Ponemon INSTITUTE

The Challenges to Ensuring Information Is Secure, Compliant and Ready for AI

Sponsored by OpenText

Independently conducted by Ponemon Institute LLC

Publication Date: August 2025

Ponemon Institute© Research Report

The Challenges to Ensuring Information Is Secure, Compliant and Ready for AI

August 2025

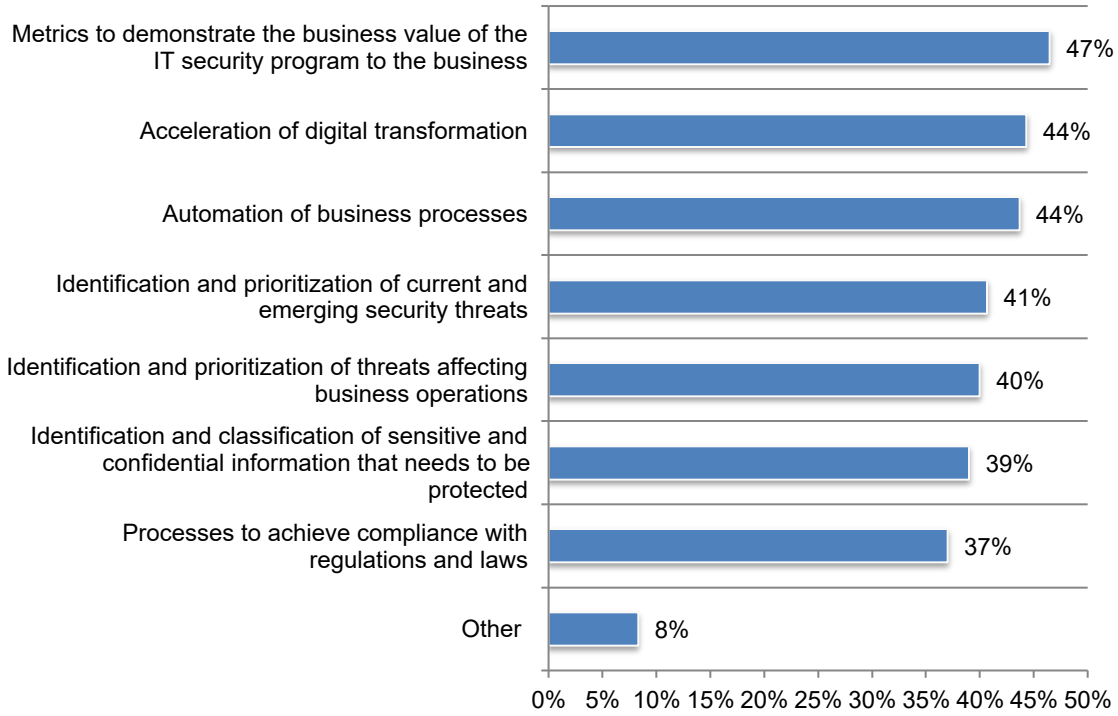
Part 1. Introduction

The purpose of this research is to drive important insight into how IT and IT security leaders are ensuring the security of information without hindering business goals and innovation.
A key takeaway is that IT and IT security leaders are under pressure to ensure sensitive and confidential information is secure and compliant without making it difficult for organizations to innovate and pursue opportunities to grow the business.

The research also reveals what needs to be done to achieve AI readiness based on the experiences of the 50 percent of organizations that have invested in AI. These include preventing the exposure of sensitive information, strengthening encryption practices and reducing the risk of poor or misconfigured systems due to over-reliance on AI for cyber risk management. When deploying, organizations should develop an AI data security program, use tools to validate AI prompts and their responses, train teams to spot AI-generated behavior patterns or threat actors, use data cleansing and governance and identify and mitigate bias in AI models for safe and responsible use.

Metrics to demonstrate the value of the IT security program to the business is the top priority in the next 12 months. As shown in Figure 1, 47 percent of respondents plan to use metrics to show the value IT security brings to the organization. This is followed by acceleration of digital transformation and automation of business processes (both 44 percent of respondents). Forty percent of respondents say a top three priority is the identification and prioritization of threats affecting business operations.

Figure 1. What are the top IT priorities for the next 12 months?
Three responses permitted



Organizations recognize the need to make AI part of their security strategy, but difficulties in adoption exist.

Fifty percent of respondents say their organizations are using AI as part of their security strategy, but 57 percent of respondents rate the adoption of AI as very difficult to extremely difficult and 53 percent of respondents say it is very difficult or extremely difficult to reduce potential AI security and legal risks. Foundational to success is to ensure AI is secure, compliant and governed.

AI deployment has the support of senior leaders. Compared to other IT initiatives, 57 percent of respondents say AI initiatives have a very or very high priority. Fifty-five percent of respondents say their CEOs and Boards of Directors consider the use of AI as part of their IT and security programs as very or extremely important. A possible reason for such support is that 54 percent of respondents are confident or very confident of their organizations' ability to demonstrate ROI from AI initiatives.

CEOs, CIOs and CISOs are most likely to have authority for setting AI strategy. Fifteen percent of CEOs, 14 percent of CIOs and 12 percent of CISOs have final authority for such AI initiatives as technology investment decisions and the priorities and timelines for deployment.

Despite leadership's support for AI, IT/IT security and business goals may not be in alignment. Less than half (47 percent of respondents) say IT/IT security and business goals are in alignment with those who are responsible for AI initiatives. Fifty percent of respondents say their organizations have hired or are considering hiring a chief AI officer or a chief digital officer to lead AI strategy. Such an appointment of someone dedicated to managing the organization's AI strategy may help bridge gaps between the goals and objectives of IT/IT security with those who have final authority over AI strategy.

Concerns about privacy can cause delays in AI adoption. The inadvertent infringement of privacy rights is considered the top risk caused by AI. Forty-four percent of respondents say their biggest concern is making sure risks to privacy are mitigated. Other concerns are weak or no encryption (42 percent of respondents) and poor or misconfigured systems due to over-reliance on AI for cyber risk management.

Developing a data security program and practice is considered the most important step to reduce risks from AI. Fifty-three percent of respondents say it is very difficult or extremely difficult to reduce potential AI security and legal risks. To address data security risks in AI, 46 percent of respondents say they are developing a data security program and practice. Other steps are using tools to validate AI prompts and their responses (39 percent of respondents), training teams to spot AI-generated behavior patterns or threat actors (39 percent of respondents), using data cleansing and governance (38 percent of respondents) and identifying and mitigating bias in AI models for safe and responsible use (38 percent of respondents).

Despite being a priority, the top governance challenge is insufficient budget for investments in AI technologies. Thirty-one percent of respondents say there is insufficient budget for AI-based technologies. This is followed by 29 percent of respondents who say there is not enough time to integrate AI-based technologies into security workflows, 28 percent of respondents who say IT and IT security functions are not aligned with the organization's AI strategy and 28 percent of respondents say their organizations can't recruit personnel experienced in AI-based technologies.

The adoption of GenAI and Agentic AI

GenAI is considered very or highly important to organizations' IT and overall business strategy because it improves operational efficiency and worker productivity. Of the 50 percent of organizations that have adopted AI, 32 percent have adopted GenAI as part of their IT or overall business strategy and 26 percent will adopt GenAI in the next six months. Fifty-eight

percent of these respondents say GenAI is important to highly important to their organizations' IT and overall business strategy.

GenAI supports security operations and employee productivity. The most important GenAI use cases are supporting security operations (e.g. analyzing alerts, generating playbooks) (39 percent of respondents), improving employee productivity (e.g. drafting documents, summarizing content) (36 percent of respondents), assisting with software development (e.g. code generation or debugging) (34 percent of respondents) and accelerating threat detection or incident response (34 percent of respondents).

Copyright and other legal risks are the biggest challenges to an effective GenAI program. Respondents were asked to identify the biggest challenges to an effective GenAI program. Forty-three percent of respondents say copyright and other legal risks is the top challenge to an effective GenAI program. Thirty-seven percent of respondents say lack of in-house expertise and 36 percent of respondents say regulatory uncertainty and changes are barriers to an effective GenAI program.

Organizations are slow to adopt Agentic AI as part of their overall IT and business strategy. While 32 percent of respondents who are using AI have adopted GenAI, only 19 percent have adopted Agentic AI. Only 31 percent of the organizations that have adopted Agentic AI say it is very or extremely important to their organizations' IT and business strategy.

Organizations' approaches to securing data and supporting business innovation

Ensuring the high availability of IT services supports business innovation. Respondents were asked what is most critical to supporting business innovation. Forty-seven percent of respondents say it is ensuring high availability of IT services and 43 percent of respondents say it is recruiting and retaining qualified personnel. Another important step, according to 39 percent of respondents, is to reduce security complexity by integrating disparate security technologies.

Business innovation is dependent upon IT's agility in supporting frequent shifts in strategy. Fifty-three percent of respondents say it is very difficult to support business goals and transformation. To support innovation the most important digital assets to secure are source code (44 percent of respondents), custom data (44 percent of respondents), contracts and legal documents (42 percent of respondents) and intellectual property (42 percent of respondents).

The importance of proving the business value of technology investments

Only 43 percent of respondents say their organizations are very or highly confident in the ability to measure the ROI of investments related to securing and managing information assets. The biggest challenge in demonstrating ROI for information management and security technologies is the inability to track downstream business impacts (52 percent of respondents).

The ROI of downstream business impacts involves understanding the indirect benefits and costs that ripple outwards from an initiative, activity or technology investment. Examples to measure include reduced errors and rework, increased efficiency and productivity and reduced compliance risks. Other challenges are the difficulty in quantifying intangible benefits (51 percent of respondents) and competing priorities (47 percent of respondents).

Organizations are eager to see the ROI from security technologies. Calculating ROI is important to proving the business value of IT security investments. It is helpful in making informed decisions about IT security strategies and investments, evaluating performance and calculating profitability. ROI from investments is expected to be shown within six months to one year according to 55 percent of respondents. Forty-five percent of respondents say the timeline is one year to two years (21 percent) or no required timeframe (24 percent).

Security strategies and technology investments should address the risks of ransomware and malicious insiders. Fifty-three percent of respondents say their organizations had a data

breach or cybersecurity incident in the past two years. The average number of incidents was three. During this time, only 28 percent of respondents say cybersecurity incidents have decreased (18 percent) or decreased significantly (10 percent). Ransomware and malicious insiders are the most likely cyberattacks, according to 40 percent and 37 percent of respondents, respectively. The data most vulnerable to insider risks are customer or client data (58 percent of respondents), financial records (46 percent of respondents) and source code (43 percent of respondents).

Malicious insiders pose a significant risk to data security. Encryption for data in transit (39 percent of respondents), email data loss prevention (35 percent of respondents), and encryption for data at rest (35 percent of respondents) are primarily used to reduce the risk of negligent and malicious insiders.

Organizations find it difficult to reduce insider or malicious data loss incidents without jeopardizing trust. Fifty-one percent of respondents say their organizations are effective or very effective in their ability to monitor insider activity across hybrid and/or remote environments. Only 41 percent of respondents say their organizations are effective or very effective in creating trust while taking steps to reduce data loss incidents caused by negligent or malicious insiders.

Reducing complexity in organizations' IT security architecture is needed to have a strong security posture. Seventy-three percent of respondents say reducing complexity is essential (23 percent), very important (23 percent) and important (27 percent). Complexity increases because of new or emerging cyber threats (52 percent of respondents), the Internet of Things (46 percent of respondents) and the rapid growth of unstructured data (44 percent of respondents).

Accountability for reducing complexity is essential. To reduce complexity the most essential steps are to appoint one person to be accountable (59 percent of respondents), streamline security and data governance policies (56 percent of respondents) and reduce the number of overlapping tools and platforms (55 percent of respondents). On average, organizations have 15 separate cybersecurity technologies

Part 2. Key findings

Sponsored by OpenText, Ponemon Institute surveyed 1,896 senior-level IT and IT security practitioners in North America (509 respondents), the United Kingdom (335 respondents), France (276 respondents), Germany (241 respondents), Australia (198 respondents) and India (337 respondents). Fifty-three percent of these respondents are C-level executives in IT and IT security.

In this section of the report, we provide a deeper dive into the global findings from the research. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following topics.

- The promises and pitfalls of AI
- Balancing the importance of securing data and supporting business goals
- Measuring the value of information and security technologies
- The management of cybersecurity and insider risks
- The risks of security complexity
- Country and regional differences

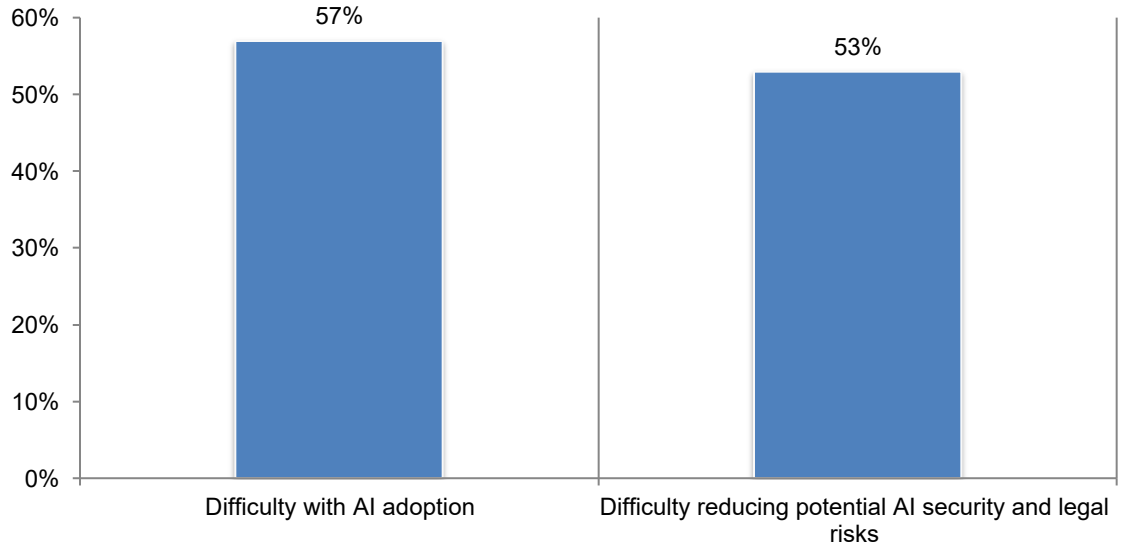
The promises and pitfalls of AI

The following findings in this section are based on the 50 percent of respondents in organizations that have adopted AI.

Organizations recognize the need to make AI part of their security strategy, but difficulties in adoption exist. Fifty percent of respondents say their organizations have adopted AI as part of their IT and overall business strategy. Nineteen percent of respondents say their organizations plan to adopt AI in the next six months.

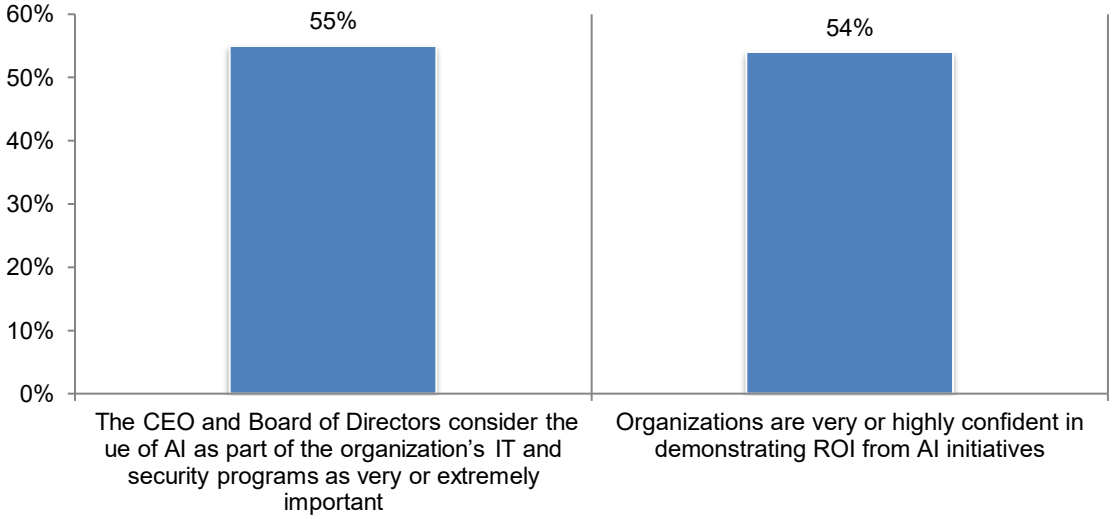
Respondents in organizations that have adopted AI were asked to rate the difficulty in adoption and the ability to reduce potential AI security and legal risks on a scale of 1 = not difficult to 10 = extremely difficult. According to Figure 2, 57 percent of respondents rate the adoption of AI as very difficult to extremely difficult and 53 percent of respondents say it is very difficult or extremely difficult to reduce potential AI security and legal risks.

