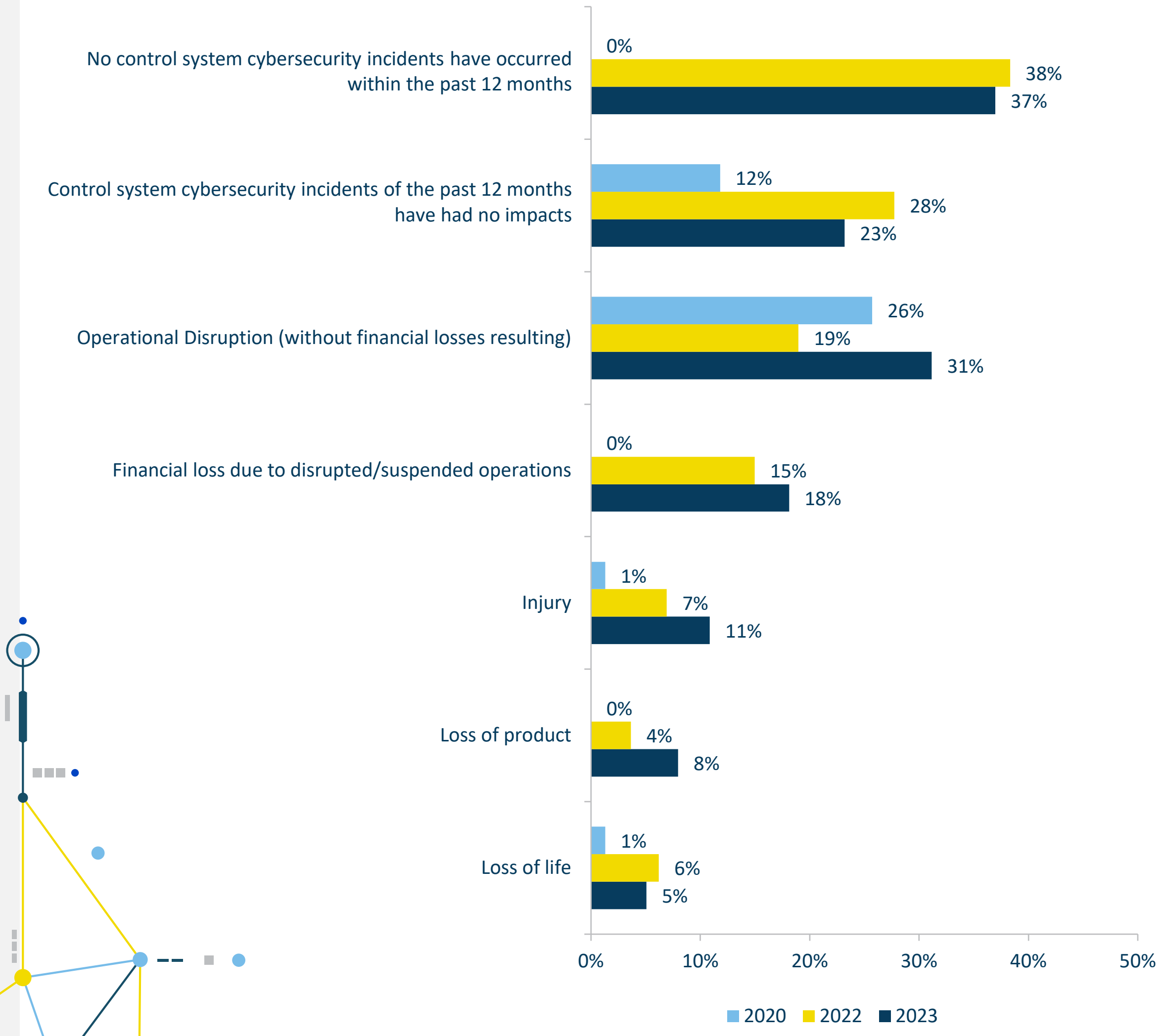
This question has changed over the years of our producing these reports, increasing the answer options to improve data (and findings) value, so there are several for which no 2020 responses were possible.

The concerning year-over-year rises in *Financial Loss Due to Disrupted Operations, Injury, Loss of Product* are the key takeaways from this data. Recall the emphasis on continuous operations revealed earlier (see charts on discretionary fund allocation priorities (page 24), vendor guidance to clients (page 25)).

The *Loss of Life* responses have been a persistent question mark over the last several years. One would expect that a malicious cyber attack causing human death(s) would be front page news. Even if the event occurs in a geography where businesses or governments suppress such reports, it is hard to see how in the last two surveys, 5-6% of respondents reported *Loss of Life* due to "cyber incidents" without a single such incident being reported in the press. Our participants include individuals protecting hospitals, health care centers, etc., where disrupted systems may directly or indirectly lead to deaths, but not so many respondents as to explain this result. Are these "incidents" in fact errors and omissions involving computers that are being confused with deliberate attacks?

> *The (CS)² survey data on intrusions show that security incidents are leading to increased disruption in operations, and that these disruptions are leading to more severe outcomes. Fortinet's 2023 State of Operational Technology and Cybersecurity Report found similar rates, with 49% of organizations experiencing some impacts in operational environments. The report also revealed that organizations reporting higher maturity experienced fewer network intrusions and fewer impacts to operations. These organizations were also more likely to include OT cybersecurity posture as a significant factor in risk reporting shared with executive leadership and boards of directors.*
>
> ***Rod Locke***
>
> *Director Product Management*
>
> *Fortinet*

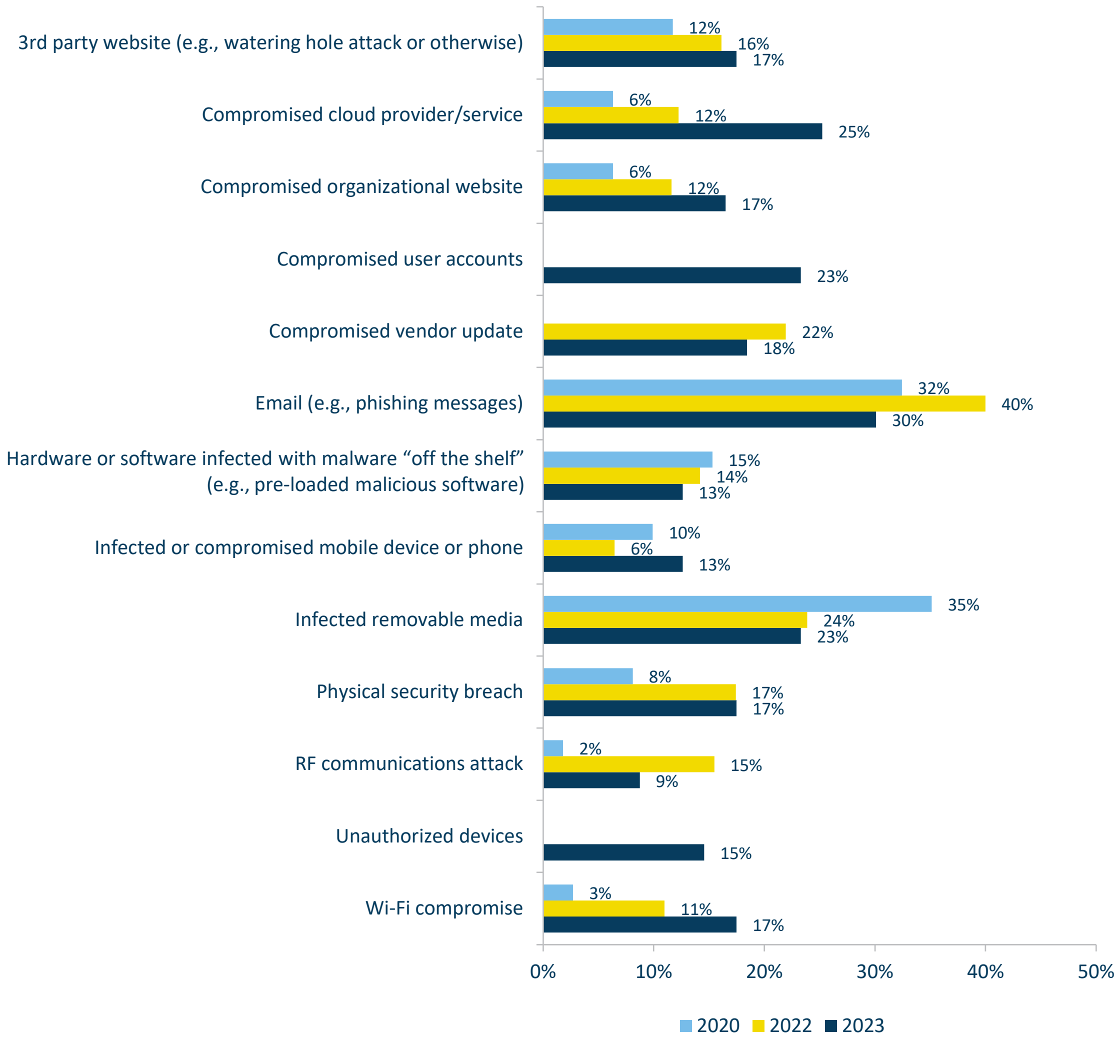
Impacts resulted from control systems security incidents at your organization in the past 12 months



