FIREEYE™

Cyber Trendscape 2020

Contents

Executive Summary

Welcome to the 2020 FireEye Cyber Trendscape report.

In 2019, FireEye worked with KANTAR, an independent market research organization to perform a large-scale cyber security research initiative involving over 800 senior executives from North America (U.S. and Canada), Europe (France, Germany and the UK) and Asia (China, Japan and South Korea).

The goal of this initiative was to identify trends impacting cyber security decisions, the top cyber security priorities for 2020 and beyond, the focus of risk mitigation strategies, and to highlight the overall beliefs and perceptions held by senior executives regarding the state of the cyber threat landscape and how the cyber security industry, governments and regulatory agencies are responding to their needs.

The study highlights five cyber security focus areas within organizations:

- The cyber threat landscape
- Top cyber security program initiatives and overall maturity
- Balancing the needs of business operations and ensuring resilience to cyber threats
- Supporting security operations
- Driving cyber security efficiency

The report provides direct insights that will help organizations benchmark their cyber security initiatives, offers data points on leading issues that can be used to support critical decision making and provides context for discussions with senior leadership, board members and other key stakeholders.

Key Findings

While the findings include regional nuances, representatives from participating organizations were remarkably consistent in their views and perspectives of cyber security. Also, different attitudes appeared to influence how individuals and organizations approach cyber security across the world.

Cyber Environments

Over 90% of organizations believe cyber threats will stay the same or worsen in 2020 and the top three industry sectors believed to be the most likely targets of a cyber attack are finance and banking, technology and government.

The biggest concerns for organizations during a cyber attack or breach event are loss of sensitive data, impacts to customers and business operation disruptions.

Financial Considerations

Over 72% of organizations consider the cost of cyber security to be reasonable or inexpensive for the value it provides.

To help better address their cyber security needs, 76% of organizations are planning cyber security budget increases for 2020 with most indicating planned increases of 1-9% over the current 2019 cyber security budget which, on average, is equivalent to 6-7% of the overall IT budget.

Security Approaches

Finding a balance between cyber security and operational requirements is a challenge for 63% of organizations.

In the US, 51% of organizations believe cloud is more secure than their on-premise environment however globally, 60% of organizations prefer an on-premise email system to cloud-based.

Globally, 88% of organizations have active initiatives related to the use of artificial intelligence and 86% have active initiatives on the use of block chain.

Preparation and Staffing

Globally, 51% of organizations do not believe they are ready or would respond well to a cyber attack or breach event. Nearly 29% of organizations who have cyber attack and breach response plans have not tested or updated their plans in 12 or more months. Over 40% of organizations do not have or have only very limited as-needed cyber security training for their employees.

While 91% of organization currently have or are planning to obtain cyber security insurance in the next 18 months, 56% of organizations who currently have cyber security insurance thought it difficult to find and overall expressed concerns over the value it provided.

Nearly 60% of organizations globally do not have a security information and event manager (SIEM) within their environments.

The average staffing of a security operations center (SOC) is 11-30 people and 60% of organizations who have a SOC are planning to grow this staffing level over the next 18 months. Germany has over 250% more organizations that do not have a SOC than the global average.

Views on Attacks

Organizations believe the most likely attribution for the attacks they experienced over the past 12 months are hacker groups, individual hackers and criminal organizations. Globally, nation states were considered the least likely source of cyber attacks. Only in South Korea were they considered one of the top three most likely sources.

Methodology and Participants

This research study was commissioned by FireEye and delivered by KANTAR, an independent market research organization. The results were derived from an online survey fielded in July and August of 2019 for a total of over 800 responses spanning across North America (US and Canada), Europe (France, Germany and the UK) and Asia (China, Japan and South Korea).

Setup questions were used to ensure that only cyber security executives were in the sample. The findings represent the views from three senior organizational roles with 45% of participants at C-level an above, 17% at the vice president level and 38% at the senior director level. The participants were 68% men and 32% women. Canada had the largest percentage of women participants (42%).

Higher education was universally valued with 46% of all participants possessing university degrees and a further 34% indicating they had also completed graduate studies.

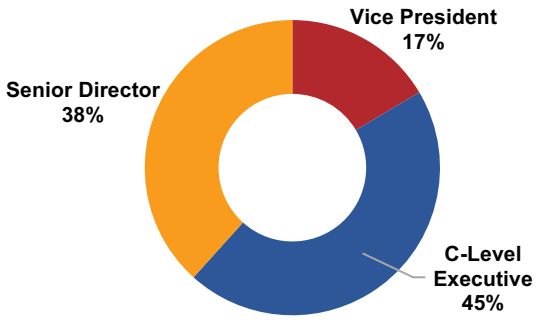


Figure 1. Participant role in their organization.

Line of Business and Industry Sector

Globally, 53% of participants reported into the IT organization, 20% reported to business operations, 13% to finance, 11% to a dedicated cyber security function and 4% to legal.

In the U.S. the breakdown was more pronounced with 78% reporting to IT, 10% to business operations, 6% to finance, 4% to cyber security and 2% to legal.

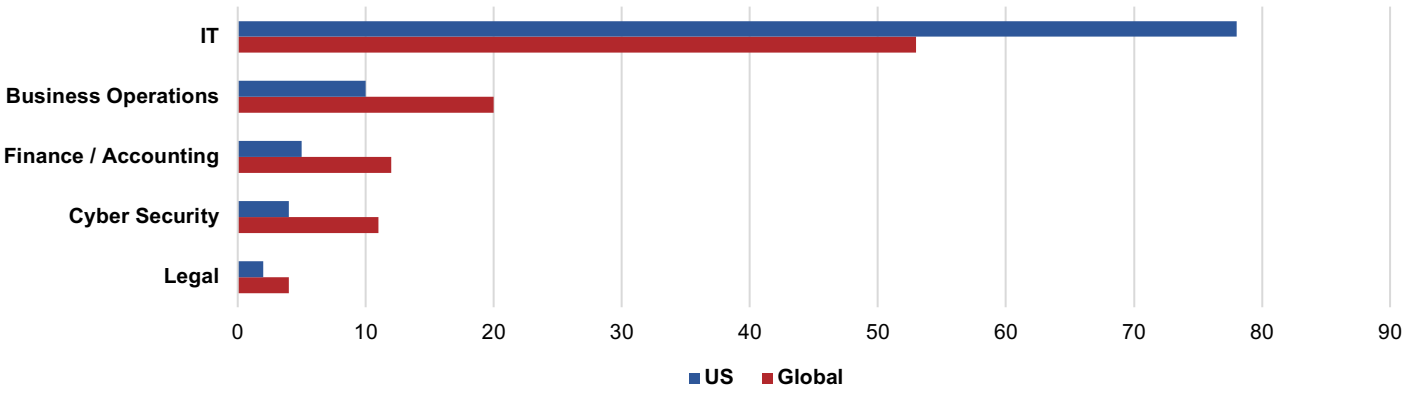


Figure 2. Department of the participant.

Participants had operational oversight, budgeting oversight and were responsible for setting the overall cyber security priorities with their organizations.

Nearly a dozen industry segments were represented in the study. The top three industries, technology, industrial and manufacturing and banking and finance accounted for 71% of all participants.

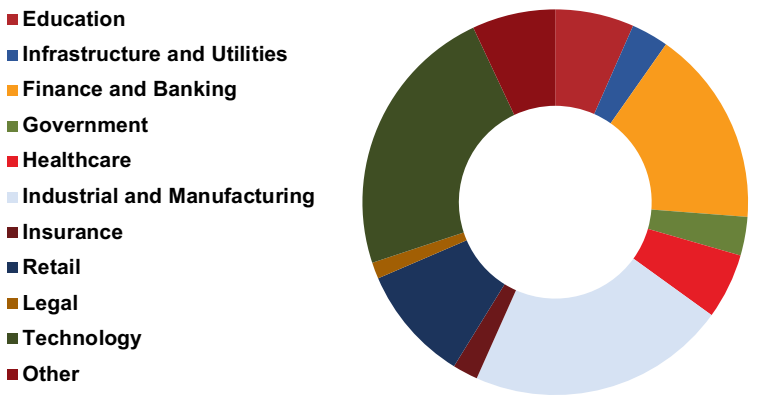


Figure 3. Participant industry segment.

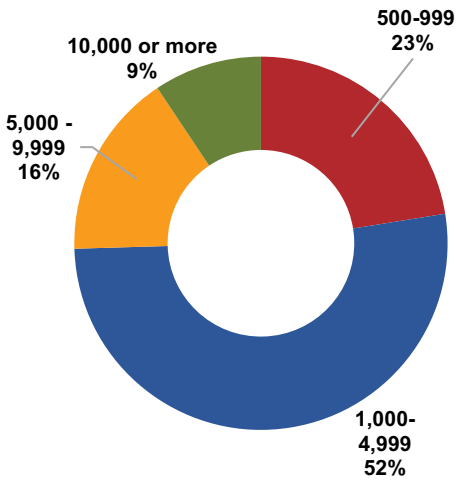


Figure 4. Participant organization size.

Organizational Structure

Sixty-two percent of participants reported that their organizations had a formal CIO or similar role, while others reported a CISO/CSO role (50%), chief compliance officer (34%), chief risk officer (26%), chief privacy officer (24%) and general counsel (20%).

The regions with the highest presence of chief compliance officers or similar roles were the UK (43%), France (41%), the U.S. (40%) and China (38%).

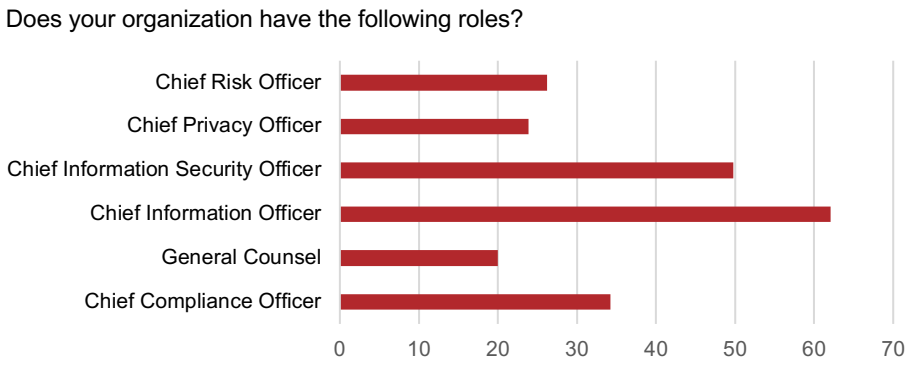


Figure 5. Presence of senior roles in organization.

Analyst Observation

While the reporting of industries and size of the participating organizations in Japan and Germany were consistent with global data, and thus not creating a bias in the survey in these countries towards the concerns, issues or operations of a particular type of organization, 14% of participants from Japan and 12% from Germany reported that their organizations lacked any of the formal roles identified in the study, contrasting sharply with an average of less than 3% for similar responses from each of the other regions.

Assessing and Addressing Cyber Risks

Organizations were asked to provide their assessment of the 2020 cyber security threat landscape and their plans for addressing cyber risks. This included insights into:

- Their cyber security budgets and the focus of their risk mitigation strategies.
- Their assessment of the performance and value of cyber security solutions and of government and regulatory agencies.
- The most likely and most vulnerable targets of cyber attacks.
- The most likely source of cyber attacks they experienced over the past 12 months.

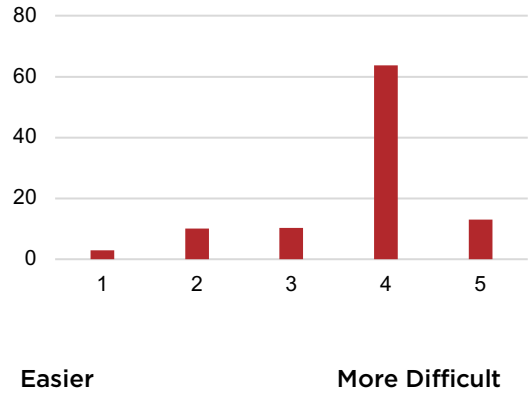


Figure 6. Understanding and defending against cyber threats.

The overall perception of the outlook for cyber risks in 2020 by global participants was grim with 56% believing that it would worsen over the next 12 months and 33% were of the opinion it would stay the same. The most pessimistic participant views were from U.S. (74%) and Japan (72%) where risks from cyber threats were expected to worsen over the next 12 months.

Participants also believed that cyber threats were becoming more difficult to understand and defend against. Responses 4 and 5 ("more difficult") accounted on average a total of 70% of responses globally. However, in Canada and Korea, 84% of respondents chose responses 4 and 5, signaling increased concerns in these countries over the evolving complexity of the cyber threat landscape.

Balancing Cyber Security and Operations

Organizations universally reported that it was more difficult to find a balance between cyber security and operational requirements with 14% reporting it to be very difficult and 49% difficult. Only 14% of organizations found it easy and 3% found it easier to find a balance. Globally, 18% of organizations were neutral on the issue.

Participants from Japan reported that 54% of their organizations found it difficult and 18% very difficult to find a balance between cyber security and operational requirements as did organizations in Germany with 53% reporting difficult and 13% more difficult.

In France, 26% of organizations reported that it was neither easier nor more difficult than before to find a balance between cyber security and operations requirements.