Figure 2. AI deployment is difficult but a priority
On a scale from 1 = not difficult to 10 = extremely difficult, 7+ responses presented



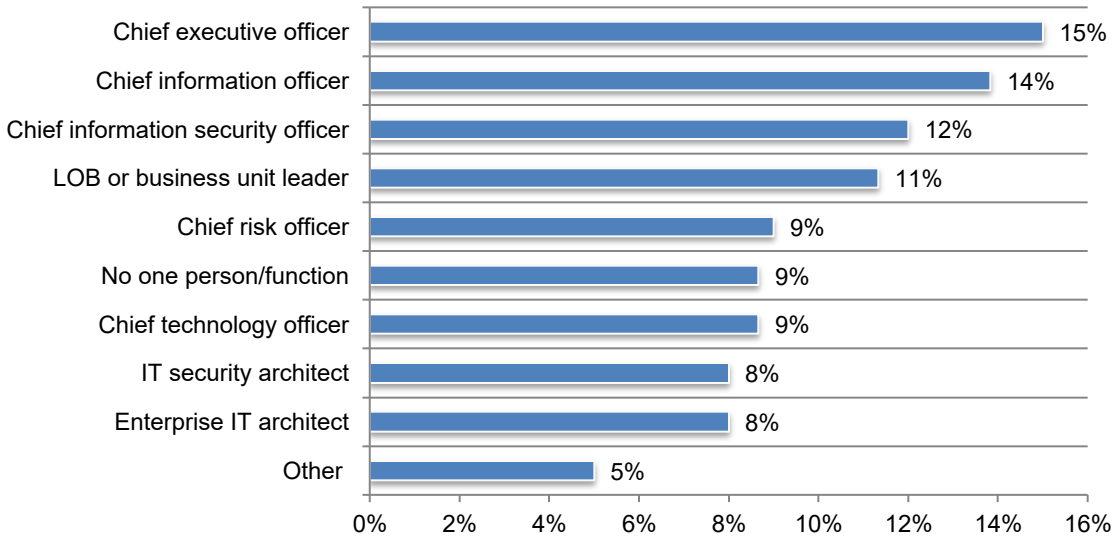
AI deployment has the support of senior leaders. Compared to other IT initiatives, 57 percent of respondents say AI initiatives have a high or very high priority. As shown in Figure 3, 55 percent of respondents say their CEOs and Boards of Directors consider the use of AI as part of their IT and security programs as very or extremely important. A possible reason for such support is that 54 percent of respondents are confident or very confident of their organizations' ability to demonstrate ROI from AI initiatives.

Figure 3. Leadership's perception of AI's importance and confidence in demonstrating ROI from AI initiatives
On a scale from 1 = not important/confident to 10 = extremely important/confident, 7+ responses presented



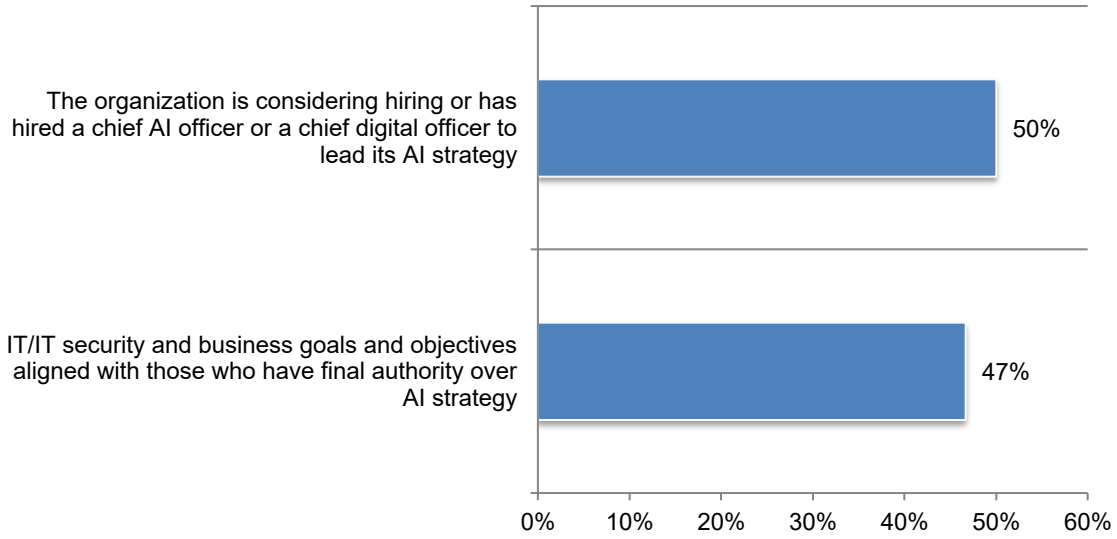
CEOs, CIOs and CISOs are most likely to have authority for setting AI strategy. Figure 4 lists the functions that could be most responsible for AI. As shown, 15 percent of CEOs, 14 percent of CIOs and 12 percent of CISOs have final authority for such AI initiatives as technology investment decisions and the priorities and timelines for deployment.

Figure 4. Who is the final authority for setting your organization's AI strategy?



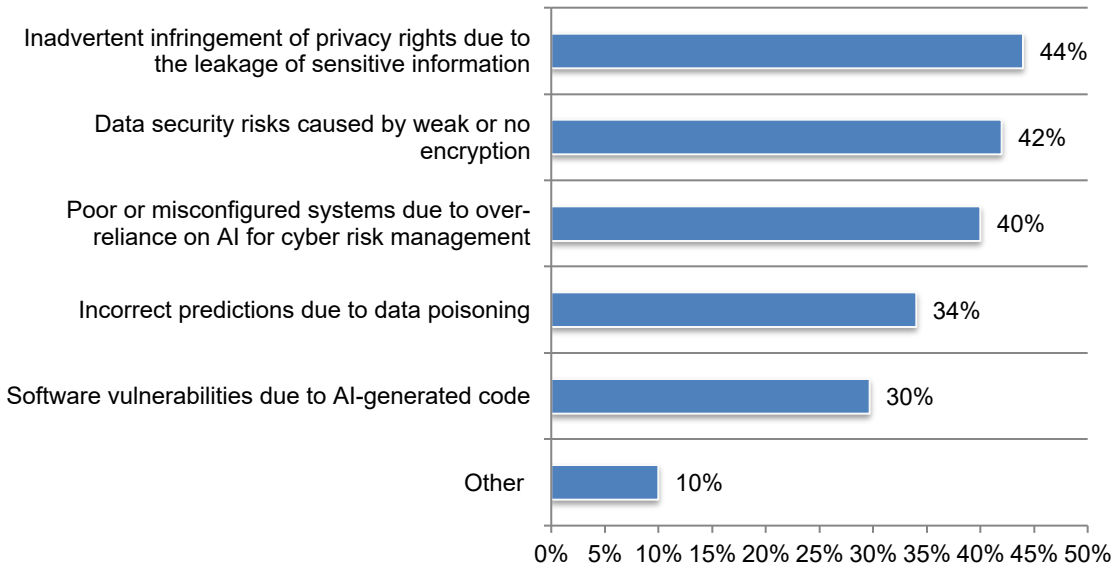
Despite leadership's support for AI, IT/IT security and business goals may not be in alignment. According to Figure 5, less than half (47 percent of respondents) say IT/IT security and business goals are in alignment with those who are responsible for AI initiatives. Fifty percent of respondents say their organizations have hired or are considering hiring a chief AI officer or a chief digital officer to lead AI strategy. Such an appointment of someone dedicated to managing the organization's AI strategy may help bridge gaps between the goals and objectives of IT/IT security with those who have final authority over AI strategy.

Figure 5. The lack of alignment between IT/IT security and business goals and objectives for AI strategy
Yes responses presented



Concerns about privacy can cause delays in AI adoption. The inadvertent infringement of privacy rights is considered the top risk caused by AI. According to Figure 6, 44 percent of respondents say their biggest concern is making sure risks to privacy are mitigated. Other concerns are weak or no encryption (42 percent of respondents) and poor or misconfigured systems due to over-reliance on AI for cyber risk management.

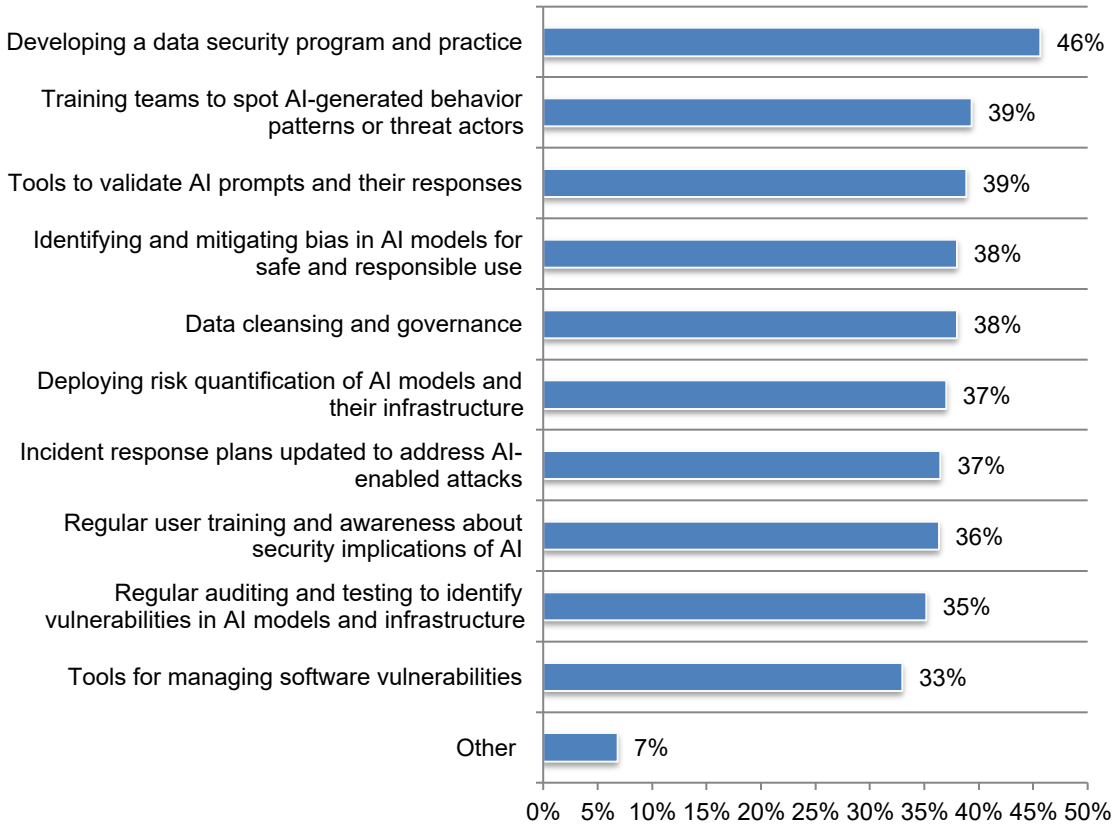
Figure 6. What risks caused by AI concern your organization the most?
Two responses permitted



Developing a data security program and practice is considered the most important step to reduce risks from AI. Fifty-three percent of respondents say it is very difficult or extremely difficult to reduce potential AI security and legal risks.

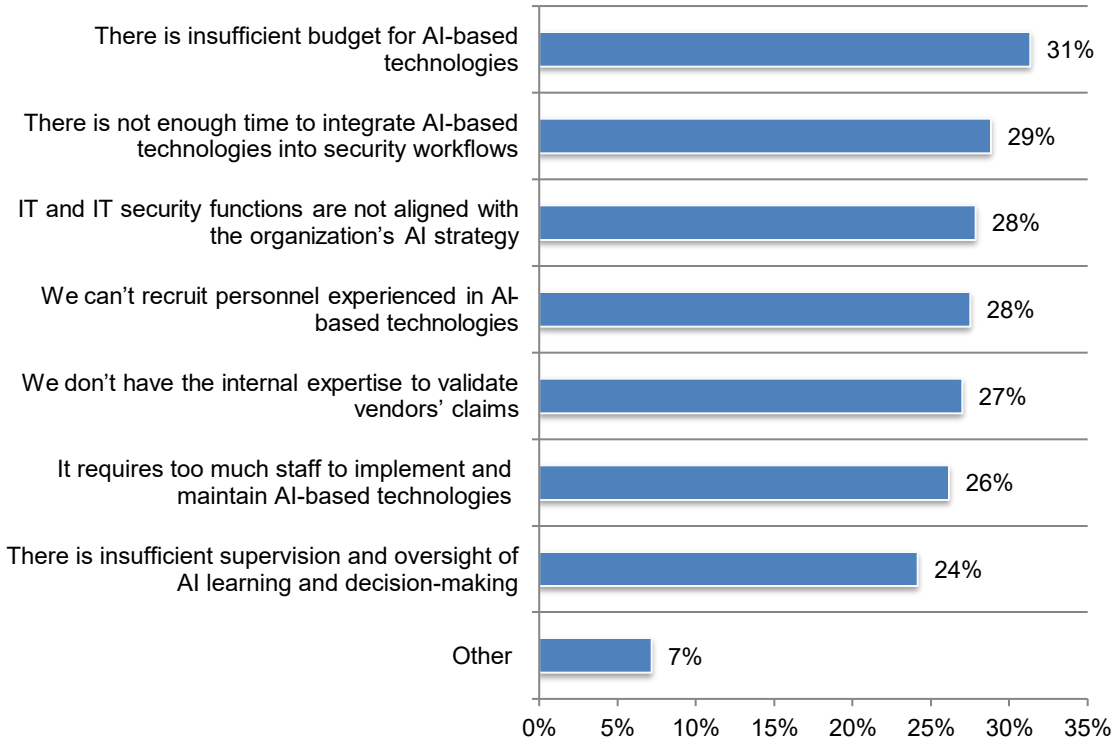
As shown in Figure 7, to address data security risks in AI, 46 percent of respondents say they are developing a data security program and practice. Other steps are using tools to validate AI prompts and their responses (39 percent of respondents), training teams to spot AI-generated behavior patterns or threat actors (39 percent of respondents), using data cleansing and governance (38 percent of respondents) and identifying and mitigating bias in AI models for safe and responsible use (38 percent of respondents).

Figure 7. What steps is your organization taking to reduce risks caused by AI?
More than one response permitted



Despite being a priority, the top governance challenge is insufficient budget for investments in AI technologies. According to Figure 8, 31 percent of respondents say there is insufficient budget for AI-based technologies. This is followed by 29 percent of respondents who say there is not enough time to integrate AI-based technologies into security workflows, 28 percent of respondents who say IT and IT security functions are not aligned with the organization's AI strategy and 28 percent of respondents say their organizations can't recruit personnel experienced in AI-based technologies.