Recent (CS)^2 Attack Vectors – Longitudinal Analysis

Elsewhere we considered frequency of specific attack vectors for regional differences. Here we look for year-over-year trends, finding several clear growth patterns. The ongoing increase in *Compromised Cloud Provider/Service* (2020 6% vs 2023 25%), *Wi-Fi Compromise* (2020 3% vs 2023 18%) and *Compromised Organizational Website* (2020 6% vs 2023 17%) responses are particularly noteworthy and support threat research reporting that attackers are expanding beyond phishing to other parts of their targets' attack surfaces. The *Cloud* and *Wi-Fi* may be at least partially attributable to increases in the use of those solutions within (CS)^2 environments in recent years. Note that *Compromised User Accounts* and *Unauthorized Devices* were new choices this year, so do not appear in 2020-2022 data. *Compromised Vendor Update* was added in 2022.

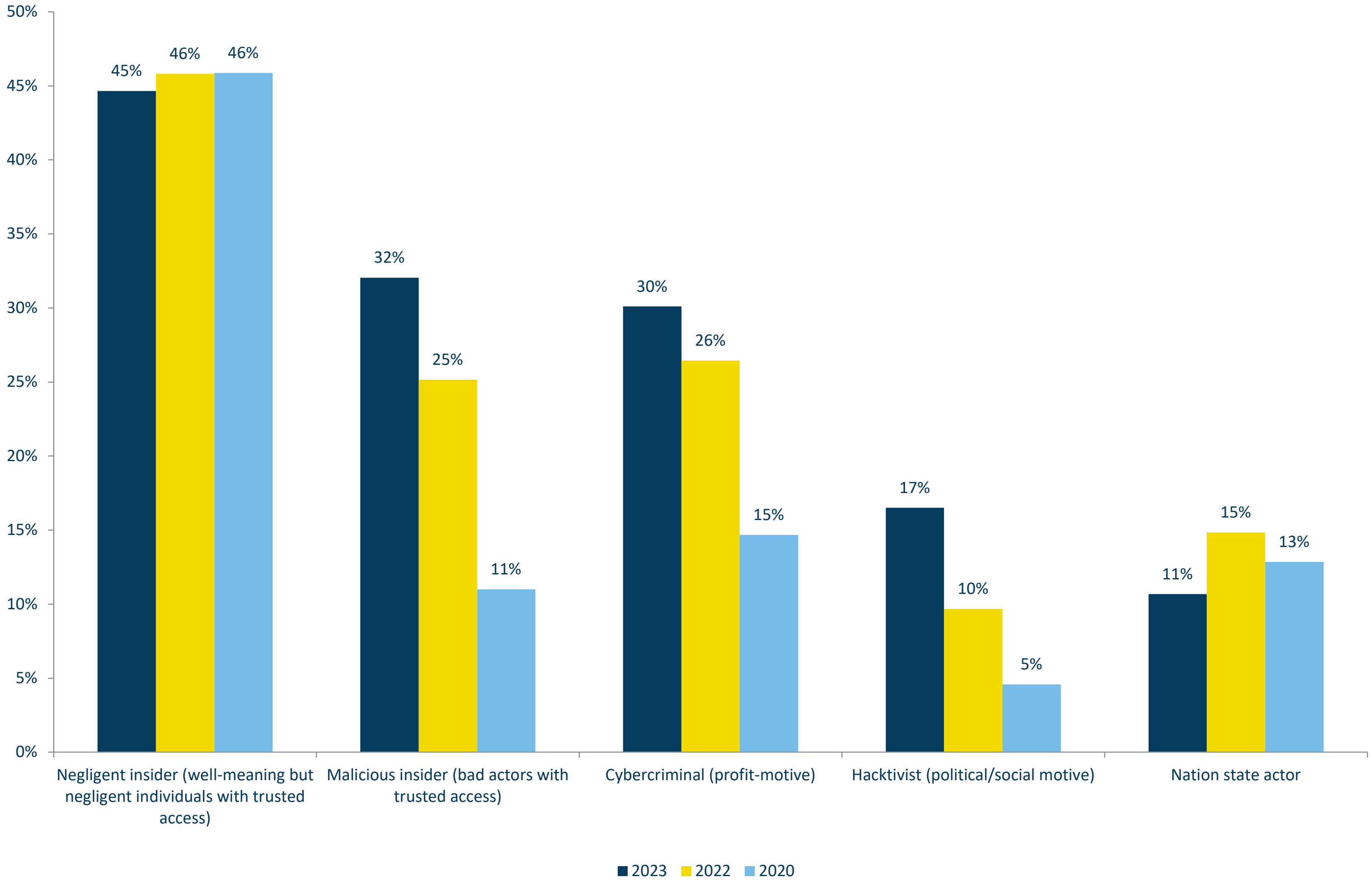
Attack vectors used in any of the (CS)^2 incidents in organizations in the past 12 months



(CS)^2 Threat Actors – Longitudinal Analysis

With *Nation State Actor* and *Negligent Insider* relatively flat (the latter continuing to be the most cited), an annual increase in reporting of *Hacktivist, Cybercriminal*, and *Malicious Insider* activity is noteworthy. We did not find any significant regional differences. Media reporting and national intelligence agencies support the belief that profit-motive driven cybercriminal activity has been increasing steeply in recent years, and our findings agree. The rise of (CS)^2 compromises from *Malicious Insiders*, on the other hand, has not been in the public eye. It may be a by-product of increasing societal divisiveness and tensions.