There were no significant regional differences for organizations that indicated it was easy or easier to find a balance between security and operations; they corresponded closely to global results.

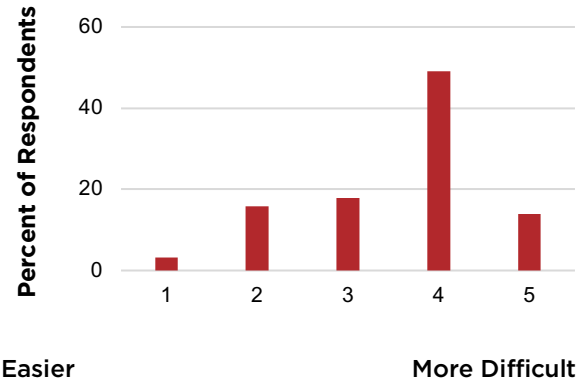
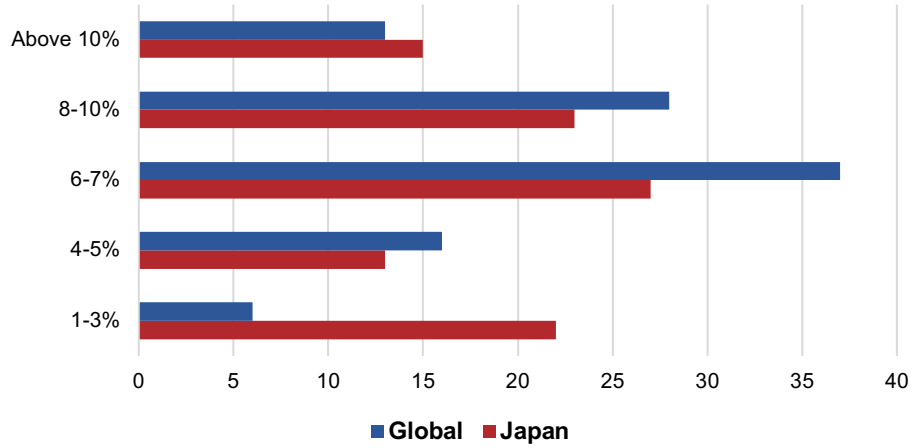


Figure 7. Ease of finding a good balance between cyber security and operational requirements.

Cyber Security Budgets

When planning to protect themselves against the cyber threat landscape, 78% of organizations reported security budgets that were over 6% of the overall IT budget. The largest concentration of responses accounted for 37% of the total and identified security budgets in the 6-7% range.



Analyst Observation

In the US, 25% of participants indicated they had security budgets representing a greater than a 10% share of the overall IT budget. The largest security budgets outside of the US were identified in China (19%) and France (16%).

Japan was the most frugal in terms of security budgets with 22% of organizations reporting a spend of only between 1-3% of the overall IT budget. This is notable, considering that 72% of organizations in Japan perceived the risks from cyber threats worsening over the next 12 months.

Figure 8. Current size of security budget as a percentage of the overall IT budget.

Globally, 76% of organizations reported planning net security budget increases in 2020. In the U.S., 39% of participants were planning security budget increases of 10% or more compared with the UK (30%), Korea (22%), China (17%), France (17%) and Canada (13%).

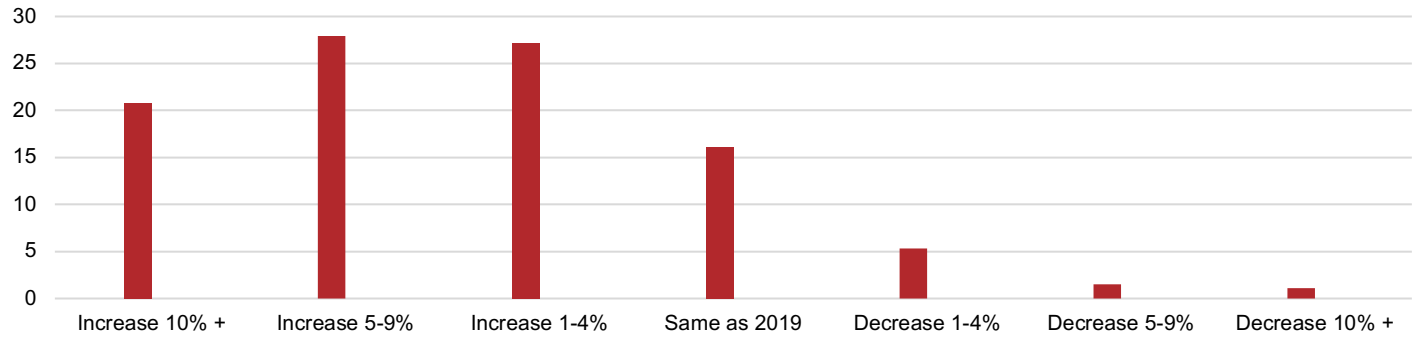


Figure 9. Planned budget change for 2020.

In Japan and Korea, a full 25% of organizations were planning to keep their 2020 security spend at the same level as 2019 compared with a global average of 13%.

The only countries where organizations were planning to decrease their security budget by more than 10% were France (3%), Japan (3%), Korea (2%) and China (1%).

Globally, organizations allocated their cyber security budgets into four main categories: prevention (42%), detection (28%), containment (16%) and remediation (14%).

Japan was the only country that changed the order slightly with an emphasis on detection being expressed by 40% of organizations followed by prevention (35%), containment (13%) and remediation (12%).

Value of Cyber Security Solutions, Government and Regulatory Agencies

Organizations broadly (57%) believed that the cost of cyber security was reasonable for the value it provides. A further 25% believed it was inexpensive. Countries perceiving cyber security as inexpensive for the value it provides were Canada (42%) and the UK (38%).

Participants in Japan (29%) and the U.S. (28%) believed cyber security was expensive for the benefits it provides.

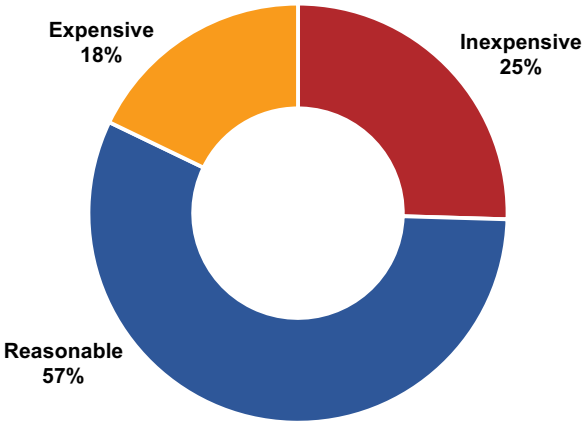


Figure 10. Value of cyber security spend for value provided.

Participants offered a mixed view, nearly equally positive and negative, in their assessment of technology providers and cyber security vendors, and how well they were protecting their environment.

Only 8% believed that technology providers and cyber security vendors were doing a very good job of protecting their environments which is similarly low to the 6% assessment for a very bad rating. Nearly matching results were also obtained for good with 34% and bad with 30%. Lastly 22% of organizations did not favor a net positive or negative assessment.

Organizations were slightly more positive in their assessment of governments and regulatory agencies and how well they were doing at protecting their environments.

A majority of participants believed governments and regulatory agencies were doing a good job (42%) or a very good job (11%). A neutral rating was provided by 19% of global respondents. Of the remaining organizations 23% believed governments and regulatory agencies were doing a bad job and 4% a very bad job.

Analyst Observation

The U.S. expressed the highest rate of the most negative views of governments and regulatory agencies with very bad gathering over 15% of the views. The U.S. response for bad was in line with other regions (21%).

China expressed the most negative perception overall with 41% reporting a bad job 4% reporting a very bad job.

The most positive perceptions were from Japan with 54% good 10% very good followed by the UK with 49% good and 15% very good.

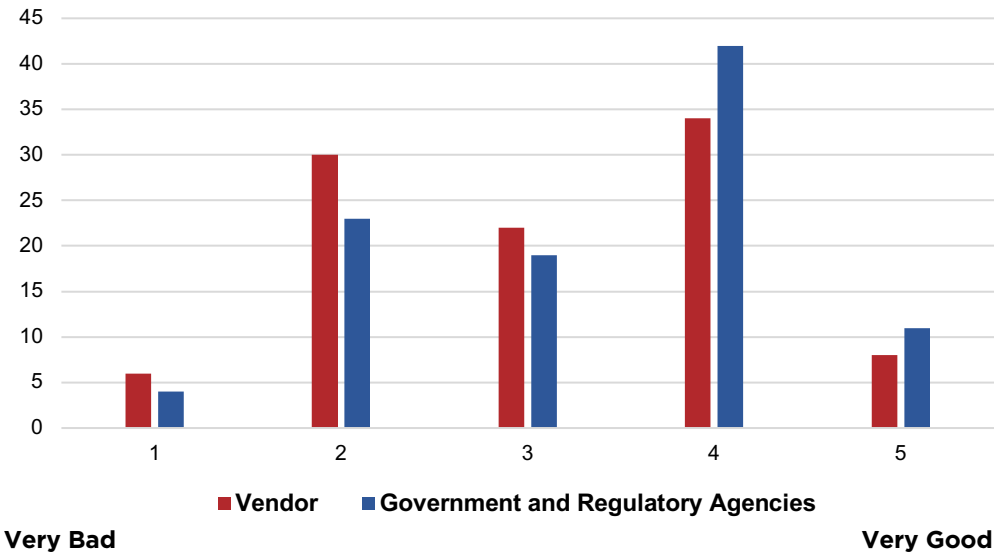


Figure 11. Scorecard of vendors, governments and regulatory agencies.

Analyst Observation

Korea expressed the most positive assessment of vendors with 35% reporting good and 14% reporting very good. In contrast, the U.S. had 36% reporting bad and 15% very bad. Japan had the highest neutral assessment with 30% of participants not favoring a net positive or negative assessment.

Cyber Attacks

Over 90% of organizations believe cyber threats will stay the same or worsen in 2020.

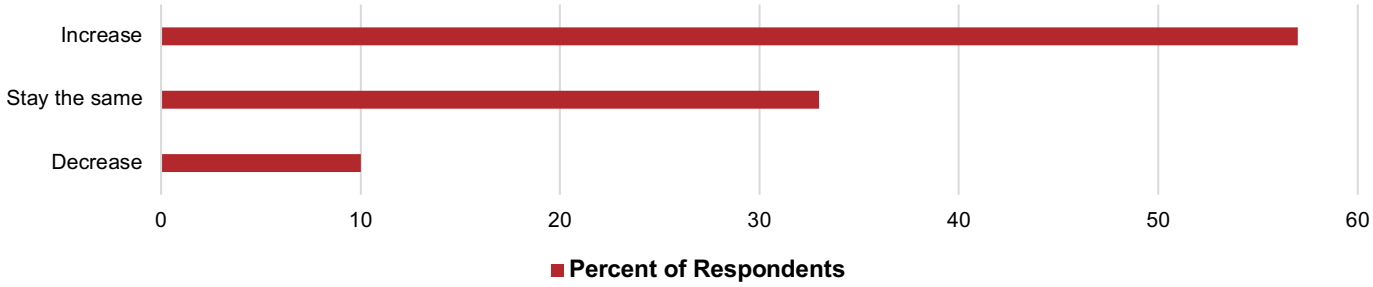


Figure 12. Expected change in cyber threats for 2020.

Participants believe that the top three industry sectors most likely to be targeted by cyber attacks are finance and banking (20%), followed by technology (16%) and government (10%).

These results were consistent across nearly all countries represented with only a modest change in emphasis between them as to which was first and second. The exception was China, where participants believe finance and banking would be the most likely target, followed by industrial and manufacturing.

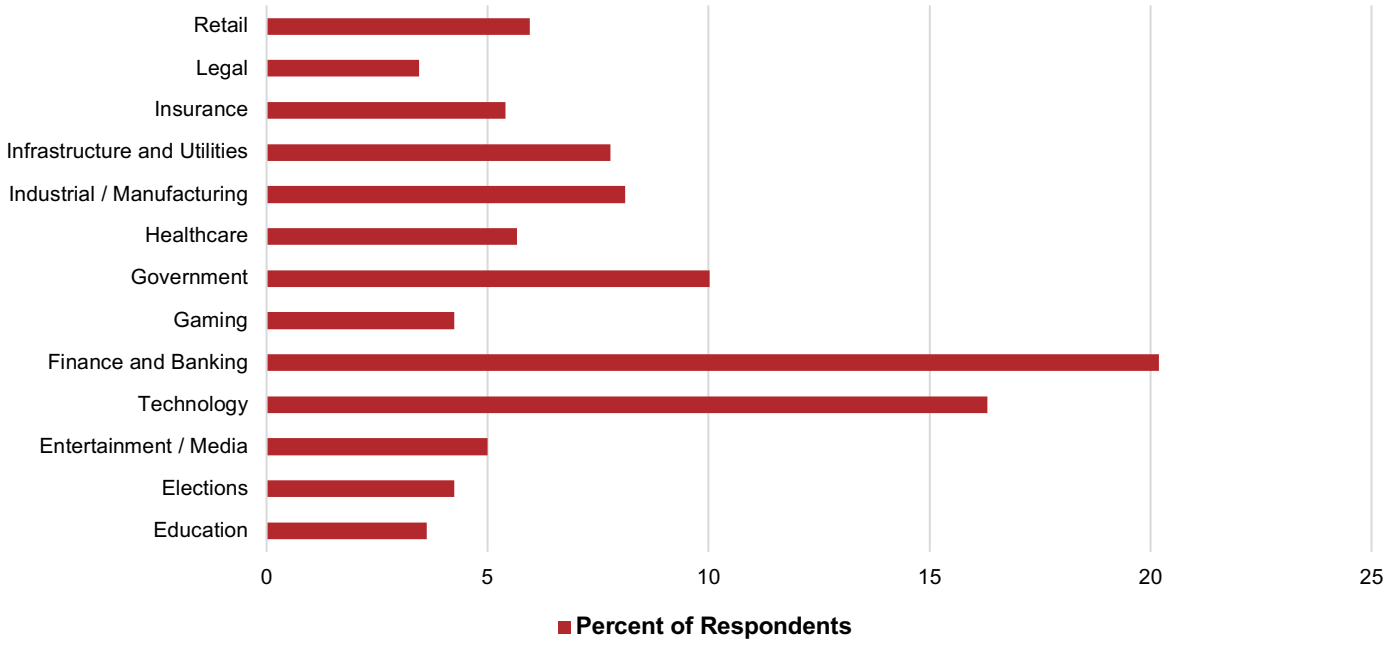


Figure 13. Industry sector most likely to be the target of a cyber attack.

