

Cyber Resilient Organization Report ²⁰²⁰

Table of contents

Executive summary	3
What's new in 2020	4
Key findings	5
Additional insights	8
Steps to improve cyber resilience	14
Complete findings	16
How many organizations experienced a cybersecurity incident	16
How improvements are measured	17
Reasons why cyber resilience improved	18
Reasons why cyber resilience did not improve	19
How use of cloud services improved cyber resilience	20
Specific response plans used	21
How severity is measured	22
How threat intelligence improves cyber resilience	23
Causes for improvement for high performers	24
Reasons why high performers are more cyber resilient	25
High performers' cyber resilience confidence level	26
How the number of security solutions affects incident response	27
Different types of cyberattacks by geography	28
Value of cloud services by geography	29
How use of cloud services improved cyber resilience by industry	30
How use of CSIRPs differ by industry	31
Factors that justify funding for cybersecurity function	32
Cybersecurity budget allocated to cyber resilience	33
Organizational characteristics	34
Methodology	39
Definitions	40
Research limitations	41
About Ponemon and IBM Security	42
Next steps	43

Executive summary

The fifth annual *Cyber Resilient Organization Report* from IBM Security is based on research from Ponemon Institute surveying more than 3,400 IT and security professionals around the world in April 2020 to determine their organizations' ability to detect, prevent, contain and respond to cybersecurity incidents.

The volume of cybersecurity incidents has risen, causing significant disruption to IT and business processes. At the same time, the percent of organizations that reported achieving a high level of cyber resilience increased from 35% in 2015 to 53% in 2020, growing 51%. A cyber resilient enterprise can be defined as one that more effectively prevents, detects, contains and responds to a myriad of serious threats against data, applications and IT infrastructure.

More than one-quarter of respondents now use an enterprise-wide, consistent cybersecurity incident response plan (CSIRP) to ensure their cyber resilience. A majority of organizations rely on automation, machine learning, AI, cloud and orchestration to fortify their security environments.

But challenges remained — from resource and budget constraints, continuing sophistication of threats and complexity of IT environments to a decline in the security team's ability to contain cyberattacks.

The report examines the approaches and best practices organizations took to improve their overall cyber resilience. It details the importance of cyber resilience to minimize business disruption in the face of cyberattacks as part of a strong security posture. Finally, we offer recommendations to help your organization become more cyber resilient.

Cyber Resilient Organization Report facts

51%

Amount of organizations reporting a **significant business disruption** during the past two years due to a cybersecurity incident

26%

Percentage of organizations using an **enterprise-wide CSIRP**

55%

Portion of high performing organizations reporting **improved cyber resilience** through **automation tools**

52%

Ratio of respondents who say that **Cloud services improved cyber resilience**.

45

Average number of **security solutions** and **technologies** in use

What's new in the 2020 report

To reflect the evolving security landscape, this year's report examines for the first time how the use of cloud services improved organizations' cyber resilience and what the main benefits were. Also added were questions about organizations' use of specific response plans to address common security attacks, such as malware and phishing.

We expanded on questions introduced last year about the number of security solutions to further understand the number of tools used to investigate and respond to a security incident.

Similar to last year, we created a benchmark for measuring cyber resilience by isolating the most cyber resilient organizations, i.e. "high performers," and uncovering their differentiators. The report highlights what tactics enhanced high performing organizations' level of cyber resilience, such as leveraging automation tools, using cloud services and emphasizing interoperability.



Key findings



Organizations using a CSIRP experienced **less business disruption**.

Cybersecurity incident response plans (CSIRPs) minimize business disruption.

The adoption of enterprise-wide CSIRPs has slowly improved, growing 44% since 2015. Despite this progress and the benefit, 51% of respondents said their CSIRPs were not applied consistently across the enterprise or, worse, the plan was informal or ad hoc.

Of those with a formal CSIRP, only one-third have attack-specific playbooks in place for common attacks such as DDoS or malware. Even fewer respondents had plans for emerging threats like ransomware.

Furthermore, only 7% of organizations reviewed their CSIRPs quarterly — a figure that did not change much over the last five years. In fact, 40% of organizations had no set time period for reviewing and updating the plan, an increase of 8% since 2015. Without an up-to-date CSIRP that is applied across the business, 23% more organizations experienced a significant disruption to their IT and business processes.

While it's impossible to thwart every attack, the preparation and processes an organization uses to respond can greatly reduce damage. The lack of due diligence around a CSIRP revealed by the study potentially limits its effectiveness in an aggressive threat environment.



-8%

Organizations with **more than 50 tools** ranked **8% lower** in the ability to detect a cyberattack.

Too many tools weaken cyber resilience, but automation, visibility and interoperability improve incident response.

Organizations used a high volume of tools to manage their security environments and respond to cybersecurity incidents. Nearly 30% of organizations used more than 50 separate security solutions and technologies, and 45% used more than 20 tools when specifically investigating and responding to a cybersecurity incident.

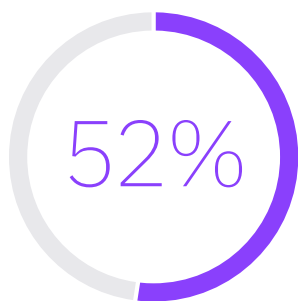
However, an excessive use of disconnected tools creates complex environments, which can inhibit efficiency. The study revealed that the number of security solutions and technologies an organization used had an adverse effect on its ability to detect, prevent, contain and respond to a cybersecurity incident.

In fact, companies with more than 50 tools ranked 8% lower in the ability to detect a cyberattack and ranked 7% lower in the ability to respond to an attack compared to companies using less than 50 tools.

Visibility into applications and data has been one of the top ways organizations improved their cyber resilience for the last three years. Automation stands out this year as another compelling reason — especially for high performers. High performers reported that using interoperable tools helped increase their cyber resilience: 63% compared with 46% of other organizations.

The emphasis on interoperability helped provide the much needed visibility across multiple vendors' solutions, while at the same time reduced complexity.





Number of respondents who say that **cloud services improved cyber resilience**

Cloud services lead to greater cyber resilience.

The use of cloud services improved cyber resilience, according to 52% of respondents. When separating out high performers, 63% cited the use of cloud services in improving their cyber resilience compared to 49% of other organizations.

Not surprisingly, 60% of financial services organizations, early adopters of cloud, stated that use of cloud services had improved their organization's cyber resilience. Healthcare and retail organizations as well as the public sector also report above average improvements due to cloud services.

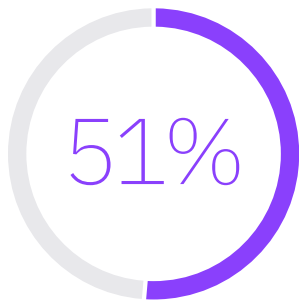
Companies in the United Kingdom, Germany, France, the United States and Canada led the way in valuing cloud services and their importance to achieving cyber resilience. Specifically, more than two-thirds of organizations in these countries value the use of cloud services.

According to high performers, the leading reasons for improvement due to cloud services were the benefits of leveraging a distributed environment, economies of scale and availability of service level agreements. On the other hand, 30% of organizations reported that poorly configured cloud services inhibited their progress in cyber resilience.

Investing in cloud services alone is not enough, optimization is imperative for the environment to be effective.



Additional insights

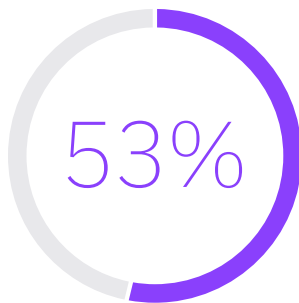


Number of organizations **significantly disrupted by a cyberattack** in the past two years

The volume and severity of cyberattacks has increased.

The majority (53%) of responding organizations experienced a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information during the past two years. Nearly as many (51%) reported a cybersecurity incident that resulted in a significant disruption to their organizations' IT and business processes in the past two years.

Sixty-seven percent and 64% said that the volume and severity, respectively, have significantly increased over the past 12 months. Severity is primarily (57%) measured by leakage of high value information assets, followed by (50%) diminished employee productivity.



Number of organizations with **improved cyber resilience**

While cyber resilience has improved overall, the ability to prevent attacks has increased most during the past five years.

The strength of organizations' cyber resilience has escalated, with a reported 51% improvement over the last five years. This uptick coincides with a significant increase in organizations' ability to prevent cyberattacks — up from 38% in 2015 to 53% in 2020.

In fact, a majority of organizations (56%) measure cyber resilience improvement through the number of cyberattacks prevented. Other key metrics used to measure improvements in cyber resilience were time to contain the incident and increased productivity of employees.

The ability to detect an attack grew slightly (11%) since 2015 and is the second most popular (51%) way organizations benchmark their cyber resilience. Response capabilities remained flat, but containment appears to be progressively challenging, with respondents reporting a 13% decline in this area.

This drop is not surprising when considering that, despite 77% of organizations having cybersecurity incident response plans (CSIRPs), only 26% apply those plans across the enterprise. Plus, of the 77%, one-quarter described their plans as informal or ad hoc.

<50%

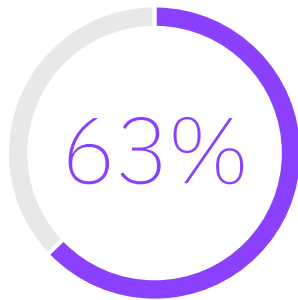
Organizations that **report cyber resilience to C-suite/board**

Lack of budget and skills are still obstacles to stronger cyber resilience.

Predictably, loss of skilled staff (41%) and lack of budget (40%) are the top reasons why organizations said they did not improve. As much as respondents report technology as key to a stronger security posture, some struggle with getting the latest tools or getting the most out of the tools they have.

The challenges included: silo and turf issues (31%), a lack of advanced technologies such as automation (25%) and fragmented IT and security infrastructure (22%).

Surprisingly, only 45% of respondents said their organizations issue a formal report on the state of cyber resilience to their executives or boards. But executive buy in, support for the cybersecurity function and board reporting were ranked the least important reasons why cyber resilience had not improved.

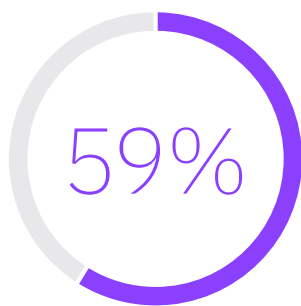


Number of organizations that said **automation, machine learning, AI and orchestration increases cyber resilience**

Analytics, automation, AI and machine learning enhance security posture.

Respondents said the implementation of technologies like analytics (46%), automation (42%) and AI and machine learning (41%) improved cyber resilience.

Overall, 63% of organizations said these tools lead to a strong cyber resilience security posture, followed by a strong privacy posture (60%). As will be explored later in the report, technology can mean the difference between being a high performing cyber resilient organization and not.

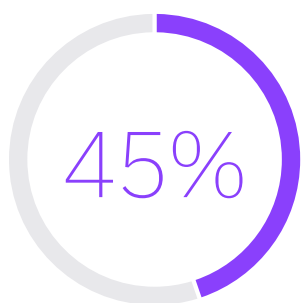


Number of organizations that said **sharing threat intelligence improves cyber resilience**

Fostering collaboration is the primary benefit of sharing threat intelligence.

The belief that sharing threat intelligence improves cyber resilience was held by 59% of respondents. To foster collaboration, 57% of organizations participate in an initiative or program for sharing information with government and/or industry peers about cyber threats and vulnerabilities.

Asked why they do not share information about cyber threats, respondents' most cited reasons were: no perceived benefit to my organization (70%), lack of resources (58%) and cost (54%).



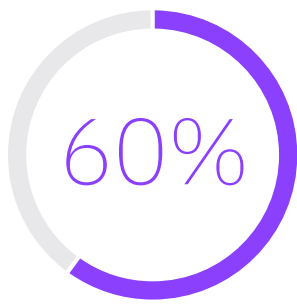
Number of organizations with **no plans in place for ransomware attacks**

DDoS is the most common type of attack-specific response plan.

For the first time, the survey asked about the use of response plans to address specific types of attacks. The most commonly used plans were distributed denial of service (DDoS), malware (including spyware, viruses, trojans and worms), insider incidents and phishing.

Not surprisingly, the use of attack plans differed by industry. Malware was the most used response plan in industries such as public sector, retail, manufacturing and consumer products, whereas a response plan for an insider incident was most widely used in industrial environments. Other industries stated that DDoS was the most widely used plan.

Even among those using attack-specific playbooks, less than half (45%) had plans in place for ransomware attacks — a threat vector which spiked by nearly 70% in recent years according to our [2020 X-Force Threat Index](#). As the vast majority of organizations were not frequently updating their CSIRPs, the lack of planning for this key risk area highlights the importance of reviewing and updating plans more frequently to reflect the latest attack methods.



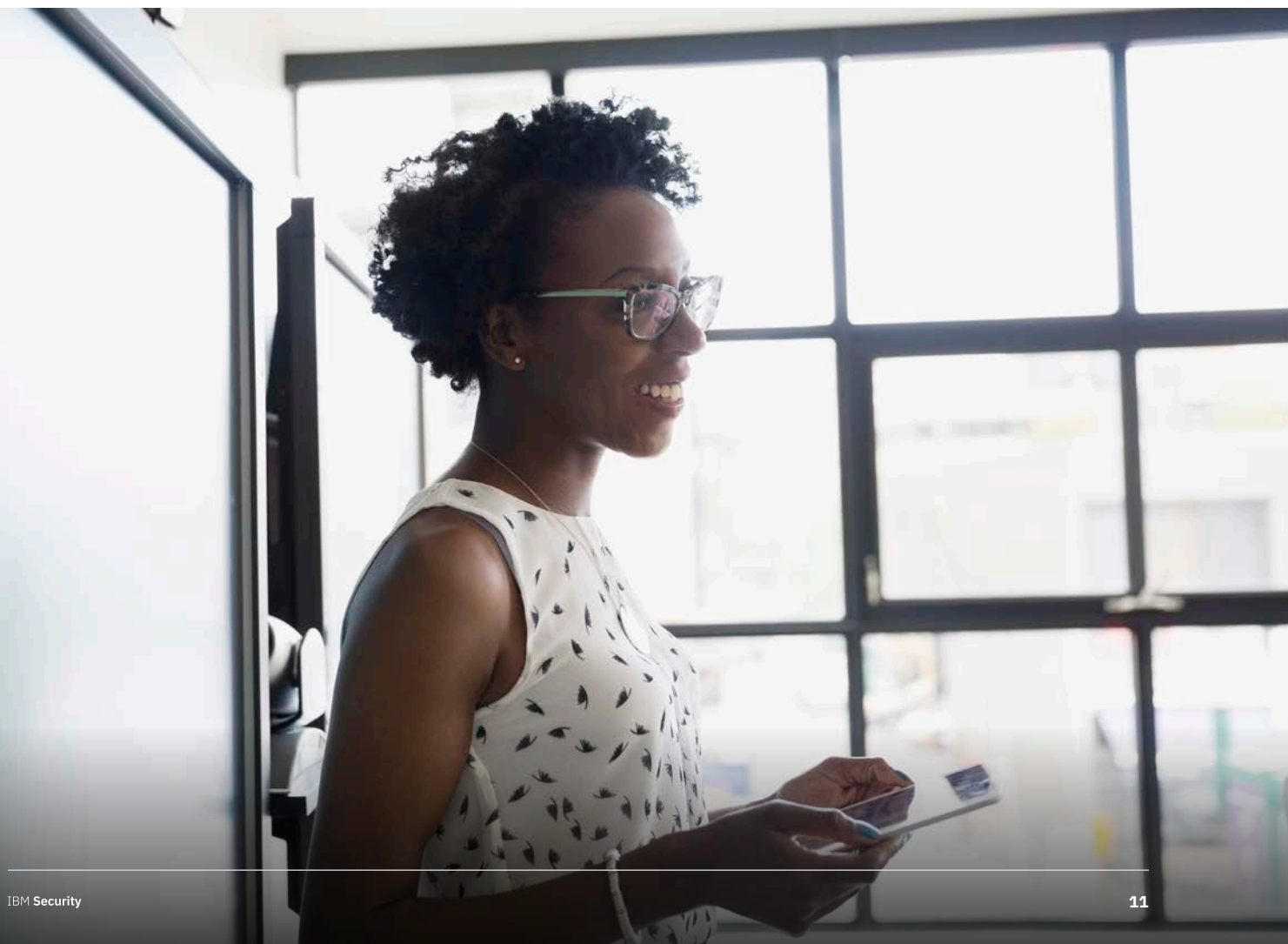
Amount of respondents who said a **strong privacy posture is important** to achieving cyber resilience

Privacy is essential to ensuring cyber resilience.