Threat actor(s) in recent (CS)^2 compromises



Vendor Guidance

Client KPI Focus Guidance – Vendors

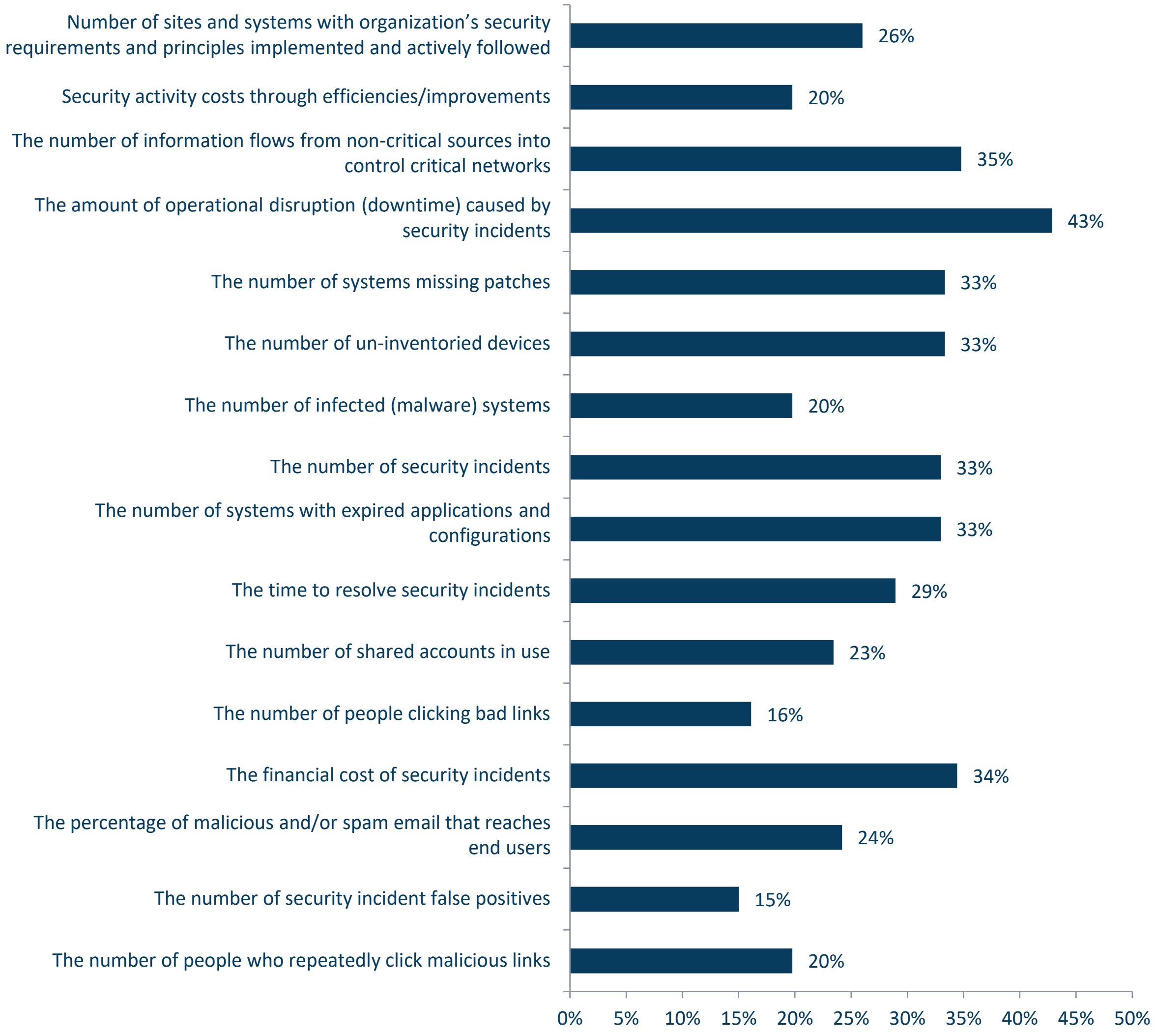
The Waterfall Security and ICSStrive 2023 Threat Report shows that attacks with OT consequences have risen exponentially over the last 4 years. Here we see the top three focus KPIs are operational disruption (downtime), the number of informational flows entering critical networks, and the financial costs of these incidents.

These KPIs show both a strong desire to both mitigate consequences and deploy robust solutions. In support of these ambitions are powerful engineering-grade solutions that both reduce physical consequences and deterministically control informational flows, solutions that are part of the new Cyber Informed Engineering strategy led by Idaho National Laboratories.

Andrew Ginter

VP Industrial Security,
Waterfall Security Solutions

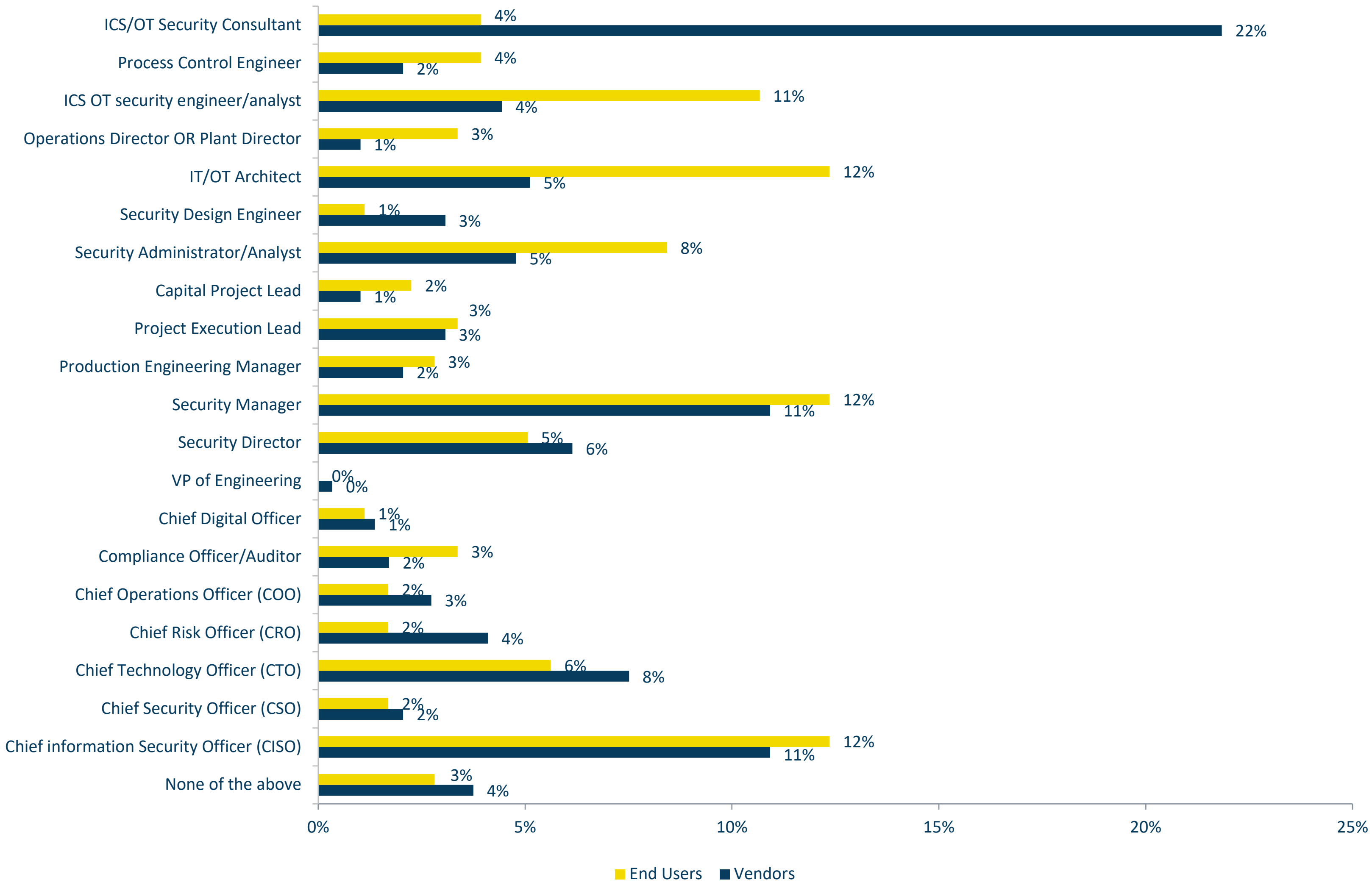
Security program KPIs for clients to focus on in the coming year