Participants were asked to identify the top three components they believed to be the most likely to be targeted by cyber attacks and which top three components they believed were the most likely to be vulnerable to a cyber attack.

Participants were globally consistent in their belief that servers and server operating systems, web servers, medical devices and endpoints were the top three components in both categories.

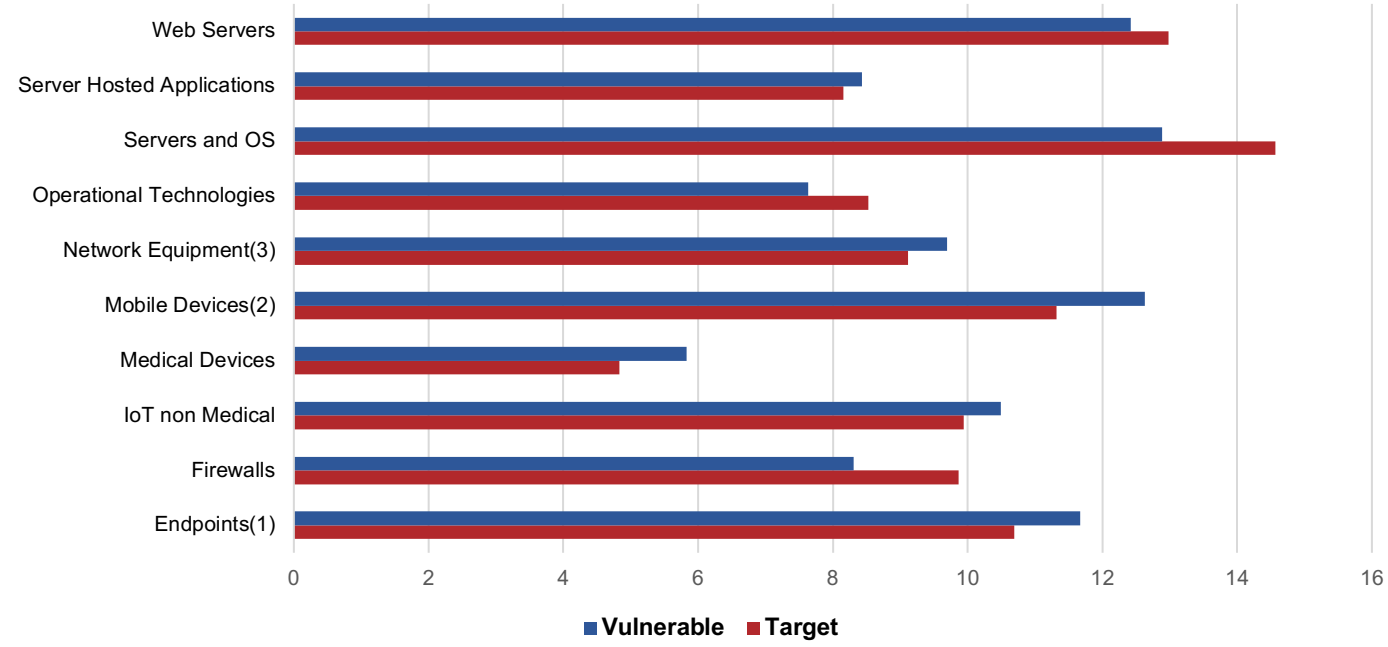
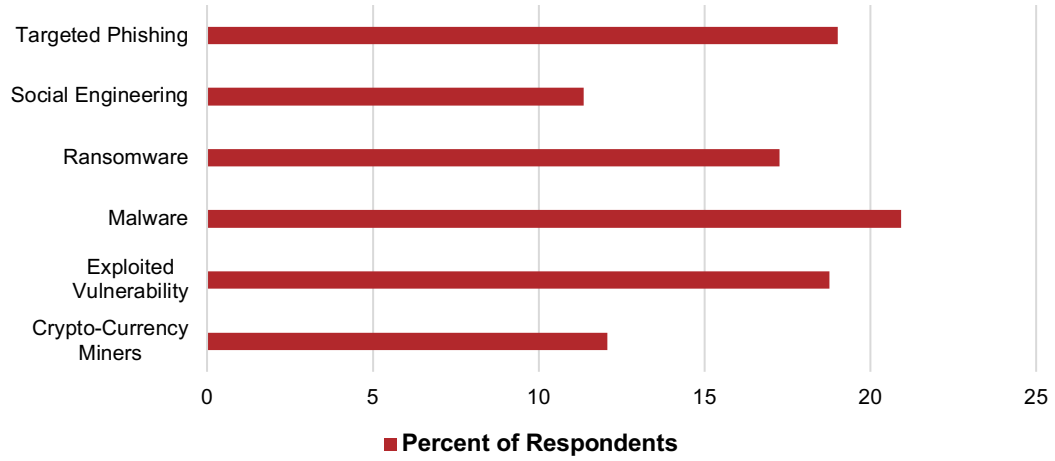


Figure 14. Components most likely to be a target of or vulnerable to a cyber attack.
Notes: (1) Laptop and desktop, (2) smart phones and tablets, (3) excluding firewalls.

Participants were asked which attack types they believed were most likely to lead to a breach. The responses globally were generally consistent, identifying the top three as malware (21%), targeted phishing (19%) and exploited vulnerability (18%).



Analyst Observation

The participants from China reported that successful attacks based on exploited vulnerabilities occurred 70% more often than the overall average. Canada and Korea reported the success of similar attacks occurred 30% more often than the overall average.

Figure 15. Types of cyber attacks most likely to be the cause a breach.

Similar findings were reported regarding the types of cyber attacks that participant organizations had experienced over the last 12 months.

Globally, 93% of organizations reported some form of successful cyber attack in the past 12 months. Fifteen percent of organizations in Japan (more than double the global average of 7%) indicated that they had not experienced a successful cyber attack in the past 12 months.

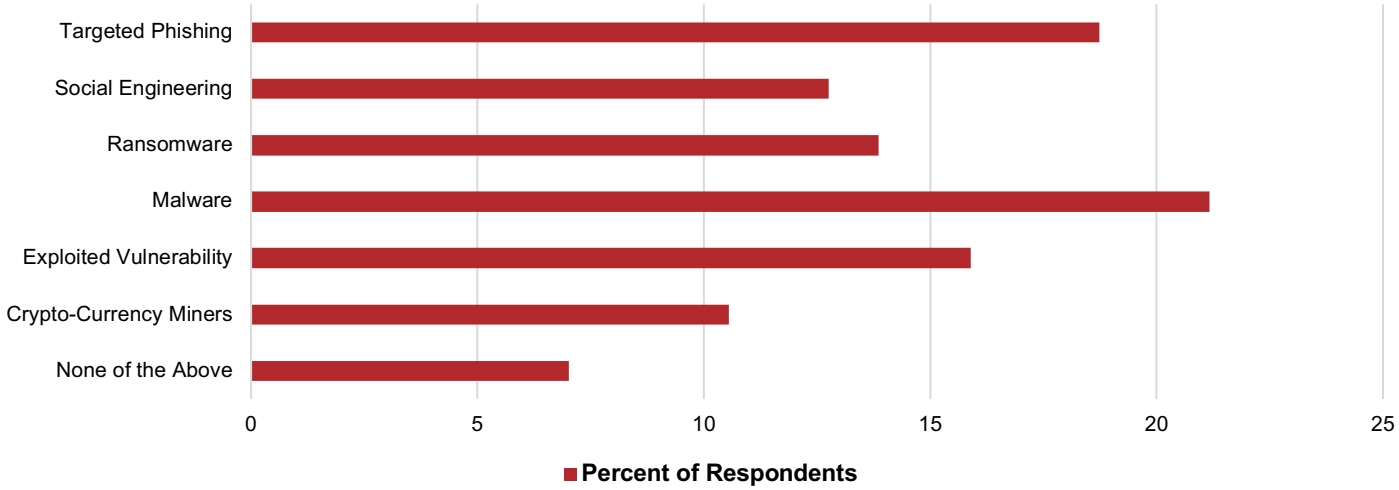


Figure 16. Types of cyber attacks experienced in the last 12 months.

Source of Attacks

Organizations were asked to identify the most likely source of attacks against their organizations. Globally, the results were highly consistent across all countries with hacker groups (31%), individual hackers (18%) and criminal organizations (17%) coming in as the top three suspects.

Participants in Japan (25%) and Germany (23%) believed the most likely source of cyber attacks were criminal organizations.

Globally, nation states were considered the least likely source of cyber attacks totaling less than 8% of responses. Only in South Korea did it make the top three most likely source with over 19% of responses.

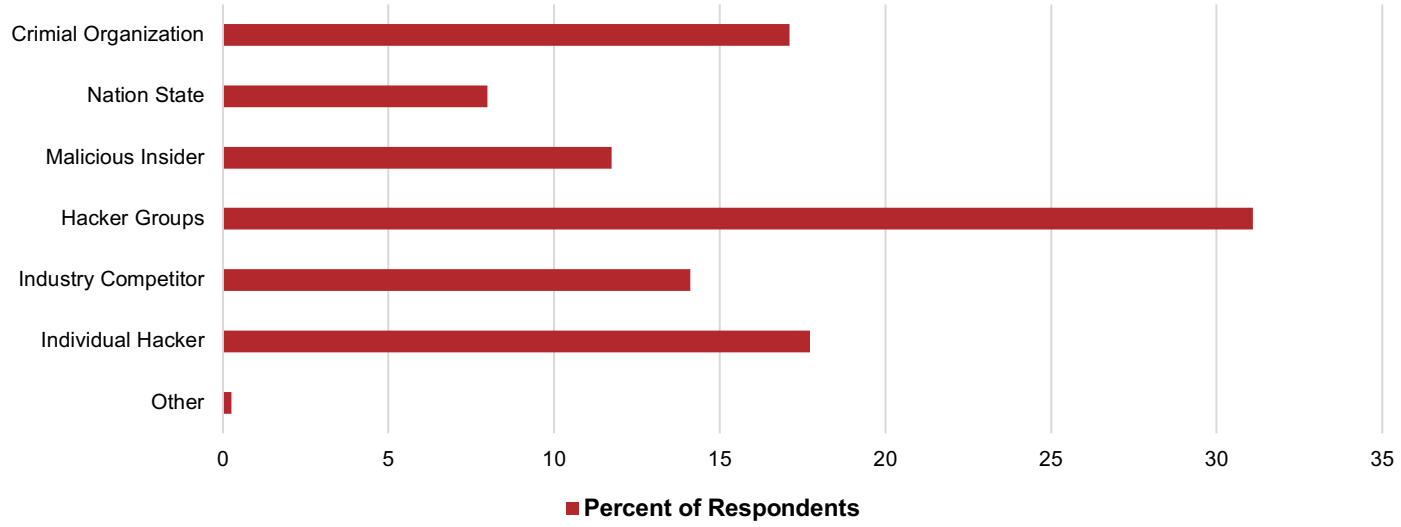


Figure 17. Sources of cyber attacks experienced by organization.

Organizational Maturity and Resilience to Cyber Threats

Many factors impact the maturity of an organization's cyber security program and its ability to be resilient against cyber threats.

Participants were asked to provide their insights into the formative elements of their own cyber security program, how the program was developed and how effective their organization was at responding to and addressing cyber security issues.

Participants were also asked to describe their internal challenges to maturing their cyber security program and their biggest fears in the event of a breach.

Security Program Maturity

When assessing their cyber security programs, 27% of participants characterized them as semi-formal approaches where efforts were mostly compliance-driven and focused on addressing mandatory regulations, while 24% saw their programs as informal where the primary focus was addressing critical issues as they occurred.

Globally, 23% of organizations reported formal security programs with a broad, risk-based focus supporting continuous optimization of processes and approaches, compared to the U.S. (41%) and China (38%).

Only 19% of organizations identified their security program as strategic with intelligence data driving investment decisions, operational priorities and other critical cyber security factors.

Overall, 7% of organizations indicated they did not have a cyber security program at all. In Canada, this response jumped to 18%.