With 53% of organizations experiencing disruption from a data breach involving more than 1,000 records containing sensitive or confidential information in the past 2 years, it is not surprising that 95% of respondents recognize the importance of a privacy role — that is, someone in the organization who is charged with protecting customer and employee data.

But, while more than one-third consider the role essential, only 1% of organizations have a chief privacy officer responsible for directing their organizations' efforts to ensure cyber resilience. Twenty-two percent each said that a business unit leader or the CIO were primarily responsible.

Sixty percent of respondents said a “strong privacy posture” is important to achieving cyber resilience, same as 2019. Fifty-seven percent cited complying with data protection regulations such as the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) as important to achieving cyber resilience.

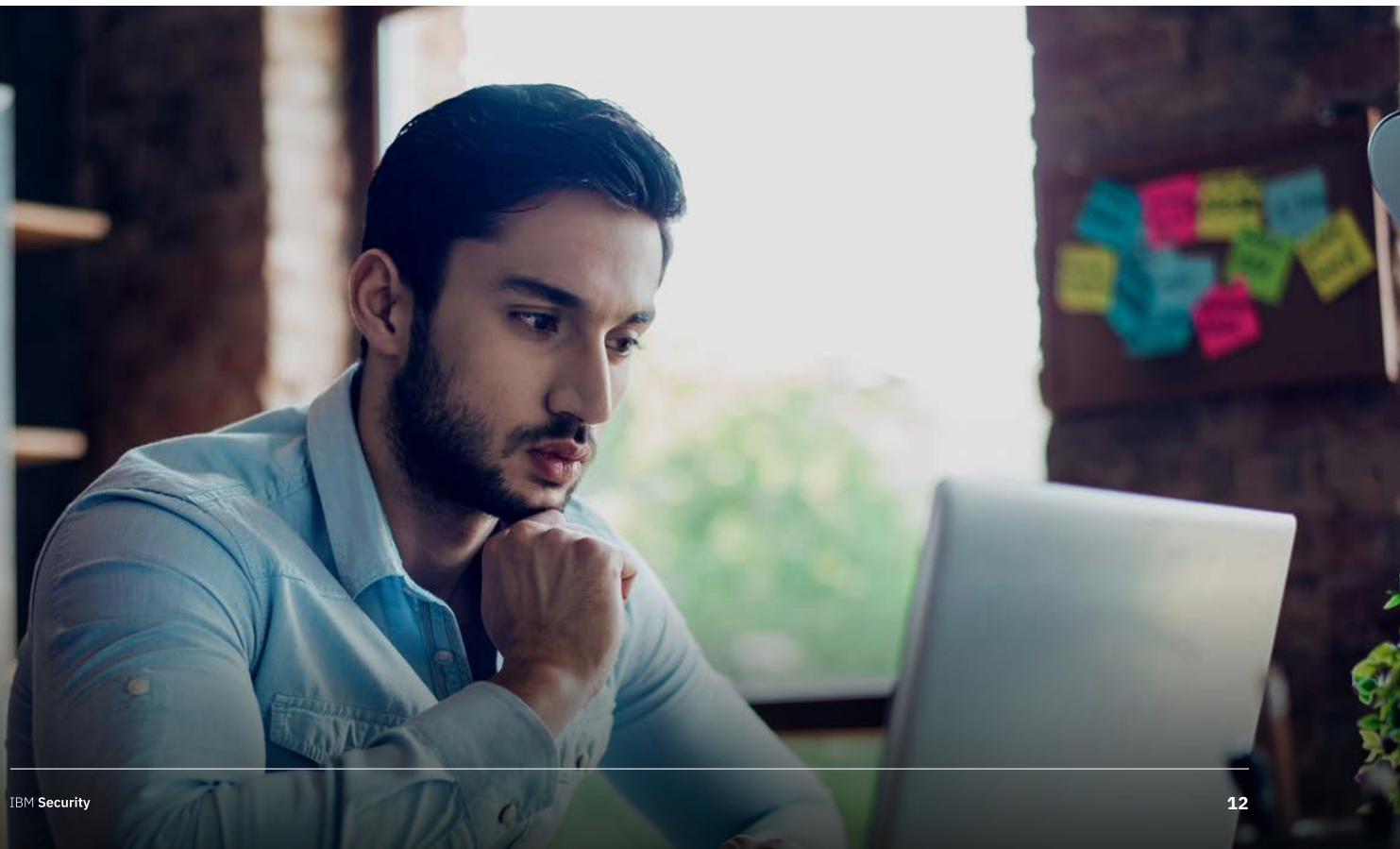


What high performing organizations do differently

When asked to assess their cyber resilience on a scale of 1 to 10, close to one-quarter of respondents gave themselves a rating greater than nine. Of that group, 59% said their organizations improved significantly in the last year. We refer to these organizations as high performers.

Similar to last year, high performers outperformed other organizations in their abilities to prevent, detect, contain and respond to a cyber attack. This year, however, the gap is much larger. The biggest differences were in containing and responding to an attack.

While high performers outperformed other organizations last year by 14% when containing an attack, this difference grew to 35%. Similarly, last year the difference between high performers and others was 15% for responding to a cyberattack. The gap in 2020 is 31%.



Clearly, high performers were utilizing best practices from which other organizations can learn. Some of the characteristics and approaches of high performers are:

Implementation of enterprise-wide CSIRPs:

Forty-three percent of high performing organizations use an enterprise-wide CSIRP that is applied consistently compared to 20% of other organizations. More than double the percent of high performers review and test this plan either every quarter or twice a year.

Use of attack-specific response plans:

Fifty percent use attack-specific response plans compared to 37% of other organizations.

Investment in technologies:

Seventy-three percent viewed automation, machine learning, AI and orchestration as key to achieving a strong cyber resilience security posture compared to 60% of other organizations.

Significant use of automation:

Seventy percent reported significant or moderate use of automation. Of this group:

- 70% used automation to improve operational efficiency.
- 64% used automation to support their IT security teams.

Threat intelligence sharing:

Sixty-nine percent shared threat intelligence that helped improve their abilities to detect, contain, and respond to cyber threats compared to 50% of other organizations.

C-level visibility:

More than half of high performers provide a formal report to C-level executives and/or their boards.

High performers compared to other organizations

39%

more likely to have realized improvements through automation tools

25%

more likely to have made improvements by deploying cloud services

20%

more likely to have experienced improvements using AI and machine learning

31%

more likely to have achieved improvements via interoperable cybersecurity tools

Steps to improve cyber resilience*



Implement an enterprise-wide CSIRP to minimize business disruption.

Just having a CSIRP is not enough; it should be implemented across the organization and reviewed on a regular basis. As the volume and severity of attacks increases year after year, the lack of an updated CSIRP may increase the risk of experiencing a significant disruption to IT and business processes.



Tailor response plans to specific attacks in your industry.

Cybersecurity attacks come in many forms. Organizations can strengthen their security postures by understanding the top threats in their industries and preparing detailed response plans to help ensure team members know the steps needed to investigate and remediate a specific attack.

Embrace interoperability to increase visibility and reduce complexity.

As organizations navigate complex security environments, the most effective teams leverage interoperability to increase visibility of tools and data to help prevent and detect attacks. Approaches that streamline workflows help increase the productivity of the security operations center.

Invest in technologies to accelerate incident response.

Technologies such as automation, analytics, AI and machine learning as well as cloud services were leading reasons why organizations improved their cyber resilience. Automation, in particular, helps companies improve operational efficiencies and reduce team churn by freeing up time to focus on the high value tasks needed to investigate and respond.

*Recommendations for security practices are for educational purposes and do not guarantee results.

Align your security and privacy teams.

Organizations with stronger cyber resilience recognize that security and privacy go hand-in-hand. Eliminate silos and encourage a culture of collaboration to more effectively respond to data breaches. Bringing these two teams together early and often will improve security posture sooner than if they work together for the first time during a massive security incident.

Formalize C-level/board reporting to raise the visibility of the organization's cyber resilience.

Business leaders recognize that cyber resilience effects revenue and reputation, thus, keeping cyber resilience performance front and center is imperative to ensure it receives the required level of investment and resources.



Complete findings

Figure 1

How many organizations experienced a cybersecurity incident

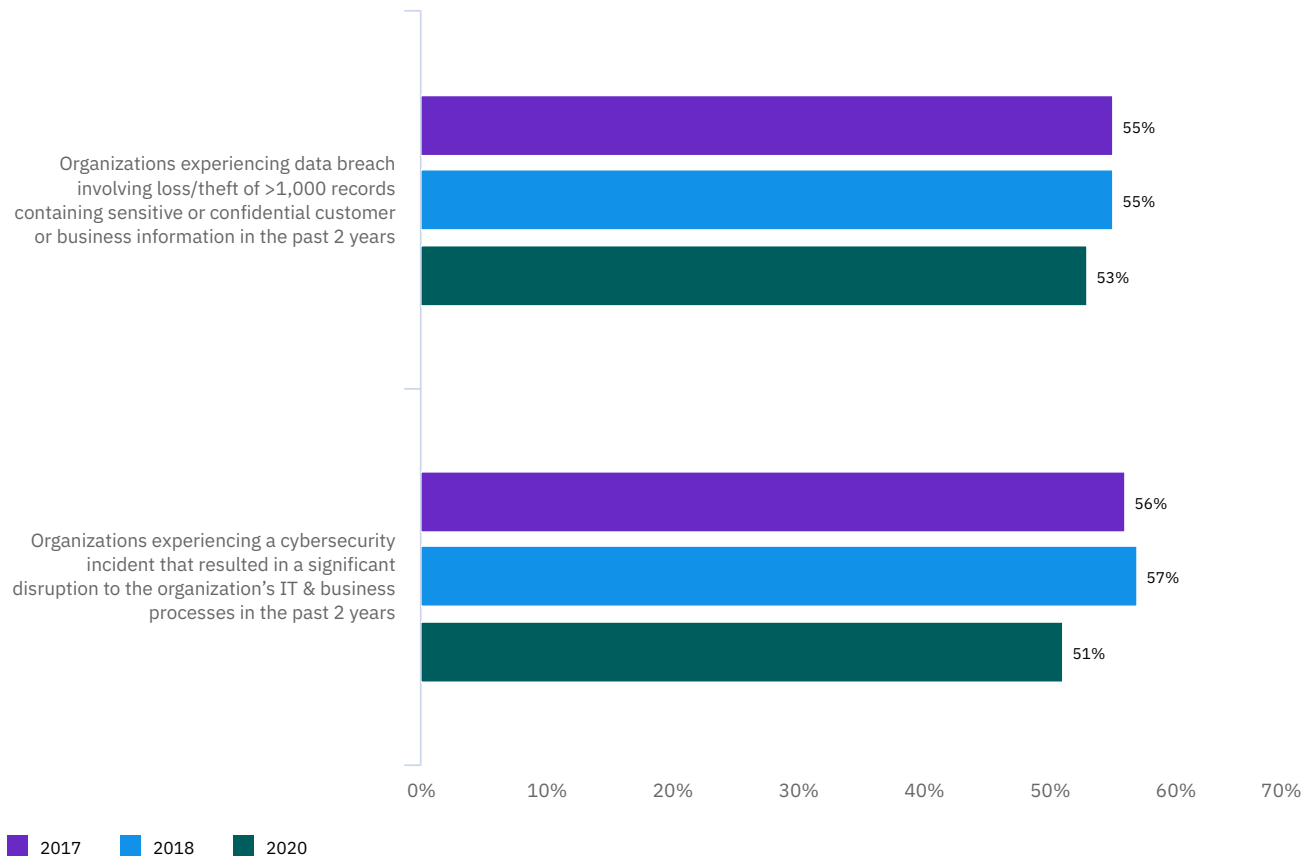


Figure 1 indicates how many organizations experienced a data breach or cybersecurity incident during the past 2 years.