Appendix A: Demographics

Respondent Titles – End Users & Vendors

Titles of respondents in relation to control system security-related work

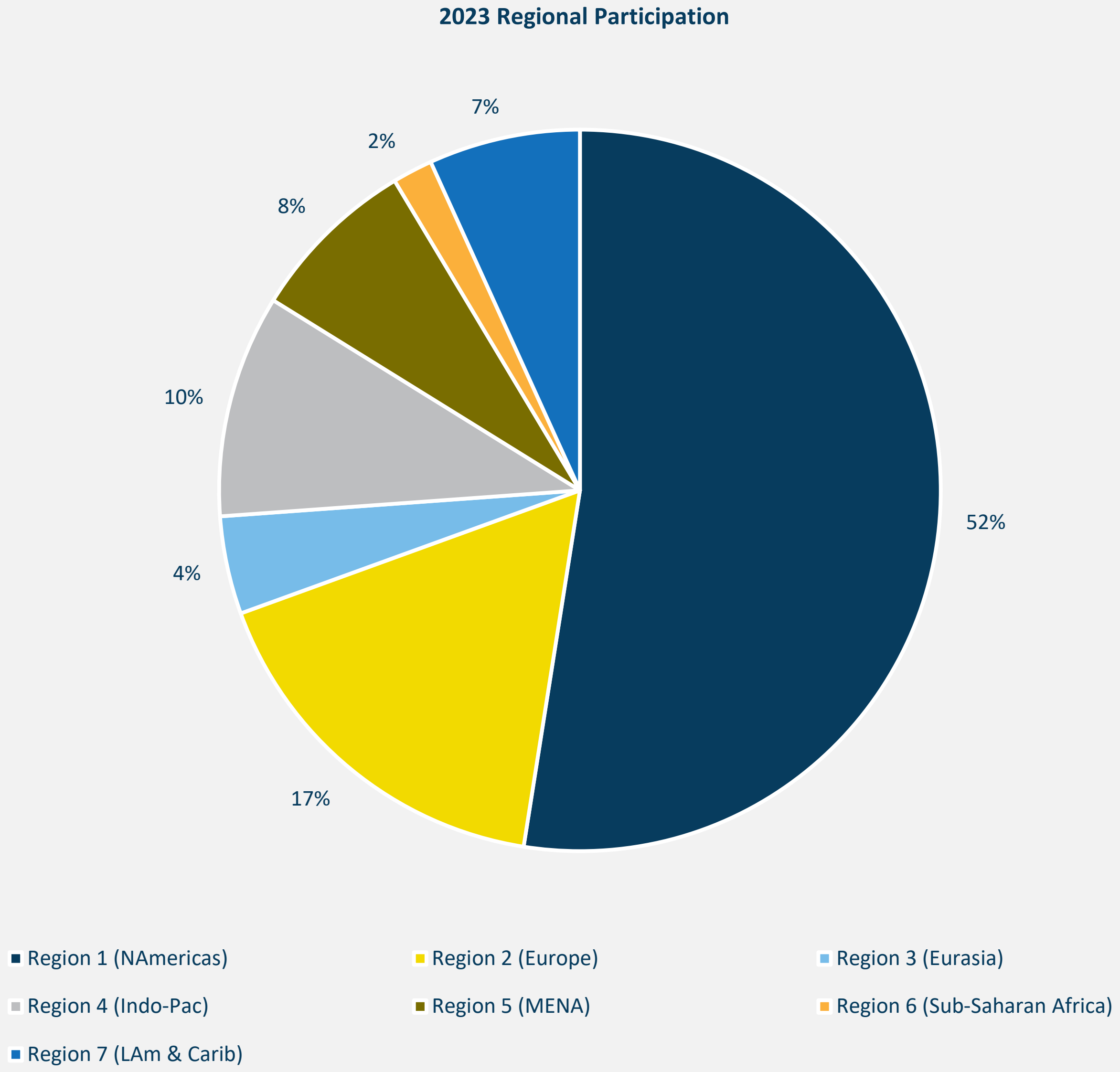


Participation by Region

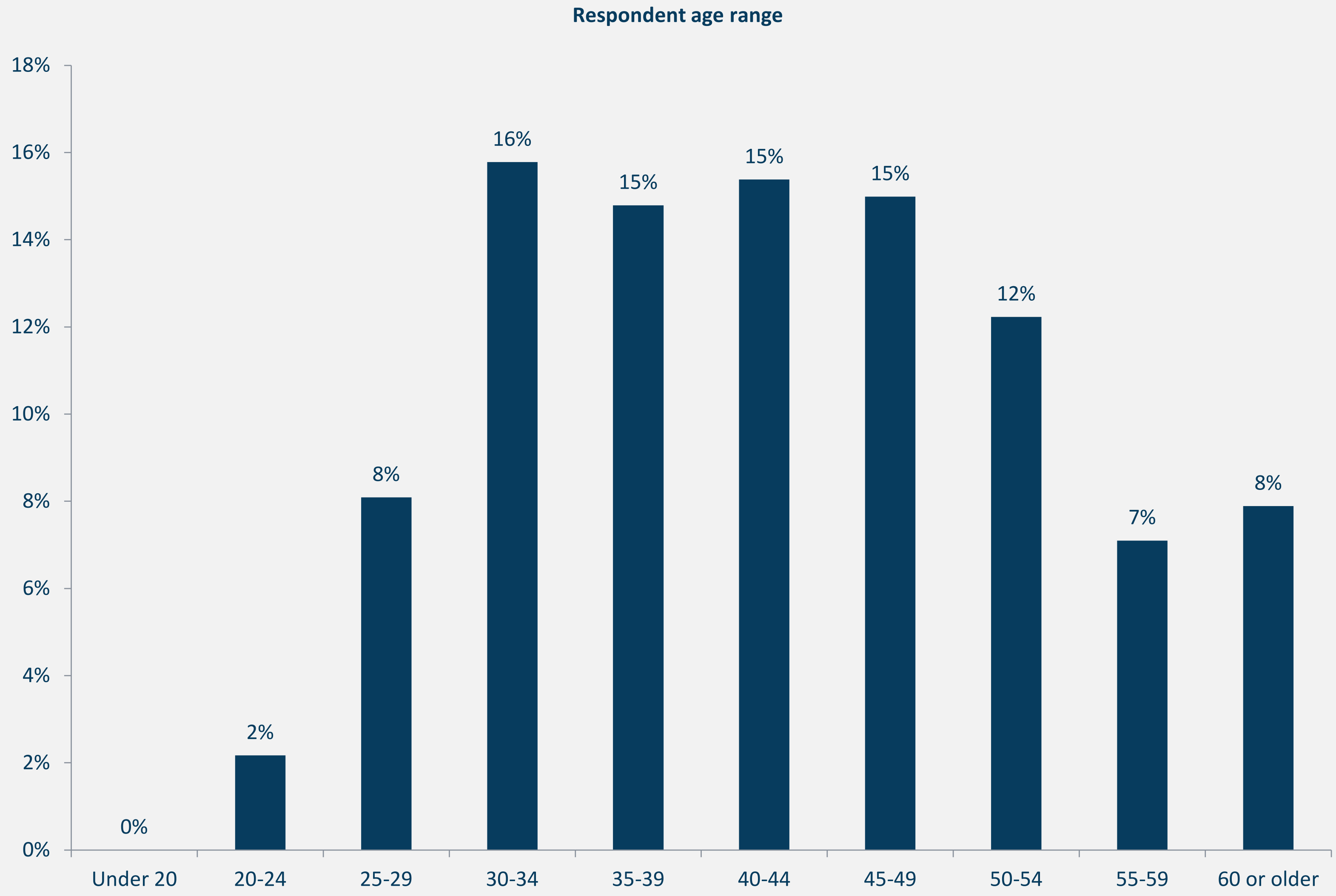
The Control System Cybersecurity Association International is organized into seven Regions:

1. North America
2. Europe (Central, Western, Northern and Southern)
3. Eurasia
4. Indo-Pacific
5. Middle East-North Africa
6. Sub-Saharan Africa
7. Latin America-Caribbean

Representation grew this year in Regions 2, 5 and 7. It is our ongoing goal to increase participation in all Regions, both to gain sufficient responses on all questions for statistical analysis and to reach more consumers of (CS)2 information, whether practitioners, managers, executives, or students.