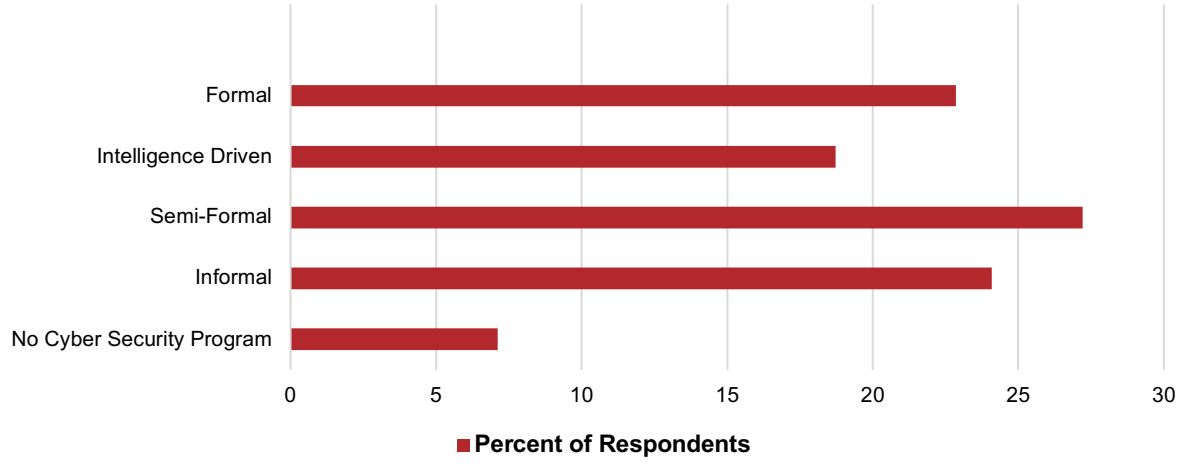


Figure 18. Security program maturity.

Cyber Attack and Breach Response Plans

Cyber attack and breach event response plans are critical for ensuring organizational focus and resilience during a cyber security event.

These plans consist of pre-established and agreed upon actions, procedures, communications and leadership structure invoked in the event of a cyber incident. To minimize delays and distractions, plans also include legal agreements and pre-negotiated contracts with all third-parties that might augment operations or render assistance during an event.

Among all organizations excluding those from the U.S., 29% indicated the existence of mature cyber attack and breach event response and communications plans that are regularly reviewed and updated. The highest results were from the U.S. (62%) and China (39%).

However, 29% of organizations reported that while they had cyber plans, they had not been tested or updated in 12 or more months.

Over 30% of organizations indicated that cyber attack and breach event response plans were owned and maintained by individual businesses or applications and that they were not coordinated within an overall organization-wide plan.

While only 8% of organizations did not have any cyber attack and breach event response plans, the results were higher in Canada (19%) and Japan (15%).

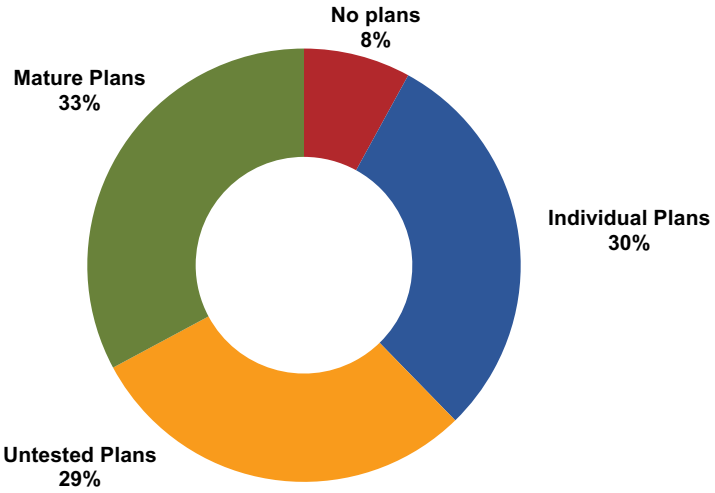


Figure 19. Cyber attack and breach response plans.

Organizations universally identified the chief information officer (CIO) as the leading representative involved in the development or review of the cyber attack or breach response plan, followed by the chief compliance officer (CCO), IT security and finally IT operations staff (Fig. 20).

Analyst Observation

Overall, internal and external legal counsel were identified as among the roles least involved in the development of plans (Fig. 20). This is in sharp contrast to recommended industry best practices, given that the main focus of legal counsel is to protect the organization from and minimize its exposure to risks. Legal counsel provides guidance on the acceptable levels of risks and obligations for their organization and ensures that legal frameworks are adhered to before, during and after a cyber attack or breach event to mitigate further impact.

Line of business and business operations were consistently and universally identified as the least involved in the development and review of plans. This is notable because these groups are considered critical stakeholders in plans presumably designed to maintain business operations during an event.

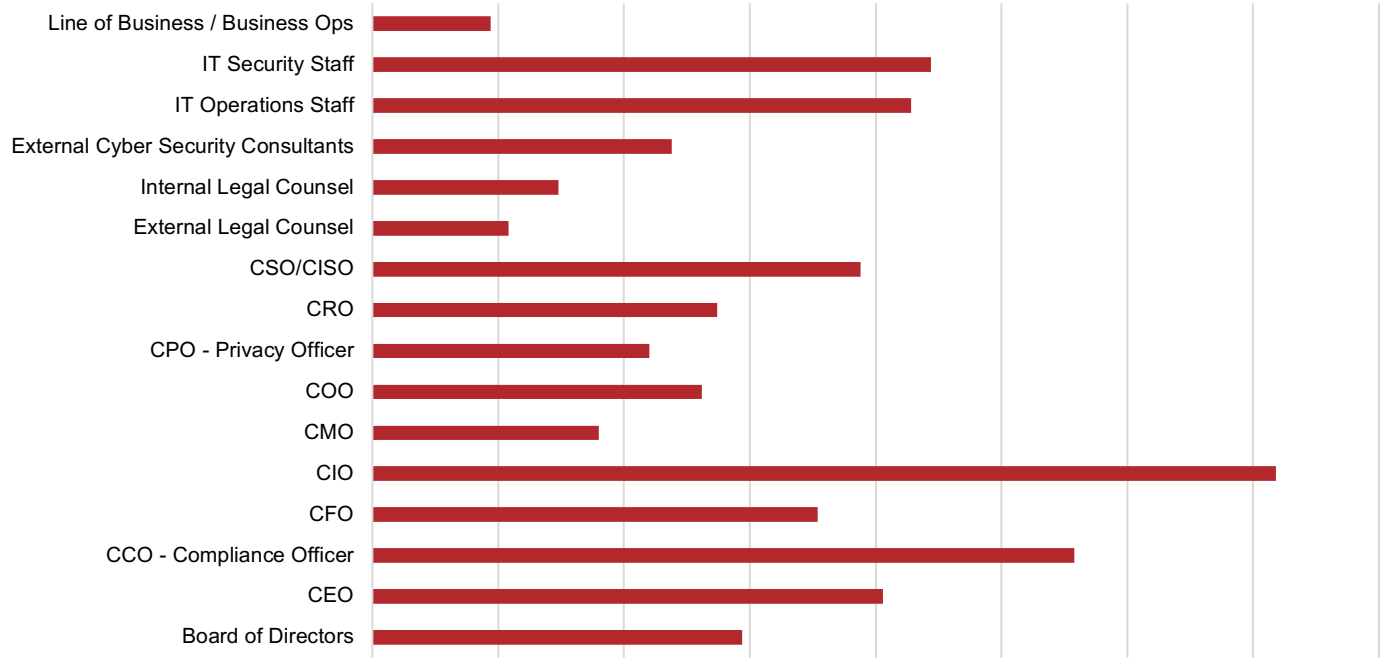


Figure 20. Roles involved in the development and review of cyber attack and breach response plans.

Organizations reported that the main challenges they faced in maturing their organization's overall cyber security posture were primarily IT and security technology maturity followed by IT and security process maturity and then visibility into threats.

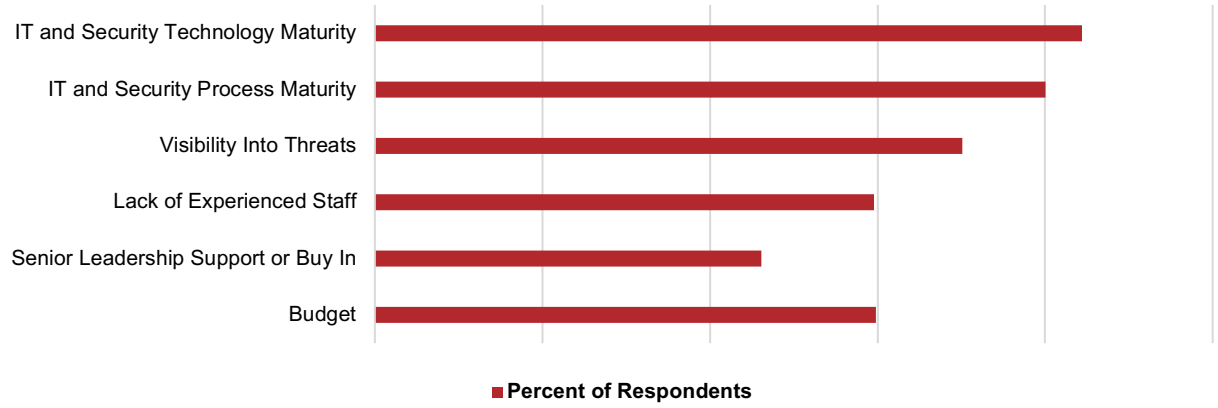


Figure 21. Challenges in maturing cyber security posture.

Organizational Readiness Against a Cyber Attack or Breach Event

When asked how they would rate their organization's readiness to address a cyber attack or breach event, the respondents were nearly equally split. Forty-nine percent considered their organization to be fully ready with the ability to respond well and 47% indicated that some portions of their organization would be ready, but overall they would struggle to respond well. In the U.S., 72% of respondents were confident in their organization's readiness to respond well to a cyber attack or breach incident, sharply contrasting with Japan (24%).

Fourteen percent of organizations in Japan believed they were not ready and would not respond well to a cyber attack or breach event, which is significantly higher than the global average (just over 2%, excluding responses from Japan).

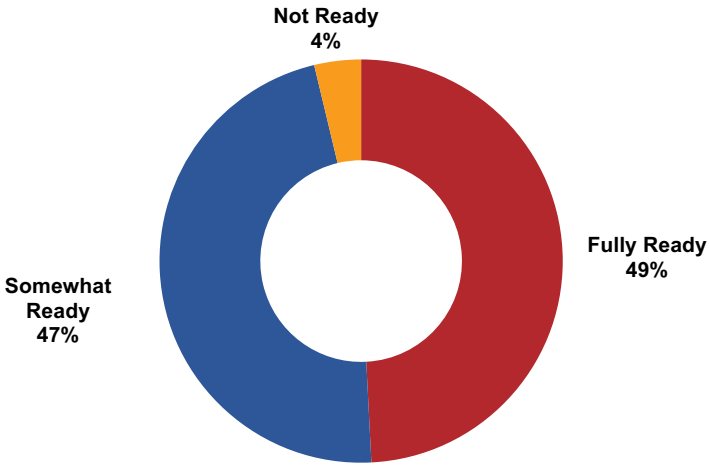


Figure 22. Readiness to respond to a cyber attack or breach event.

Cyber Security Protection

Solutions deployed to protect organizations from cyber attacks range in capability, applicable scope and cost to acquire and maintain. Organizations were asked which solutions they currently deployed in their organization, which components they believed provided the best protection and where they would focus future investments if they had unlimited budgets.

Globally, participants were quite consistent when they identified the components that currently contributed the most positive impact to their organization's ability to prevent a cyber attack or breach. Specifically, vulnerability management had an edge over security software (both slightly above 16%). These were followed by employee training (14%) and then response plans and security hardware (both slightly above 12%).

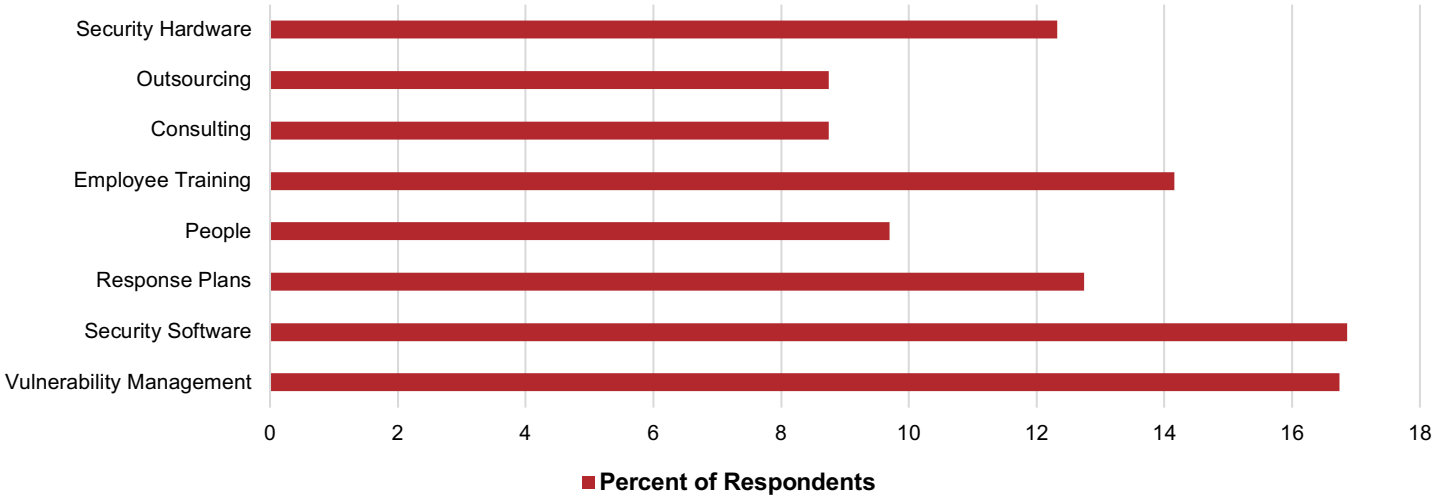


Figure 23. Components that currently had the most positive impact on security.