Figure 2

How improvements are measured

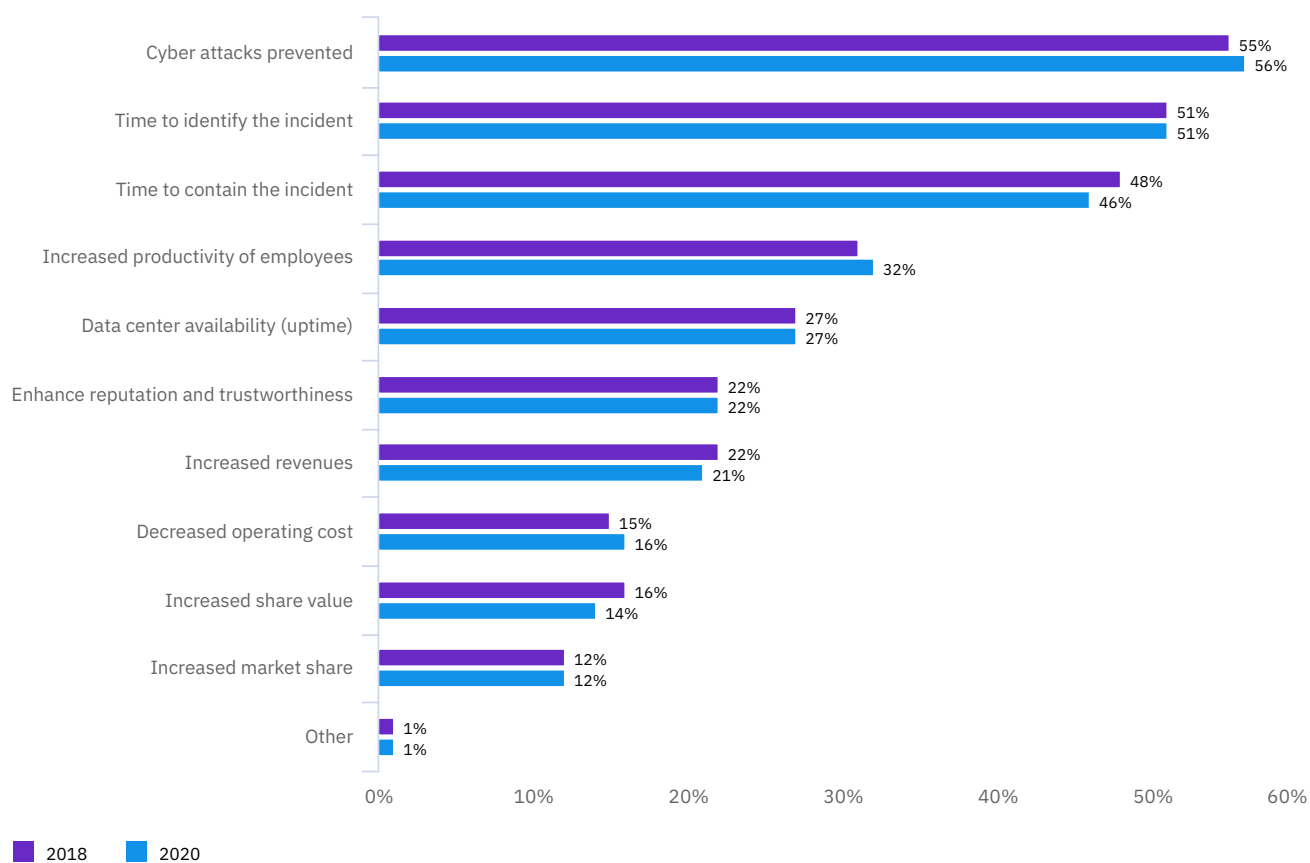


Figure 2 provides insight into how organizations measure improvements in cyber resilience. Out of 10 factors, the top three were: number of cyberattacks prevented, time to identify the incident and time to contain.

Figure 3

Reasons why cyber resilience improved

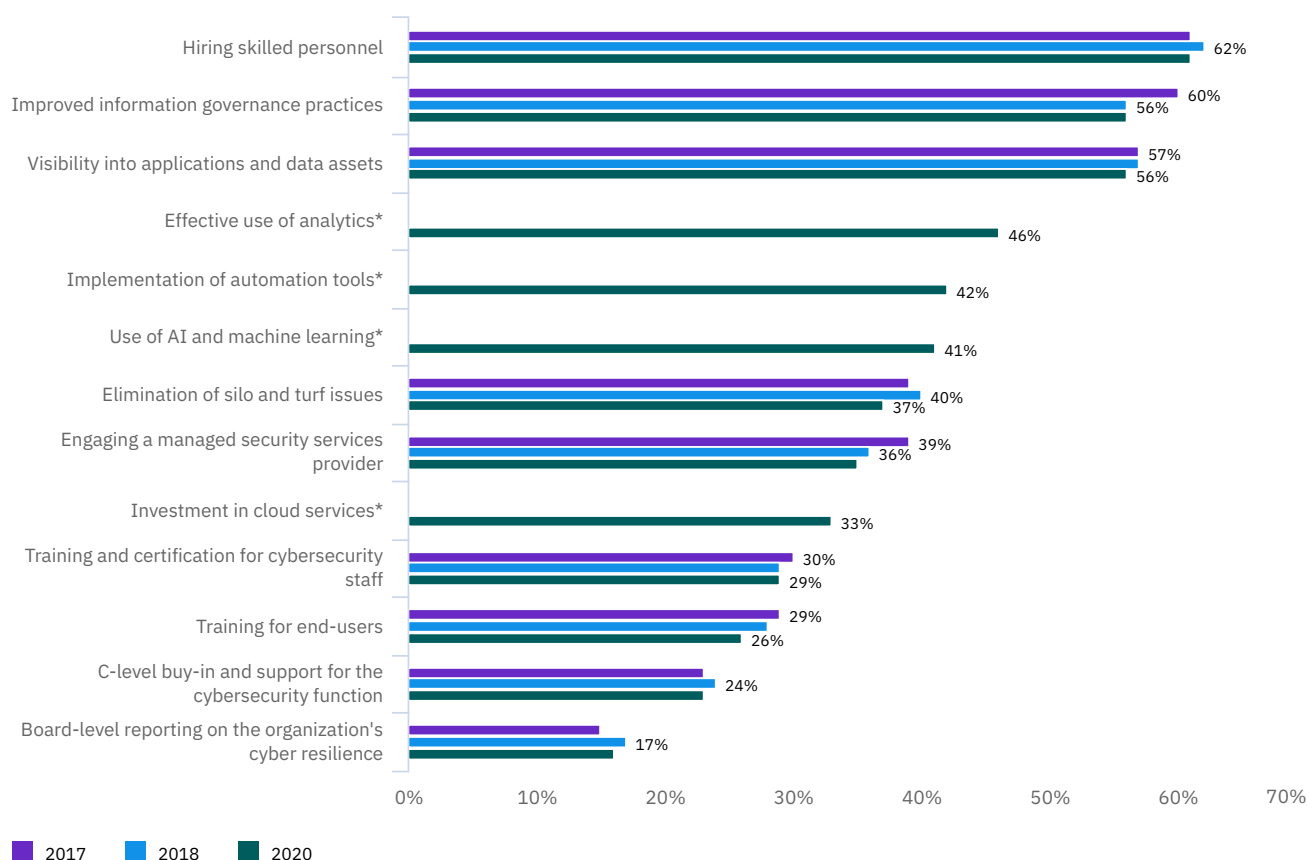


Figure 3 shows the reasons why organizations improved their cyber resilience. While the top three have not changed much year-over-year, analytics, automation and AI and machine learning played prominent roles this year.

Figure 4

Reasons why cyber resilience did not improve

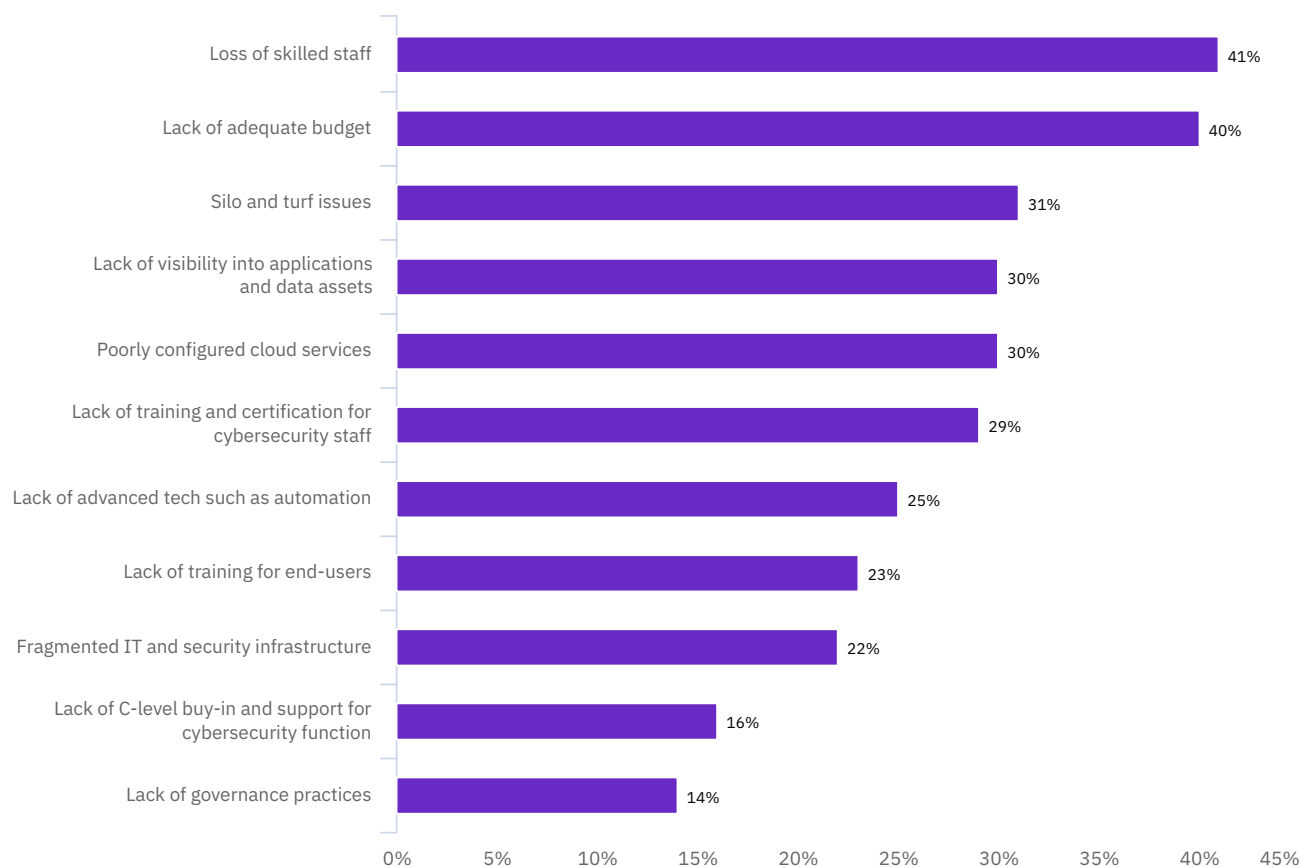


Figure 4 explains why organizations believe they did not improve their cyber resilience. A mix of people, process and technology created challenges.

Figure 5

How use of cloud services improved cyber resilience

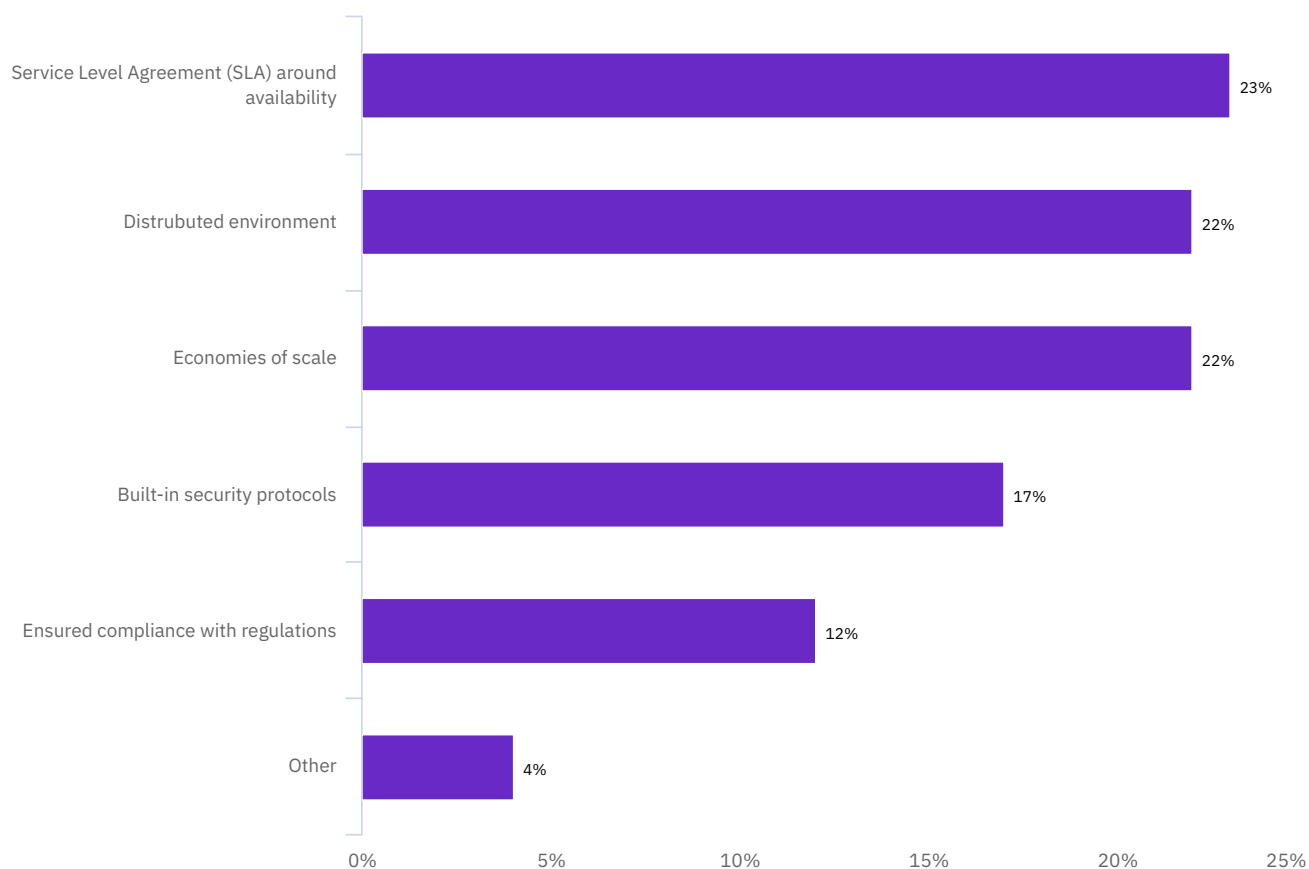


Figure 5 breaks down how the use of cloud services has helped organizations become more cyber resilient. The top three reasons were service level agreements around availability, the distributed environment and economies of scale.

Figure 6

Specific response plans used

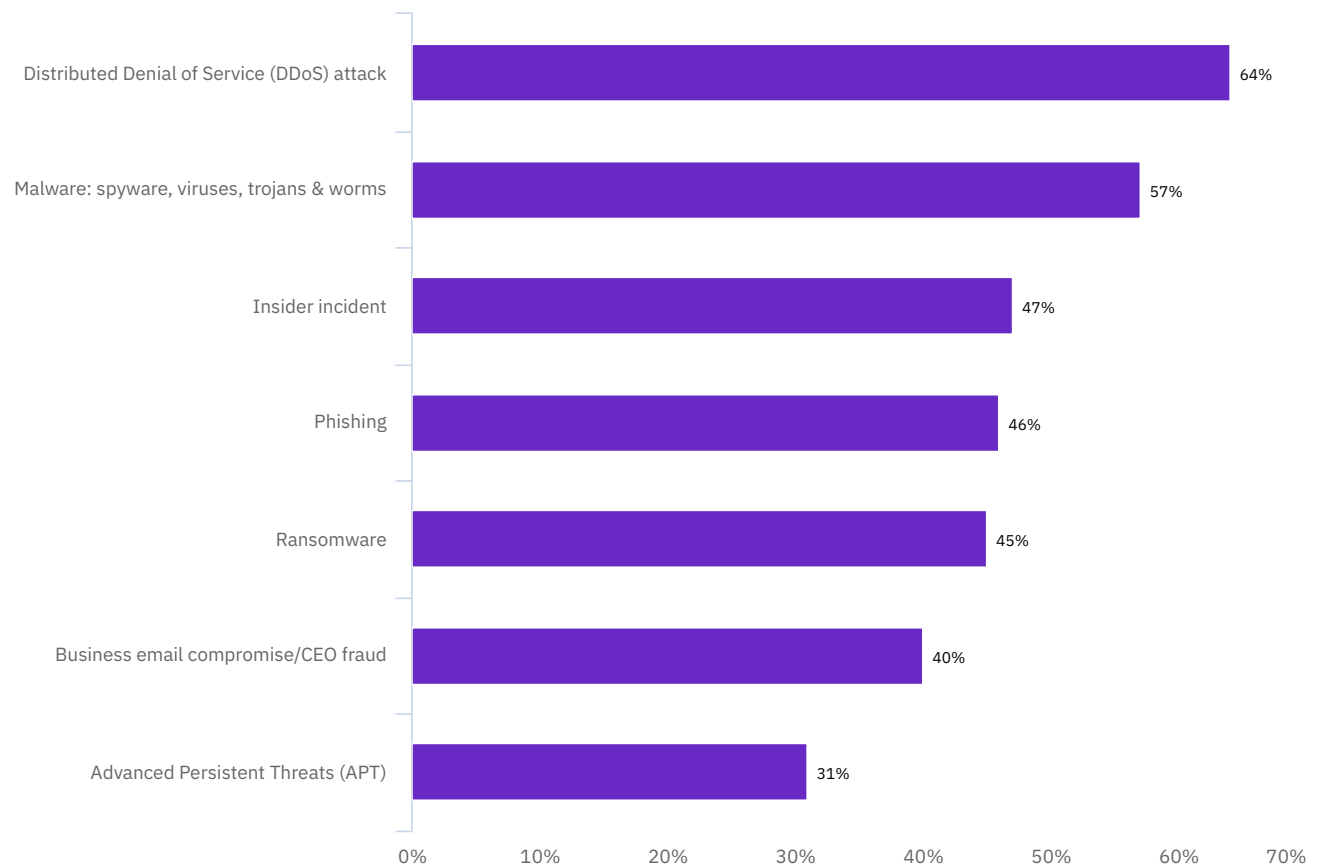


Figure 6 goes into the specific types of threats for which organizations have tailored response plans. DDoS attacks, malware and insider attaches are the top three.

Figure 7

How severity is measured

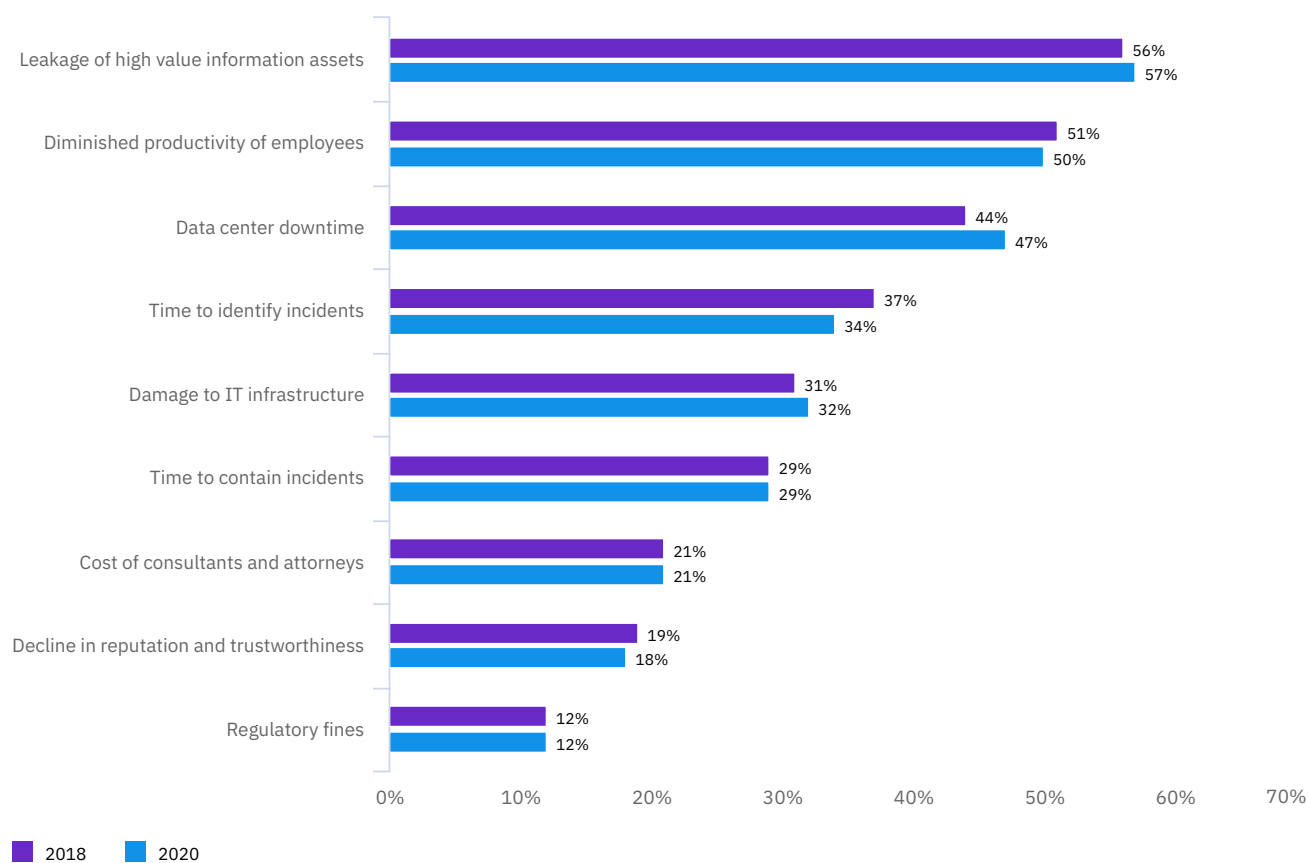


Figure 7 reveals how organizations gauge the severity of an attack with leakage of high value information assets remaining on top for the past two years.

Figure 8

How threat intelligence improves cyber resilience

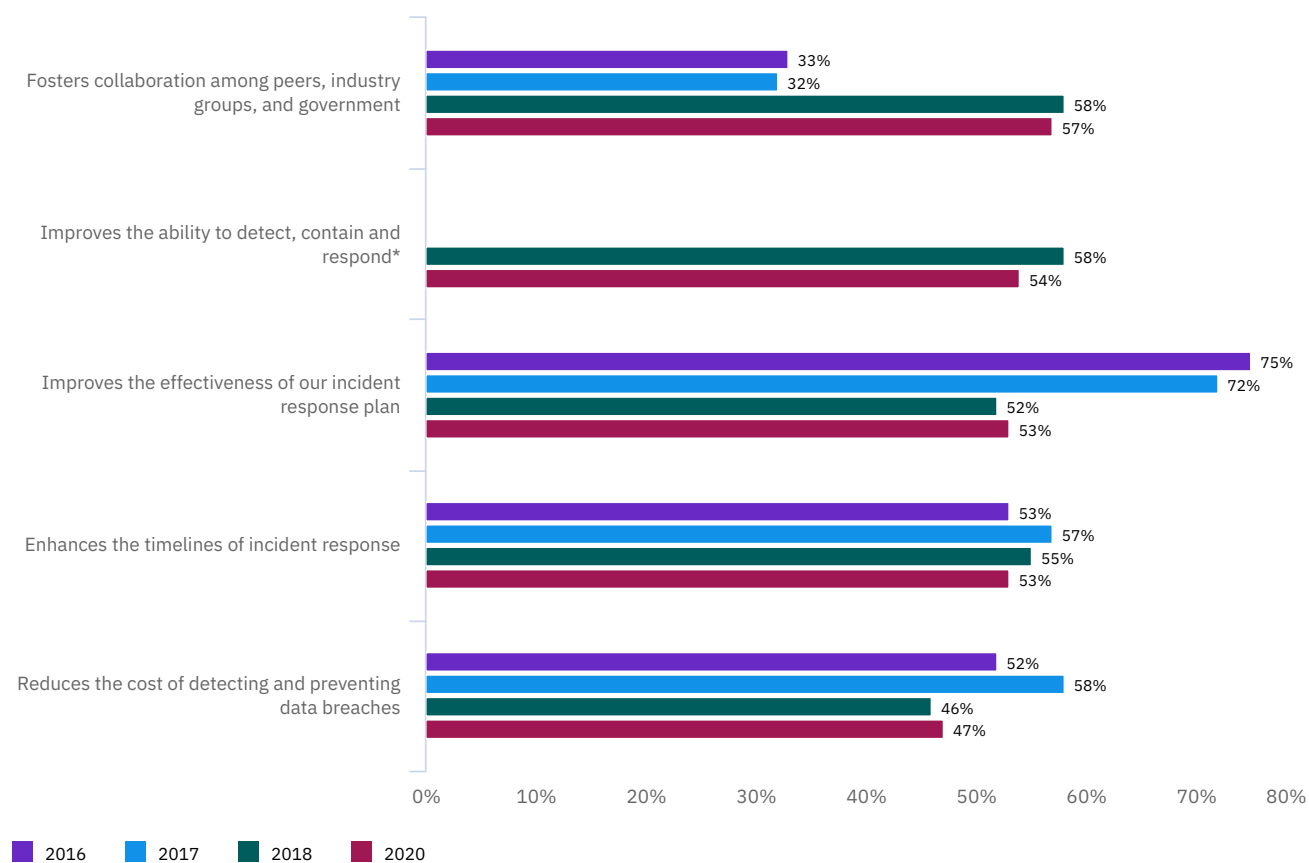


Figure 8 assesses the perceived value of sharing threat intelligence. Over the last four years, respondents' belief in its ability to improve the effectiveness of their incident response plans has gone down by 29%.

Figure 9

Causes for improvement for high performers

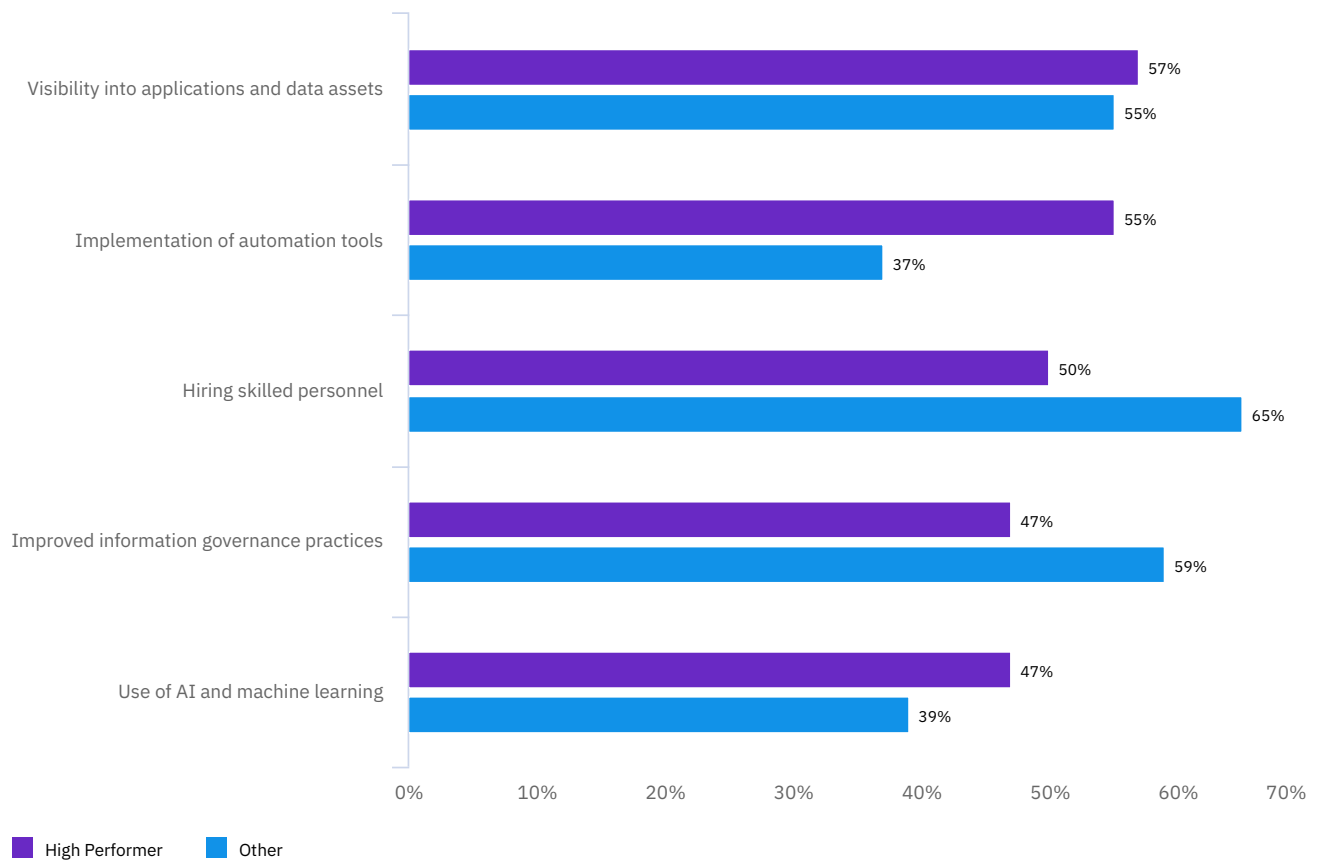


Figure 9 shows the reasons why cyber resilience improved for high performers compared to other organizations.

Figure 10

Reasons why high performers are more cyber resilient

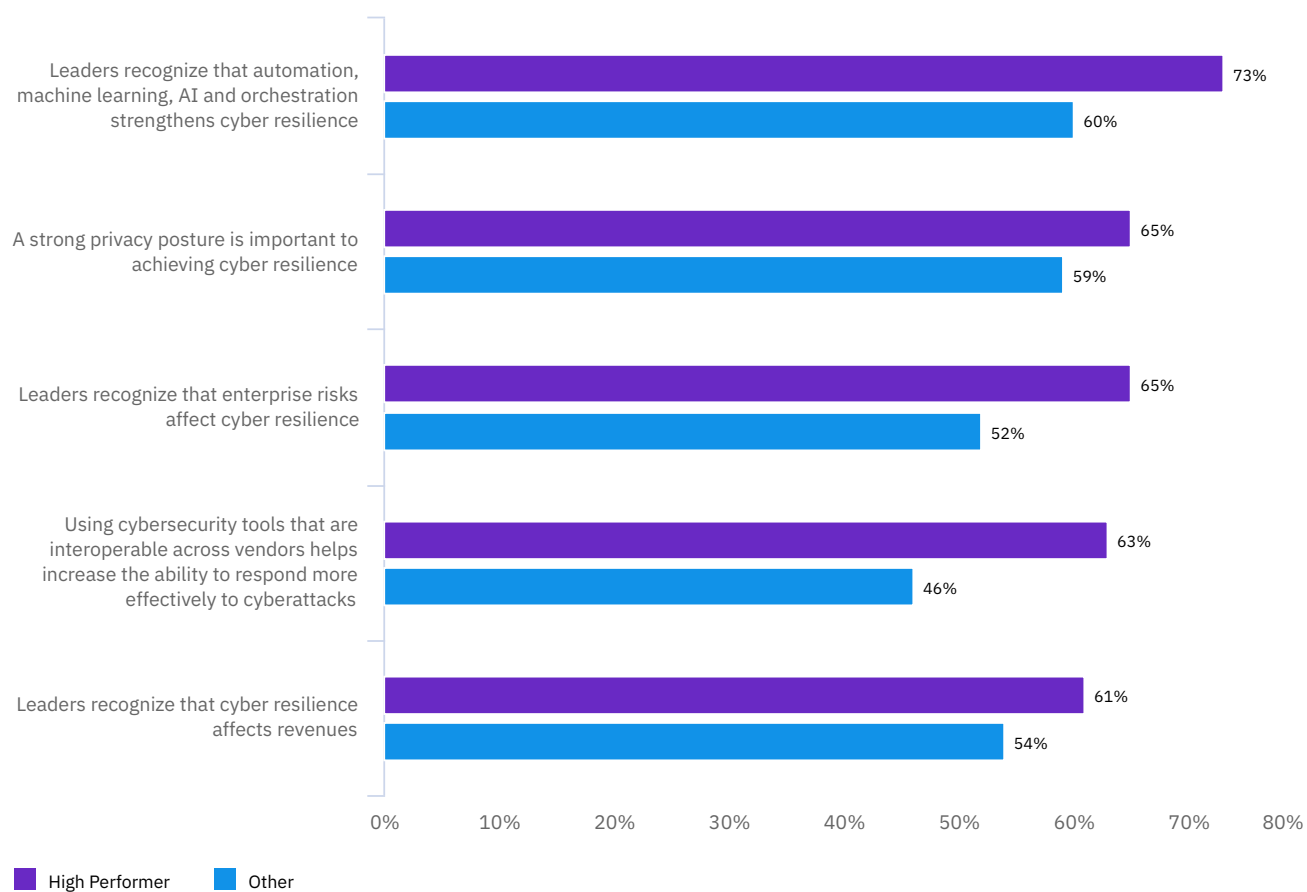


Figure 10 shows reasons why high performers are more cyber resilient.

Figure 11

High performers' cyber resilience confidence level

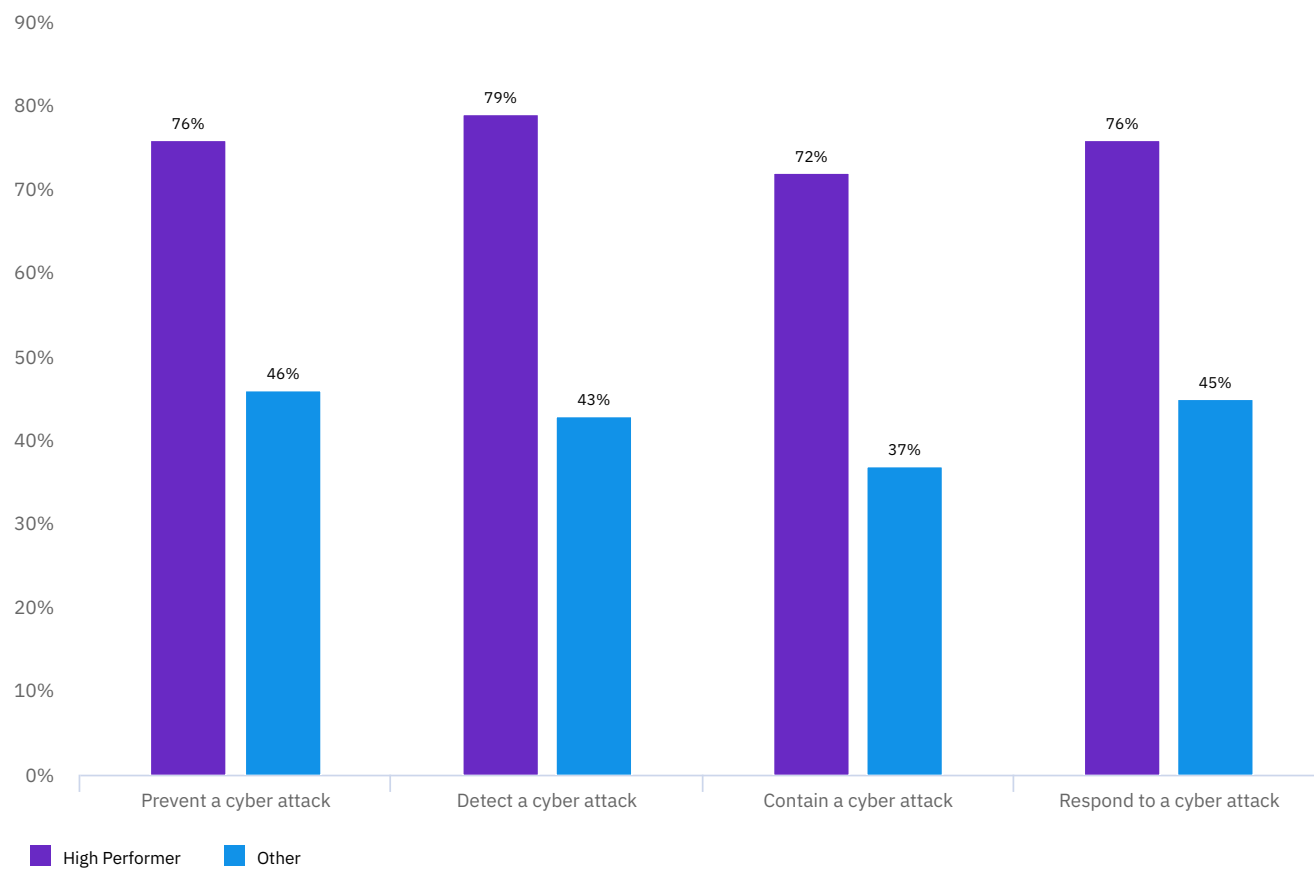


Figure 11 shows high performers' confidence regarding a cyberattack. The biggest gap between high performers and other organizations is in detecting a cyberattack.

Figure 12

How the number of security solutions affects incident response

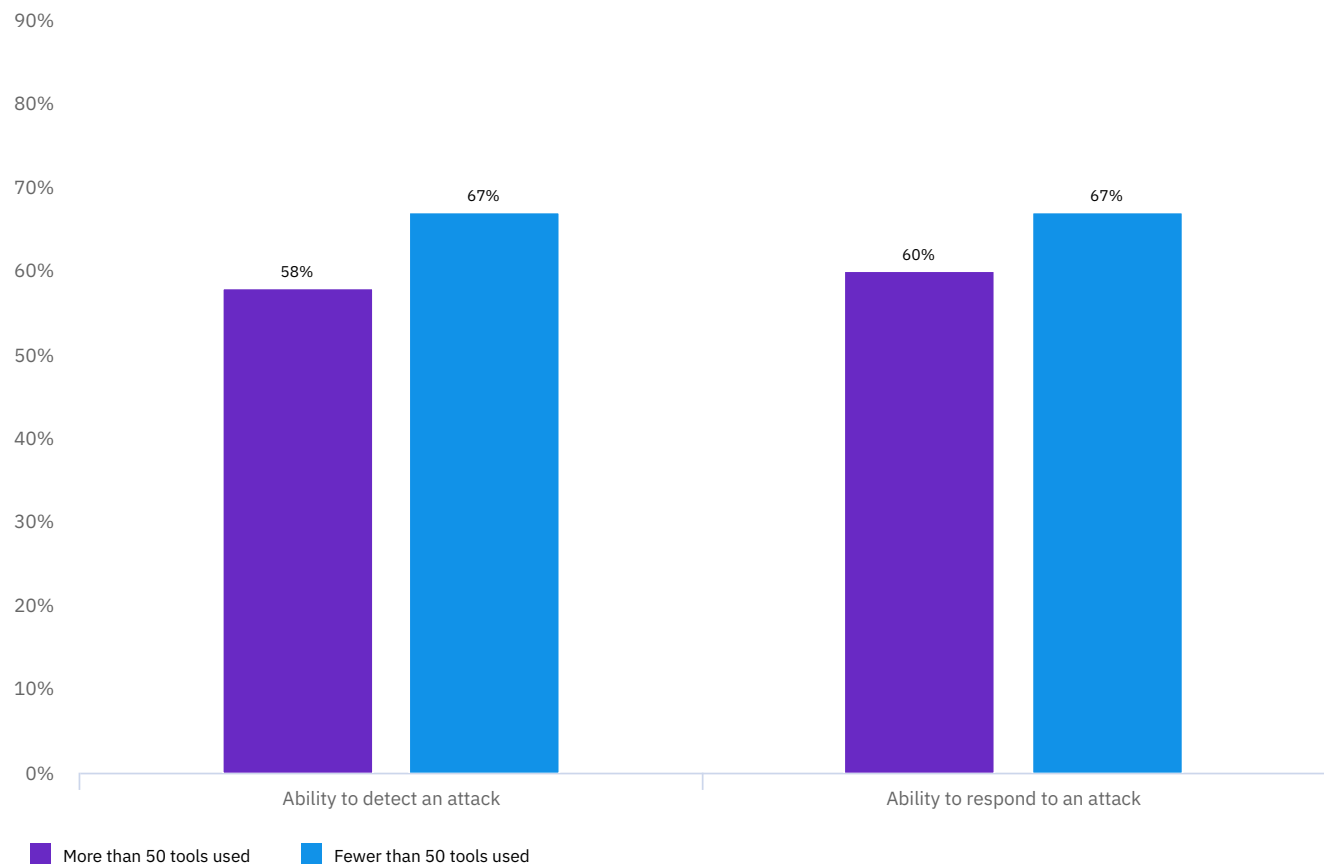


Figure 12 shows the impact of having more than 50 security solutions on responding to an incident. Organizations that used less than 50 tools reported a stronger ability to handle a cyberattack.

Figure 13

Use of attack-specific response plans by geography

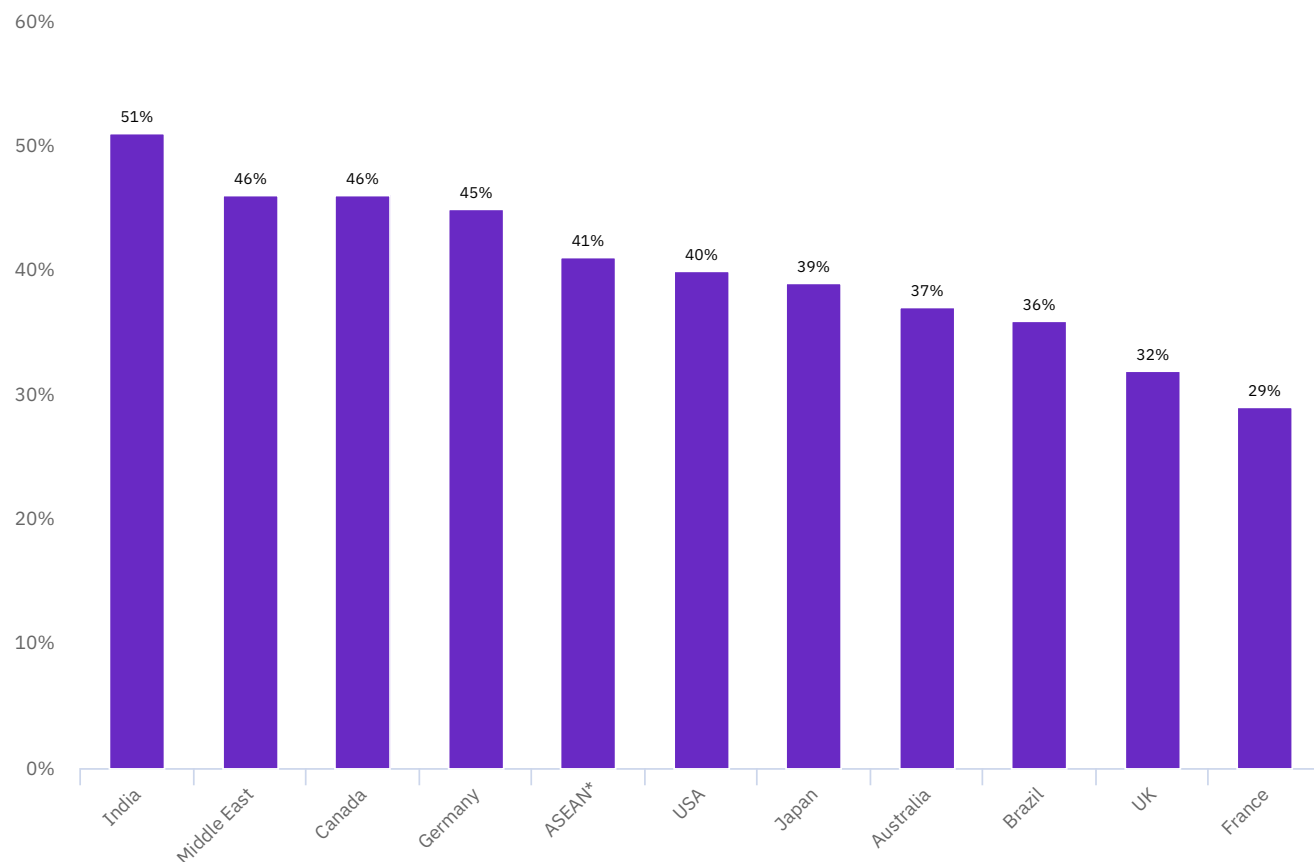


Figure 13 shows the differences among countries represented in the research. Indian organizations were more likely to have specific response plans for different types of cyberattacks. The United Kingdom and France were least likely to have such plans.

*ASEAN represents a sample of respondents located in Singapore, Philippines, Vietnam, Thailand, Malaysia and Indonesia.

**Middle East represents a sample of respondents located in United Arab Emirates and Saudi Arabia.

Figure 14

Value of cloud services to achieving a high level of cyber resilience by geography

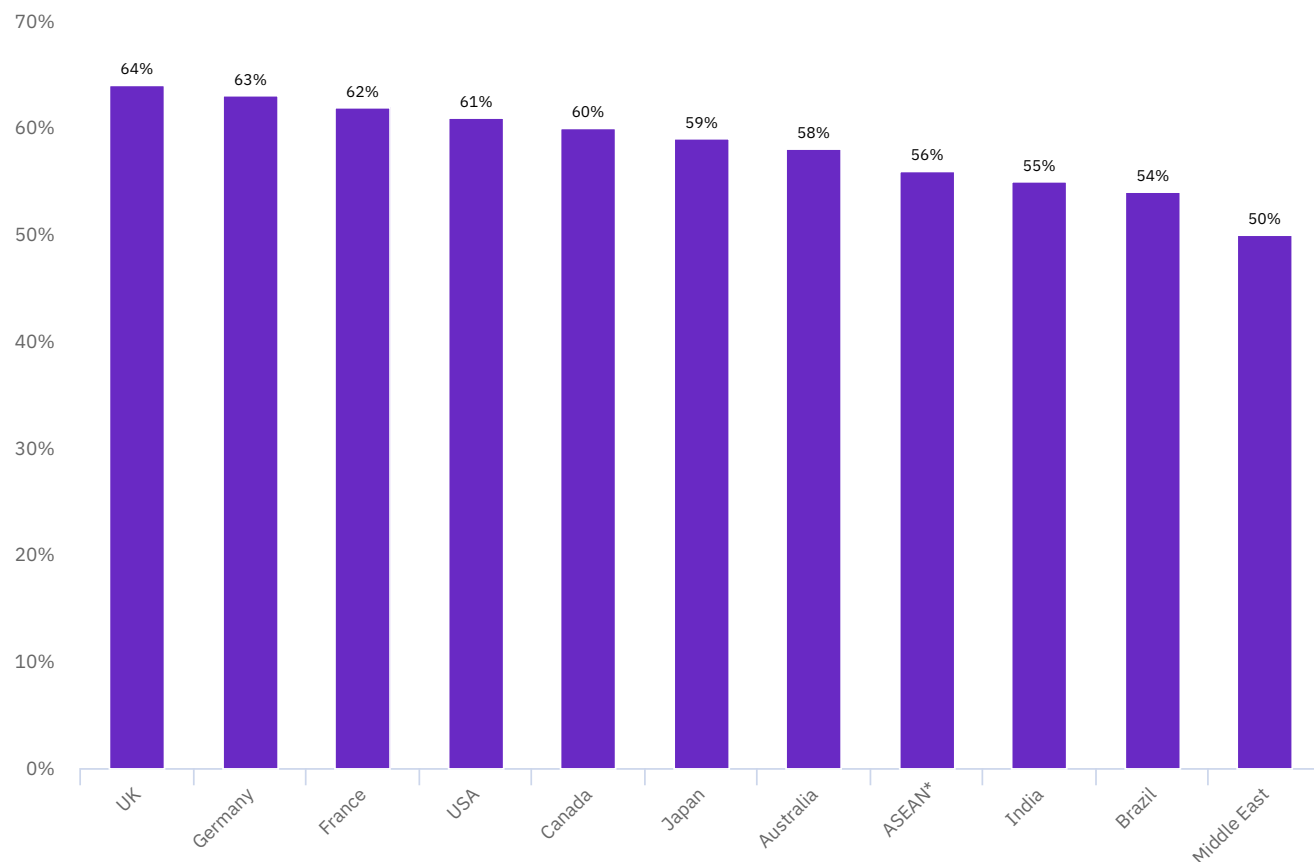


Figure 14 illustrates the regional differences in the perceived impact of cloud services on cyber resilience. The United Kingdom, Germany, France and the United States aligned closely.

*ASEAN represents a sample of respondents located in Singapore, Philippines, Vietnam, Thailand, Malaysia and Indonesia.

**Middle East represents a sample of respondents located in United Arab Emirates and Saudi Arabia.

Figure 15

How use of Cloud services improved cyber resilience by industry*

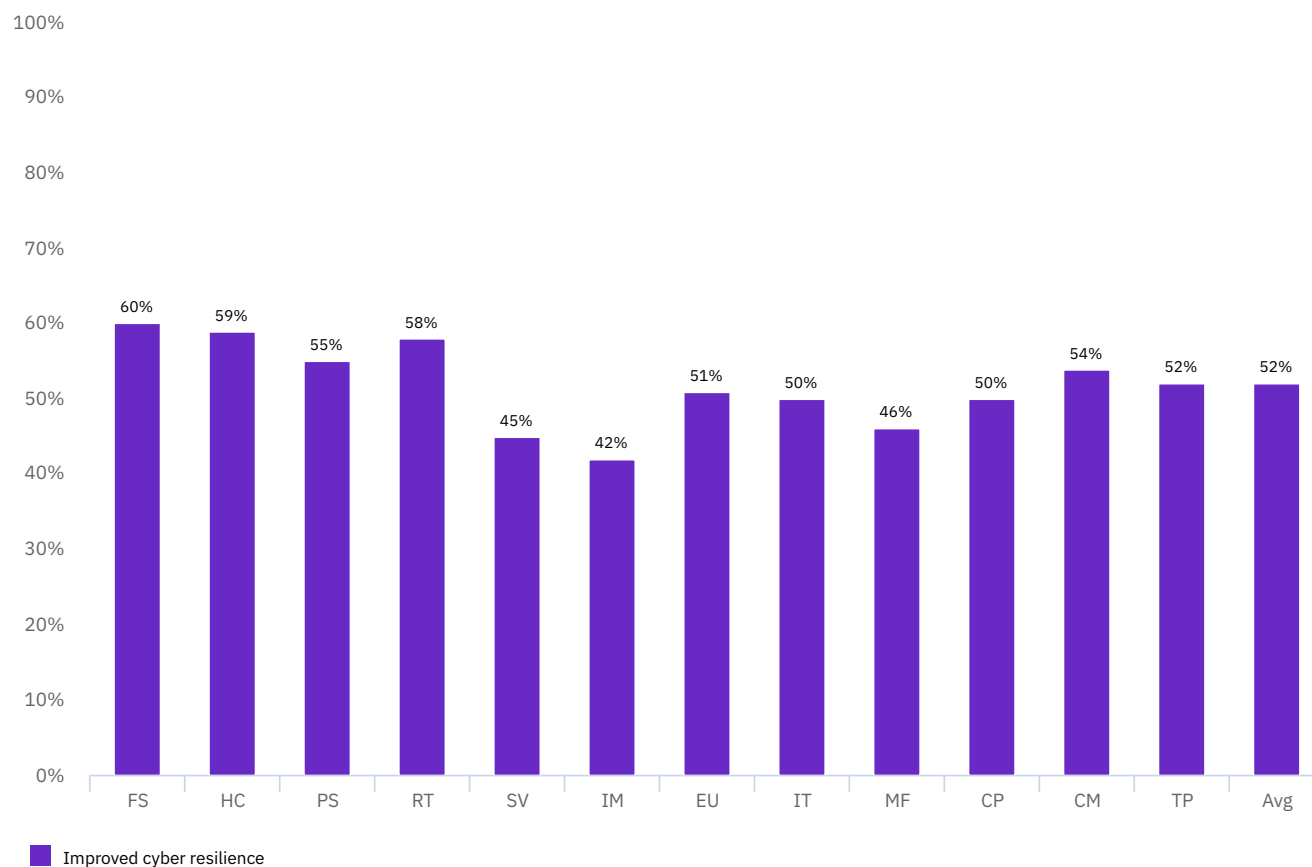


Figure 15 shows differences in how the use of Cloud services improved cyber resilience by industry

*Industry abbreviations: Financial services (FS), Healthcare & pharmaceutical (HC), Public sector (PS), Retailing (RT), Services (SV), Industrial (IM), Energy & utilities (EU), IT & technology (IT), Manufacturing (MF), Consumer products (CP), Communications (CM), Transportation (TP), Entertainment & media (EM), Education & research (ED), Hospitality (HP), Defense & aerospace (DF), Agriculture & food services (AG), Logistics & distribution (LD). For full list of industry definitions, see page 34.

Figure 16

How use of CSIRPs differ by industry*

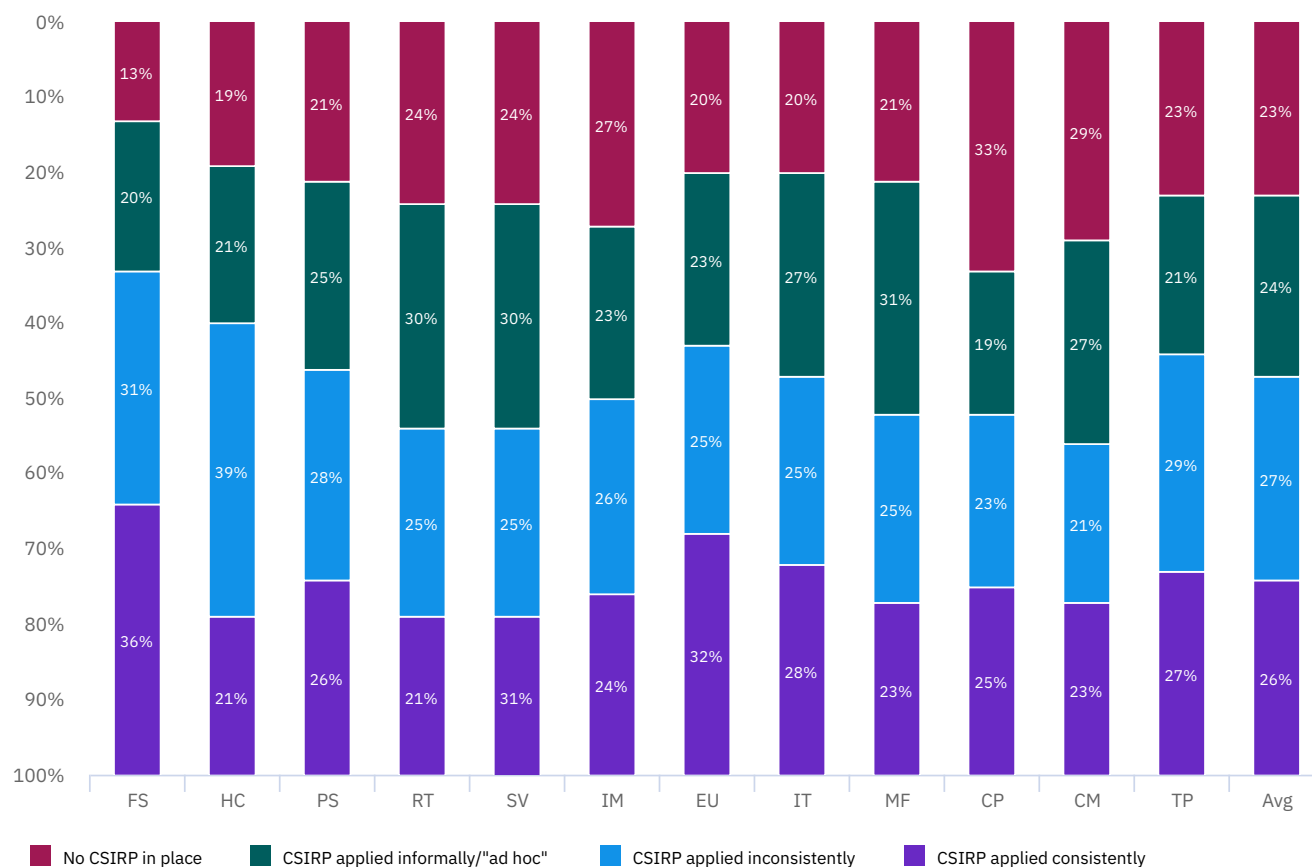


Figure 16 shows the differences in use of a CSIRP by industry

*Industry abbreviations: Financial services (FS), Healthcare & pharmaceutical (HC), Public sector (PS), Retailing (RT), Services (SV), Industrial (IM), Energy & utilities (EU), IT & technology (IT), Manufacturing (MF), Consumer products (CP), Communications (CM), Transportation (TP), Entertainment & media (EM), Education & research (ED), Hospitality (HP), Defense & aerospace (DF), Agriculture & food services (AG), Logistics & distribution (LD). For full list of industry definitions, see page 34.

Figure 17

Factors that justify funding for cybersecurity function

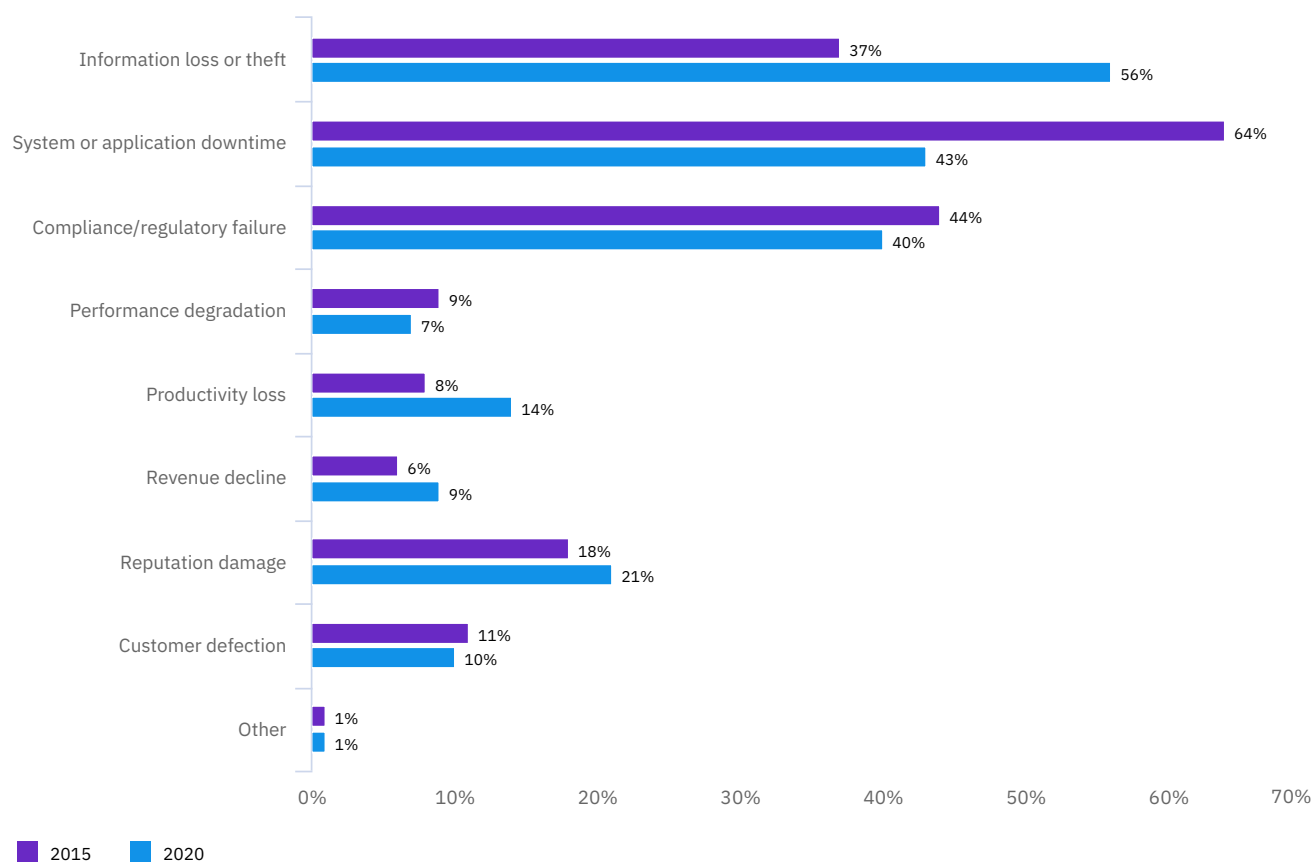


Figure 17 shows the factors that justify cybersecurity funding. Budget justification since 2015 has shifted from system or application downtime to information loss or theft.

Figure 18

Cybersecurity budget allocated to cyber resilience

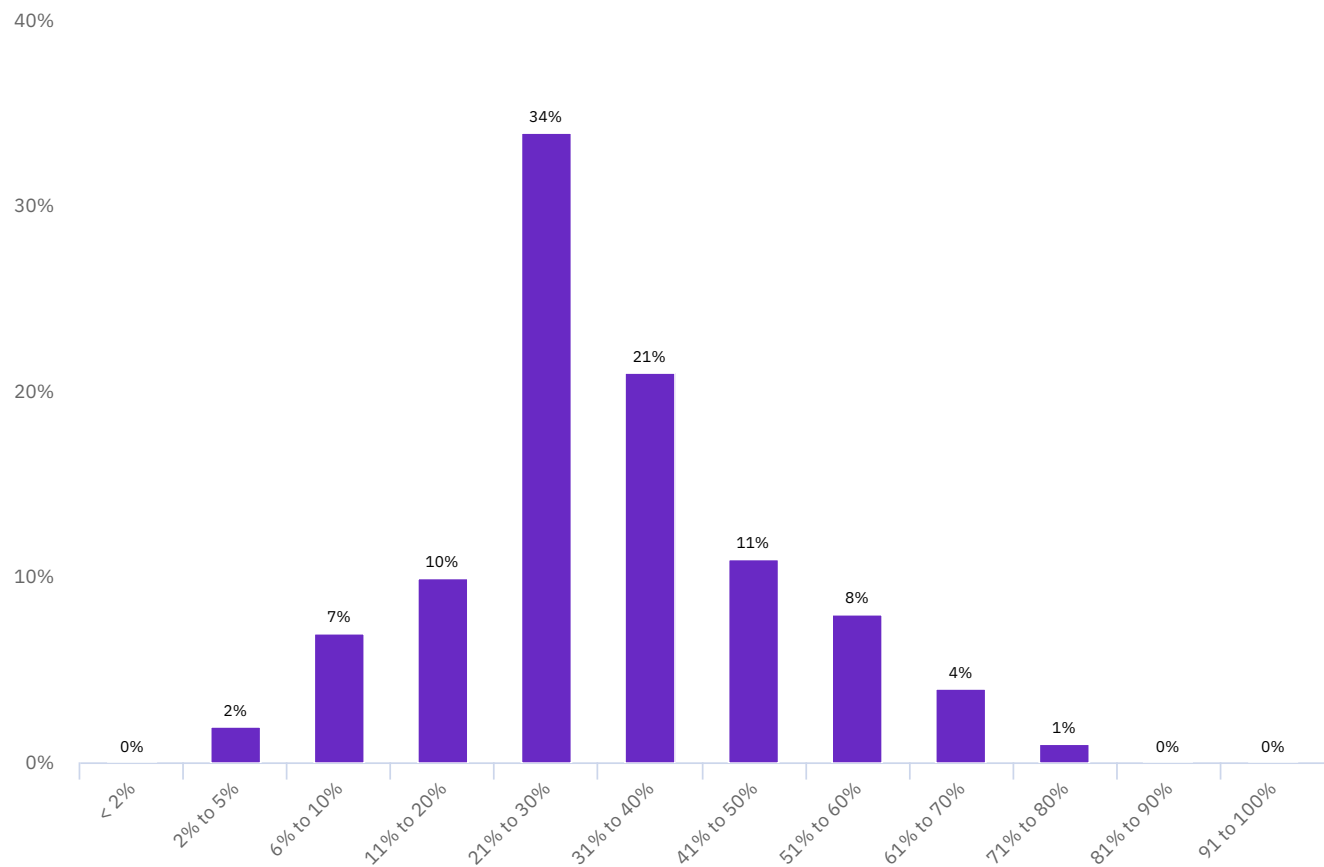


Figure 18 shows the percent of budget allocated to cyber resilience related activities.

Organizational characteristics

This 2020 Cyber Resilient Organization Report includes responses from 3,439 IT and Security practitioners in United States, India, Germany, United Kingdom, Brazil, Japan, Australia, France, Canada, ASEAN* and the Middle East**.

Represented industries

18 industry segments were included in the sample.

Financial services

Banking, insurance, investment companies

Health & pharmaceutical

Hospitals, clinics, and biomedical life sciences

Retail

Brick and mortar and e-commerce

Manufacturing

Large-scale producers of goods or components

Hospitality

Hotels, restaurant chains, cruise lines

Public sector

Federal, state and local government agencies and NGOs

Transportation

Airlines and railroads

Energy & utilities

Oil and gas companies, utilities, alternative energy producers and suppliers

Consumer products

Manufacturers and distributors of consumer products

Logistics & distribution

Trucking and delivery companies, supply chain management

Industrial

Chemical process, engineering and manufacturing companies

Communications

Newspapers, book publishers, public relations and advertising agencies

IT & technology

Software and hardware companies

Services

Professional services such as legal, accounting and consulting firms

Entertainment & media

Movie production, sports, gaming and casinos

Agriculture & food services

Farming, commercial producers of food (plants and livestock)

Defense & aerospace

Producers and designers of commercial or defense-related aircraft and systems

Education & research

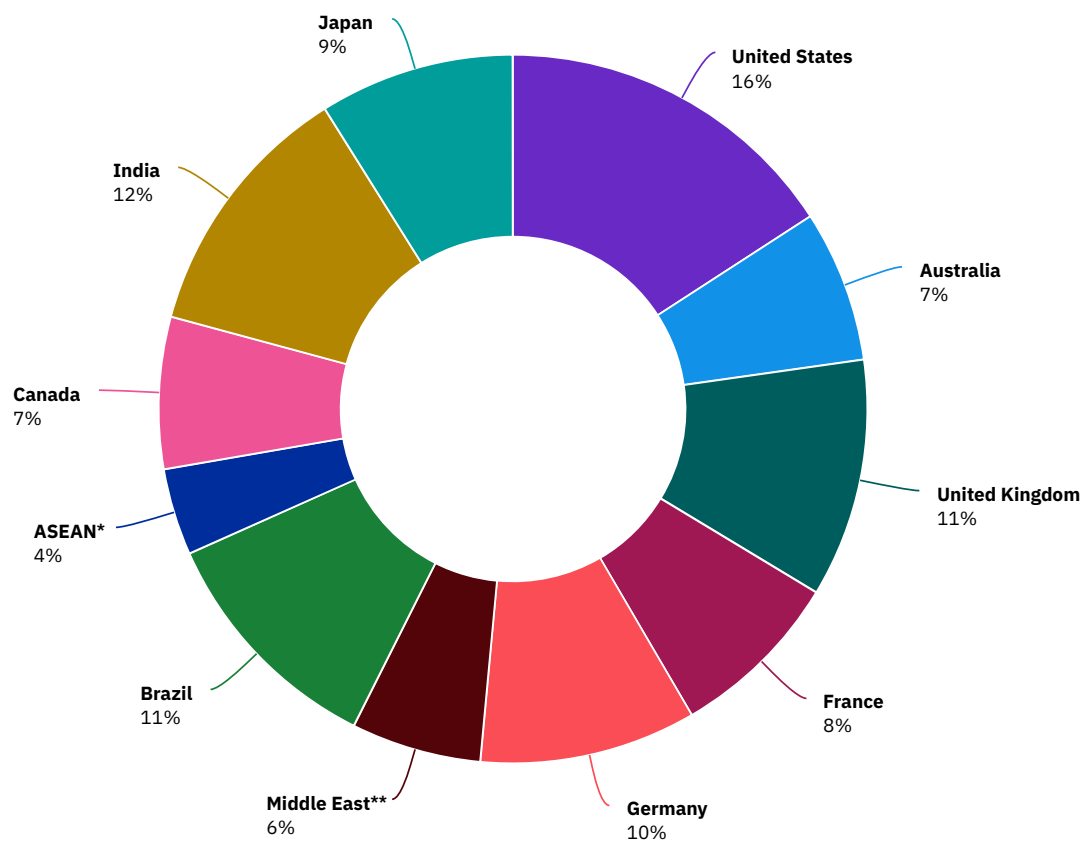
Market research, think tanks, R&D, public and private universities and colleges, training and development companies

*ASEAN represents a sample of respondents located in Singapore, Philippines, Vietnam, Thailand, Malaysia and Indonesia.

**Middle East represents a sample of respondents located in United Arab Emirates and Saudi Arabia.

Figure 19

Distribution of the sample by country or region



*ASEAN represents a sample of respondents located in Singapore, Philippines, Vietnam, Thailand, Malaysia and Indonesia.

**Middle East represents a sample of respondents located in United Arab Emirates and Saudi Arabia.

Figure 20

Distribution of the sample by industry

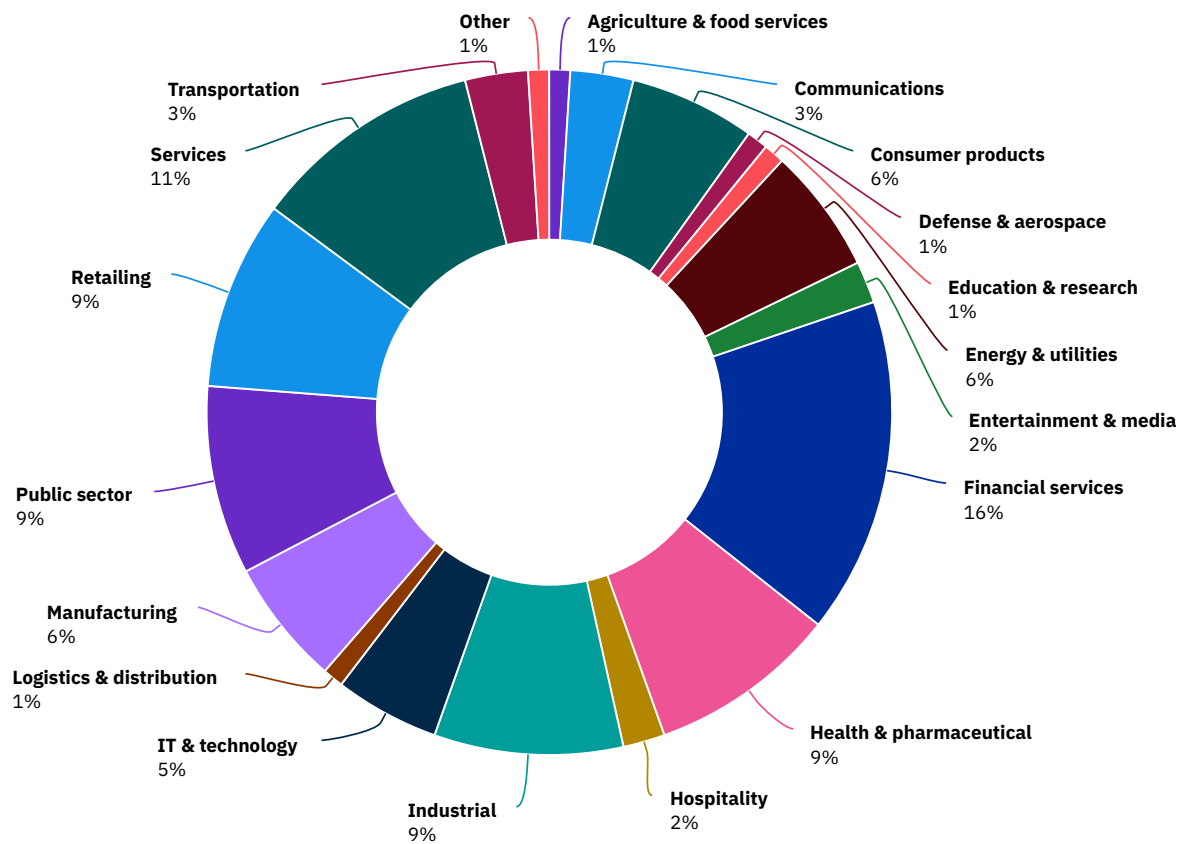


Figure 21

Distribution by job role

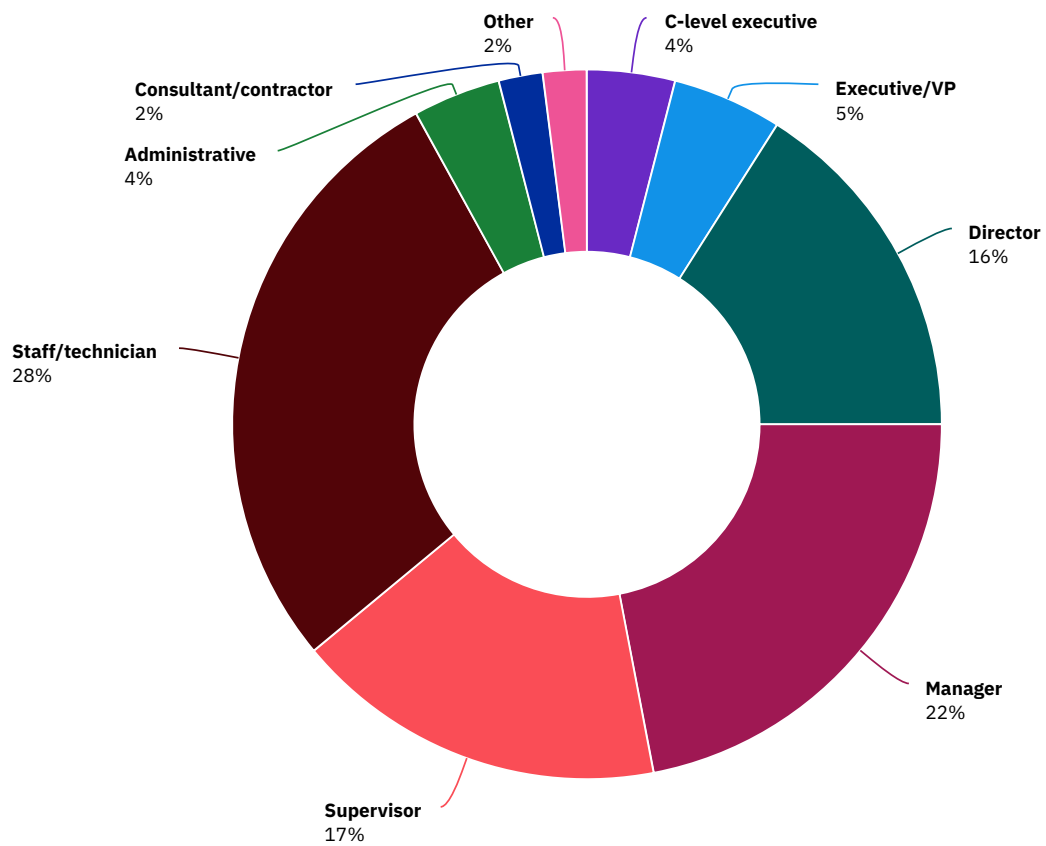
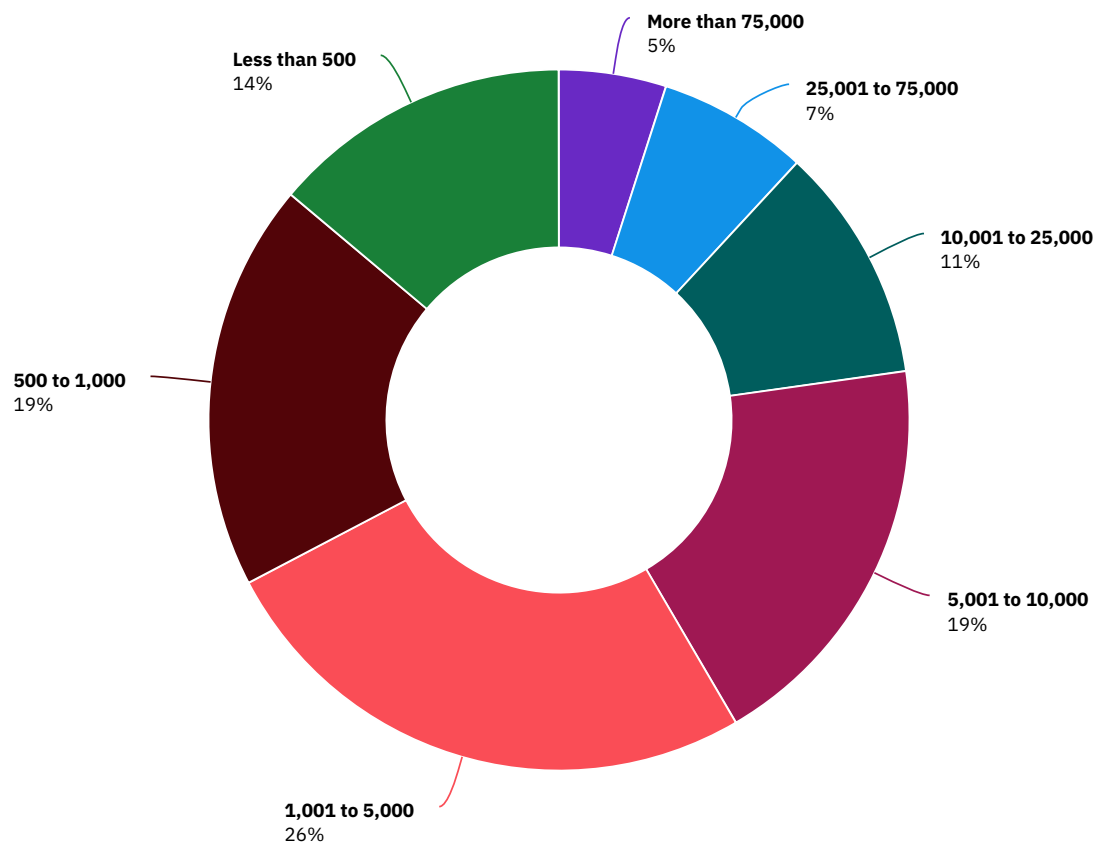


Figure 22


Distribution by size of company



Methodology

IT and security practitioners located in the United States, India, Germany, the United Kingdom, Brazil, Japan, Australia, France, Canada, ASEAN and the Middle East were asked to complete an online survey.

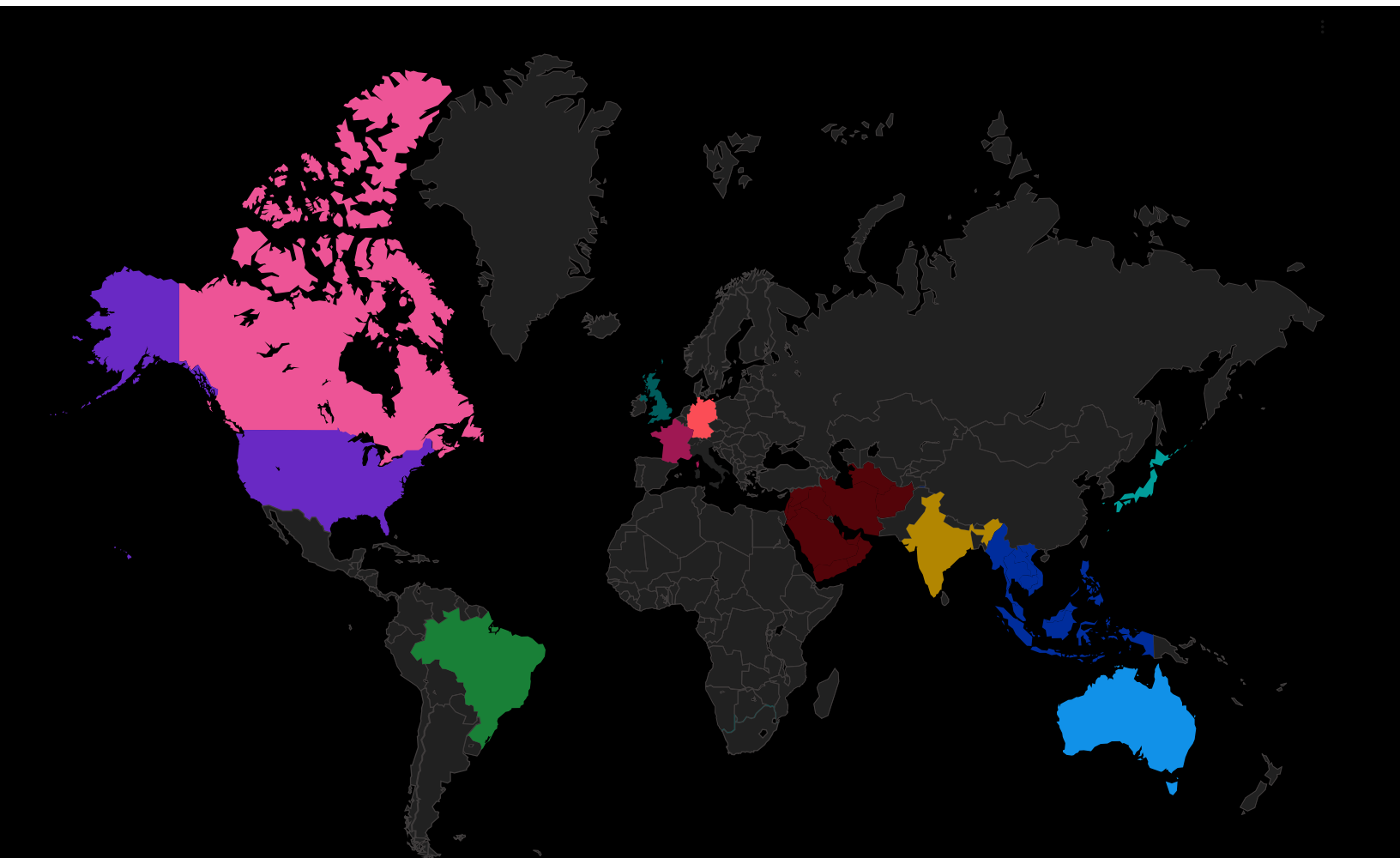
The final sample of respondents consisted of 3,439 surveys, for an overall 3.3% response rate.

11 

Countries and regions

3,439 

Respondents



ASEAN represents a sample of respondents located in Singapore, Philippines, Vietnam, Thailand, Malaysia and Indonesia.

**Middle East represents a sample of respondents located in United Arab Emirates and Saudi Arabia.

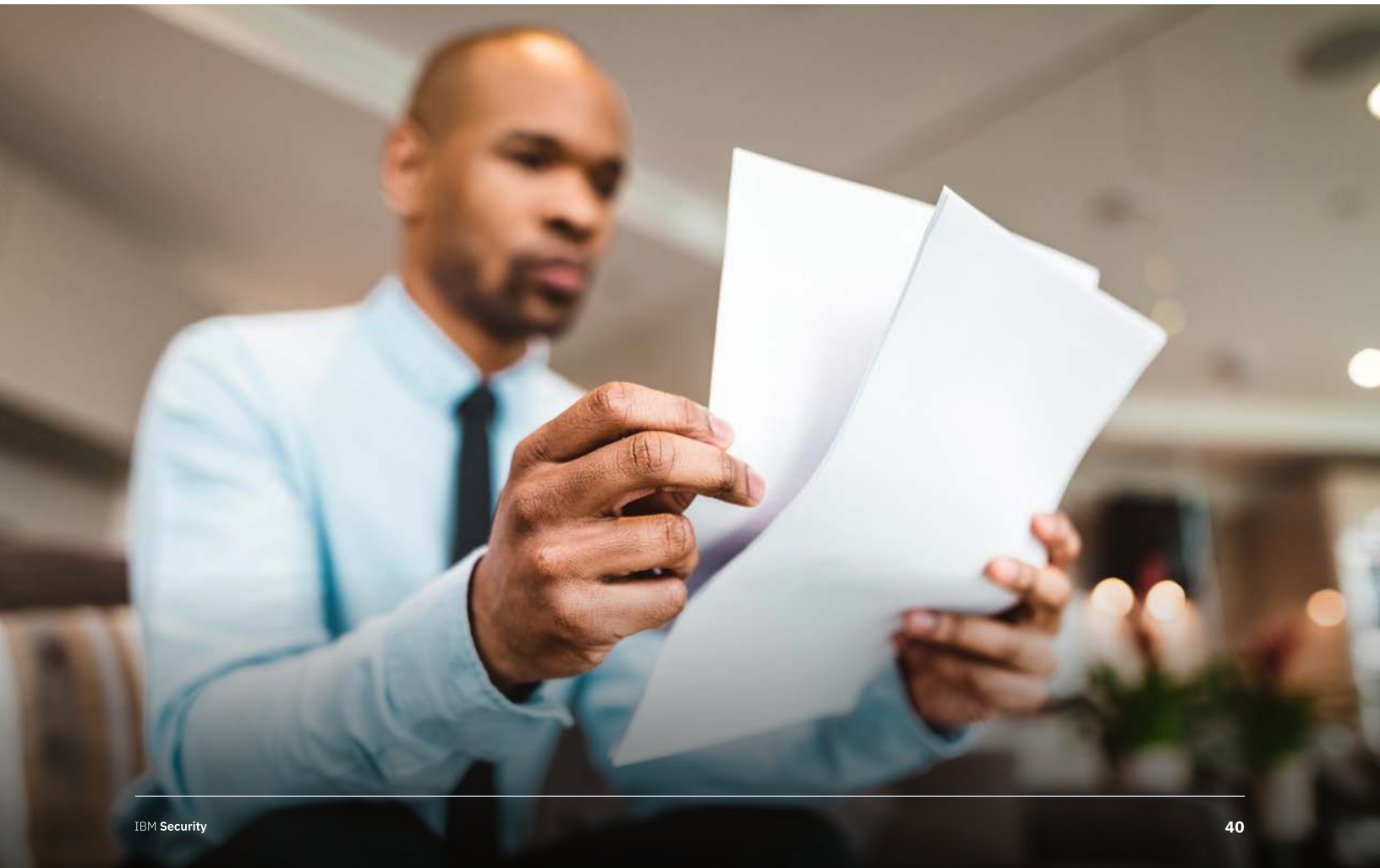
Definitions

Cyber resilience

Cyber resilience is defined as the alignment of prevention, detection and response capabilities to manage, mitigate and move on from cyberattacks. This refers to an enterprise's capacity to maintain its core purpose and integrity in the face of cyberattacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from a myriad of serious threats against data, applications and IT infrastructure.

High performer

As part of this research, we identified respondents that self-reported their organizations had achieved a high level of cyber resilience and were better able to mitigate risks, vulnerabilities and attacks. We refer to these organizations as high performers.



Research limitations

Survey research has inherent limitations that need to be carefully considered before drawing inferences from findings. The following items are specific limitations germane to most web-based surveys.

Non-response bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias

The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

About Ponemon Institute and IBM Security

The *Cyber Resilient Organization Report* is produced jointly between Ponemon Institute and IBM Security. The research is conducted independently by Ponemon Institute and results are sponsored, analyzed, reported and published by IBM Security.



Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards, and does not collect any personally identifiable information from individuals (or company identifiable information in business research). Furthermore, strict quality standards ensure that subjects are not asked extraneous, irrelevant or improper questions.



IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than two trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

If you have questions or comments about this research report, including for permission to cite or reproduce the report, please contact by letter, phone call or email:

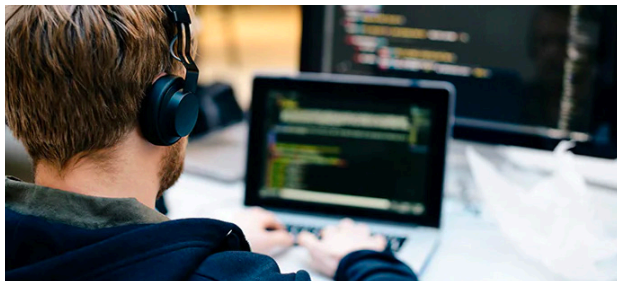
Ponemon Institute LLC

Attn: Research Department
2308 US 31 North
Traverse City, Michigan
49686 USA

1.800.887.3118

research@ponemon.org

Next steps



Integrate tools across multicloud environments

[Learn more →](#)



Detect threats

[Learn more →](#)



Orchestrate your response

[Learn more →](#)



Remediate and recover

[Learn more →](#)

© Copyright IBM Corporation 2020

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2020

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.