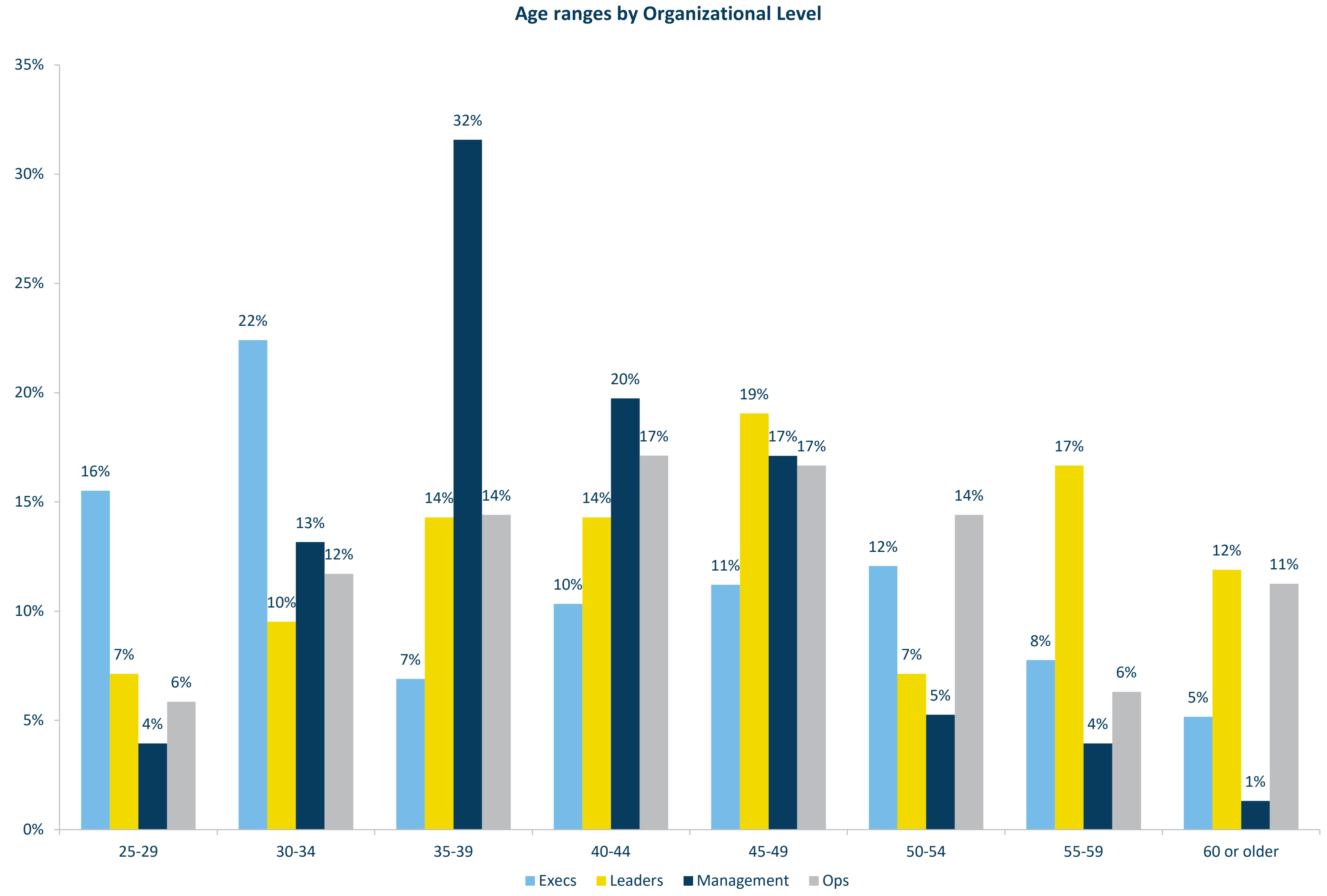


Respondent Ages



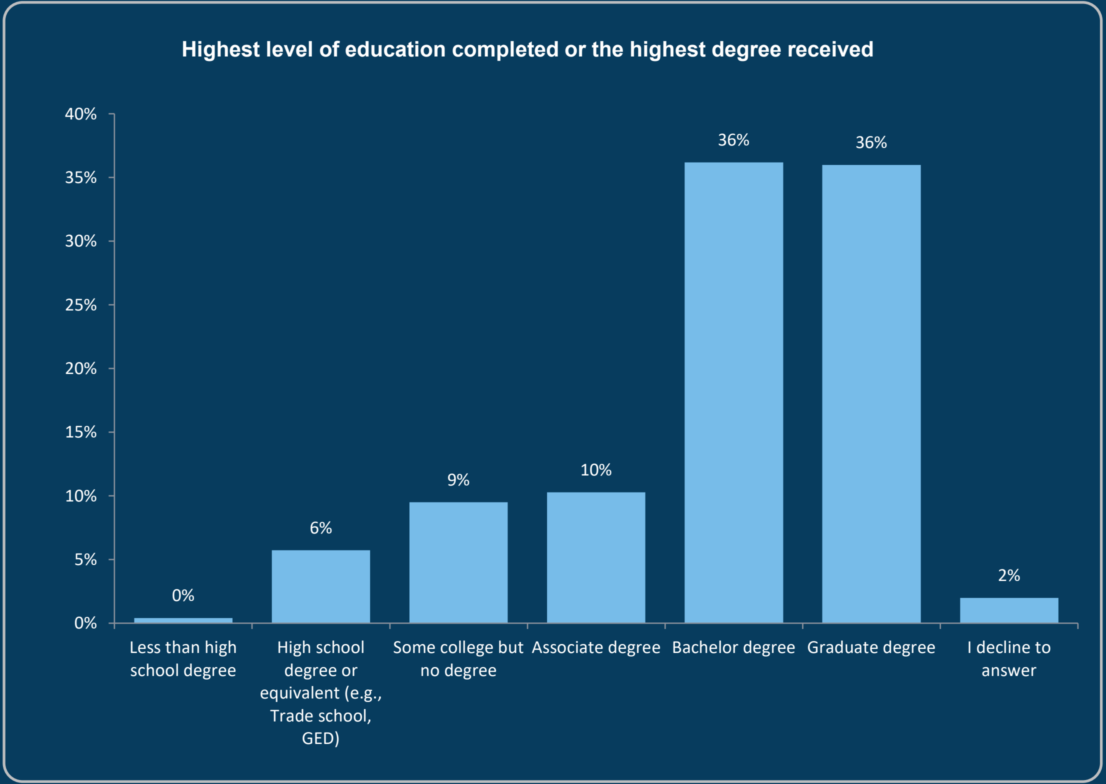
Respondent Age by Organizational Level

Strong majority (N>60%) of respondents in 30-50 age range. We tend to focus heavily on the Operations group as they work most directly with the assets/systems and make up a critical bank of technical knowledge and expertise which leaves with them when they retire. Preserving that generational store while keeping up to date with evolutionary developments is crucial to maintaining and improving protection of our control systems, so it is positive that cohorts in their mid and early careers, those learning from more senior resources, are represented in such strong numbers.



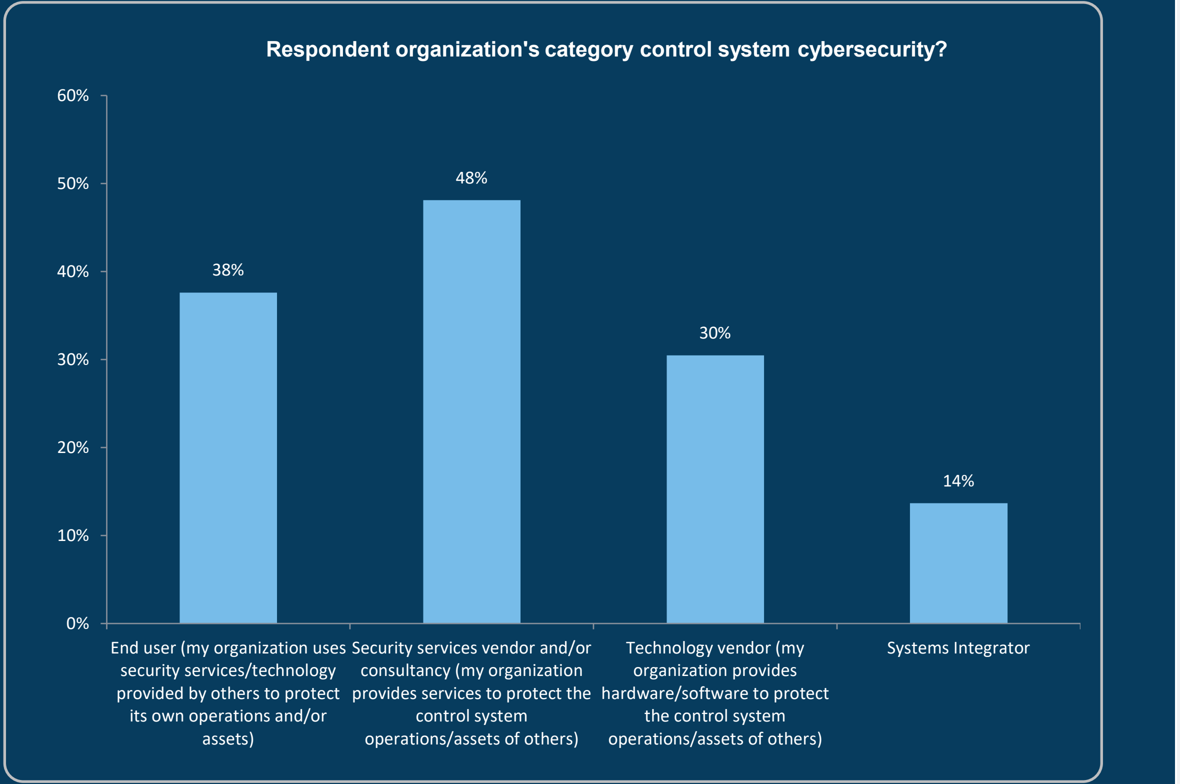
Respondent Education Levels

The profile of participant’s education is very similar to previous years.