Figure 8. What are the top two organizational or governance challenges to successfully deploying AI-based security technologies within your organization?
Two responses permitted



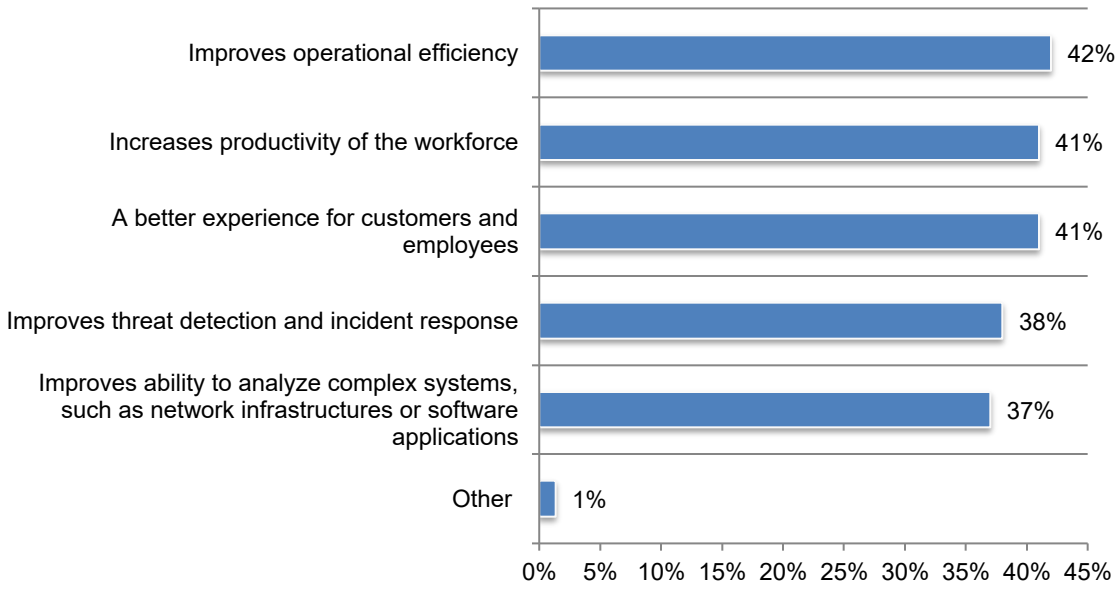
The next phase of AI: adoption of GenAI and Agentic AI.

Generative artificial intelligence refers to a category of AI algorithms that generates new outputs based on the large language models they have been trained on. This is unlike ML systems that are designed to recognize patterns and make predictions. Recent advancements in generative AI, compared to the standard neural network-based generative AI associated with large language models, further advances threat detection and response capabilities. Dynamic-based generative AI models are better positioned to analyze complex systems, such as network infrastructures or software applications, to identify vulnerabilities, detect novel threats and mitigate risks.

GenAI is considered very or highly important to organizations' IT and overall business strategy because it improves operational efficiency and worker productivity. Of the 50 percent of organizations that have adopted AI, 32 percent have adopted GenAI as part of their IT or overall business strategy and 26 percent will adopt GenAI in the next six months. Fifty-eight percent of these respondents say GenAI is important to highly important to their organizations' IT and overall business strategy.

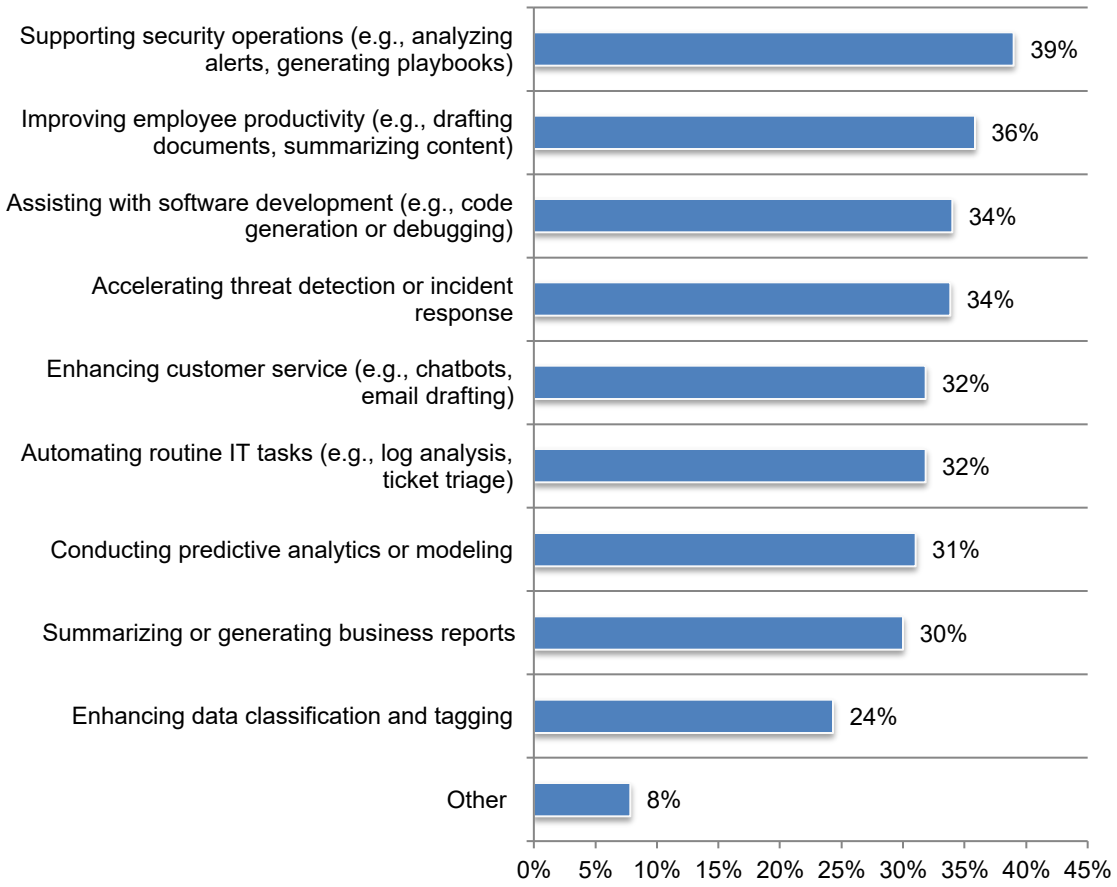
Forty-five percent of respondents say their organizations have realized benefits from GenAI. According to Figure 9 the most significant benefits are improvements in operational efficiency (42 percent of respondents), a better experience for customers and employees (41 percent of respondents) and increases in productivity of the workforce (41 percent of respondents).

Figure 9. What are the most significant benefits from GenAI?
Two responses permitted



GenAI supports security operations and employee productivity. Figure 10 presents the top use cases for GenAI. The most important GenAI use cases are supporting security operations (e.g. analyzing alerts, generating playbooks) (39 percent of respondents), improving employee productivity (e.g. drafting documents, summarizing content) (36 percent of respondents), assisting with software development (e.g. code generation or debugging) (34 percent of respondents) and accelerating threat detection or incident response (34 percent of respondents).

Figure 10. What are the top use cases for GenAI within your organization?
Three responses permitted



Copyright and other legal risks are the biggest challenges to an effective GenAI program. Respondents were asked to identify the biggest challenges to an effective GenAI program. As shown in Figure 11, 43 percent of respondents say copyright and other legal risks, 37 percent of respondents say lack of in-house expertise and 36 percent of respondents say regulatory uncertainty and changes are the biggest challenges to an effective GenAI program.

Figure 11. What are the biggest challenges to an effective GenAI program?
Three responses permitted

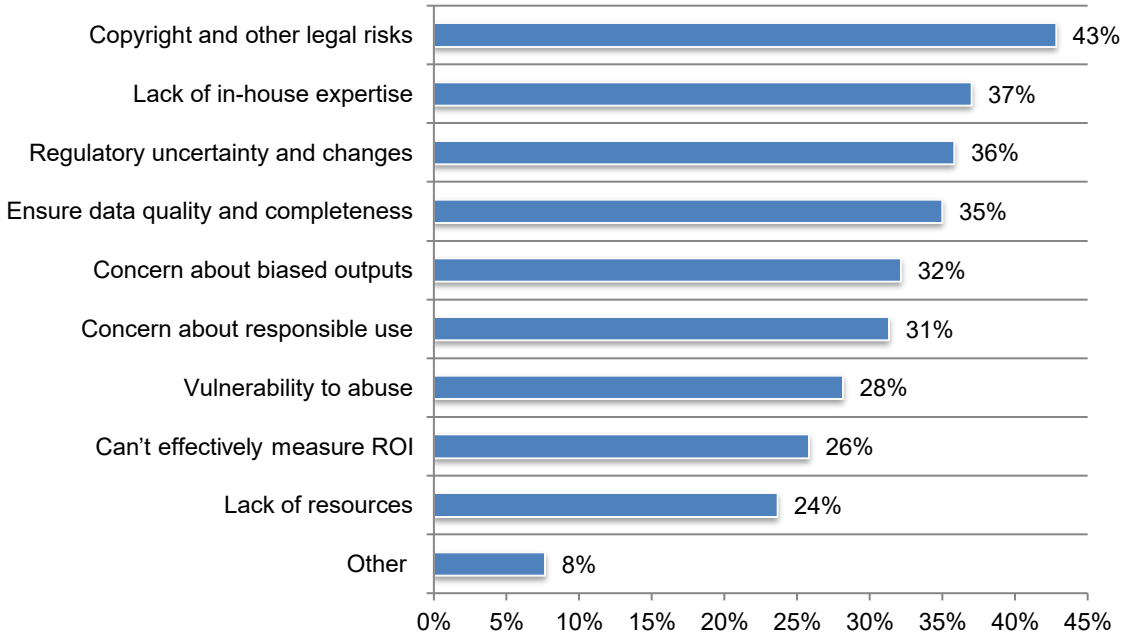


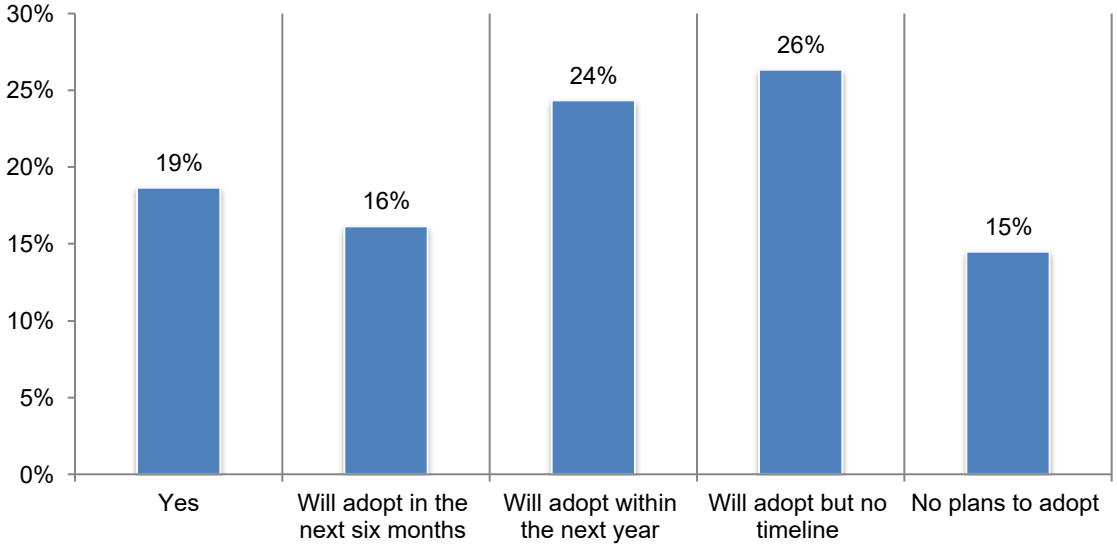
Table 1 highlights the primary uses for GenAI and the most significant barriers to an effective GenAI deployment.

Table 1. Top three use cases and challenges for GenAI adoption	Respondents
Following are the top three use cases	
Supporting security operations (e.g., analyzing alerts, generating playbooks)	39 percent
Improving employee productivity (e.g., drafting documents, summarizing content)	36 percent
Assisting with software development (e.g., code generation of debugging	34 percent
Following are the top three challenges	
Copyright and other legal risks	43 percent
Lack of in-house expertise	37 percent
Regulatory uncertainty and changes	36 percent

Agentic AI refers to a type of artificial intelligence that can autonomously make decisions, take actions, and learn on its own to achieve specific goals. It's characterized by autonomy, the ability to initiate and complete tasks without constant oversight, and reasoning, where sophisticated decision-making is based on context.

Organizations are slow to adopt Agentic AI as part of their overall IT and business strategy. While 32 percent of AI organizations have adopted GenAI, only 19 percent of organizations have adopted Agentic AI and 16 percent will adopt in the next six months, as shown in Figure 12. Only 31 percent of the organizations that have adopted Agentic AI say it is very or extremely important to their organizations' IT and business strategy.

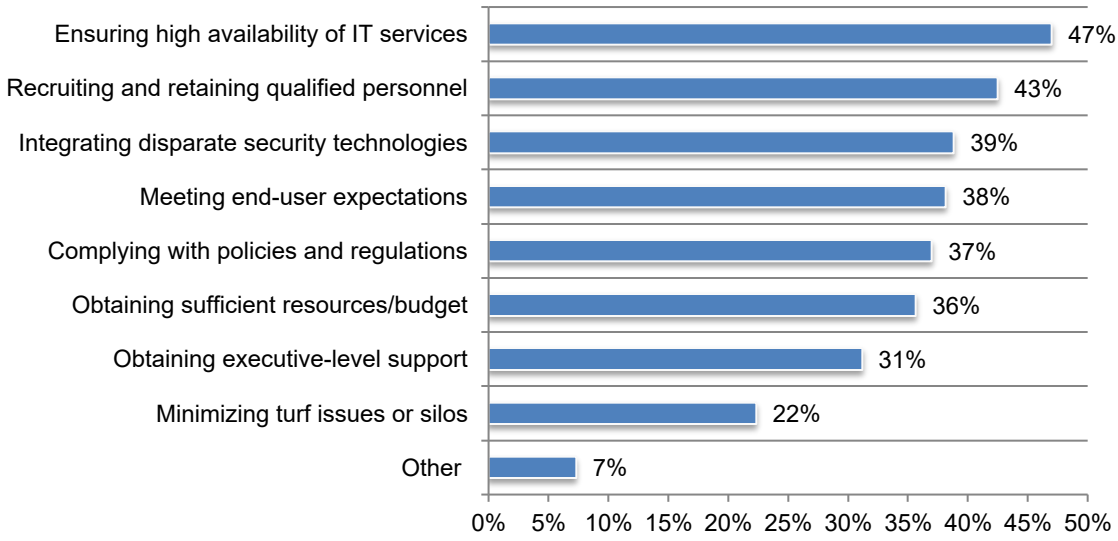
Figure 12. Has your organization adopted Agentic AI?