Organizations were then asked which component they believed would most positively impact their organization's ability to prevent a cyber attack or breach if they had the opportunity to dramatically increase its the budget or presence.

The results were globally consistent: 15% of organizations believed that increasing the investment and presence of vulnerability management solutions within their environment would generate the most impactful results, followed by threat intelligence (13.7%), threat hunting (12.6%) and employee training (12%).

Analyst Observation

Organizations in France believed employee training was the cyber security investment area with the highest potential positive impact against a cyber attack. Their response was 67% higher than the global average (excluding France).

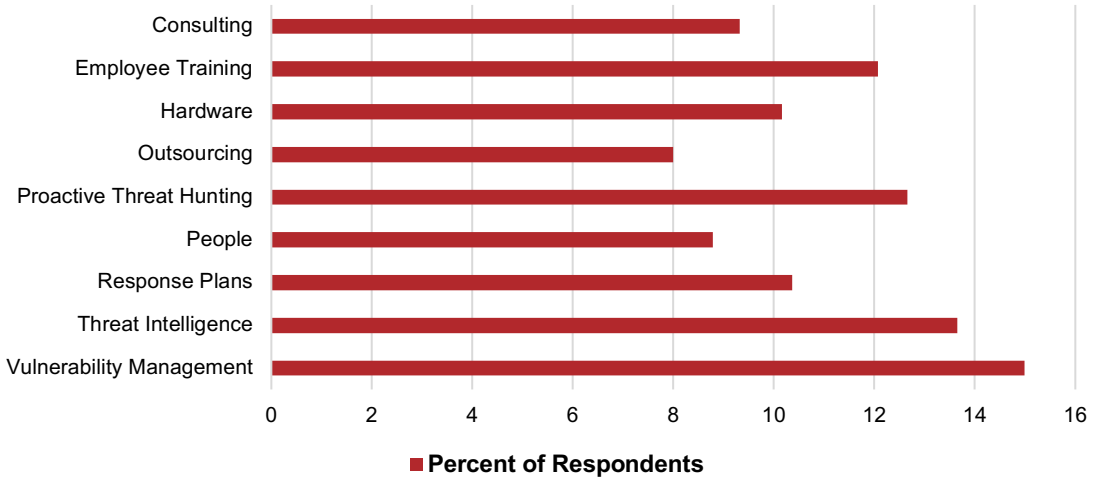


Figure 24. Components that could most positively impact security, assuming unlimited budget.

Looking more deeply into employee cyber security awareness training (Fig. 25):

- 35% of organizations had semi-formal training conducted at regular intervals that addressed compliance and typical cyber security awareness topics.
- 29% of organizations had informal training programs focused on meeting core compliance requirements that are conducted on an as-needed basis
- 25% had advanced training programs designed to promote broad cyber security awareness and behavioral changes through regular mandatory training and evaluation.
- Over 11% of organizations had no internal employee cyber security training programs.

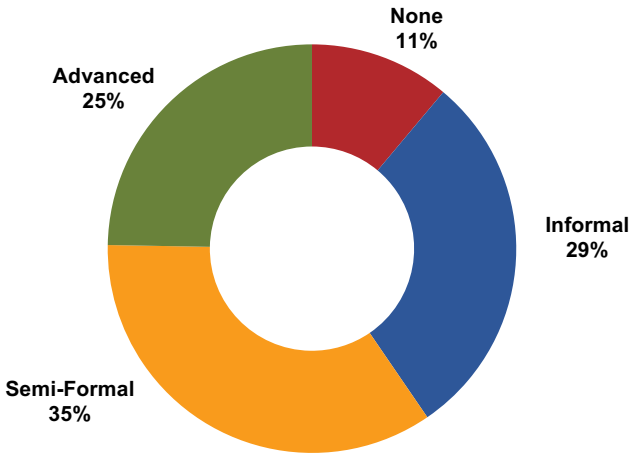


Figure 25. Status of employee cyber security training program.

Analyst Observation

Less than 1% of organizations in France indicated they did not have any cyber security training programs, the lowest rate among all countries included in this study. This stands in stark contrast to the responses in Germany (25%) and Canada (23%) where no security training program was in place.

Significant presence of advanced cyber security training programs was reported in the U.S. (48%), UK (34%) and China (37%).

Organizations consistently reported their greatest concern regarding a cyber attack or breach event as the loss of sensitive data, followed by customers and business operation disruption.

In the U.S. the greatest concern was business operations disruption. U.S. organizations were least concerned by the possibility of physical damage to real-world infrastructure.

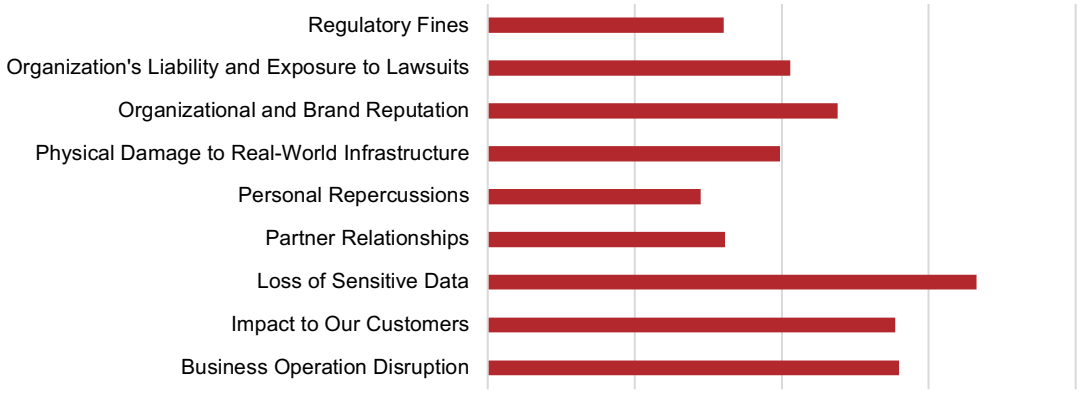


Figure 26. Concerns from a cyber attack or breach.

Analyst Observation

Although fines were highlighted as a concern, this option never reached top three status in any of the countries represented. This is notable considering 27% of organizations characterized their cyber security programs as being semi-formal where their efforts were mostly compliance driven and focused on addressing mandatory regulations (Fig. 18).

Over 56% of organizations reported that they actively tested their security posture with automated tools and attack simulation, while 37% indicated that they had plans to do so in the next 18 months. Only 7% reported they currently did not and had no plans to do so in the next 18 months.

The highest reported use of automated tools was by U.S. organizations (78%) followed by the UK (70%). The lowest reported use of automated tools was in Germany (13%) and Japan (13%).

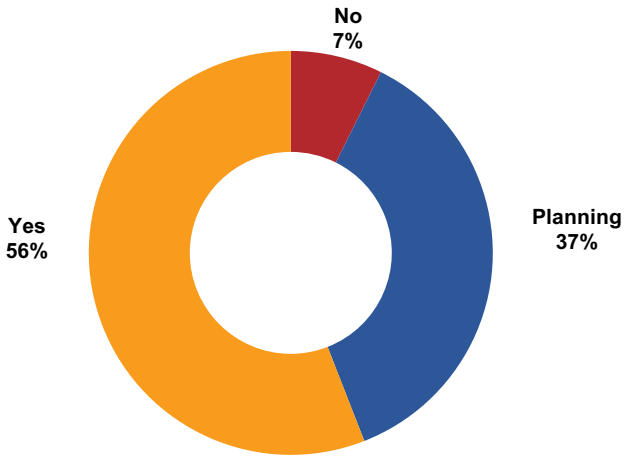


Figure 27. Use of automated security posture testing.

Cloud Initiatives

Cloud is a significant initiative for organizations globally and a hot topic of discussion. Participants were asked to provide insights into their overall readiness to adopt cloud technologies, their intended outcomes from cloud deployments, their perceptions of cloud security and how far along they had progressed toward the cloud.

Drivers for Cloud Initiatives

Participants consistently identified that the top three motivations to pursue cloud were to reduce overall IT costs (27%), broaden enterprise agility (25%) and reduce datacenter footprint (20%).

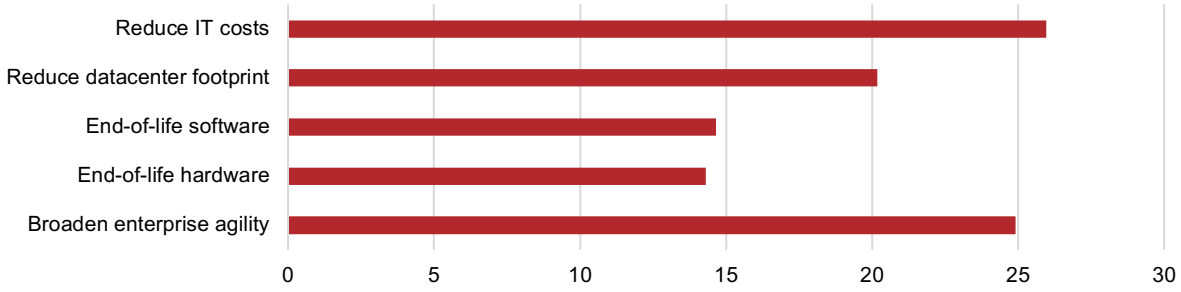


Figure 28. Drivers for cloud.

Maturity of Cloud Initiatives

Only 10% of participants reported that they had not begun investigating cloud and that it was not a priority at this time for their organizations. Countries reporting higher than this average were Canada (20%) and Germany (15%).

Overall, 31% of organizations had initiated projects to understand cloud, but security was not currently a main concern.

Organizations with a basic understanding of cloud and cloud security issues represented 21% of all responses. Another 21% indicated they had a moderate understanding of cloud and had initiated pilot deployments.

Globally, 17% of organizations reported a strong understanding of cloud and cloud security and had established a formal approach.

Analyst Observation

In the U.S., 41% of organizations reported they had established a formal approach to cloud and had a strong understanding of cloud and cloud security issues. France (22%) and the UK (19%) also had a solid representation with this response.

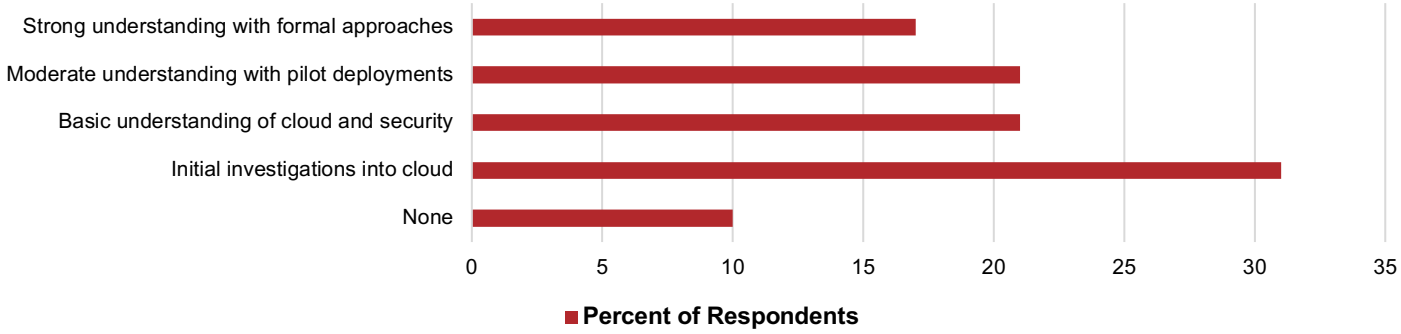


Figure 29. Cloud readiness.

Over 44% of organizations reported that they currently had transitioned some of their environment to the cloud, but they were being cautious and planned to monitor their experience closely. Thirty-five percent had transitioned some of their environment and were planning to continue adoption.

Overall, 17% of organizations identified they had a cloud-first approach and their entire environment was cloud-centric. The most cloud-centric organizations were in the U.S. (37%).

Only 4% of organizations did not have any plans to migrate any of the existing environment to the cloud.