Respondent Organizational Category

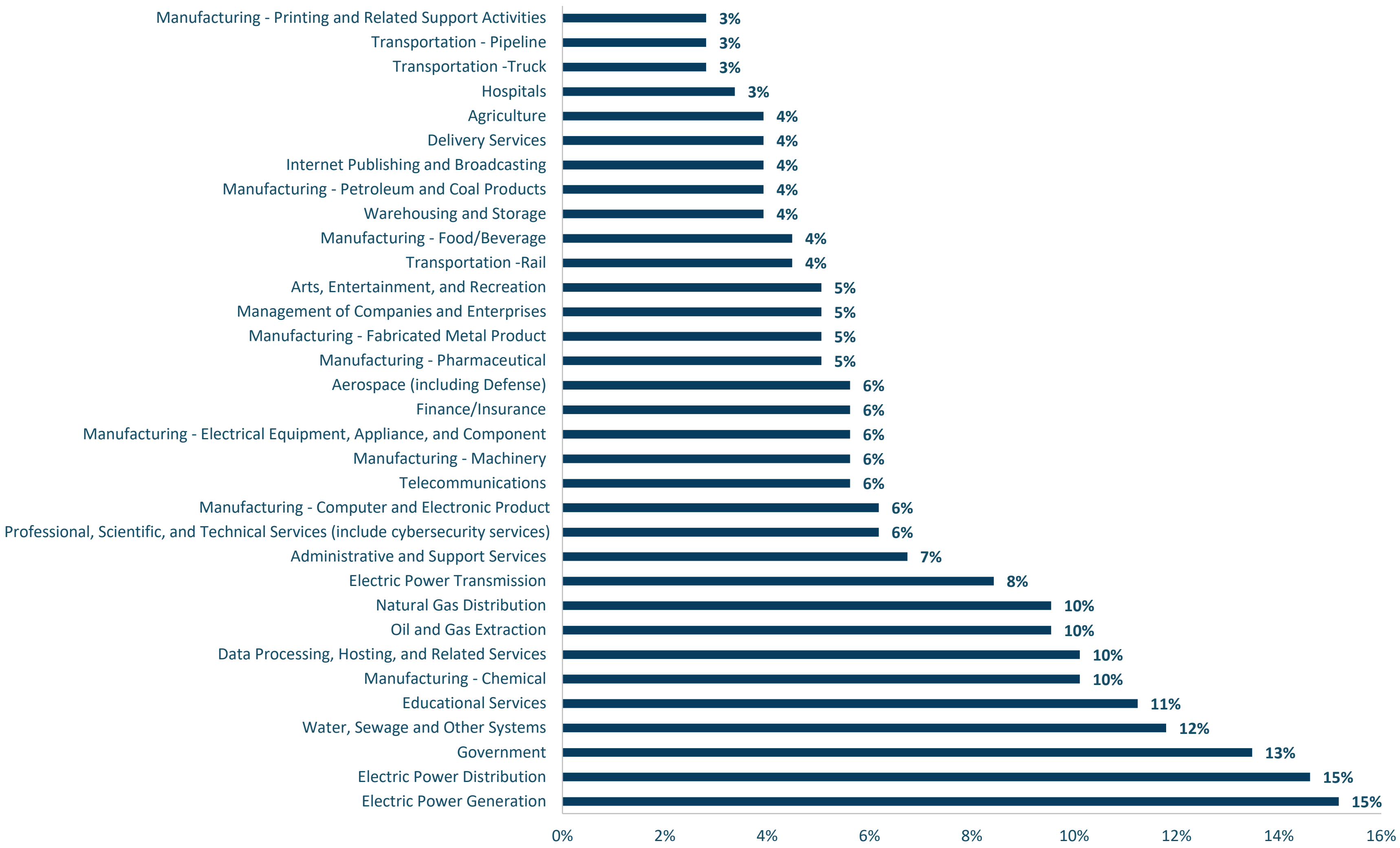
Nearly an even percentage swap between End User and Technology Vendor (EU down 10 points, TV up 7). Systems Integrator was a new category this year. This was a Pick-All-That-Apply (PATA) question, so the total is well over 100%. There was also an Other category this year, which received 5% of responses.



Participation by Industry (End Users Only)

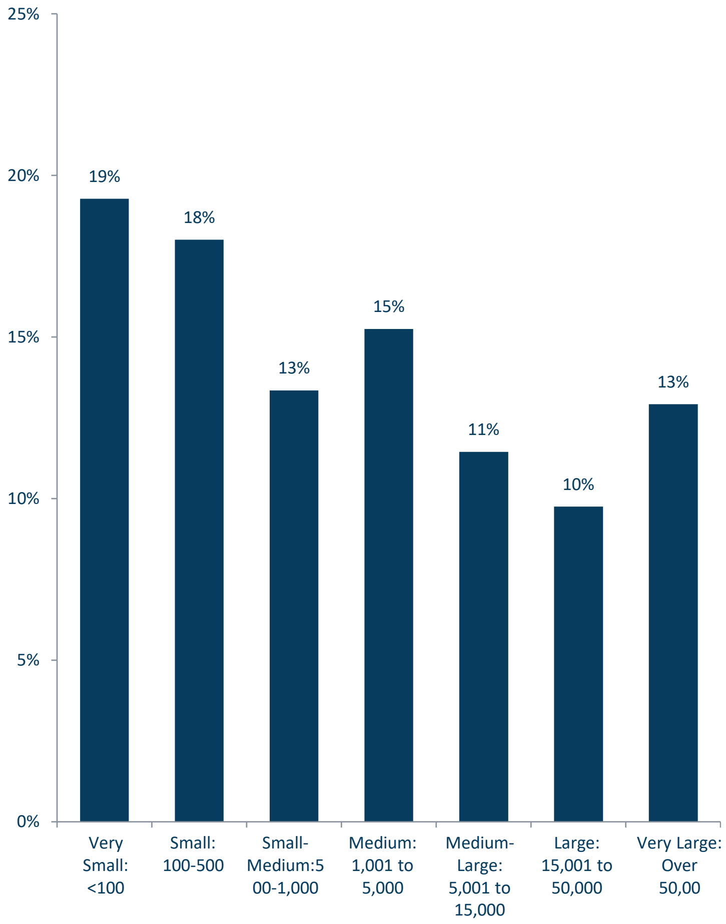
Where do organizations go to find the aid they need to protect their (CS)^2 assets, people, and operations? Everywhere they can, according to our respondents. The standout response of Internal IT Security Resources (56.2%) suggests that OT cybersecurity is being driven by IT groups in most organizations, with the concomitant likelihood that IT security methods and technologies are being applied in these environments.