Balancing the importance of securing data and supporting business goals and innovation

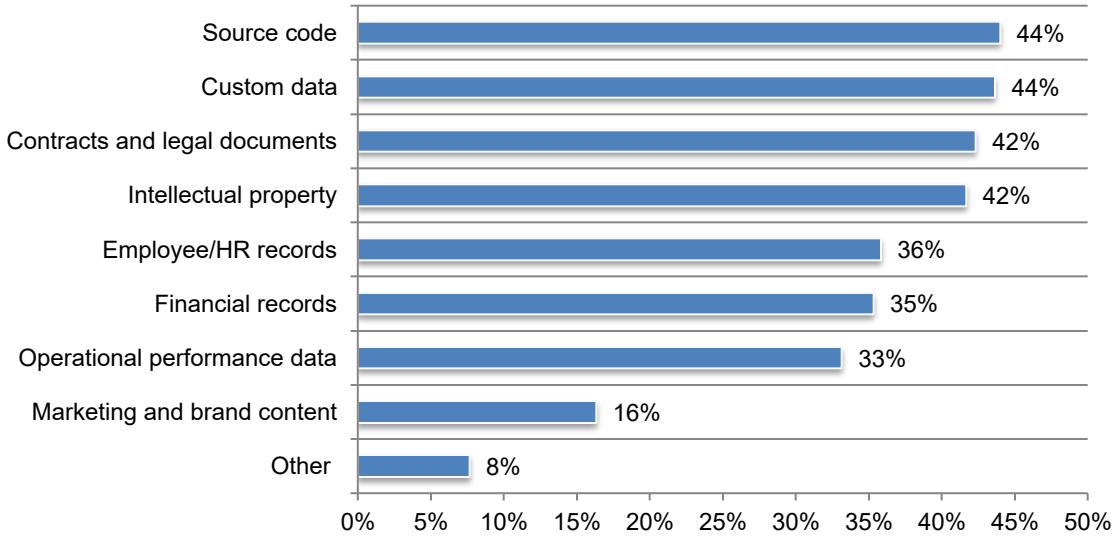
Ensuring the high availability of IT services supports business innovation. Respondents were asked what is most critical to supporting business innovation. As shown in Figure 13, 47 percent of respondents say it is ensuring high availability of IT services and 43 percent of respondents say it is recruiting and retaining qualified personnel. Another important step, according to 39 percent of respondents, is to reduce security complexity by integrating disparate security technologies.

Figure 13. What are the most important IT responsibilities critical to supporting business innovation?



As shown in Figure 14, to support innovation the most important digital assets to secure are source code (44 percent of respondents), custom data (44 percent of respondents), contracts and legal documents (42 percent of respondents) and intellectual property (42 percent of respondents).

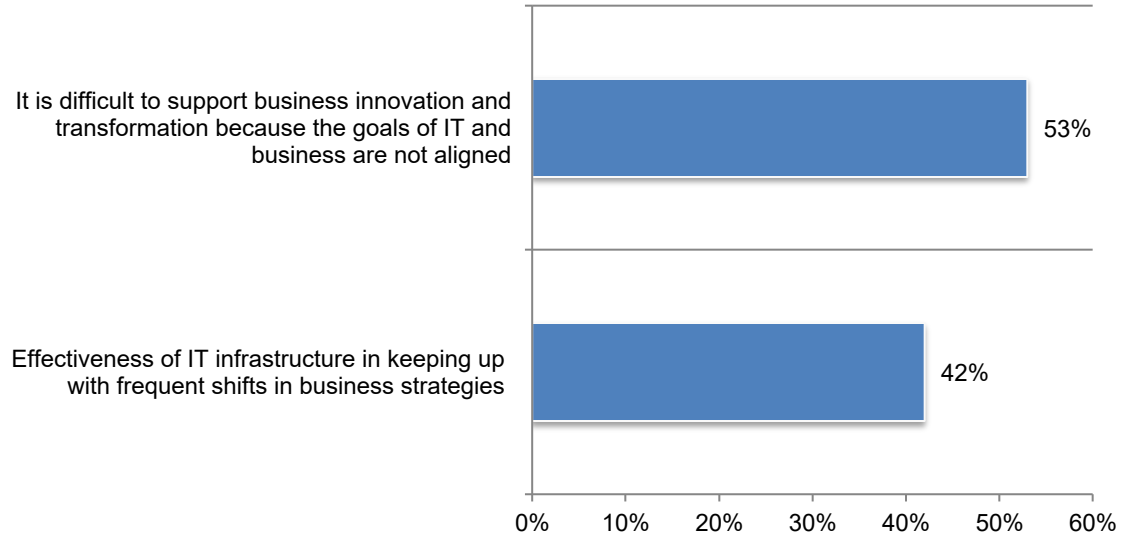
Figure 14. Which types of digital assets are most important to secure and manage in your organization?
Three responses permitted



Measuring the value of information and security technologies

Business innovation is dependent upon IT's agility in supporting frequent shifts in strategy. As shown in Figure 15, respondents were asked to rate how effective IT is in keeping up with frequent shifts in business strategies on a scale of 1 = not effective to 10 = highly effective Only 42 percent of respondents say their organizations are very or highly effective in keeping up with frequent shifts in business strategies. Fifty-three percent of respondents say it is very difficult to support business innovation because the goals of IT and business are not aligned.

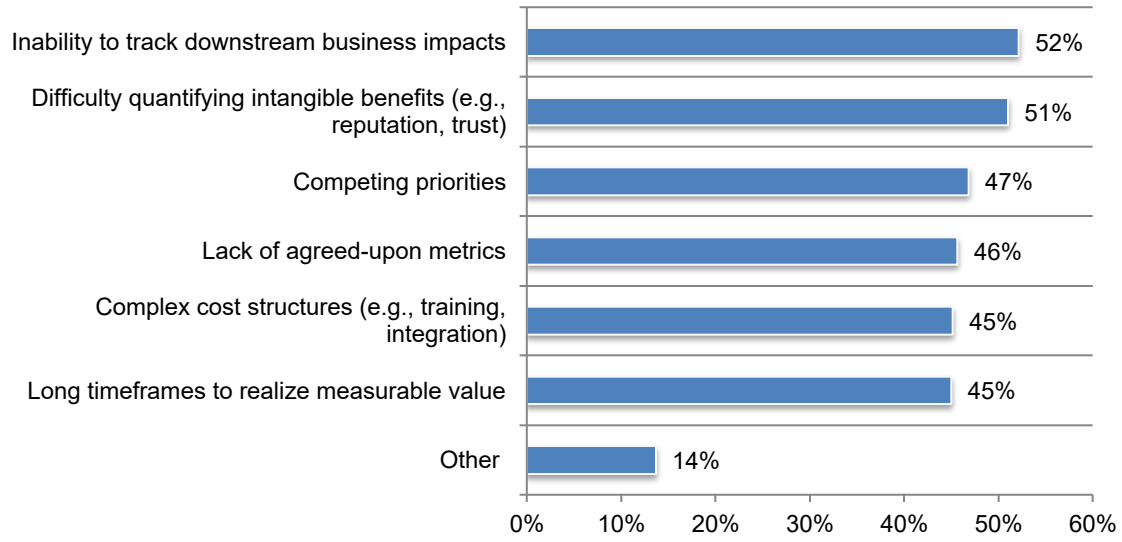
Figure 15. Can IT keep up with frequent shifts in business strategies and is it able to measure the ROI of security investments
On a scale from 1 = not effective/strongly disagree to 10 = extremely effective/strongly agree, 7+ responses presented



Only 43 percent of respondents say their organizations are very or highly confident in the ability to measure the ROI of investments related to securing and managing information assets. The biggest challenge in demonstrating ROI for information management and security technologies is the inability to track downstream business impacts (52 percent of respondents), as shown in Figure 16.

The ROI of downstream business impacts involves understanding the indirect benefits and costs that ripple outwards from an initiative, activity or technology investment. Examples to measure include reduced errors and rework, increased efficiency and productivity and reduced compliance risks. Other challenges are the difficulty in quantifying intangible benefits (51 percent of respondents) and competing priorities (47 percent of respondents).

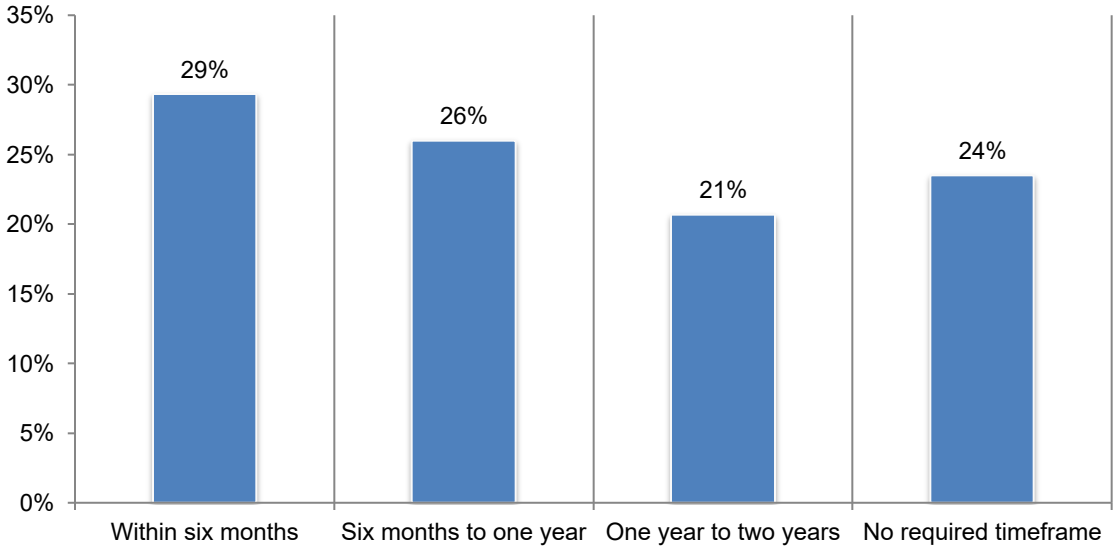
Figure 16. What are the most significant challenges in demonstrating ROI from information management and security challenges?
Three responses permitted



Organizations are eager to see the ROI from security technologies. Calculating ROI is important to proving the business value of IT security investments. It is helpful in making informed decisions about IT security strategies and investments, evaluating performance and calculating profitability.

According to Figure 17, ROI from investments is expected to be shown within six months to one year according to 55 percent of respondents. Forty-five percent of respondents say the timeline is one year to two years (21 percent) or no required timeframe (24 percent).

Figure 17. In what timeframe does your organization require ROI from investments

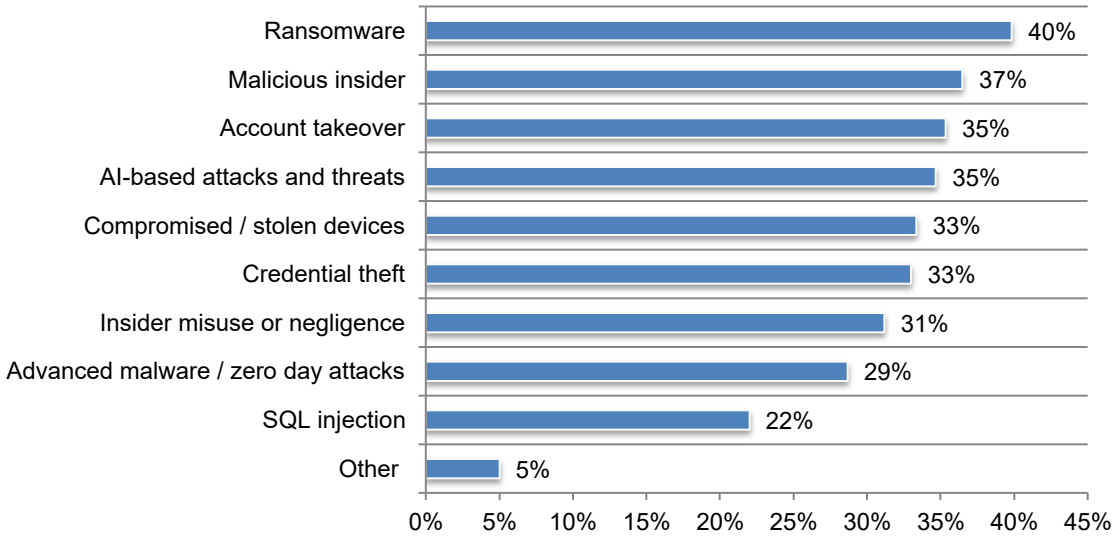


The management of cybersecurity and insider risks

Security strategies and technology investments should address the risks of ransomware and malicious insiders. Fifty-three percent of respondents say their organizations had a data breach or cybersecurity incident in the past two years. The average number of incidents was three. During this time, only 28 percent of respondents say cybersecurity incidents have decreased (18 percent) or decreased significantly (10 percent).

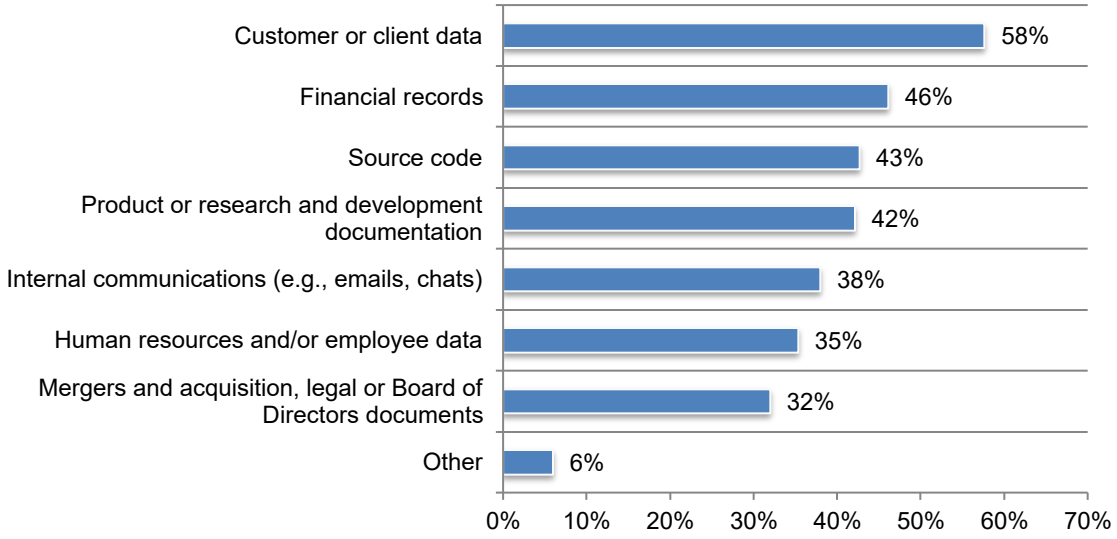
As shown in Figure 18, ransomware and malicious insiders are the most likely cyberattacks, according to 40 percent and 37 percent of respondents, respectively.

Figure 18. Which of the following cyberattacks are most likely to hinder your organization's ability to manage and protect information?
Three responses permitted



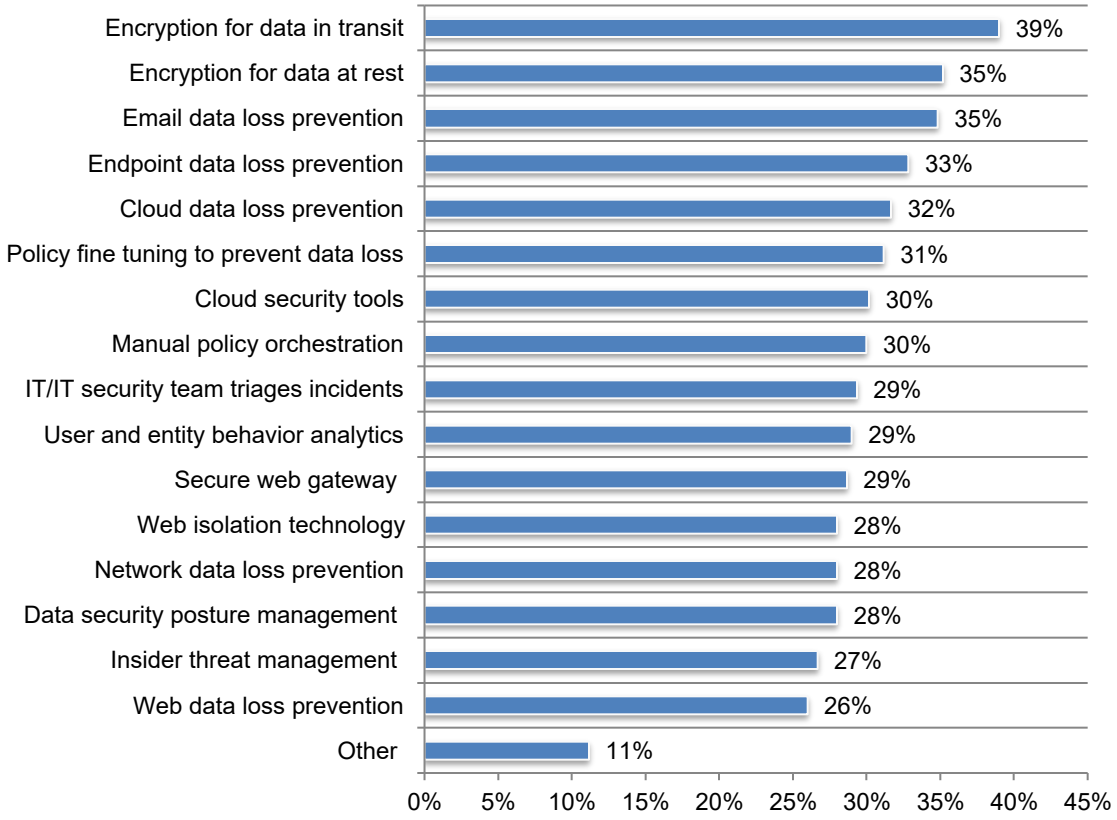
The data most vulnerable to insider risks are customer or client data (58 percent of respondents), financial records (46 percent of respondents) and source code (43 percent of respondents), according to Figure 19.