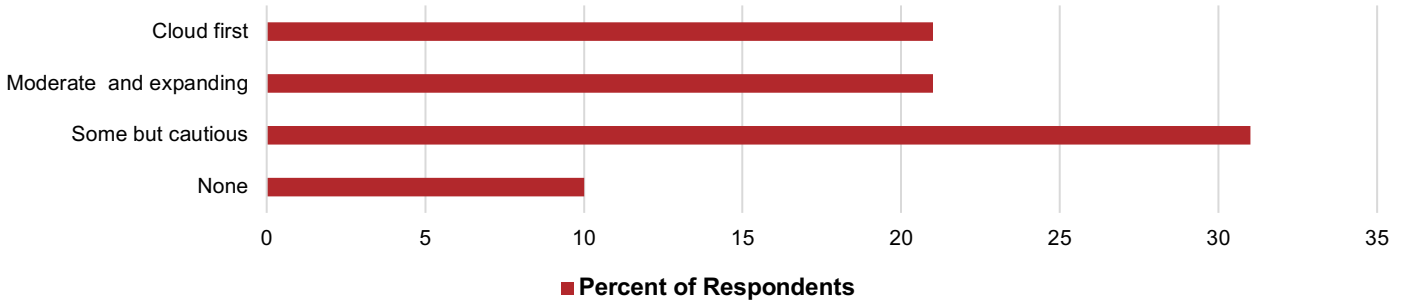


Figure 30. State of cloud initiatives.

Cloud Security

Over 45% of participants agreed with the belief that security for both their cloud and their on-premise environments was about the same, while 33% believed that cloud was more secure.

Only 18% of organizations perceived cloud as being less secure.

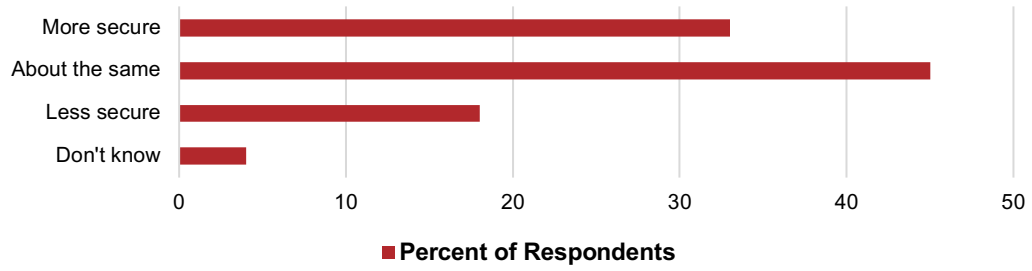


Figure 31. Perception of overall security of cloud.

Analyst Observation

In the U.S., 51% of organizations perceived cloud as being more secure than their on-premise environment.

In Japan and Germany, 24% of organizations perceived that cloud was less secure than their existing on-premise environment—significantly higher than the global average of 18%.

Security Operations

A security operations center (SOC) is a centralized group within an organization mandated to monitor and address security issues. Participants were asked to provide insights into their overall SOC maturity, staffing and 2020 plans.

Maturity and Staffing of Security Operations

On average, only 13% of organizations reported that they did not have a SOC. When excluding Germany (26%), the global average drops to 10%.

Slightly more than 45% of organizations reported that they had an on-premise SOC that they staffed during business hours on weekdays (8x5), 23% had an on-premise SOC staffed 8x5 with outsourced expertise for off-hours, 15% had an on-premise SOC staffed 24x7 and 4% reported full outsourcing of SOC responsibilities.

The highest rate of fully outsourced SOCs was reported by France (22%).

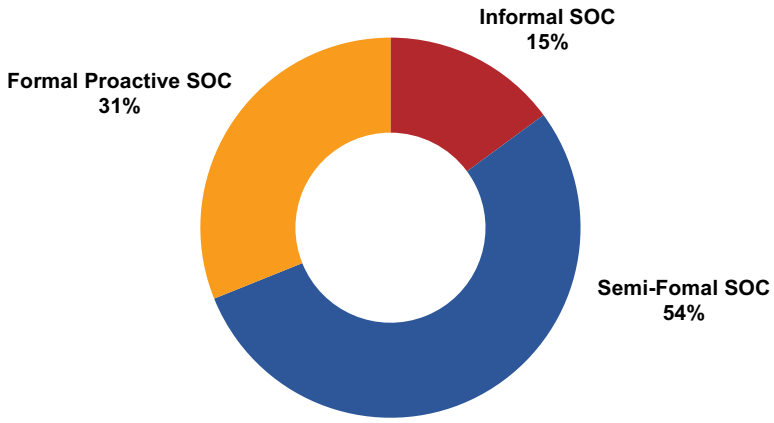


Figure 32. Maturity of security operations center (SOC).

Regarding SOC maturity, Fifty-four percent of organizations indicated they had a semi-formal SOC that was compliance-driven and focused on addressing mandatory regulations, 31% reported that they had a formal proactive SOC that provided a broad, risk-based approach with active threat hunting and continuous optimization of processes and approaches and 15% of organizations reported an informal SOC that was primarily focused on addressing critical issues as they arise.

Significant representation of formal proactive SOCs was reported in the U.S. (50%) and China (45%), compared to the global average of 25% (excluding the U.S. and China).

Security Operations Planning

Globally, organizations indicated their SOCs were staffed (internally and externally) with:

- 6-10 people (22% of organizations)
- 11-30 people (38%)
- 31-100 people (26%)

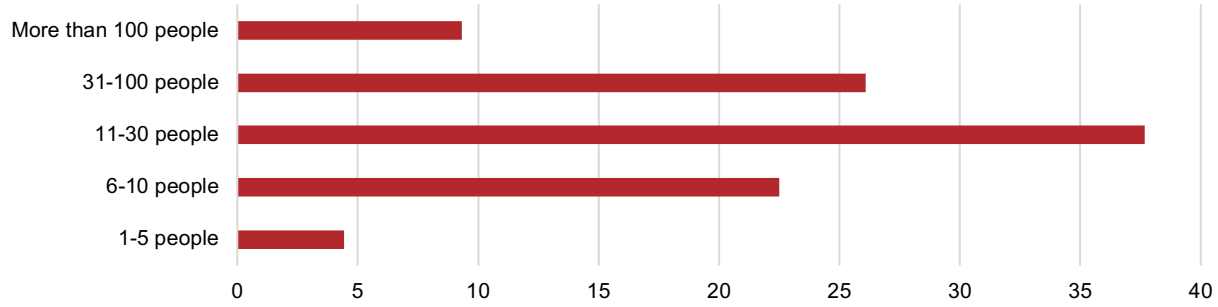


Figure 33. Size of security operations team (internal and outsourced staff).

Organizations in Korea (78%) and China (76%) planned to increase their levels of internal SOC staffing. This was significantly higher than the global average of 57% (excludes Korea and China).

Globally, 65% of organizations with outsourced SOC personnel planned to increase staffing levels. Regionally, participants in China (84%), Canada (75%) and the UK (74%) planned to increase their levels of outsourced staffing.

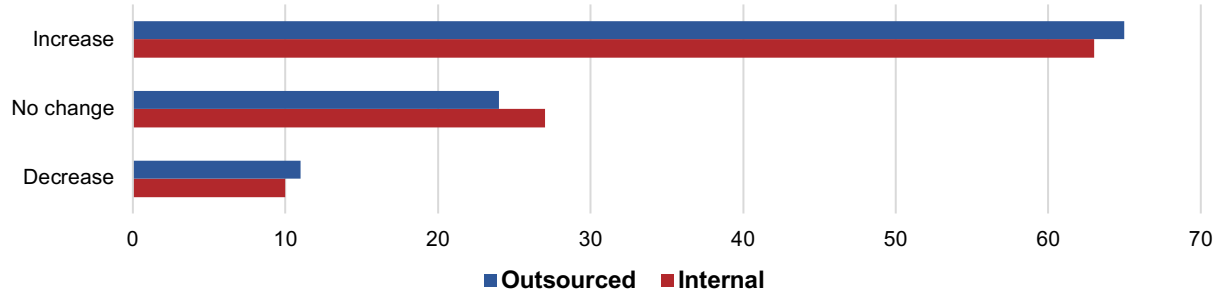


Figure 34. Security operations team growth (internal and outsourced staff).

Security Information and Event Manager (SIEM)

Security information and event management (SIEM) software solutions collect and aggregate security data from applications, services and hardware. A SIEM solution can be used to analyze the collected data in real-time or at a later date, by applying filters and search parameters to identify and characterize events and trigger actions.

Participants were asked to provide insights into their overall SIEM deployments, use cases, challenges and integration with other solutions such as security orchestration, automation and response (SOAR).

SIEM Deployments

Globally, over 60% of organizations reported no SIEM solution in their environments and 18% of all participants indicated they had no plans to deploy a SIEM solution.

In the U.S. and France, 12% of organizations reported they had two or more SIEM solutions.

In Germany, 28% of organizations lacked a SIEM and had no plans to incorporate one in their environment.

In Korea, 58% of organizations planned to add a SIEM to their environment—significantly higher than the global average (39%, excluding Korea).

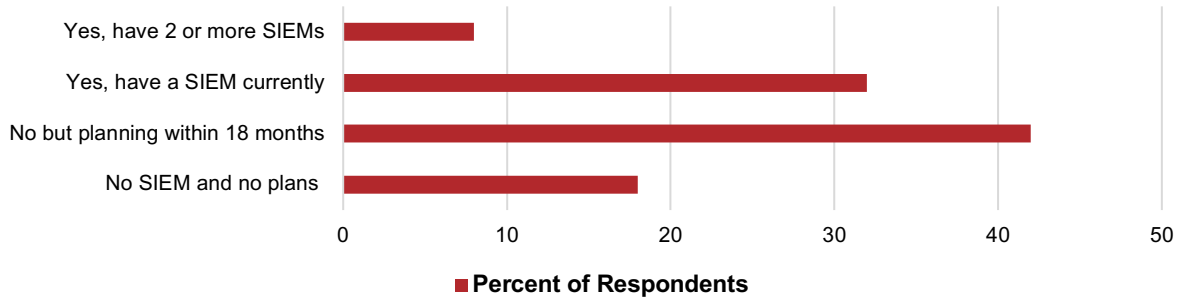


Figure 35. Number of SIEM solutions in the organization.

SIEM Use Cases

Organizations generally highlighted a balanced planned use for their SIEM solution. There was a slight edge to threat hunting as the main use case, followed by compliance. All organizations globally prioritized use cases in roughly the same way, except Korea, where compliance and discovering lateral movement from compromised trusted resources were the top two use cases, followed by log collection and monitoring in a third-place tie.

Figure 36. Planned use of SIEM solutions.

There was a nearly a four-way split across the levels of maturity of SIEM deployments for organizations and the findings were consistent across all regions.

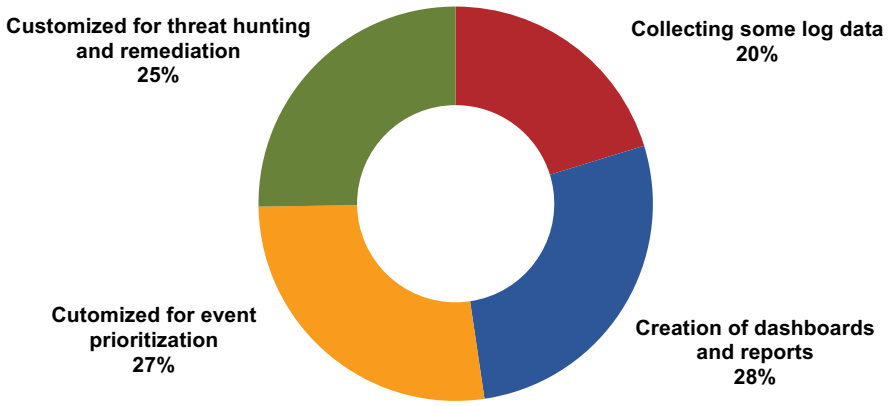


Figure 37. SIEM maturity.

SIEM Challenges

Overall, only 11% of organizations reported no challenges with their SIEM deployment.

The remainder identified their biggest challenges as the costs to acquire, maintain and support the SIEM (14%)and the overall complexity related to the operation of a SIEM (also 24%).

Analyst Observation

Compared to other regions, more U.S. organizations reported they did not have challenges with their SIEM deployment.

Organizations in France reported their biggest issue as the lack of third-party integration.

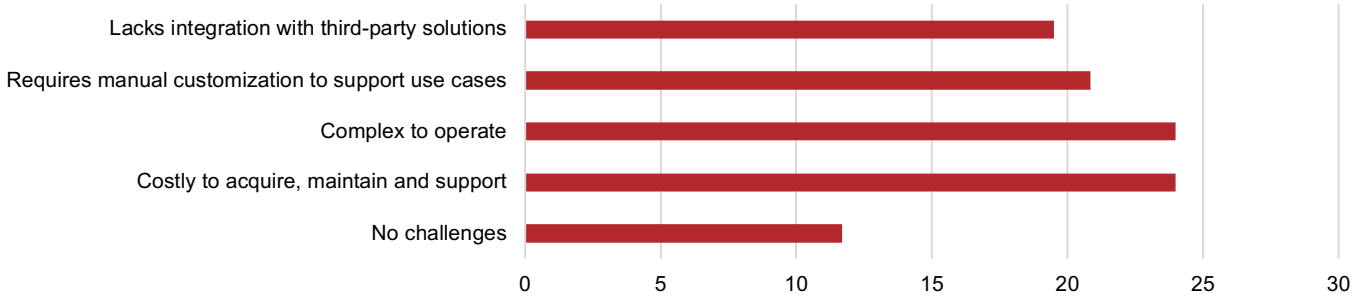


Figure 38. SIEM challenges.