Industries focused on by respondent's organization



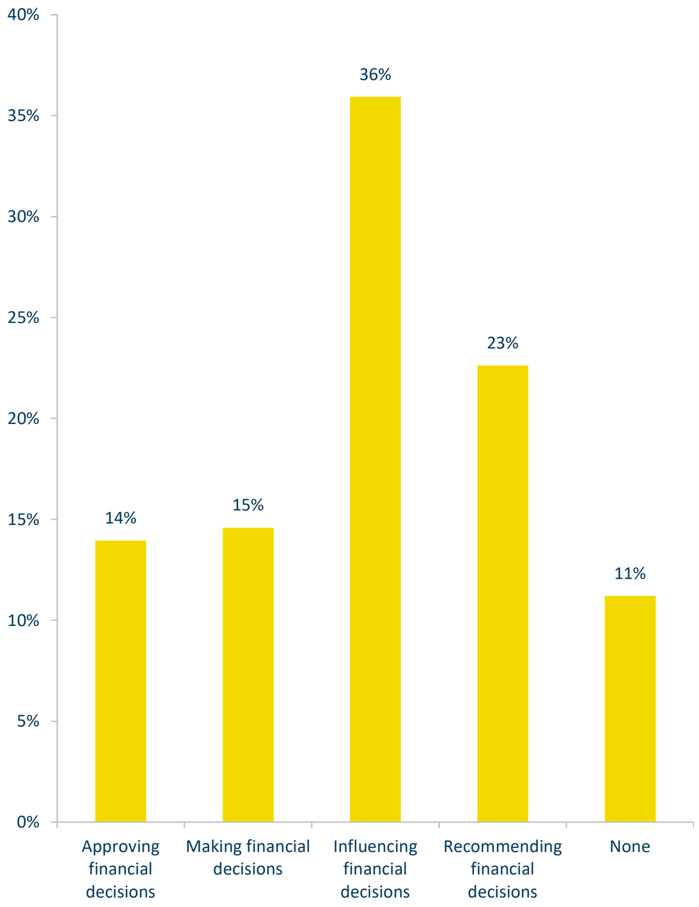
Respondent Organization Sizes

Best estimates of organization's workforce size



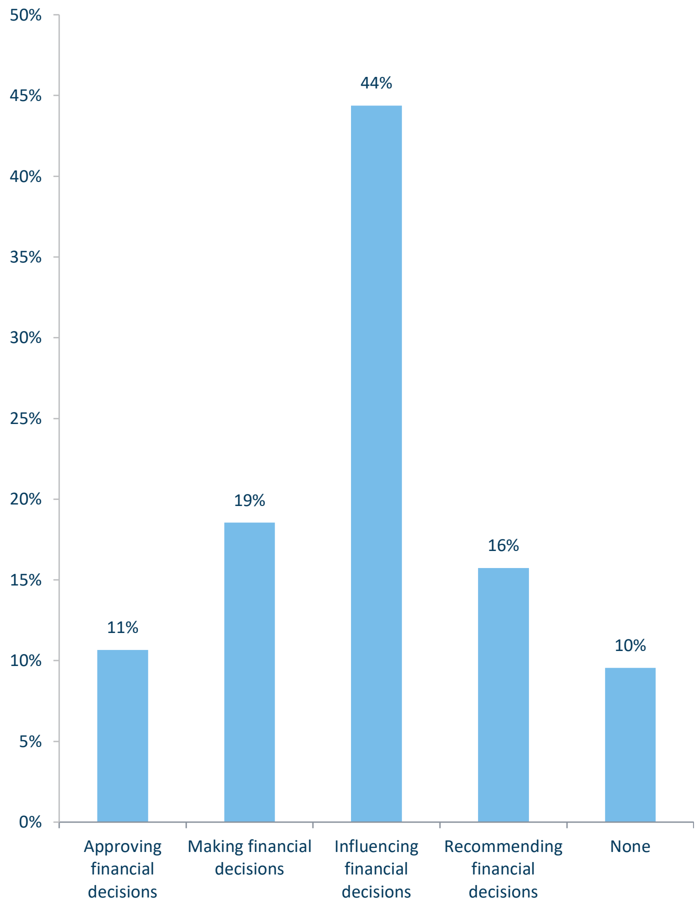
Respondent Decision Roles

Role in making decisions on control system security-related expenditures

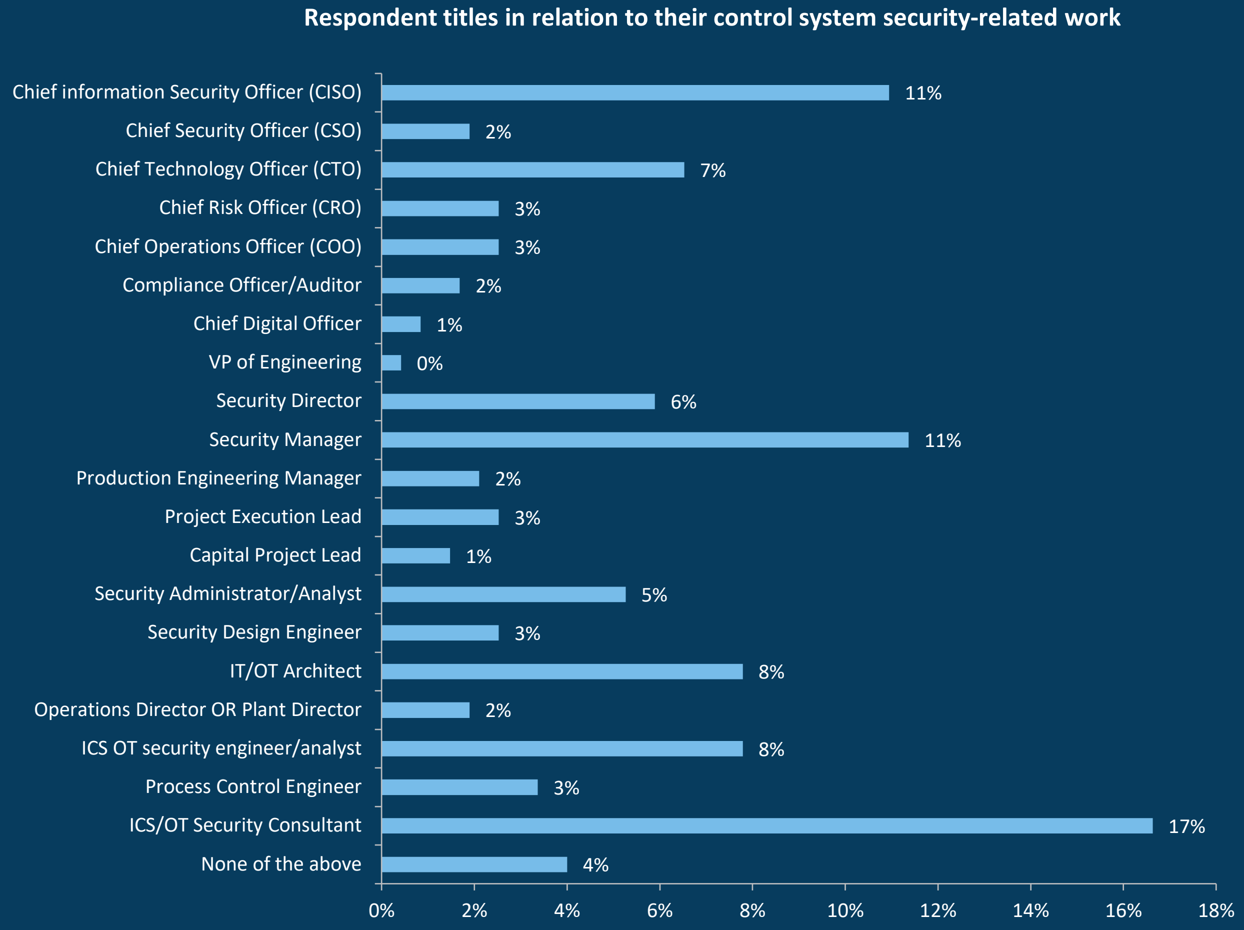


Respondent Decision Roles – End Users Only

Participant roles in making decisions on control system security-related expenditures (End Users Only)