Figure 19. Which types of content or data are most vulnerable to insider threats?
Three responses permitted



Malicious insiders pose a significant risk to data security. Figure 20 lists the top technologies used to prevent data loss caused by negligent and malicious insiders. Encryption for data in transit (39 percent of respondents), email data loss prevention (35 percent of respondents), and encryption for data at rest (35 percent of respondents) are primarily used to reduce the risk of negligent and malicious insiders.

Figure 20. What security methods and technologies have been implemented to prevent data loss caused by negligent and malicious insiders?
Five responses permitted

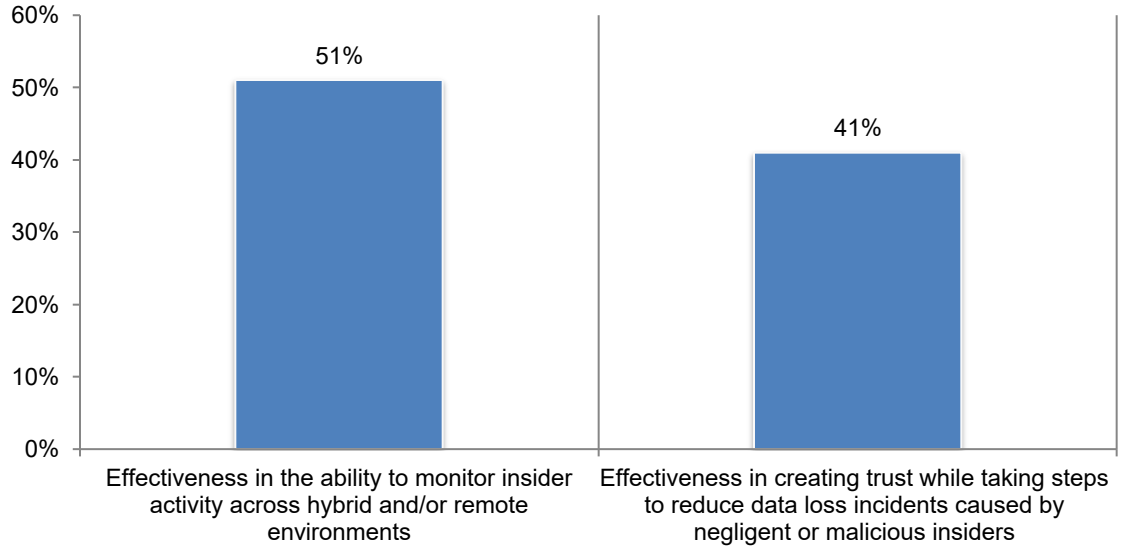


Organizations find it difficult to reduce insider or malicious data loss incidents without jeopardizing trust. Respondents were asked to rate their organizations' effectiveness in monitoring insider activity across hybrid and/or remote environments and in creating trust while taking steps to reduce data loss incidents caused by negligent or malicious insiders on a scale from 1 = not effective to 10 = highly effective.

Figure 21 shows the highly effective respondents (7+ on the 10-point scale). As shown, 51 percent of respondents say their organizations are effective or very effective in their ability to monitor insider activity across hybrid and/or remote environments. Only 41 percent of respondents say their organizations are effective or very effective in creating trust while taking steps to reduce data loss incidents caused by negligent or malicious insiders.

Figure 21. Effectiveness in reducing data loss incidents from negligent or malicious insiders

On a scale from 1 = not effective to 10 = extremely effective, 7+ responses presented

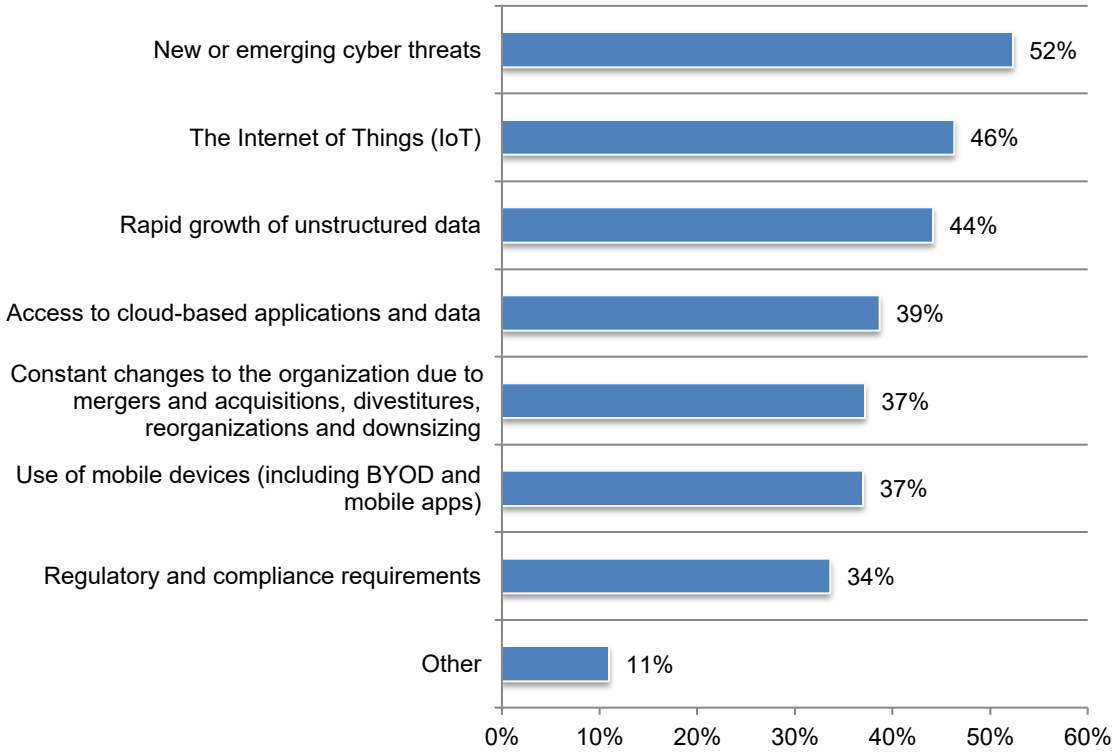


The risk of security complexity

Reducing complexity in organizations' IT security architecture is needed to have a strong security posture. Seventy-three percent of respondents say reducing complexity is essential (23 percent), very important (23 percent) and important (27 percent).

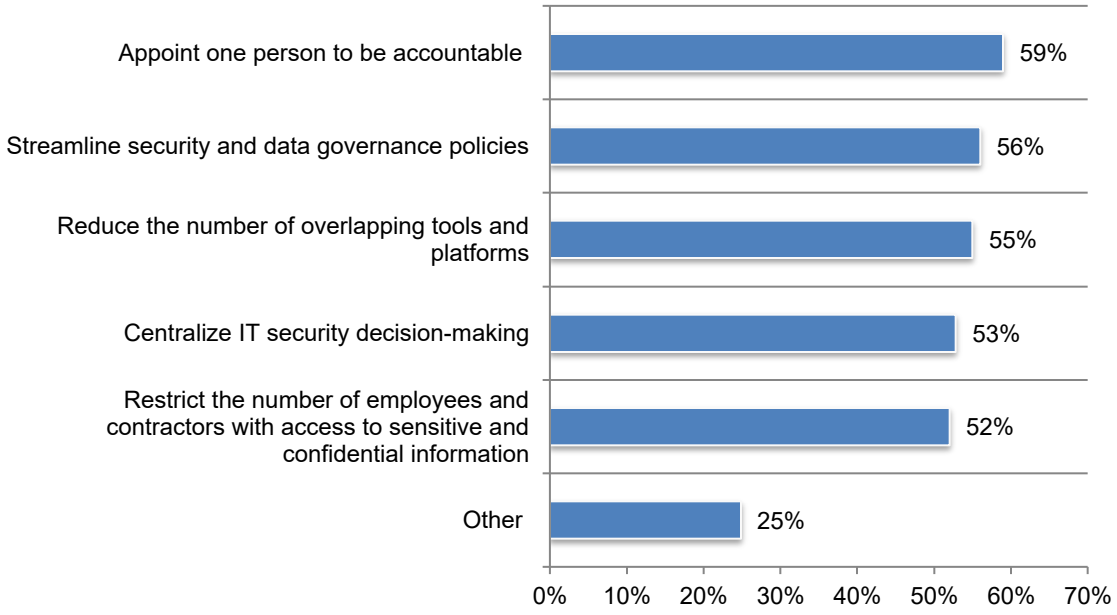
According to Figure 22, complexity increases because of new or emerging cyber threats (52 percent of respondents), the Internet of Things (46 percent of respondents) and the rapid growth of unstructured data (44 percent of respondents).

Figure 22. What increases security complexity?
Three responses permitted



Accountability for reducing complexity is essential. As shown in Figure 23, to reduce complexity the most essential steps are to appoint one person to be accountable (59 percent of respondents), streamline security and data governance policies (56 percent of respondents) and reduce the number of overlapping tools and platforms (55 percent of respondents). On average, organizations have 15 separate cybersecurity technologies

Figure 23. What steps are taken to reduce complexity?



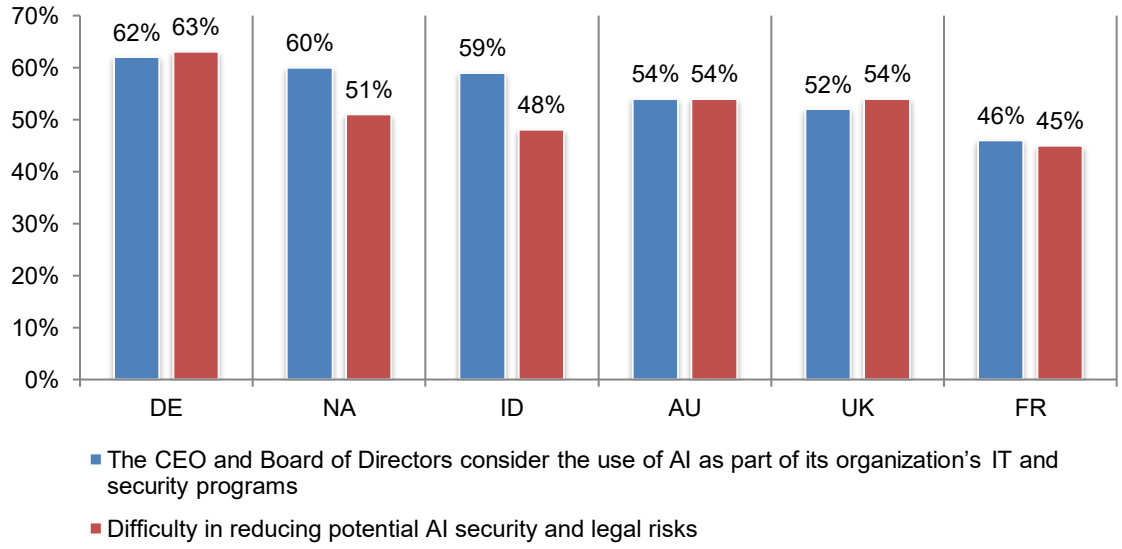
Country differences

In this section, we provide an analysis of the differences among the six countries represented in this research: North America, United Kingdom, France, Germany, Australia and India.

Countries differ in the support for AI from CEOs and Boards of Directors. Respondents were asked to rate the importance of AI and the difficulty in reducing AI security and legal risks on a scale from 1 = not important/difficult to 10 = extremely important/difficult.

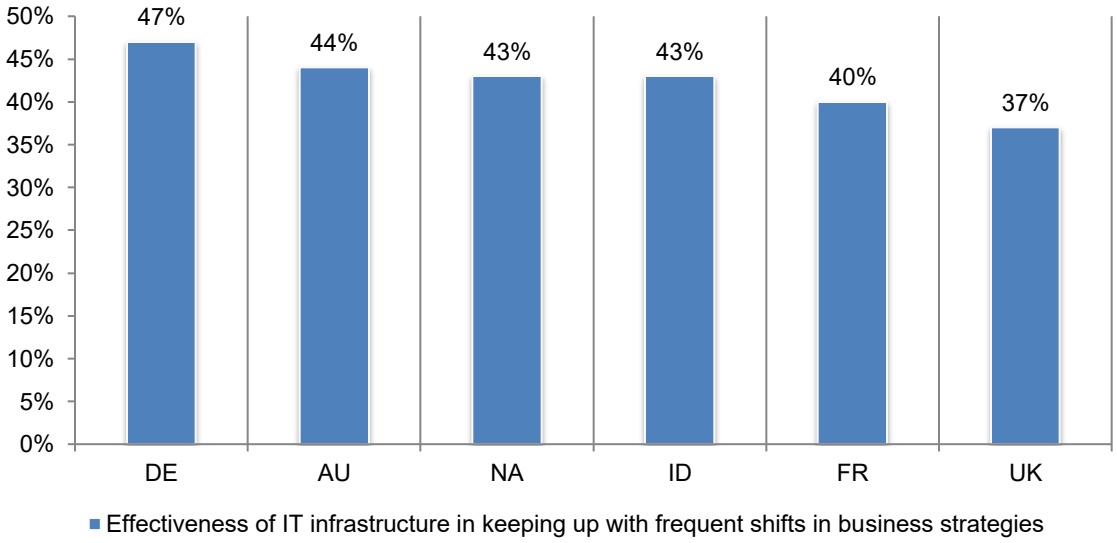
Figure 24 presents the 7+ responses on the 10-point scale. As shown, senior leadership in Germany, North America and India are more likely to believe the use of AI in security strategies is very or extremely important (62 percent, 60 percent and 59 percent of respondents respectively). France, India and North America (45 percent, 48 percent and 51 percent of respondents respectively) are least likely to say reducing potential AI security and legal risks is very or extremely difficult.

Figure 24. AI deployment challenges
On a scale from 1 = not important/difficult to 10 = extremely important/difficult, 7+ responses presented



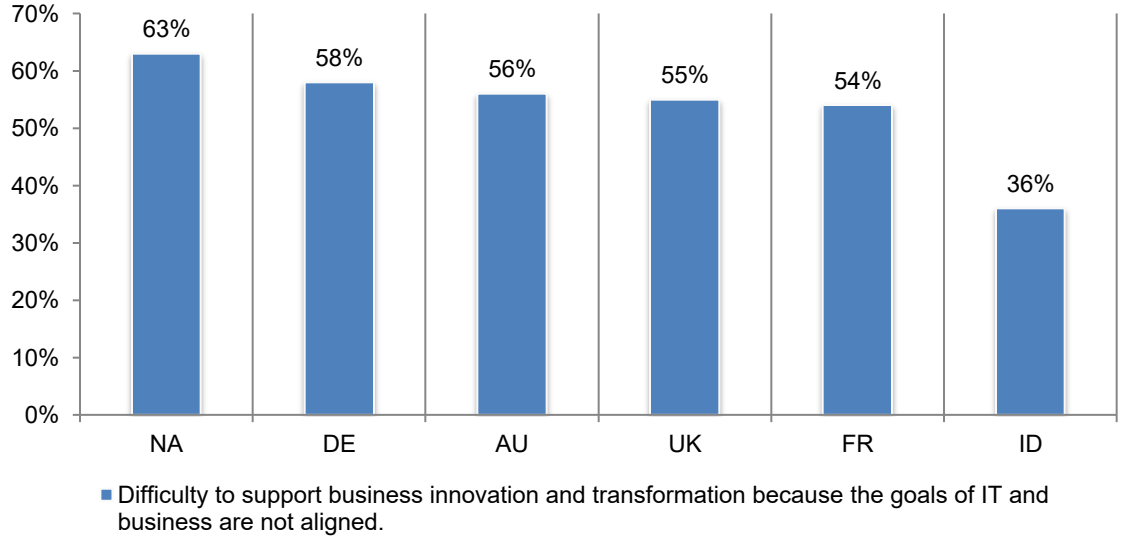
The IT infrastructures in German and Australian organizations are the most agile in responding to frequent shifts in business strategies. Figure 25 presents the very and extremely effective responses. As shown, 47 percent and 44 percent of German and Australia respondents, respectively report their IT infrastructures are very or extremely effective in keeping up with frequent shifts in business strategies. Least agile IT infrastructures are in the United Kingdom (37 percent of respondents) and France (40 percent of respondents).

Figure 25. How effective is IT infrastructure is in keeping up with frequent shifts in business strategies?
On a scale from 1 = not effective to 10 = extremely effective, 7+ responses presented



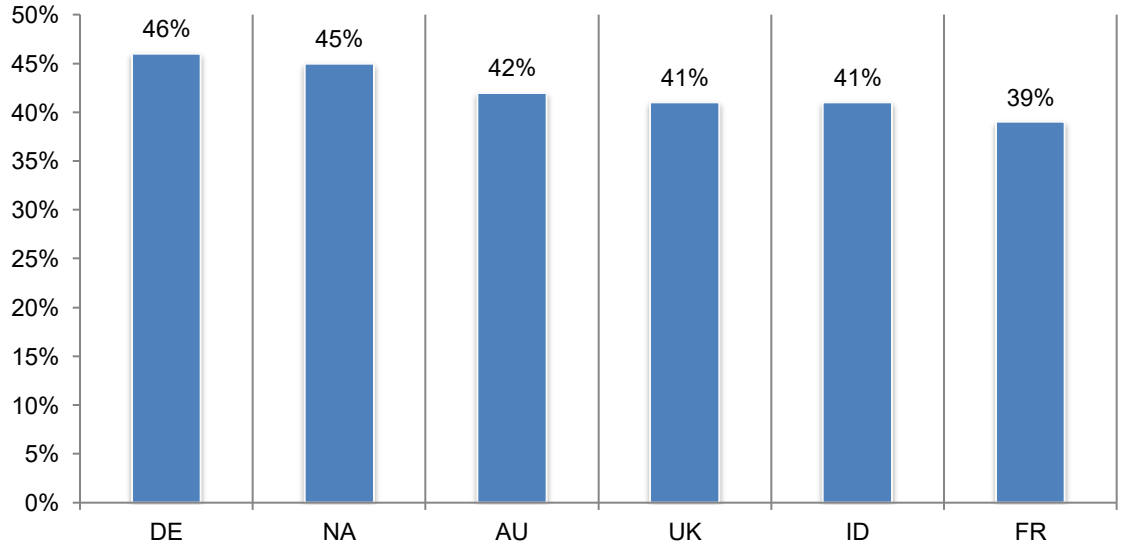
North American and German organizations are most likely to have difficulty in achieving the alignment between the goals of IT and business to support business innovation. As shown in Figure 26, 63 percent of respondents in North America and 58 percent of respondents say it is difficult to achieve alignment. In contrast, only 36 percent of organizations in India say alignment is difficult.

Figure 26. How difficult is it to support business innovation and transformation because the goals of IT and business are not aligned?
Strongly agree & Agree combined



IT and IT security organizations in Germany and North America are most confident in the ability to measure the ROI of technology investments. Figure 27 presents the very confident and extremely confident responses. As shown, 46 percent of respondents in Germany and 45 percent of respondents in North America are very or extremely confident in the calculation of ROI.

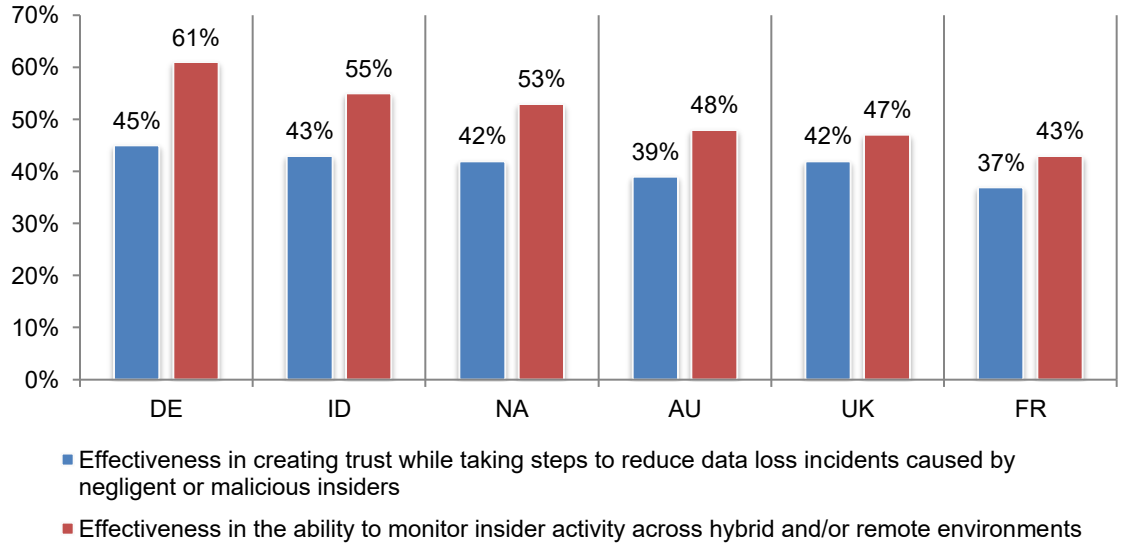
Figure 27. How confident is your organization in its ability to measure the ROI of investments?
On a scale from 1 = not confident to 10 = extremely confident, 7+ responses presented



Organizations in all countries struggle with effectively creating trust while taking steps to reduce data loss incidents. Respondents were asked to rate their organizations' effectiveness in creating trust while taking steps to reduce data loss incidents caused by negligent or malicious insiders and the ability to monitor insider activity across hybrid and/or remote environments on a scale of 1 = not effective to 10 = extremely effective.

Figure 28 shows the 7+ responses. Only 37 percent of respondents in France and 39 percent of respondents in Australia rate their ability to create trust while taking steps to reduce data loss incidents caused by negligent or malicious insiders as very or extremely effective. Germany and India are most effective in the ability to monitor insider activity across hybrid and/or remote environments.

Figure 28. Effectiveness in creating trust and monitoring insider activity to reduce data loss incidents caused by negligent or malicious insiders
On a scale from 1 = not effective to 10 = extremely effective, 7+ responses presented



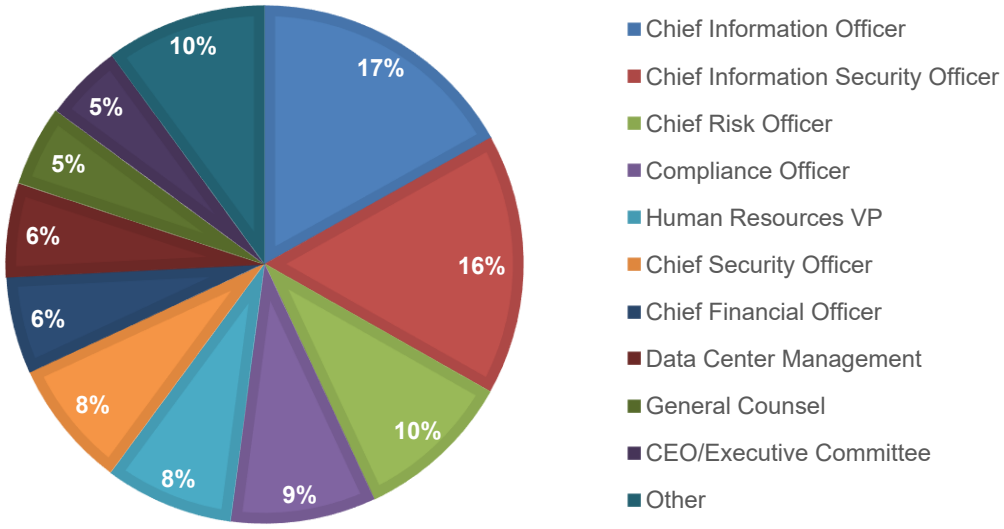
Part 3. Methodology

A sampling frame of 55,126 senior-level IT and IT security practitioners in North America (509 respondents), the United Kingdom (335 respondents), France (276 respondents), Germany (241 respondents), Australia (198 respondents) and India (337 respondents) were selected as participants to this survey. Table 1 shows 2,131 total returns. Screening and reliability checks required the removal of 397 surveys. Our final sample consisted of 1,896 surveys or a 3.4 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	55,126	100.0%
Total returns	2,131	3.9%
Rejected or screened surveys	397	0.7%
Final sample	1,896	3.4%

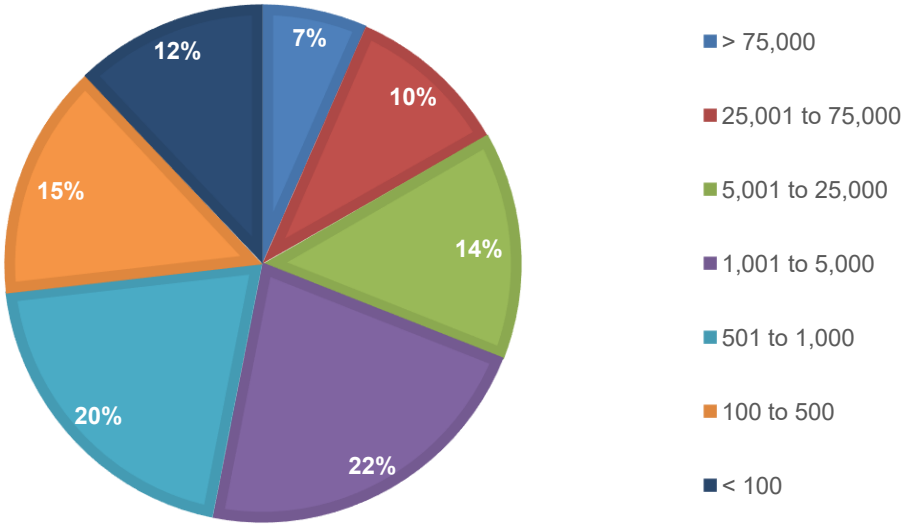
As shown in Pie chart 1, 17 percent of respondents report to the chief information officer, 16 percent of respondents report to the chief information security, 10 percent of respondents report to the chief risk officer, and 9 percent of respondents report to the compliance officer.

Pie chart 1. Direct reporting channel



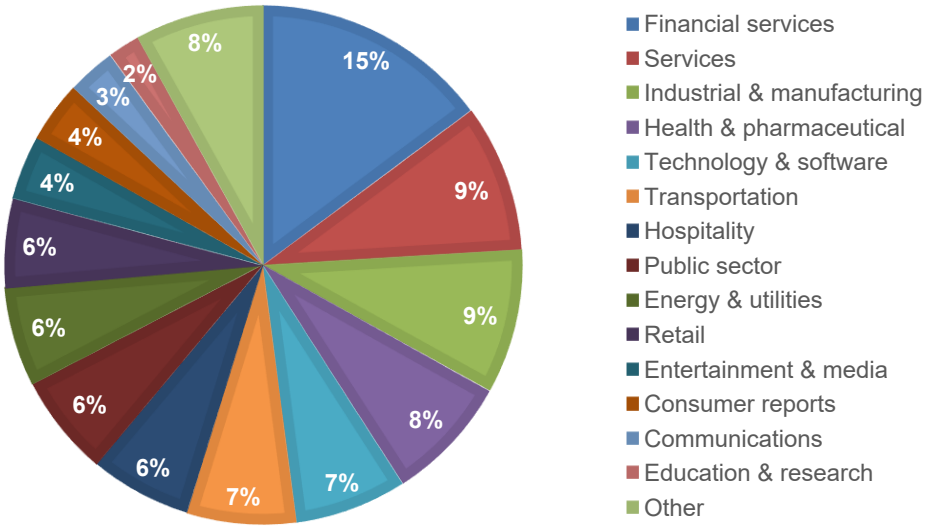
As shown in Pie chart 2, more than half (53 percent) of respondents are from organizations with a headcount of more than 1,000 employees

Pie chart 2. Worldwide headcount



Pie chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (15 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (9 percent of respondents), industrial and manufacturing (9 percent of respondents),health and pharmaceuticals (8 percent of respondents), technology and software (7 percent of respondents) and transportation (7 percent of respondents).

Pie chart 3. Primary industry classification



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are 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 and 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.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in May 2025.

Survey Response	NA	UK	FR	DE	AU	ID	Global
Total sampling frame	15,135	9,079	7,633	7,993	5,657	9,629	55,126
Total survey returns	577	401	276	241	198	438	2,131
Rejected surveys	84	58	83	69	43	60	397
Final sample	509	335	276	241	198	337	1,896
Response ratio	3.36%	3.69%	3.62%	3.02%	3.50%	3.50%	3.44%

S1. What best describes your organizational role or area of focus? Please select one choice only.	NA	UK	FR	DE	AU	ID	Global
CIO	17%	15%	16%	15%	13%	15%	15%
Cybersecurity C-level executive	9%	11%	10%	13%	10%	15%	11%
Cybersecurity VP	21%	19%	18%	15%	15%	13%	17%
Cybersecurity director/manager	16%	17%	20%	15%	16%	15%	17%
IT C-level executive	7%	8%	7%	16%	14%	8%	10%
IT VP	10%	13%	13%	10%	16%	15%	13%
IT director/manager	14%	12%	12%	10%	13%	16%	13%
None of the above (stop)	6%	5%	4%	6%	3%	3%	4%
Total	100%	100%	100%	100%	100%	100%	100%

Part 1. Artificial intelligence (AI) strategies and adoption

Q1. Has your organization adopted AI as part of its IT and overall business strategy?	NA	UK	FR	DE	AU	ID	Global
Yes	50%	45%	52%	54%	51%	48%	50%
Will adopt in the next six months (please skip to Q20)	23%	21%	19%	17%	15%	16%	19%
Will adopt within the next year (please skip to Q20)	12%	10%	9%	8%	11%	11%	10%
Will adopt but no timeline (please skip to Q20)	5%	12%	8%	10%	14%	17%	11%
No plans to adopt (please skip to Q20)	10%	12%	12%	11%	9%	8%	10%
Total	100%	100%	100%	100%	100%	100%	100%

Q2. Using the following 10-point scale, please rate the priority of AI initiatives compared to the priority of other IT initiatives from 1 = not a priority to 10 = Very high priority.	NA	UK	FR	DE	AU	ID	Global
1 or 2	13%	9%	15%	7%	14%	16%	12%
3 or 4	12%	13%	15%	11%	15%	19%	14%
5 or 6	16%	17%	18%	15%	19%	13%	17%
7 or 8	26%	36%	31%	34%	27%	26%	30%
9 or10	33%	25%	21%	33%	25%	26%	27%
Total	100%	100%	100%	100%	100%	100%	100%

Q3. Using the following 10-point scale, please rate how difficult AI adoption was from 1 = not difficult to 10 = extremely difficult.	NA	UK	FR	DE	AU	ID	Global
1 or 2	11%	9%	13%	7%	15%	14%	11%
3 or 4	14%	13%	15%	10%	15%	22%	15%
5 or 6	17%	17%	19%	15%	18%	16%	17%
7 or 8	24%	31%	29%	33%	27%	22%	28%
9 or10	34%	30%	24%	35%	25%	26%	29%
Total	100%	100%	100%	100%	100%	100%	100%

Q4. Using the following 10-point scale, please rate how difficult it is to reduce potential AI security and legal risks from 1 = not difficult to 10 = extremely difficult.	NA	UK	FR	DE	AU	ID	Global
1 or 2	12%	11%	14%	11%	16%	16%	13%
3 or 4	15%	14%	19%	13%	13%	21%	16%
5 or 6	22%	21%	22%	13%	17%	15%	18%
7 or 8	22%	26%	25%	33%	29%	21%	26%
9 or10	29%	28%	20%	30%	25%	27%	27%
Total	100%	100%	100%	100%	100%	100%	100%

Q5. Using the following 10-point scale, please rate how important the CEO and Board of Directors consider the use of AI as part of your organization's IT and security programs from 1 = not important to 10 = extremely important.	NA	UK	FR	DE	AU	ID	Global
1 or 2	12%	13%	15%	13%	18%	16%	15%
3 or 4	15%	14%	16%	13%	15%	13%	14%
5 or 6	13%	21%	23%	12%	13%	12%	16%
7 or 8	25%	26%	25%	33%	29%	32%	28%
9 or10	35%	26%	21%	29%	25%	27%	27%
Total	100%	100%	100%	100%	100%	100%	100%

Q6. Who is the final authority for setting your organization's AI strategy? Please select one choice only.	NA	UK	FR	DE	AU	ID	Global
Chief executive officer	14%	13%	15%	16%	15%	14%	15%
Chief information officer	16%	15%	13%	13%	10%	16%	14%
Chief information security officer	12%	11%	10%	13%	16%	12%	12%
Chief risk officer	9%	8%	10%	8%	7%	9%	9%
Chief technology officer	8%	9%	9%	9%	9%	8%	9%
Enterprise IT architect	7%	6%	7%	9%	12%	7%	8%
IT security architect	8%	8%	9%	8%	9%	8%	8%
LOB or business unit leader	12%	12%	11%	11%	10%	12%	11%
No one person/function	9%	9%	8%	9%	8%	9%	9%
Other (please specify)	5%	9%	8%	4%	4%	5%	5%
Total	100%	100%	100%	100%	100%	100%	100%

Q7. Are the IT/IT security and business goals and objectives aligned with those who have final authority over your organization's AI strategy?	NA	UK	FR	DE	AU	ID	Global
Yes	52%	47%	39%	55%	41%	46%	47%
No	40%	46%	50%	40%	51%	46%	45%
Unsure	8%	7%	11%	5%	8%	8%	8%
Total	100%	100%	100%	100%	100%	100%	100%

Q8. Is your organization considering hiring or has hired a chief AI officer or a chief digital officer to lead its AI strategy?	NA	UK	FR	DE	AU	ID	Global
Yes	55%	52%	36%	60%	48%	49%	50%
No	45%	48%	64%	40%	52%	51%	50%
Total	100%	100%	100%	100%	100%	100%	100%

Q9. Using the following 10-point scale, please rate how confident your organization is in demonstrating ROI from AI initiatives from 1 = not confident to 10 = very confident.	NA	UK	FR	DE	AU	ID	Global
1 or 2	12%	11%	17%	13%	9%	18%	13%
3 or 4	16%	14%	12%	14%	18%	17%	15%
5 or 6	11%	21%	25%	17%	20%	14%	18%
7 or 8	30%	24%	25%	29%	28%	29%	28%
9 or10	31%	30%	21%	27%	25%	22%	26%
Total	100%	100%	100%	100%	100%	100%	100%

Q10. What risks caused by AI concern your organization the most? Please select the top 2 concerns.	NA	UK	FR	DE	AU	ID	Global
Data security risks caused by weak or no encryption	38%	50%	45%	38%	41%	39%	42%
Inadvertent infringement of privacy rights due to the leakage of sensitive information	46%	38%	41%	46%	43%	51%	44%
Incorrect predictions due to data poisoning	33%	35%	32%	33%	31%	37%	34%
Poor or misconfigured systems due to over-reliance on AI for cyber risk management	42%	34%	45%	42%	39%	36%	40%
Software vulnerabilities due to AI-generated code	31%	29%	27%	31%	31%	29%	30%
Other (please specify)	10%	14%	10%	10%	15%	8%	10%
Total	200%	200%	200%	200%	200%	200%	200%

Q11. What steps is your organization taking to reduce risks caused by AI? Please select all that apply.	NA	UK	FR	DE	AU	ID	Global
Tools to validate AI prompts and their responses	43%	36%	51%	38%	34%	31%	39%
Data cleansing and governance	37%	34%	48%	31%	45%	33%	38%
Deploying risk quantification of AI models and their infrastructure	35%	41%	42%	37%	34%	33%	37%
Developing a data security program and practice	51%	48%	54%	43%	37%	41%	46%
Identifying and mitigating bias in AI models for safe and responsible use	48%	45%	43%	41%	30%	21%	38%
Tools for managing software vulnerabilities	32%	29%	31%	42%	37%	27%	33%
Incident response plans updated to address AI-enabled attacks	45%	36%	33%	43%	34%	28%	37%
Regular auditing and testing to identify vulnerabilities in AI models and infrastructure	36%	35%	33%	41%	29%	37%	35%
Regular user training and awareness about security implications of AI	39%	34%	41%	36%	37%	31%	36%
Training teams to spot AI-generated behavior patterns or threat actors	44%	40%	43%	41%	37%	31%	39%
Other (please specify)	7%	8%	6%	7%	8%	5%	7%
Total	417%	386%	425%	400%	362%	318%	385%

Q12. Please select the top 2 organizational or governance challenges to successfully deploying AI-based security technologies within your organization.	NA	UK	FR	DE	AU	ID	Global
IT and IT security functions are not aligned with the organization's AI strategy	30%	29%	26%	28%	25%	29%	28%
It requires too much staff to implement and maintain AI-based technologies	29%	23%	24%	28%	29%	24%	26%
There is insufficient budget for AI-based technologies	41%	28%	27%	40%	26%	26%	31%
There is insufficient supervision and oversight of AI learning and decision-making	19%	21%	27%	23%	25%	30%	24%
There is not enough time to integrate AI-based technologies into security workflows	30%	29%	27%	25%	34%	28%	29%
We can't recruit personnel experienced in AI-based technologies	23%	33%	25%	29%	26%	29%	28%
We don't have the internal expertise to validate vendors' claims	28%	30%	35%	18%	25%	26%	27%
Other (please specify)	0%	7%	9%	9%	10%	8%	7%
Total	200%	200%	200%	200%	200%	200%	200%

Q13. Has your organization adopted GenAI as part of its IT or overall business strategy?	NA	UK	FR	DE	AU	ID	Global
Yes	38%	31%	29%	36%	29%	28%	32%
Will adopt in the next six months (please skip to Q18)	27%	23%	22%	29%	31%	27%	26%
Will adopt in the next year (please skip to Q18)	13%	15%	19%	22%	21%	23%	19%
Will adopt but no timeline (please skip to Q18)	14%	11%	17%	8%	10%	16%	13%
No plans to adopt GenAI (please skip to Q18)	8%	20%	13%	5%	9%	6%	10%
Total	100%	100%	100%	100%	100%	100%	100%

Q14. Using the 10-point scale, please rate how important GenAI is to your organization's IT and overall business strategy from 1 = not important to 10 = highly important	NA	UK	FR	DE	AU	ID	Global
1 or 2	14%	15%	14%	8%	9%	17%	13%
3 or 4	15%	10%	13%	9%	11%	19%	13%
5 or 6	22%	19%	12%	11%	18%	16%	16%
7 or 8	28%	30%	35%	32%	17%	21%	27%
9 or10	21%	26%	26%	40%	45%	27%	31%
Total	100%	100%	100%	100%	100%	100%	100%

.

Q15. What are the biggest challenges to an effective GenAI program? Please select the top 3 challenges	NA	UK	FR	DE	AU	ID	Global
Ensure data quality and completeness	34%	32%	39%	34%	39%	35%	35%
Copyright and other legal risks	50%	45%	46%	27%	44%	45%	43%
Concern about biased outputs	21%	32%	34%	37%	23%	46%	32%
Concern about responsible use	41%	43%	27%	26%	22%	29%	31%
Can't effectively measure ROI	22%	25%	23%	29%	26%	30%	26%
Vulnerability to abuse	19%	21%	21%	34%	32%	42%	28%
Lack of resources	20%	19%	24%	26%	34%	19%	24%
Lack of in-house expertise	45%	39%	40%	40%	37%	21%	37%
Regulatory uncertainty and changes	41%	36%	37%	41%	36%	24%	36%
Other (please specify)	7%	8%	9%	6%	7%	9%	8%
Total	300%	300%	300%	300%	300%	300%	300%

Q16a. Has your organization realized benefits from GenAI?	NA	UK	FR	DE	AU	ID	Global
Yes	54%	49%	32%	52%	46%	37%	45%
No	46%	51%	68%	48%	54%	63%	55%
Total	100%	100%	100%	100%	100%	100%	100%

Q16b. If yes, what were the most significant benefits? Please select the top 2 benefits.	NA	UK	FR	DE	AU	ID	Global
A better experience for customers and employees	44%	35%	44%	46%	41%	36%	41.0%
Improves operational efficiency	39%	47%	50%	36%	45%	37%	42.0%
Increases productivity of the workforce	38%	34%	39%	44%	41%	50%	41.0%
Improves threat detection and incident response	35%	38%	39%	45%	35%	36%	38.0%
Improves ability to analyze complex systems, such as network infrastructures or software applications	41%	45%	26%	28%	38%	40%	37.0%
Other (please specify)	3%	1%	2%	1%	0%	1%	1%
Total	200%	200%	200%	200%	200%	200%	200%

Q17. What are the top use cases for GenAI within your organization? Please select the top 3 uses.	NA	UK	FR	DE	AU	ID	Global
Automating routine IT tasks (e.g., log analysis, ticket triage)	37%	36%	38%	29%	23%	28%	32%
Accelerating threat detection or incident response	43%	39%	27%	36%	37%	21%	34%
Enhancing customer service (e.g., chatbots, email drafting)	28%	30%	35%	29%	36%	33%	32%
Assisting with software development (e.g., code generation or debugging)	35%	23%	23%	36%	43%	42%	34%
Summarizing or generating business reports	29%	29%	26%	25%	25%	44%	30%
Supporting security operations (e.g., analyzing alerts, generating playbooks)	33%	32%	37%	44%	45%	46%	39%
Conducting predictive analytics or modeling	28%	32%	33%	26%	32%	39%	31%
Improving employee productivity (e.g., drafting documents, summarizing content)	40%	45%	43%	45%	22%	20%	36%
Enhancing data classification and tagging	21%	27%	28%	21%	30%	19%	24%
Other (please specify)	6%	7%	10%	9%	7%	8%	8%
Total	300%	300%	300%	300%	300%	300%	300%

Q18. Has your organization adopted Agentic AI? Please select one choice only.	NA	UK	FR	DE	AU	ID	Global
Yes	18%	20%	16%	23%	17%	18%	19%
Will adopt in the next six months (please skip to Q20)	14%	11%	15%	18%	19%	20%	16%
Will adopt within the next year (please skip to Q20)	23%	25%	24%	25%	26%	23%	24%
Will adopt but no timeline (please skip to Q20)	30%	29%	29%	19%	24%	27%	26%
No plans to adopt (please skip to Q20)	15%	15%	16%	15%	14%	12%	15%
Total	100%	100%	100%	100%	100%	100%	100%

Q19. Using the following 10-point scale, please rate how important Agentic AI will become to your organization's IT and overall business strategy from 1 = not important to 10 = extremely important	NA	UK	FR	DE	AU	ID	Global
1 or 2	13%	15%	13%	15%	18%	20%	16%
3 or 4	24%	21%	26%	23%	23%	30%	24%
5 or 6	30%	30%	33%	27%	30%	25%	29%
7 or 8	12%	18%	13%	13%	15%	12%	14%
9 or10	21%	16%	15%	22%	14%	13%	17%
Total	100%	100%	100%	100%	100%	100%	100%

Part 2. IT leaders' priorities and pressures

Q20. What are the top three IT priorities for the next 12 months? Please select the top 3 choices only.	NA	UK	FR	DE	AU	ID	Global
Acceleration of digital transformation	36%	39%	43%	45%	49%	54%	44%
Automation of business processes	53%	49%	35%	38%	44%	43%	44%
Identification and classification of sensitive and confidential information that needs to be protected	37%	35%	32%	43%	43%	44%	39%
Identification and prioritization of current and emerging security threats	36%	38%	50%	35%	43%	42%	41%
Identification and prioritization of threats affecting business operations	45%	46%	45%	28%	43%	36%	40%
Metrics to demonstrate the business value of the IT security program to the business	50%	46%	52%	54%	37%	40%	47%
Processes to achieve compliance with regulations and laws	36%	36%	34%	48%	35%	33%	37%
Other (please specify)	7%	11%	9%	9%	6%	8%	8%
Total	300%	300%	300%	300%	300%	300%	300%

Q21. Which types of digital assets are most important to secure and manage in your organization? Please select the top 3 choices only.	NA	UK	FR	DE	AU	ID	Global
Contracts and legal documents	41%	43%	38%	51%	38%	43%	42%
Intellectual property	43%	38%	45%	37%	41%	46%	42%
Custom data	38%	44%	49%	44%	46%	41%	44%
Financial records	36%	37%	28%	33%	35%	43%	35%
Employee/HR records	37%	34%	38%	37%	32%	37%	36%
Source code	50%	38%	43%	41%	48%	44%	44%
Operational performance data	29%	37%	32%	33%	36%	32%	33%
Marketing and brand content	18%	20%	19%	18%	16%	7%	16%
Other (please specify)	8%	9%	8%	6%	8%	7%	8%
Total	300%	300%	300%	300%	300%	300%	300%

Q22. Using the following 10-point scale, please rate how effective IT infrastructure is in keeping up with frequent shifts in business strategies using the following 10-point scale from 1 = low effective to 10 = high effectiveness?	NA	UK	FR	DE	AU	ID	Global
1 or 2	19%	25%	23%	20%	18%	19%	21%
3 or 4	22%	23%	20%	19%	24%	25%	22%
5 or 6	16%	15%	17%	14%	14%	13%	15%
7 or 8	25%	24%	25%	24%	25%	26%	25%
9 or10	18%	13%	15%	23%	19%	17%	17%
Total	100%	100%	100%	100%	100%	100%	100%

Q23. It is difficult to support business innovation and transformation because the goals of IT and business are not aligned.	NA	UK	FR	DE	AU	ID	Global
Strongly agree	33%	28%	29%	30%	27%	17%	27%
Agree	30%	27%	25%	28%	29%	19%	26%
Unsure	11%	11%	12%	12%	20%	20%	15%
Disagree	16%	18%	23%	17%	12%	21%	18%
Strongly disagree	10%	16%	11%	13%	12%	23%	14%
Total	100%	100%	100%	100%	100%	100%	100%

Q24. What are the most important IT responsibilities critical to supporting business	NA	UK	FR	DE	AU	ID	Global

innovation? Please select the top 3 choices only.							
Ensuring high availability of IT services	53%	50%	47%	51%	39%	42%	47%
Meeting end-user expectations	31%	32%	35%	39%	47%	45%	38%
Integrating disparate security technologies	38%	41%	37%	42%	36%	39%	39%
Obtaining sufficient resources/budget	37%	39%	32%	31%	34%	41%	36%
Complying with policies and regulations	44%	33%	41%	38%	31%	35%	37%
Recruiting and retaining qualified personnel	48%	43%	43%	32%	49%	40%	43%
Obtaining executive-level support	27%	31%	31%	30%	37%	31%	31%
Minimizing turf issues or silos	17%	23%	26%	31%	18%	19%	22%
Other (please specify)	5%	8%	8%	6%	9%	8%	7%
Total	300%	300%	300%	300%	300%	300%	300%

Part 3. Measuring the ROI and value of investments

Q25. Using the following 10-point scale, please rate how confident your organization is in its ability to measure the ROI of investments related to securing and managing of information assets from 1 = not confident 10 = highly confident?	NA	UK	FR	DE	AU	ID	Global
1 or 2	18%	24%	21%	20%	20%	21%	21%
3 or 4	21%	20%	19%	19%	21%	22%	20%
5 or 6	16%	15%	21%	15%	17%	16%	16%
7 or 8	25%	25%	24%	26%	22%	26%	25%
9 or10	20%	16%	15%	20%	20%	15%	18%
Total	100%	100%	100%	100%	100%	100%	100%

Q26. What are the most significant challenges in demonstrating ROI for information management and security technologies? Please select the top 3 challenges.	NA	UK	FR	DE	AU	ID	Global
Difficulty quantifying intangible benefits (e.g., reputation, trust)	51%	52%	46%	49%	51%	60%	51%
Long timeframes to realize measurable value	44%	56%	37%	48%	47%	38%	45%
Inability to track downstream business impacts	56%	55%	56%	52%	55%	39%	52%
Complex cost structures (e.g., training, integration)	50%	47%	44%	44%	41%	45%	45%
Lack of agreed-upon metrics	37%	41%	56%	46%	48%	46%	46%
Competing priorities	51%	37%	46%	50%	43%	54%	47%
Other (please specify)	11%	12%	15%	11%	15%	18%	14%
Total	300%	300%	300%	300%	300%	300%	300%

Q27. Which of the following metrics are most often used to determine the effectiveness of your organization's information management and security technologies? Please select the top 3 choices.	NA	UK	FR	DE	AU	ID	Global
Decreased false negative rate	22%	25%	28%	42%	21%	32%	28%
Decreased false positive rate	34%	22%	35%	39%	44%	34%	35%
Decreased security risk	33%	31%	33%	21%	36%	23%	29%
Increased detection rate	36%	35%	32%	30%	34%	21%	31%
Increased prevention rate	24%	24%	21%	22%	31%	27%	25%
Increased user productivity	26%	15%	29%	16%	18%	34%	23%
Mean time to contain an attack (MTTC)	27%	25%	30%	28%	28%	29%	28%
Mean time to identify an attack (MTTI)	31%	33%	15%	32%	18%	23%	25%
Passing grade on compliance audit or assessment	15%	25%	26%	20%	28%	29%	24%
Return on investment (ROI)	18%	33%	18%	17%	14%	12%	19%
Total cost of ownership (TCO)	23%	20%	23%	22%	15%	21%	21%
Other (please specify	11%	12%	10%	11%	13%	15%	12%
Total	300%	300%	300%	300%	300%	300%	300%

Q28. In what timeframe does your organization require ROI from investments in information security?	NA	UK	FR	DE	AU	ID	Global
Within six months	37%	25%	19%	41%	21%	33%	29%
Six months to one year	24%	21%	26%	33%	25%	30%	26%
One year to two years	16%	21%	33%	11%	26%	17%	21%
No required timeframe	23%	33%	22%	15%	28%	20%	24%
Total	100%	100%	100%	100%	100%	100%	100%

Part 4. Cybersecurity risks

Q29. Which of the following cyberattacks are most likely to hinder your organization's ability to manage and protect its information? Please select the top 3 cyberattacks that put the management and security of information at risk.	NA	UK	FR	DE	AU	ID	Global
AI-based attacks and threats	33%	35%	26%	44%	36%	34%	35%
Account takeover	39%	41%	34%	29%	27%	42%	35%
Advanced malware / zero day attacks	21%	29%	24%	34%	26%	38%	29%
Compromised / stolen devices	33%	31%	40%	35%	39%	22%	33%
Credential theft	32%	27%	27%	31%	39%	42%	33%
Malicious insider	38%	35%	40%	30%	44%	32%	37%
Ransomware	45%	44%	43%	36%	36%	35%	40%
SQL injection	20%	22%	21%	24%	24%	21%	22%
Insider misuse or negligence	35%	31%	41%	31%	23%	26%	31%
Other (please specify)	4%	5%	4%	6%	6%	8%	5%
Total	300%	300%	300%	300%	300%	300%	300%

Q30a. Did your organization have a data breach or cybersecurity incident in the past 2 years?	NA	UK	FR	DE	AU	ID	Global
Yes	60%	56%	54%	41%	59%	51%	53%
No (please skip to Q31)	35%	38%	42%	56%	37%	43%	42%
Unsure (please skip to Q31)	5%	6%	4%	3%	4%	6%	5%
Total	100%	100%	100%	100%	100%	100%	100%

Q30b. If yes, how frequently did these data breaches or cybersecurity incidents occur during the past 2 years?	NA	UK	FR	DE	AU	ID	Global
Only once	34%	44%	37%	41%	46%	44%	41%
2 to 3 times	34%	26%	31%	31%	31%	27%	29%
4 to 5 times	17%	21%	19%	11%	13%	18%	17%
More than 5 times	15%	9%	13%	17%	10%	11%	13%
Total	100%	100%	100%	100%	100%	100%	100%
Extrapolated ave							2.92

Q31. How has the frequency and severity of cyberattacks change in the past 2 years?	NA	UK	FR	DE	AU	ID	Global
Increased significantly	21%	19%	21%	15%	22%	26%	21%
Increased slightly	27%	26%	21%	18%	20%	22%	22%
Stayed the same	31%	27%	28%	30%	32%	28%	29%
Decreased slightly	14%	18%	16%	27%	16%	14%	18%
Decreased significantly	7%	10%	14%	10%	10%	10%	10%
Total	100%	100%	100%	100%	100%	100%	100%

Q32. What security methods and technologies have been implemented to prevent data loss caused by negligent and malicious insiders? Please select the top 5.	NA	UK	FR	DE	AU	ID	Global
Cloud data loss prevention	39%	34%	36%	27%	31%	23%	32%
Cloud security tools	31%	26%	27%	49%	23%	25%	30%
Data security posture management (DSPM)	24%	21%	33%	36%	27%	25%	28%
Email data loss prevention	35%	34%	28%	36%	42%	34%	35%
Encryption for data at rest	35%	40%	37%	36%	39%	24%	35%
Encryption for data in transit	40%	41%	39%	34%	37%	43%	39%
Endpoint data loss prevention	35%	29%	26%	40%	25%	42%	33%
Insider threat management (ITM)	23%	25%	24%	25%	32%	31%	27%
IT/IT security team triages incidents	28%	34%	26%	21%	27%	40%	29%
Manual policy orchestration	34%	31%	41%	28%	25%	24%	30%
Network data loss prevention	28%	25%	32%	29%	26%	31%	28%
Policy fine tuning to prevent data loss	29%	34%	31%	23%	39%	31%	31%
Secure web gateway (SWG)	31%	27%	26%	31%	28%	29%	29%
User and entity behavior analytics (UEBA)	25%	25%	30%	23%	41%	33%	29%
Web data loss prevention	25%	33%	24%	23%	22%	26%	26%
Web isolation technology	24%	29%	29%	29%	25%	30%	28%
Other (please specify)	14%	12%	11%	10%	11%	9%	11%
Total	500%	500%	500%	500%	500%	500%	500%

Q33. Which types of content or data are most vulnerable to insider threats in your organization? Please select the top 3 choices.	NA	UK	FR	DE	AU	ID	Global
Customer or client data	56%	55%	60%	60%	55%	60%	58%
Source code	47%	39%	31%	50%	45%	44%	43%
Internal communications (e.g., emails, chats)	40%	36%	33%	43%	38%	38%	38%
Financial records	46%	50%	48%	41%	52%	40%	46%
Mergers and acquisition, legal or Board of Directors documents	34%	32%	31%	29%	30%	36%	32%
Human resources and/or employee data	30%	39%	45%	34%	32%	32%	35%
Product or research and development documentation	42%	45%	47%	37%	41%	41%	42%
Other (please specify)	5%	4%	5%	6%	7%	9%	6%
Total	300%	300%	300%	300%	300%	300%	300%

Q34. Using the following 10-point scale, please rate how effective your organization is in creating trust while taking steps to reduce data loss incidents caused by negligent or malicious insiders from 1 = not effective to 10 = very effective..	NA	UK	FR	DE	AU	ID	Global
1 or 2	12%	23%	24%	15%	22%	10%	18%
3 or 4	25%	15%	16%	16%	19%	14%	18%
5 or 6	21%	20%	23%	24%	20%	33%	23%
7 or 8	23%	24%	23%	23%	18%	28%	23%
9 or10	19%	18%	14%	22%	21%	15%	18%
Total	100%	100%	100%	100%	100%	100%	100%

Q35. Using the following 10-point scale, please rate how effective your organization is in its ability to monitor insider activity across hybrid and/or remote environments from 1 =not effective to 10 = very effective.	NA	UK	FR	DE	AU	ID	Global
1 or 2	10%	12%	15%	9%	11%	13%	12%
3 or 4	21%	24%	27%	11%	24%	13%	20%
5 or 6	16%	17%	15%	19%	17%	19%	17%
7 or 8	26%	23%	13%	24%	14%	25%	21%
9 or10	27%	24%	30%	37%	34%	30%	30%
Total	100%	100%	100%	100%	100%	100%	100%
Extrapolated ave							6.30

Part 7. The risk of security complexity

Q36. Approximately, how many separate cybersecurity technologies does your organization own today?	NA	UK	FR	DE	AU	ID	Global
Fewer than 10	41%	49%	42%	42%	44%	46%	44%
10 to 20	41%	32%	41%	40%	37%	38%	38%
21 to 30	11%	12%	11%	13%	10%	9%	11%
31 to 50	3%	2%	1%	1%	3%	4%	2%
51 to 75	1%	2%	2%	3%	1%	2%	2%
76 to 100	2%	3%	3%	1%	4%	1%	2%
More than 100	1%	0%	0%	0%	1%	0%	0%
Total	100%	100%	100%	100%	100%	100%	100%
Extrapolated ave							15.30

Q37a. How important is reducing complexity within your organization's IT security architecture to have a strong security posture?	NA	UK	FR	DE	AU	ID	Global
Essential	23%	21%	18%	30%	29%	19%	23%
Very important	27%	23%	16%	25%	25%	23%	23%
Important	23%	25%	25%	36%	26%	28%	27%
Not important (please skip to Q38)	16%	21%	22%	7%	15%	21%	17%
Irrelevant (please skip to Q38)	11%	10%	19%	2%	5%	9%	10%
Total	100%	100%	100%	100%	100%	100%	100%

Q37b. What steps would your organization take to reduce complexity? [If essential, very important or important] Please select the top 3 steps.	NA	UK	FR	DE	AU	ID	Global
Appoint one person to be accountable	60%	57%	56%	65%	61%	59%	59%
Centralize IT security decision-making	45%	63%	55%	48%	52%	54%	53%
Streamline security and data governance policies	56%	54%	56%	63%	53%	52%	56%
Restrict the number of employees and contractors with access to sensitive and confidential information	47%	49%	57%	48%	50%	61%	52%
Reduce the number of overlapping tools and platforms	60%	45%	60%	53%	61%	51%	55%
Other (please specify)	32%	32%	16%	23%	23%	23%	25%
Total	300%	300%	300%	300%	300%	300%	300%

Q38. Which of the following factors increases the complexity of your organization the most? Please select the top 3 factors.	NA	UK	FR	DE	AU	ID	Global
Access to cloud-based applications and data	38%	35%	37%	45%	40%	37%	39%
Constant changes to the organization due to mergers and acquisitions, divestitures, reorganizations and downsizing	36%	37%	31%	39%	42%	38%	37%
The Internet of Things (IoT)	44%	46%	43%	41%	54%	50%	46%
New or emerging cyber threats	57%	60%	56%	55%	44%	42%	52%
Rapid growth of unstructured data	48%	45%	46%	43%	47%	36%	44%
Regulatory and compliance requirements	39%	40%	38%	23%	25%	37%	34%
Use of mobile devices (including BYOD and mobile apps)	26%	29%	35%	41%	38%	49%	37%
Other (please specify)	12%	8%	14%	13%	10%	11%	11%
Total	300%	300%	300%	300%	300%	300%	300%

Part 8. Your role and organization

D1. Check the Primary Person you or your IT security leader reports to within the organization.	NA	UK	FR	DE	AU	ID	Global
CEO/Executive Committee	7%	5%	4%	3%	4%	6%	5%
Chief Financial Officer	5%	9%	7%	5%	6%	7%	6%
General Counsel	4%	5%	8%	4%	4%	5%	5%
Chief Information Officer	16%	15%	18%	19%	17%	16%	17%
Chief Information Security Officer	18%	14%	13%	21%	15%	16%	16%
Compliance Officer	8%	12%	9%	9%	10%	9%	9%
Human Resources VP	6%	7%	10%	8%	7%	8%	8%
Chief Security Officer	9%	8%	7%	7%	9%	7%	8%
Data Center Management	8%	7%	5%	4%	5%	6%	6%
Chief Risk Officer	10%	11%	9%	9%	11%	9%	10%
Other (please specify)	9%	7%	10%	11%	12%	11%	10%
Total	100%	100%	100%	100%	100%	100%	100%

D2. What is the worldwide headcount of your organization?	NA	UK	FR	DE	AU	ID	Global
< 100	10%	15%	16%	9%	14%	11%	12.0%
100 to 500	13%	21%	20%	12%	10%	12%	14.7%
501 to 1,000	18%	23%	19%	23%	22%	18%	20.0%
1,001 to 5,000	23%	19%	26%	18%	21%	22%	22.0%
5,001 to 25,000	15%	11%	10%	19%	14%	16%	14.2%
25,001 to 75,000	13%	7%	6%	12%	12%	11%	10.2%
> 75,000	8%	4%	3%	7%	7%	10%	6.5%
Total	100%	100%	100%	100%	100%	100%	100%

D3. What industry best describes your organization's industry focus (stratified list)?	NA	UK	FR	DE	AU	ID	Global
Agriculture & food service	1%	0%	3%	0%	2%	2%	1%
Communications	2%	4%	2%	3%	3%	4%	3%
Consumer reports	5%	4%	5%	3%	4%	2%	4%
Education & research	1%	0%	4%	2%	2%	5%	2%
Energy & utilities	6%	7%	8%	5%	7%	4%	6%
Entertainment & media	4%	6%	5%	3%	4%	2%	4%
Financial services	17%	18%	14%	13%	14%	13%	15%
Health & pharmaceutical	8%	8%	7%	9%	8%	7%	8%
Hospitality	5%	7%	6%	8%	7%	5%	6%
Industrial & manufacturing	8%	10%	6%	10%	9%	11%	9%
Public sector	5%	6%	7%	9%	6%	5%	6%
Retail	5%	4%	5%	6%	6%	7%	6%
Services	9%	8%	9%	9%	9%	11%	9%
Technology & software	8%	5%	6%	5%	5%	9%	7%
Transportation	7%	8%	7%	8%	6%	5%	7%
Other (please specify)	9%	5%	6%	7%	8%	8%	7%
Total	100%	100%	100%	100%	100%	100%	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org.

Ponemon Institute
Advancing Responsible Information Management

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.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.