SIEM and SOAR integration

SOAR solutions automate security responses to threats.

Participants reported that 25% of organizations were currently exploring the integration of SOAR with their SIEM, while 24% reported that they currently have a SOAR deployment.

Organizations in Japan reported the highest lack of SOAR deployment compared to other regions, while organizations in France reported advanced SOAR deployments with automation twice as often as any other region.

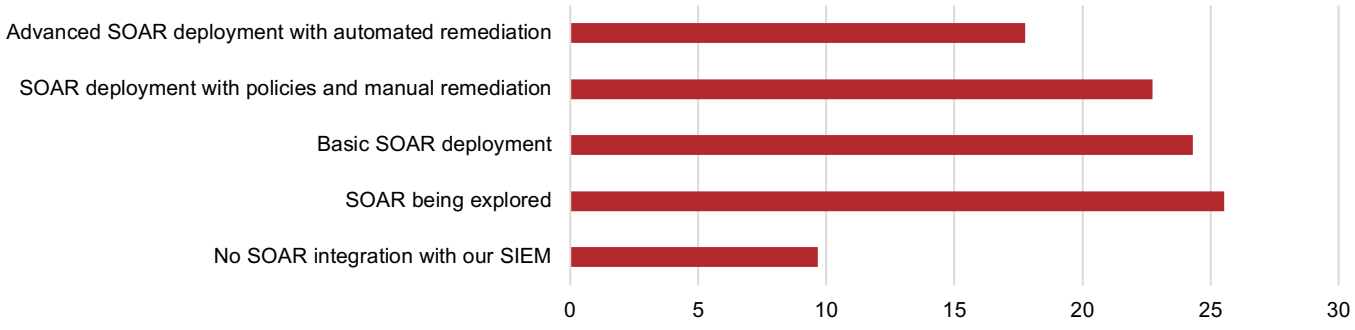


Figure 39. SOAR integration with SIEM solutions.

Cyber Threat Intelligence

Cyber threat intelligence is used by organizations to enhance their security effectiveness, improve decision making and reduce business risks.

This intelligence is built from collection of reports that contain a wide range of information, such as vulnerability data, detailed descriptions of tools and techniques used by attackers and comprehensive attribution of a threat actor with a full history of their activity and the intent. These reports can be used on their own to assess risks within an environment and can also be used in conjunction with SIEM and other cyber security solutions.

Participants were asked to provide insights into their adoption of threat intelligence subscriptions or feeds as well as their perceived utility, value and effectiveness of the intelligence.

Adoption of Cyber Threat Intelligence Feeds

Participants reported that 32% of organizations integrated free and paid intelligence feeds with their SIEM.

In Japan, 18% of organizations neither had nor planned to integrate intelligence feeds with their SIEM—more than three times the global average (5%, excluding Japan).

France (42%) had the highest number of organizations reporting the integration of two or more free or paid intelligence feeds through their SIEM solution, followed by the U.S. (32%), Canada (18%) and Korea (18%).

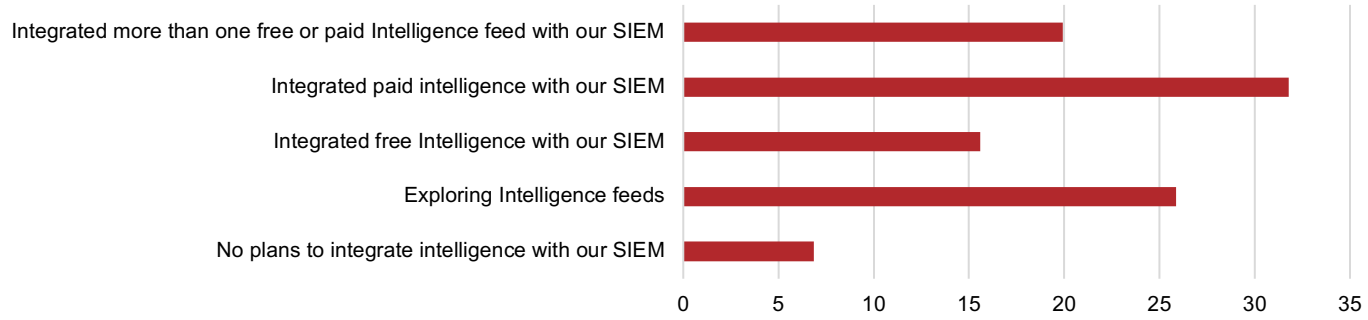


Figure 40. Intelligence Integration with SIEM solution.

Of the organizations that used free and paid intelligence, 94% reported they used more than one intelligence feed. The majority of organizations used five threat intelligence feeds. Just over 6% said they used 10 or more feeds.

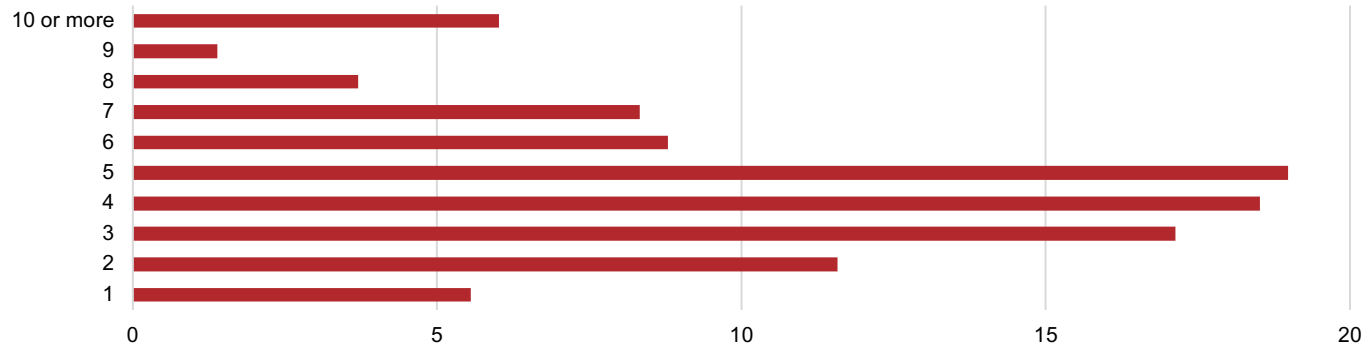


Figure 41. Number of threat intelligence feed subscriptions.

Perceptions of Threat Intelligence Feeds

Organizations responded that it was overall more easy than difficult to find providers of free and paid intelligence feeds.

Figure 42. Ease of finding providers of intelligence feeds.

Organizations also responded that it was overall more easy than difficult to derive benefits from free and paid intelligence feeds.

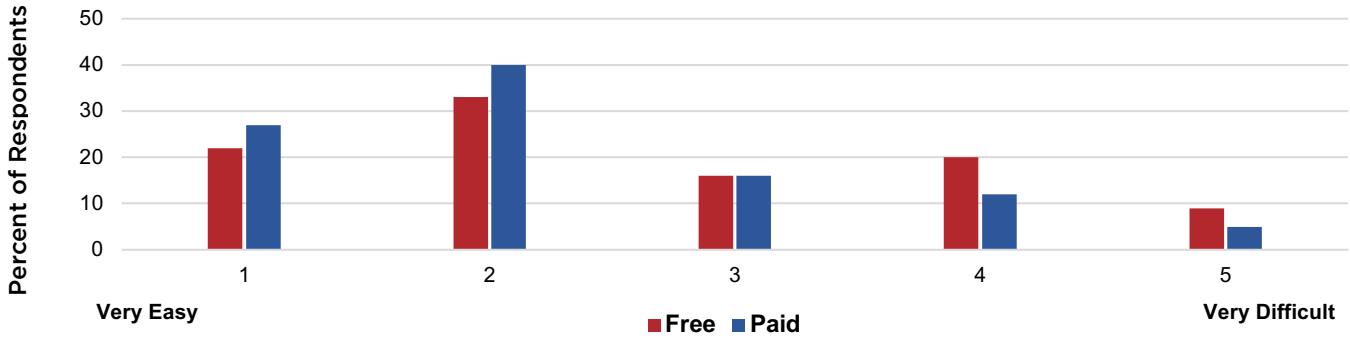


Figure 43. Ease of deriving benefits from intelligence feeds.

Organizations indicated that free and paid intelligence feeds were overall more actionable than not.

Figure 44. Feed actionability.

Organizations generally indicated that the scope of insights provided by free and paid intelligence feeds were broad enough for their use and were not considered limited or in need of improvements.

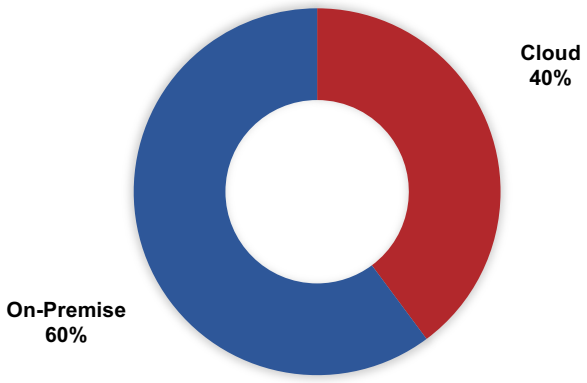
Figure 45. Scope of insights from intelligence feeds.

Email Security Solutions

While email solutions are ubiquitous in every organization, their deployment, management and security vary. Participants were asked to provide insights into their adoption of email such as on-premise vs cloud, how they manage their email solutions and their plans for securing email.

Email Adoption

Globally, organizations reported a preference for on-premise (60%) versus cloud-based (40%) email systems.



Analyst Observation

The regions with the highest response rate for on-premise email were from Canada (79%), Germany (57%) and Korea (62%).

The regions with the highest response rate for cloud-based email were the U.S. (62%), followed by China (49%) and France (44%).

Figure 46. Email deployments.

Email Management

Organizations reported a minor preference for managing their own email solution (52%) over outsourcing management (48%).

Organizations inclined to manage their own solutions were concentrated in China (67%), followed by the U.S. (63%) and then Germany (57%).

Leading the preference for outsourced management of email were Japan (63%), Korea (56%) and Canada (53%).

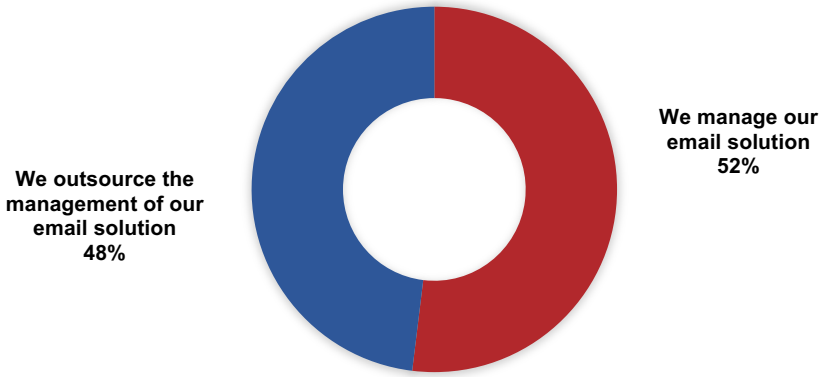


Figure 47. Self-managed or outsourced email management.

Email Security

Participants were nearly evenly split between the use of third-party email security solutions (51%) and integrated email security solutions (49%).

Organizations preferring third-party email security solutions were mostly located in Canada (67%) and the UK (55%). Those preferring integrated solutions were in China (60%) Korea (53%) and the U.S. (53%).

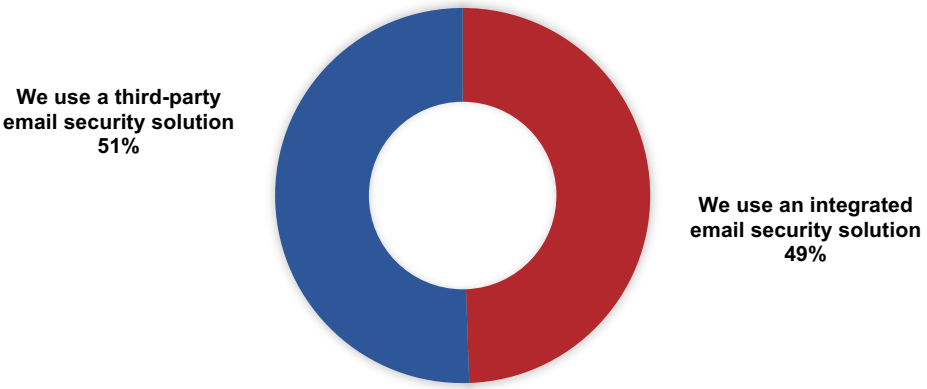


Figure 48. Security solution for email.

Endpoint Security Solutions

Endpoint security solutions are designed to protect systems from the different forms of cyber attacks. Here, organizations described the solutions they deployed to secure their endpoints.

Endpoint Security Adoption

Globally, the top three endpoint security solutions identified by participant organizations were application privilege control, anti-malware or antivirus prevention and encryption.

Figure 49. Endpoint security capabilities.

Top Endpoint Security Solution Adoption by Country

Table 1. Top three endpoint security capabilities by region.