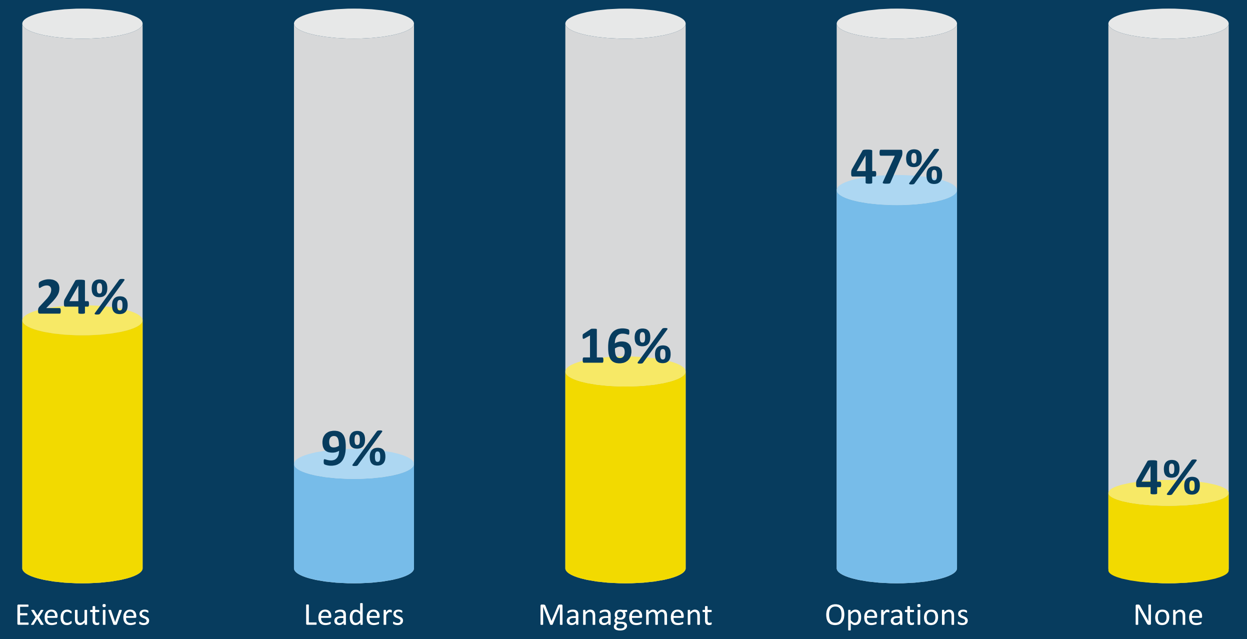


Respondent Titles and Organizational Level Representation



Respondent Titles and Organizational Level Representation (cont.)

Respondent Organizational Level Representation



Appendix B: Annual Report Steering Committee & Contributors

Derek Harp

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

derek.harp@cs²ai.org

Bengt Gregory-Brown

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

bengt.gregory-brown@cs²ai

Walter Risi

(CS)²AI Strategic Alliance Partner Liaison

Survey Design and Report Analysis Teams

Global OT Cybersecurity Leader
KPMG International and Partner and Head of Consulting, KPMG in Argentina

wrisi@kpmg.com.ar

Andrew Ginter

Survey Design and Report Analysis Teams
(CS)²AI Founding Fellow

Author and Lecturer
VP Industrial Security
Waterfall Security Solutions

andrew.ginter@waterfall-security.com

We would like to thank the following people for their contributions to the analysis, design, and other work in developing this report.

Ana Girdner VP of Security, Cognite

Brent Huston CEO, MicroSolved

Daryl Haegley Technical Director, Control Systems Cyber Resiliency, US DoD

Mark Bristow Director, CIPIC MITRE

Michael Chipley President, The PMC Group

Rees Machtemes Director of Industrial Security, Waterfall Security Solutions

Rod Locke Director of Product Management, Fortinet

Steve Mustard President & CEO, National Automation

Vivek Ponnada Technology Solutions Director, Nozomi Networks

Anish Mitra, Director, KPMG in India

Hossain Alshedoki, Director, KPMG in Saudi Arabia

Jayne Goble, Director, KPMG in the UK

Craig Morris, Director, KPMG Australia

Joshua Turner, Consultant, KPMG in Japan

Brad Raiford, Director, KPMG in the US

Pablo Almada, Partner, KPMG in Argentina

Thomas Gronenwald, Senior Manager, KPMG in Germany

Marko Vogel, Partner, KPMG in Germany

Eddie Toh, Partner, KPMG in Singapore

Sarah Puziewicz Senior Associate, KPMG in Germany

Valentin Steinforth Cybersecurity Consultant, KPMG in Germany

Appendix C: About (CS)²AI

Vision

Strengthen global critical infrastructure by fostering control system cybersecurity peer-to-peer networking and development.

Mission

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

Goals

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

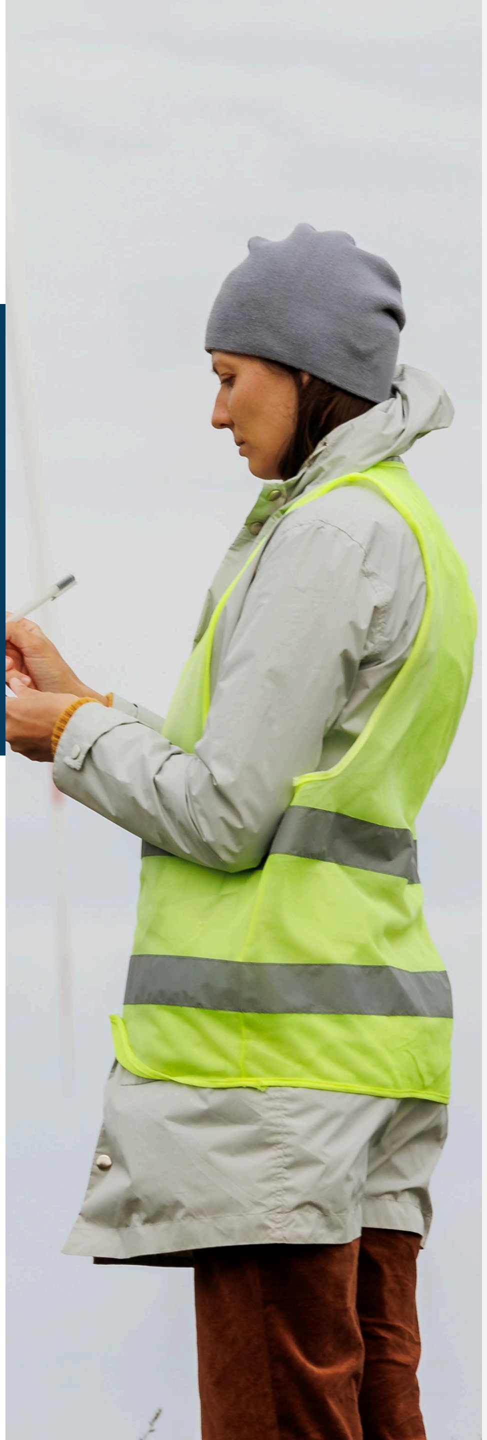
(CS)²AI ("See-Say" for short) is a rapidly growing global nonprofit association approaching 34,000 members worldwide. The premier global not-for-profit workforce development organization supporting professionals of all levels charged with securing control systems. We provide the platform for members to help members, foster meaningful peer-to-peer exchange, continue professional education and directly support cybersecurity professional development in every way.

https://www.cs2ai.org

Peer-to-peer networking on a global scale

As a member of (CS)²AI, you join a global community of Control System Cybersecurity 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.

If you are not already an active member of the Control System Cybersecurity 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.



Appendix D: Report Sponsors

Tier 1 Sponsor

KPMG

Tier 3 Sponsor

Fortinet
Waterfall Security Solutions

Tier 5 Sponsor

Opscura
Network Perception

Tier 6 Sponsor

Bridewell

Walter Risi

Global OT Cybersecurity Leader
KPMG International and
Partner and Head of Consulting
KPMG in Argentina

Pablo Almada

Global OT Cybersecurity Deputy Leader
KPMG International and
Partner and Head of OT Cybersecurity
KPMG in Argentina

http://www.cs2ai.org/

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.

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 kpmg.com/governance.

CREATE: CRT152075