	Canada	China	France	Germany	Japan	Korea	UK	US
Vulnerability management and remediation	1	1	3		2	2		3
Endpoint firewall	2	2		3		1	2	1
Endpoint encryption	3			2	1		1	
Anti-malware or anti-virus prevention		3	1	1	3		1	2
Port and device control			2					
Application privilege control					3			
Application behavior analytics						3		
Endpoint detection and response (EDR)							3	

Cyber Security Insurance

Participants were asked to share how they used cyber security insurance, its availability in the marketplace and its perceived value.

Adoption of Cyber Security Insurance

Globally, 50% of organizations reported they had cyber insurance as a complement to their cyber security programs. Forty-one percent planned to add it in the next 18 months. Only 9% of organizations lacked cyber insurance and did not plan to acquire it over the next 18 months.

Analyst Observation

The U.K. (68%) had the highest rate of existing cyber insurance, followed by the U.S. (67%). Organizations in Japan (16%) and Germany (11%) lacked and did not plan to add cyber insurance over the next 18 months.

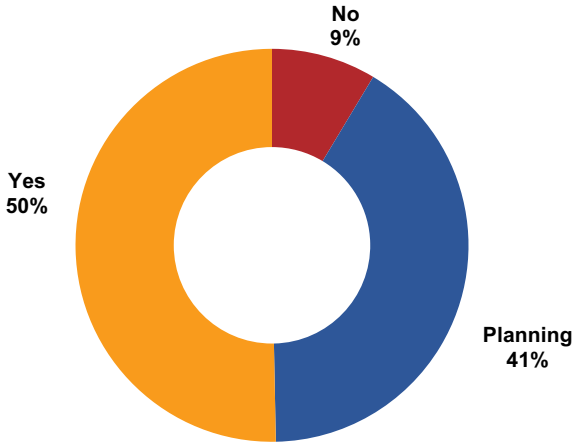


Figure 50. Use of cyber insurance.

Perceptions of Cyber Security Insurance

Participants reported that it was difficult (47%) or very difficult (8%) to find cyber insurance providers.

On the other hand, fewer organizations reported that it was simple (20%) or very simple (8%).

Globally, 15% of organizations found it neither easy nor difficult to find cyber insurance providers.

Participants in the U.S. reported the greatest ease in finding cyber insurance with 38% indicating simple and 16% indicating very simple.

Participants in Korea reported the most difficulty in finding cyber insurance providers with 12% 55% reporting it as difficult and 12% as very difficult. Japan also found it challenging, with 49% difficult and 7% very difficult.

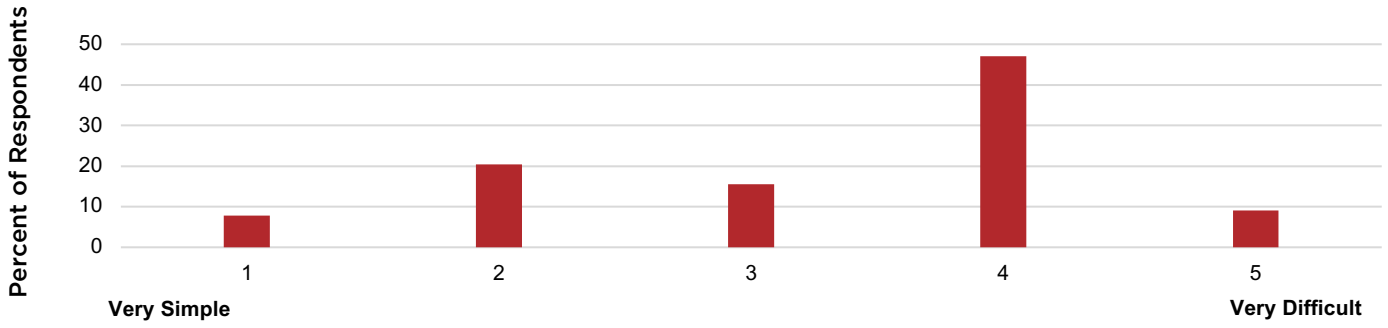


Figure 51. Ability to find cyber insurance providers.

The findings were nearly evenly split when it came to judging whether it was simple or difficult to understand the coverages provided by cyber insurance, with a slight bias toward difficult. Globally, 8% of organizations found that it was very easy compared to 10% finding it to be very difficult. Overall, 30% of organizations found it easy to understand, contrasted with 33% that found it difficult. Slightly more than 19% of organizations found it neither easy or difficult.

In the U.S., participants had the highest incidence of finding it simple (36%) to very simple (23%) to understand the scope of coverage provide by cyber insurance.

Organizations in Korea had the most challenges, reporting that it was difficult (41%) or very difficult (12%) to understand scope of coverage. Participants from Japan echoed similar concerns with 45% reporting difficult and 6% very difficult.

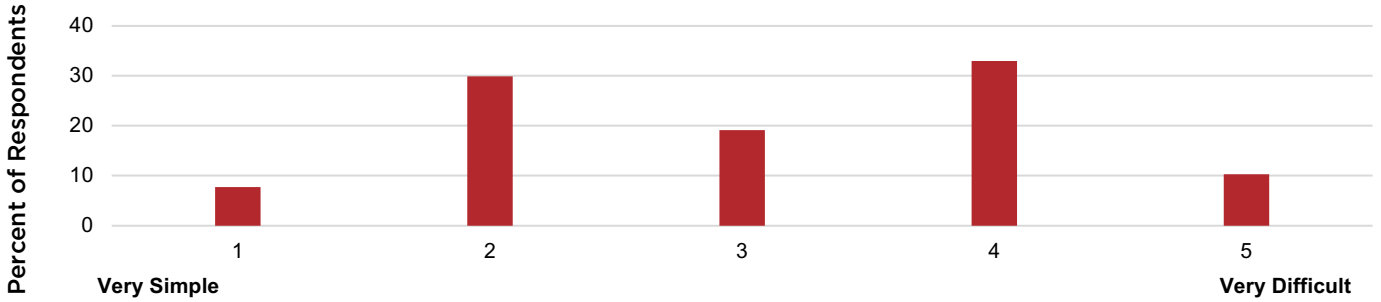


Figure 52. Ability to understand the scope of cyber insurance coverage.

Overall, most participants echoed similar views that cyber insurance offerings needed to be improved, indicating that cyber insurance provided very limited scope of protection and represented poor value.

Contrasting opposite ends of the spectrum, globally:

- 10% of organizations found insurance to provide very poor value and 9% excellent value
- 36% of organizations found insurance to provide poor value and 23% good value

Slightly more than 22% of organizations indicated that cyber insurance provided neither poor or good value.

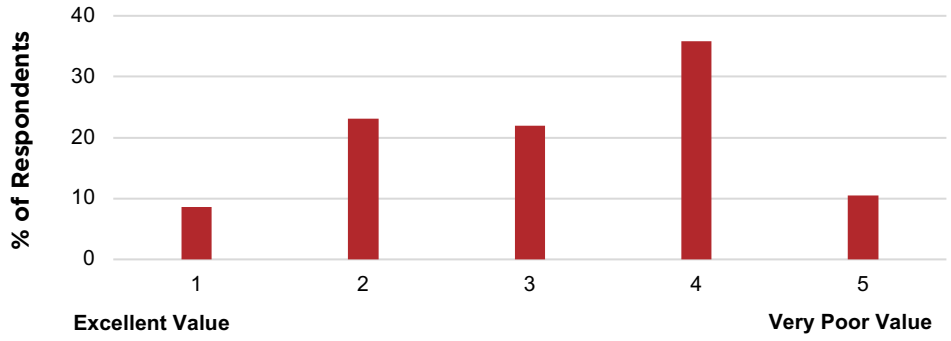


Figure 53. Perceived value of cyber insurance coverage.

Analyst Observation

Participants in the U.S. were the most positive, reporting that 30% of organizations found existing cyber insurance offerings offered good value, and 31% indicated they provided excellent value.

Organizations in Canada were the most pessimistic, with 53% reporting the value cyber insurance as poor and a further 8% indicating very poor.

Artificial Intelligence

Artificial intelligence (AI) is a computer science specialty focused on creating systems and technologies that mimic how the human brain learns and adapts to changing conditions. Its goal is to be able to reason, complete tasks and solve complex problems even when data elements are not complete.

Participants were asked to provide insights into their overall readiness for incorporating AI in their environments and for their 2020 plans.

Adoption of Artificial Intelligence

Over 88% of organizations reported they had initiated AI efforts at some level.

Globally, 34% of organizations reported they had started projects to understand AI and AI security issues and 28% had a preliminary understanding of AI and AI security with pilot deployments.

Only 12% reported that they had not investigated AI and that it was not a priority at this time.

U.S. organizations are the most advanced on the path to AI—28% reported a strong understanding of AI and AI security concerns and have established a formal approach. The U.K. (15%) and France (11%) were the next most advanced.

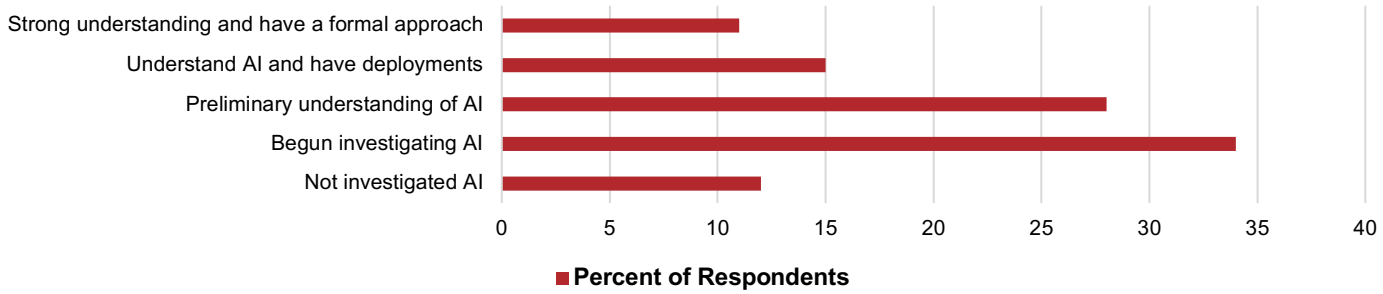


Figure 54. Adoption of AI.

Blockchain

Blockchain is a technology developed for creating distributed, transparent and immutable records or ledgers of data and events. Every data element or event recorded using blockchain is linked to both the immediate data element or event before it and following it. Each element is coded with its own unique identifier and locked in place using tamper-proof technology.

Participants were asked to provide insights into their overall readiness for incorporating blockchain in their environments and associated 2020 plans.

Adoption of Blockchain

Over 86% of organizations reported blockchain initiatives.

Globally, 30% of organizations had begun an initiative to understand blockchain and related security issues and 27% have a preliminary understanding of blockchain security with pilot deployments.

Only 14% of organizations reported that they had not investigated blockchain and it was not currently a priority.

U.S. organizations were the most advanced in their path to leveraging blockchain with 29% reporting a strong understanding of blockchain and related security with a formal approach. The next most advanced organizations were France (13%) and the UK (11%).

Many countries, including Germany (21%), Canada (17%) Japan (17%) reported that they had not investigated blockchain and it was not currently a priority.

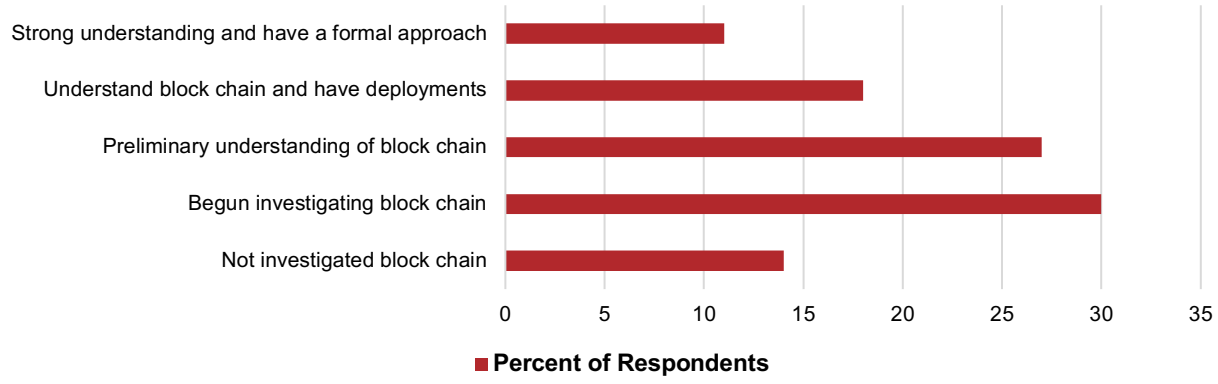


Figure 55. Adoption of blockchain.

Conclusions

The FireEye Cyber Trendscape report is a detailed point-in-time view of the state of cyber security and how organizations are responding and adapting to the changing landscape.

While there were occasional regional nuances with the findings, the most intriguing discovery was how consistent the overall views and perspective were across very diverse regions. Organizations had more in common with one other than their geographic location, size or industries would suggest.

We expect the Cyber Trendscape report to provide you with valuable data for 2020 planning and we look forward to sharing future editions that include retrospective reviews and emerging trends.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE
(347.3393) info@FireEye.com

About FireEye, Inc

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks.