imprivata® | Ponemon INSTITUTE

# The state of third-party access in cybersecurity

PONEMON REPORT 2025

# Letter from Joel Burleson-Davis SVP Engineering, Cyber

Businesses in all industries have increased their reliance on external vendors, partners, and contractors, and in turn, the risks associated with third-party access have evolved into a pressing cybersecurity challenge.

Year after year, we've seen the impact of third-party attacks – for example, the MOVEit breach in 2023 and Change Healthcare in 2024. But just how widespread is the problem?

**Over the last 12 months or so, roughly half of organizations reported experiencing a breach that involved a vendor or another third party accessing their network.** Clearly this is a significant challenge, and 48% of organizations believe that third-party remote access is becoming their weakest attack surface. And it comes with real consequences, including the loss or theft of sensitive and confidential information, regulatory fines, and other operational disruptions.

As this report reveals, organizations have an access management problem when it comes to third parties. Because vendors, contractors, and other third parties are not employees, they typically do not follow the same governance procedures or identity lifecycle policies, making access difficult to manage and secure. It's not surprising, then, that 58% of organizations don't have a consistently applied access management strategy when it comes to third parties.

But they should.

A comprehensive, consistent access strategy can minimize cybersecurity risk by securing remote access to privileged assets and accounts, improve security without sacrificing productivity, and save time. This is especially critical for third-party access, which is both heavily targeted by bad actors and less scrutinized than internal users.

This report offers a deep dive into the challenges organizations are facing when it comes to securing third-party access, and what they're doing to combat those challenges.

There's still work to be done, but I'm confident we're up to the task.

# 01 Introduction

The modern enterprise relies on third parties – including vendors, contractors, suppliers, partners, and broader supply chains – to operate effectively and to be successful. But it can often be those same third parties at the source of cyber incidents, whether it be from a successful breach of the third party's system, or the third party having too much access to a client's network. In fact, **47%** of organizations experienced a breach or attack that involved third-party network access in the previous 12 months.

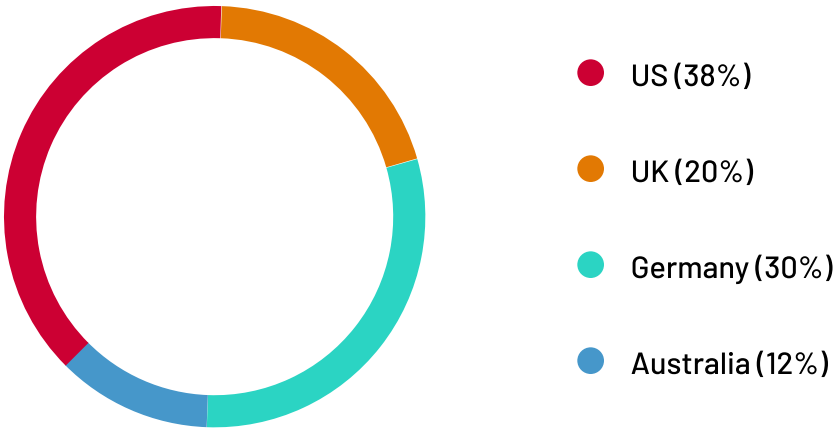
Third parties frequently need access – often privileged access – to devices, systems, applications, and networks, but providing that access creates new risks for the organizations granting it. Third parties are a frequent target of bad actors because they typically have more access than they need.

Why? Because third parties present unique access management challenges: they're not employees, and it's therefore difficult to track their lifecycle and employment status, to enforce multifactor authentication, or to appropriately set up their access rights. Armed with that knowledge, bad actors try to take advantage of third parties' access.

**47%**

**of organizations experienced a breach or attack that involved third-party network access in the previous 12 months.**

The research presented below was conducted to understand organizations' approaches to managing cybersecurity with a particular focus on managing third-party remote access risks, as well as risks posed by internal users with privileged access. The Ponemon Institute surveyed 1,942 IT and IT security practitioners in the US (733), UK (398), Germany (573), and Australia (238), who are familiar with their organizations' approach to managing privileged access, including processes and technologies used to secure privileged access, both of third parties and internal users. Represented industries include healthcare, public sector, industrial and manufacturing, and financial services.




Key findings from the research are presented in the next section of this report, including a deep dive into the research to surface the most important insights. Data will be presented in four sections:

- The third-party access threat is significant, and it's not going away
- Organizations are trying, but struggling, to respond to the third-party access threat
- Why organizations struggle to combat the third-party access threat
- Organizations need to refine and mature their strategies for securing access for both internal users and third parties

*The complete audited findings are presented in the Appendix of this report.*

# 02 Key findings

## The third-party access threat is significant, and it's not going away

**Nearly half (47%)** of all respondents reported experiencing a data breach or cyberattack in the last year that involved one of their vendors or other third-party partners accessing their network. And of those, **34%** reported that the breaches were the result of the third party having too much privileged access.

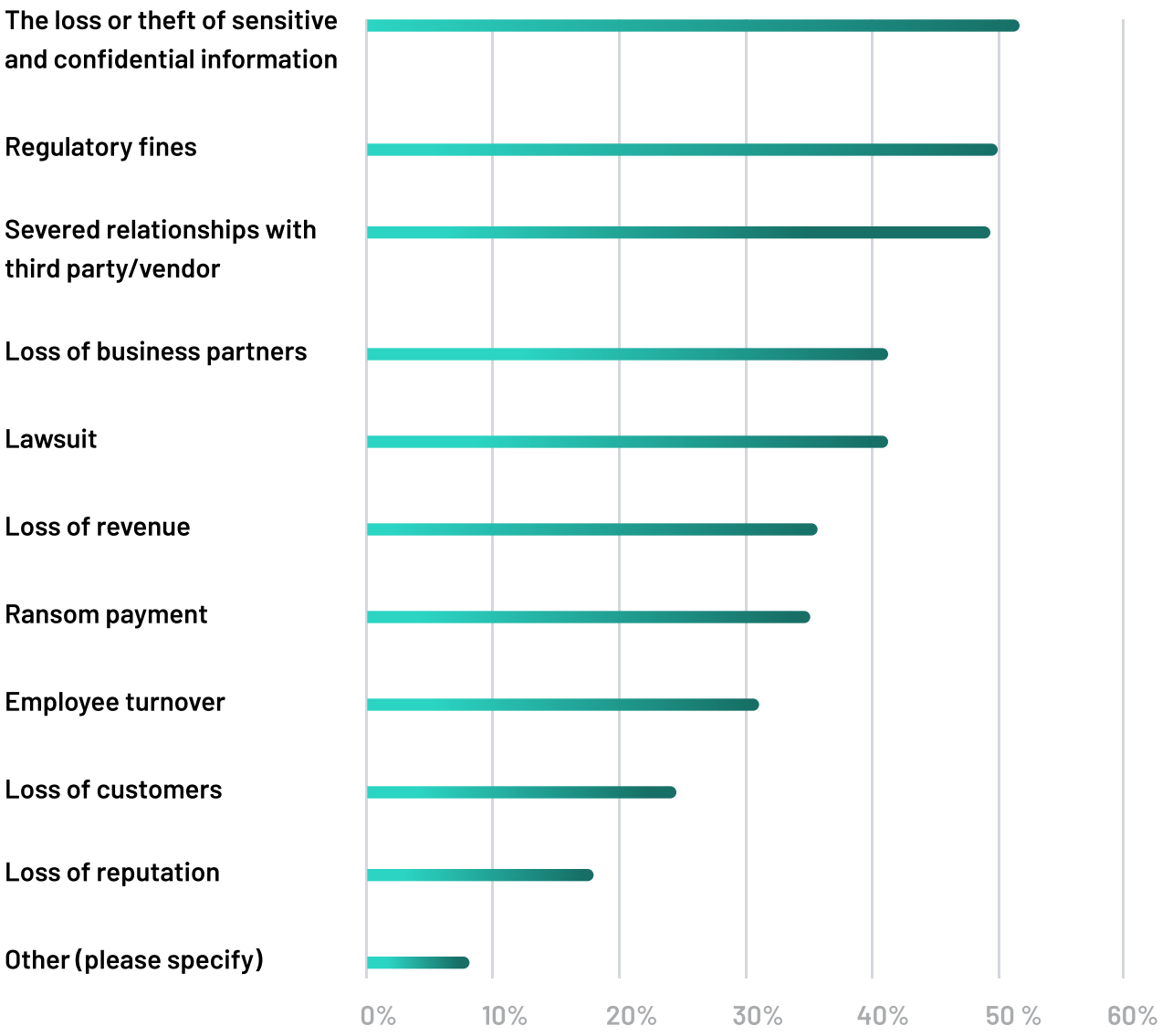
Equally worrying, if not more so, is that **35%** of respondents who experienced a breach reported being unsure about whether too much access given to third parties was the cause of those breaches. This is **up significantly from just 2% in 2022**[ii], indicating that organizations have limited (or no) insight into the number of vendors accessing their network and how they're doing it. It also implies a lack of visibility into what third parties are doing with the access they have, as well as a lack of ability to control that access and to know when it has been compromised.

**34%**

is (still) too high, but there's some good news, here. That's **down from 70% in 2022**[i]**, indicating that organizations have been improving** when it comes to managing third-party access permissions appropriately.

But no matter the direct cause, the attacks involving a third party experienced by these organizations came with serious consequences, including the loss or theft of sensitive and confidential information (**53%**), regulatory fines (**50%**), and severed relationships with the third party / vendor (**49%**). Response frequencies are presented in the chart below.

### The consequences of a breach or attack



## The third-party access security state of mind

Survey respondents were asked to predict whether breaches involving a third-party would increase, decrease, or stay the same. It wasn't great news: **64%** expect third party-related breaches to increase or stay the same over the next 12-14 months.

This, coupled with the outlook that third-party remote access is becoming an organization's weakest attack surface – agreed to by **48%** of respondents – presents a problem. An expectation of growing or flat potential breaches, coupled with the belief that third-party access is increasingly becoming the weakest attack surface, foretells continued challenges.

## Third party threats vs. threats associated with privileged internal users

Inflated third-party access is a clear threat, but it's worth looking inside, too: in fact, **44%** of respondents reported experiencing breaches or attacks that involved internal users with privileged access to their organization's network. And of that group, **45%** reported that the breach or attack was due to giving the employee too much privileged access, with only **11%** reporting that they were unsure.

While this indicates that **organizations have work to do when it comes to privileged access**, they at least have better visibility into what employees are doing, relative to visibility into third parties.

**64%**

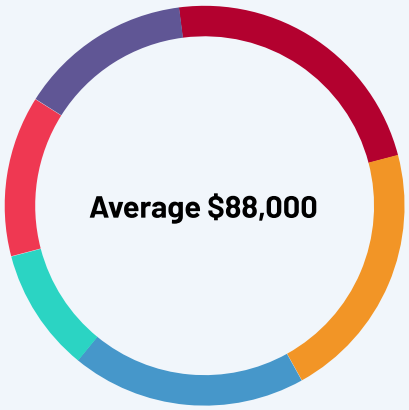
of respondents expect third party-related breaches to increase or stay the same over the next 12-14 months.

## The cost of privileged access abuse

Survey respondents were asked to approximate the cost to their organizations to restore access to third-party and privileged internal users, taking things like detecting, responding to, and recovering from a breach into consideration. While their responses were wide-ranging, **the average cost per incident was $88,000**. Full responses are shown in the table below.

**In the past 12 months, approximately how much did it cost to restore access to third party and privileged access users?**

- Less than $10,000 **(13%)**
- $10,000 to $25,000 **(14%)**
- $25,001 to $50,000 **(23%)**
- $50,001 to $100,000 **(21%)**
- $100,001 to $250,000 **(19%)**
- More than $250,000 **(10%)**

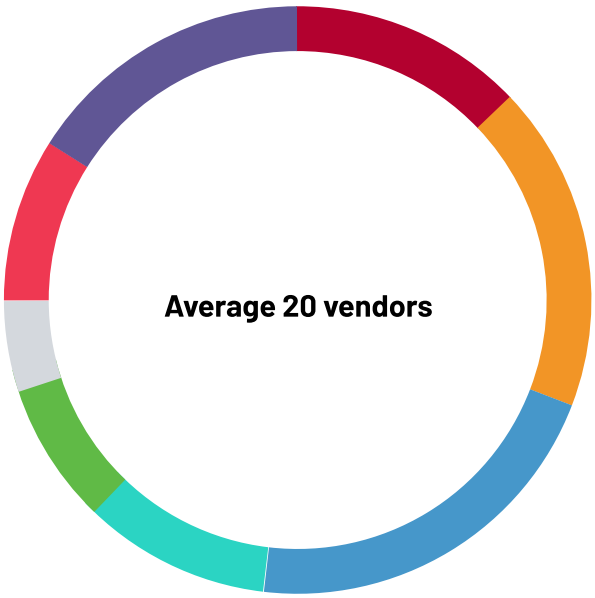


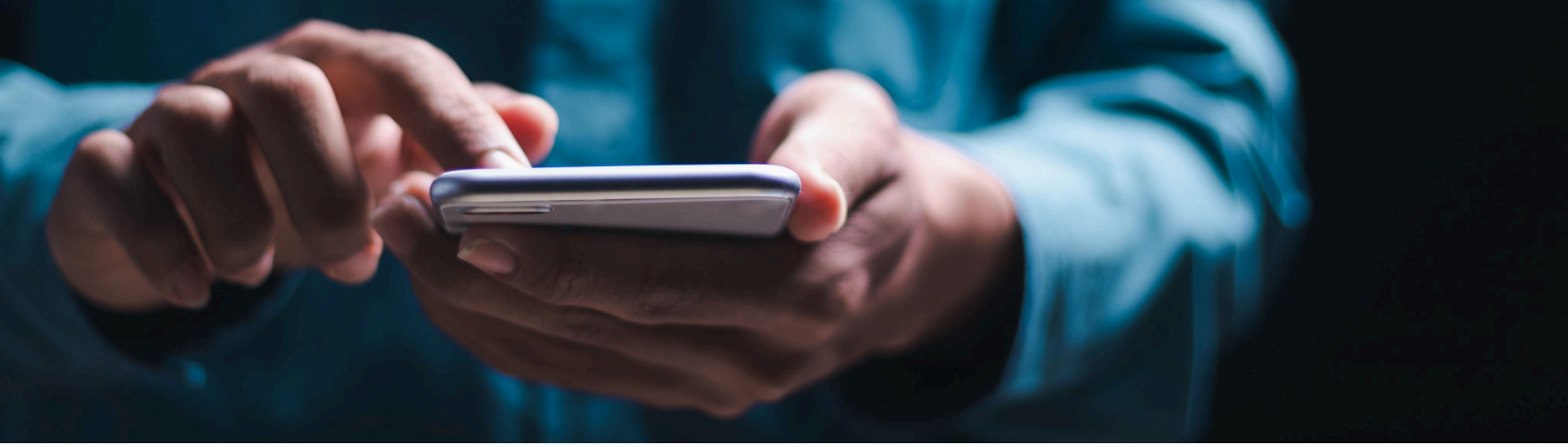

## Organizations are trying, but struggling, to respond to the third-party access threat

Survey respondents reported that **an average of 20 vendors** have access to their organization's network, with **25%** reporting that they have more than 30 vendors that do. However, only **50%** said that they have a comprehensive inventory of all third parties with access to their network, so it's possible that the average number could be much higher. Responses are shown in the table below.

**How many third parties and vendors have access to your organization's network?**

- None **(9%)**
- Less than 5 **(16%)**
- 5 to 10 **(13%)**
- 11 to 20 **(18%)**
- 21 to 30 **(21%)**
- 31 to 40 **(11%)**
- 41 to 50 **(9%)**
- More than 50 **(5%)**





With so many third parties being given network access, properly securing that access needs to be a priority. Some good news: **47%** of respondents say their organizations agree, and that their IT / IT security function makes ensuring the security of third parties' and vendors' remote access to its network a priority.

And in fact, **73%** of respondents reported that their organizations have a vendor privileged access management (VPAM) solution in place. However, only **55%** of that group expressed strong confidence that their VPAM solution was effective in reducing privileged access abuse.

Organizations clearly recognize the threat that third-party access poses, and many are trying, in earnest, to combat it. But between low confidence in solution efficacy, lack of visibility, and the number of breaches, it's clear that simply "buying a solution" is insufficient for solving their challenges. Even with a VPAM solution in place, organizations have an uphill battle when it comes to full program success.

**Only 55%**

of organizations with a VPAM solution in place have expressed strong confidence that it was effective in reducing privileged access abuse.

### Why organizations struggle to combat the third-party access threat

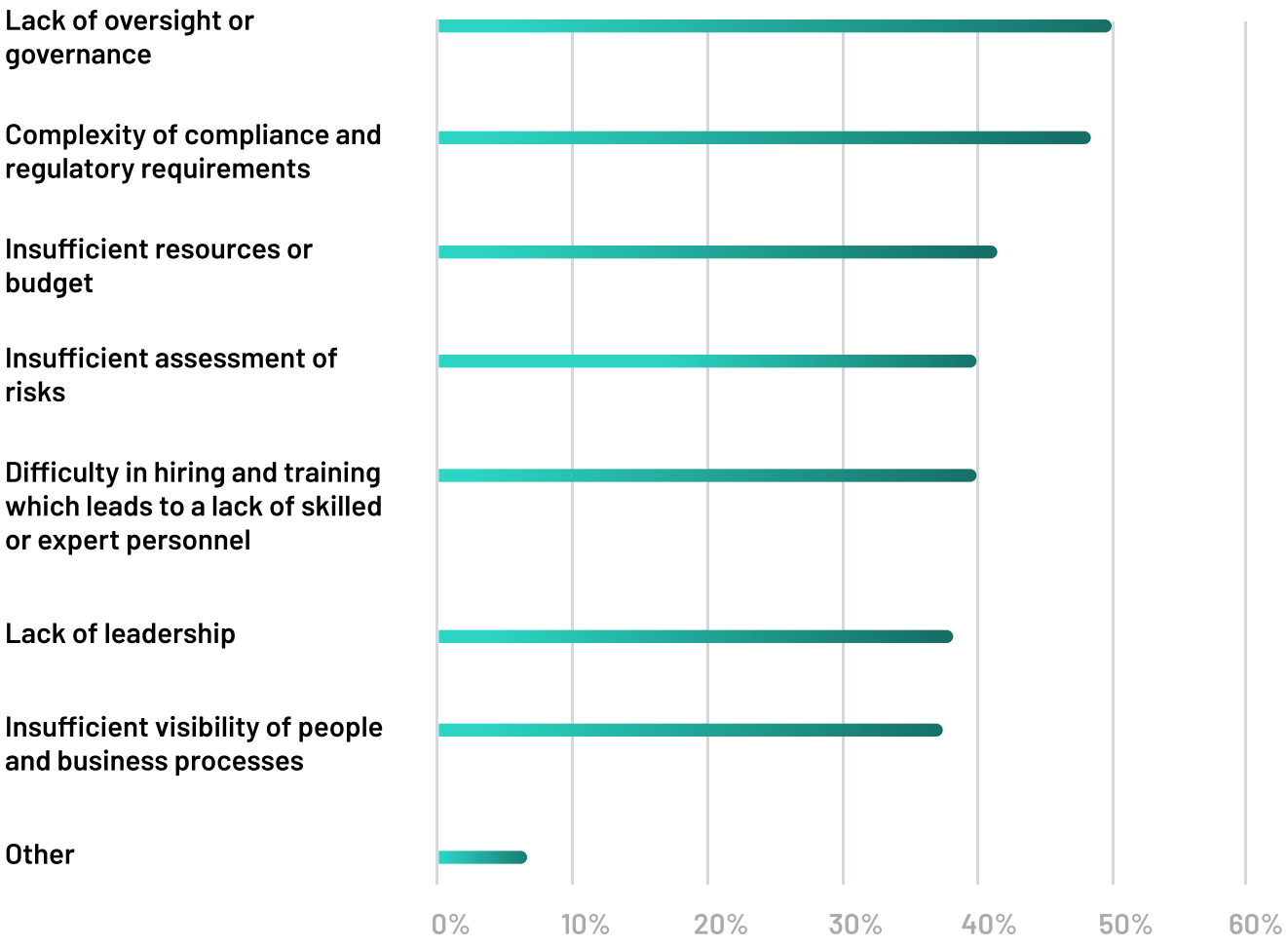
**44%** of respondents agree: managing third-party permissions and remote access to their network can be overwhelming and a drain on internal resources. And it's no wonder so many feel that way, because respondents reported that IT, security, and other related teams spend a **staggering 134 hours a week**, on average, analyzing and investigating the security of third party and privileged access. Why might that be? Underlying causes include lack of (the right) internal resources, manual processes, and no centralized control.

## Barriers, barriers, and more barriers

Organizations know there's a third-party access threat, and most are trying to do something about it. But there's so much that stands in the way. Survey respondents reported that the most significant barriers to reducing third-party access risks were lack of oversight or governance (**50%**), complexity of compliance and regulatory requirements (**48%**), and insufficient resources or budget (**41%**). The chart below presents barriers of significance, and the percentage of respondents that selected that barrier.

### What are the most significant barriers to reducing third-party and privileged access risks?

*(Note: respondents were asked to pick three from the list.)*



## Lack of a comprehensive inventory of third parties, and why

As previously noted, only 50% of respondents reported that their organizations have a comprehensive inventory of all third parties with network access. But there's the other **50%** who either didn't have, or weren't sure they had, a comprehensive inventory. Of those, the most cited reasons were lack of resources to track third parties (**45%**) and no centralized control over third-party relationships (**37%**). Reports of those, and other reasons, can be seen in the table below.

| If your organization doesn't have a comprehensive inventory of third parties with network access (or you're unsure if it does), why? | |
|---|---|
| Lack of resources | 45% |
| No centralized control over third-party relationships | 37% |
| Complexity in third-party relationships | 27% |
| Cannot keep track due to turnover in third parties | 22% |
| Not a priority | 17% |
| Other | 7% |

Survey respondents were asked to identify which one part of their organization is most responsible for managing and granting access to third parties and vendors, and their answers spanned a wide spectrum (responses and frequency of responses in the chart below). The many and varied responses given by respondents help to explain why organizations might struggle with clear, defined ownership of the third-party access problem.

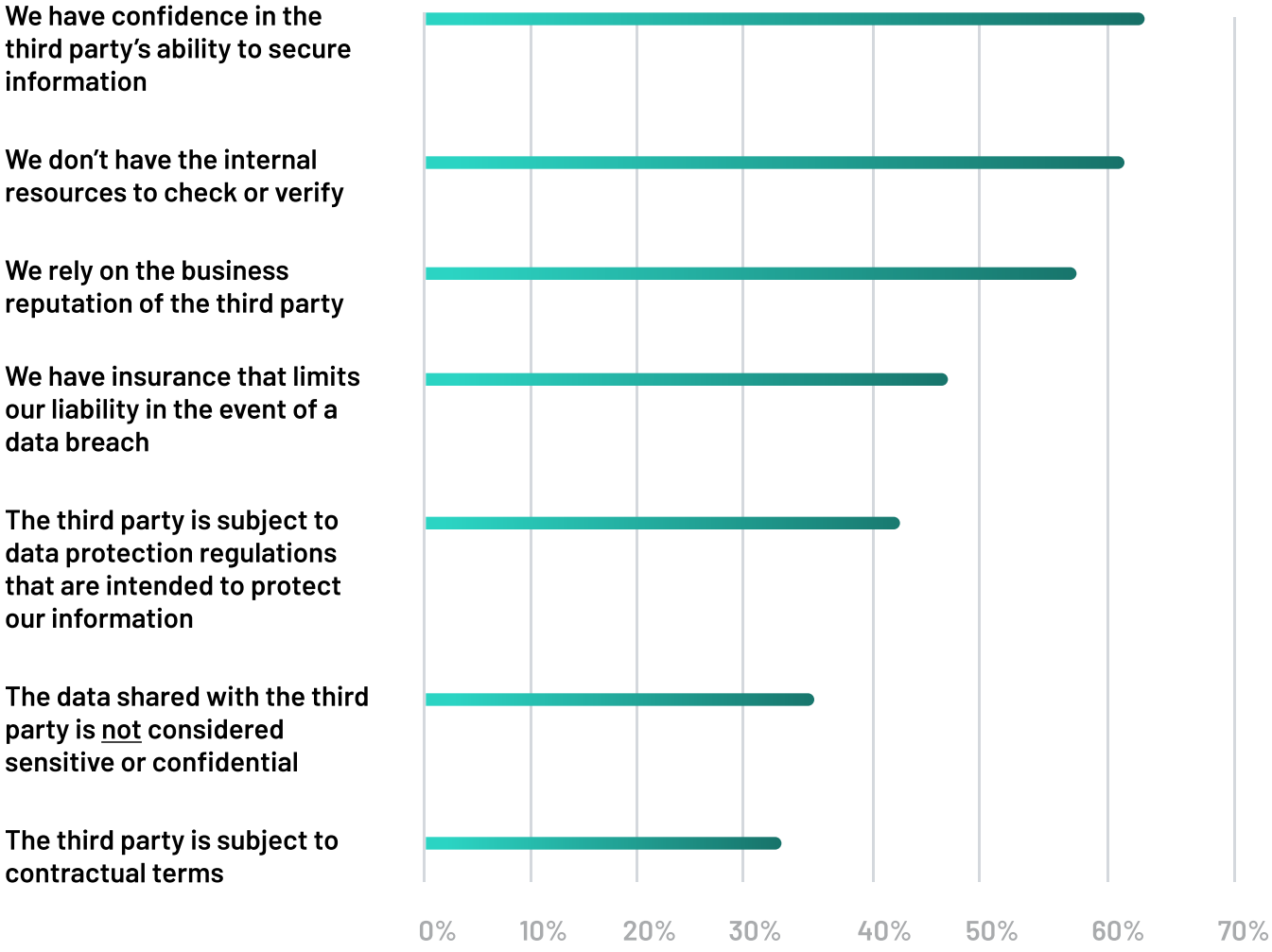
**Which part of your organization is most responsible for managing and granting access to third parties and vendors?**

- Information technology **(16%)**
- Information security **(18%)**
- Compliance / general counsel **(17%)**
- Internal audit **(15%)**
- Human resources **(11%)**
- Risk management **(9%)**
- Lines of business **(14%)**

## Third-party ecosystem security

**55%** of respondents reported that their organizations do not evaluate the security and privacy practices of third parties before they engage them in a business relationship that requires providing access to sensitive or confidential information. Among the top reasons why not: organizations have confidence in the third party's ability to secure information (**62%**), and lack of internal resources to check or verify (**61%**). Full responses and frequency of selection are presented in the chart below.

### Why evaluations are not completed before a business engagement with a third party



For context, **57%** of survey respondents stated that their organization protects itself from internal privileged access abuse by performing thorough background checks before issuing credentials. It's hard to ignore the discrepancy: organizations appear to have stricter rules for evaluating internal users than for third parties. This may start to explain why nearly half of all respondents believe that third-party remote access is becoming the weakest attack surface, and suggests a starting point. At a minimum, organizations should adopt similar evaluation principles that they utilize for internal users for third parties.

Granted, it is more difficult for organizations to perform as stringent a check on third parties than it is for internal users. But that's why having a comprehensive inventory of external users and additional security measures like granular access controls and activity monitoring are so important. As will be discussed, "trust" and "confidence" in third parties is not a sound security strategy.

### Third-party access monitoring

As was presented above, the average organization has 20 vendors with access to its network. That's 20 unique vendors, and likely many more individual people representing that vendor, with network access – and it's possible that their security and privacy practices weren't thoroughly vetted beforehand. That makes monitoring their access critically important, but **59%** of respondents' organizations do not monitor third-party access, up from 50% in 2022[iii].

**59%**
of organizations do not monitor third-party access

Of that 59%, the most cited reason for why third-party access isn't monitored was that organizations have confidence in the third party's ability to secure information (selected as a reason by **59%** of respondents). As previously noted, this was also the most cited reason for the 55% of organizations that don't evaluate third parties before a business engagement. Having confidence in third parties is an optimistic end goal – but it should be earned, with things like evaluations and proof of best-practice actions. But it could be that confidence in the third party is a reaction to the second most cited reason for why organizations don't monitor third-party access: a lack of internal resources to check or verify (**61%**).

Among the 41% of organizations that do monitor third-party access, **55%** do not automate the process. When even the third-party access monitoring processes at more than half of organizations are manual in nature, it's no wonder that so many cite lack of resources as a reason they don't.

## Organizations need to refine and mature their strategies for securing access for both internal users and third parties

**58%** of respondents shared that their organizations don't have a strategy for securing third-party access that is consistently applied (with **13%** saying they have no formal strategy for addressing these access risks). And in fact, only **34%** of organizations have solutions in place that address both internal and third-party privileged access risk – and because a comprehensive privileged access strategy requires taking both into consideration, it follows that there are at least some organizations who believe they have a consistent strategy but, in practice, don't have the correct tools in place.

Even with solutions in place, it's worth noting that only slightly more than half of organizations believe that they're effective or highly effective (**55%** of organizations with a VPAM solution, and **52%** of organizations with a PAM solution).

## Techniques and tactics organizations have adopted to address internal and third-party privileged access risks

Organizations are taking steps to ensure appropriate access to their high-value data assets. However, there is still much room for improvement as no more than **58%** of respondents reported that they leverage discrete best practice principles. The full range of responses is presented in the table below.

| Steps taken to ensure appropriate access to high-value data assets | |
|---|---|
| Enhanced physical controls (i.e., restricted control areas) | 35% |
| Restriction of network access | 44% |
| Enhanced identity and access management techniques | 29% |
| Ensure access entitlement is appropriate to the job function | 40% |
| Network segmentation / isolation | 58% |
| Remove access credentials when appropriate | 56% |
| Verification of a third party's need to have network access | 56% |
| Education of privileged users | 45% |
| Other | 5% |

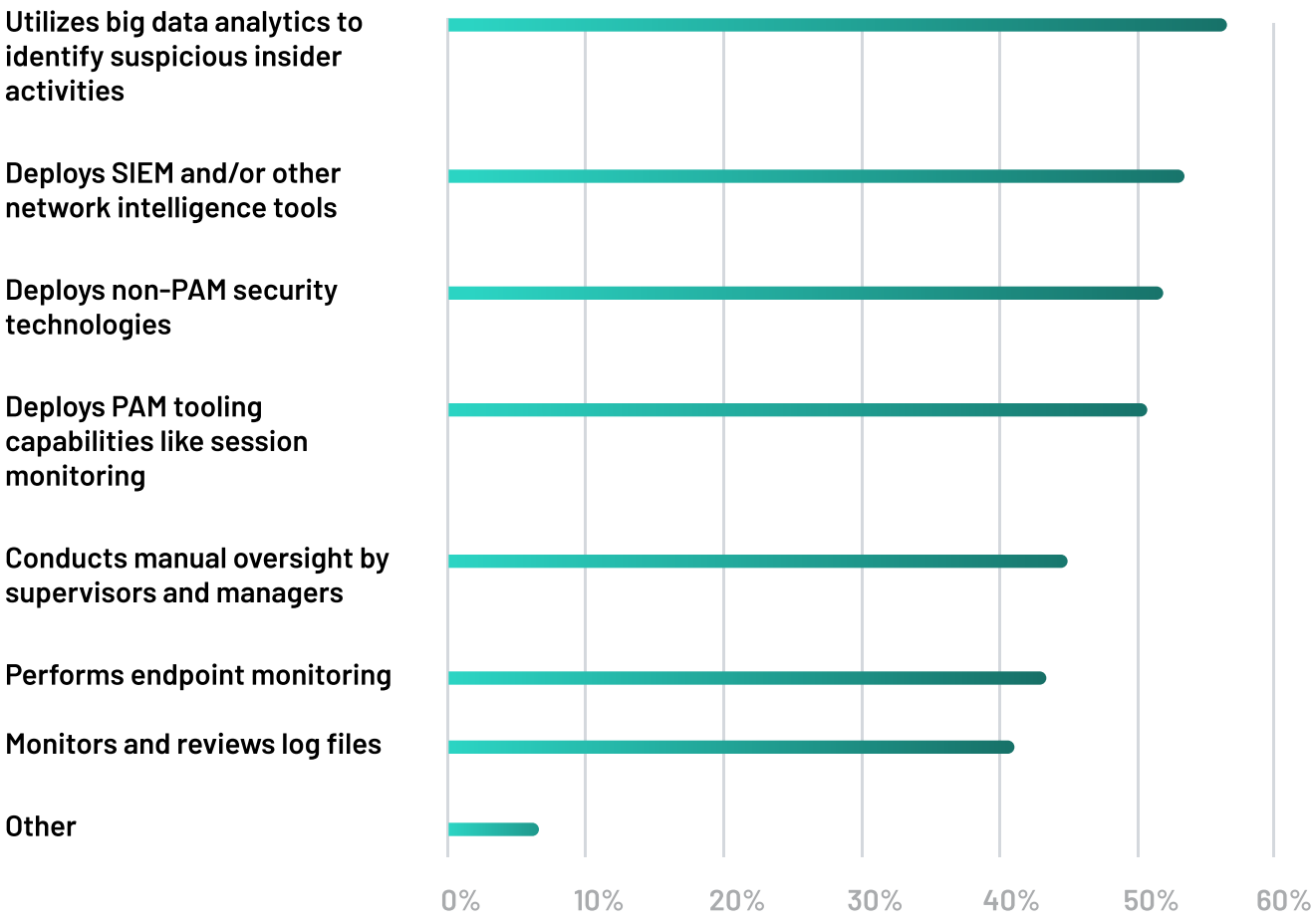
Organizations are doing what they can to reduce third-party access risks, but one specific tactic worth mentioning is the use of artificial intelligence (AI) and machine learning (ML). **40%** of respondents reported that their organizations use AI and ML as part of their strategy to reduce privileged access abuse. Top-cited reasons for AI and ML use included that it improves the efficiency of efforts to manage third-party and internal privileged access abuse (**59%**), it reduces human error related to managing third-party and internal privileged access (**51%**), and that it supports the IT security team dedicated to managing third-party and internal privileged access abuse (**50%**).

With only 40% of organizations using them as part of their privileged access strategies, it appears that AI and ML are underutilized tools. AI and ML can absolutely help bridge the resource gap that organizations are experiencing and can help cut down on manual processes. However, while AI and ML are being implemented to help support IT and security teams, and to increase efficiency, the data presented in this report shows that many organizations are still struggling with resourcing and time constraints. It is therefore critical to recognize that AI and ML are not a cure-all, and that IT and security teams must be clear, strategic, and intentional about where and how they implement these tools.

## A serious threat?

Most actions taken by a privileged user – internal, or a third party – won't be threats. But, intentional or not, some of them will be. Respondents shared how they go about determining if an action taken by an internal privileged user is truly a threat; their responses are presented in the chart below.

### How organizations determine if an action taken by an internal privileged user is truly a threat




That "utilizes big data analytics to identify suspicious insider activities" was the most reported, at **56%** of respondents, is promising. So, too, is that organizations deploy security information and event management (SIEM) and / or other network intelligence tools (**55%**). The same use of data can be leveraged for third-party access monitoring, analysis, and threat remediation.

# 03 Conclusion

Organizations still have work to do when it comes to privileged access – especially for third parties. When **64%** of respondents expect third party-related breaches to increase or stay the same over the next 12-14 months, but **58%** of organizations don't have a privileged access strategy that is consistently applied, the reality of combatting privileged access risks leaves much to be improved.

Organizations are aware of the threat, and while there are obstacles in the way – lack of resources, manual processes, and centralized control, to name a few – organizations are taking steps to ensure appropriate access to their networks and high-value assets. The opportunity is to ensure that those steps are strategic and consistently applied – for all privileged access needs.

Access security for both internal users and third parties needs to be made more efficient and effective. The threat is real and increasing – particularly from third-party network access – and the time to combat it is now.

# Methodology

A sampling frame of 46,528 IT and IT security practitioners who are familiar with their organizations' approach to managing privileged access abuse, including processes and technologies used to secure privileged access, both of third parties and internal users. The table below shows 2,172 total returns. Screening and reliability checks required the removal of 230 surveys. The final sample consisted of 1,942 surveys, or a 4.17% response rate.

| Sample response | Frequency | Percentage |
|---|---|---|
| Sampling frame | 46,528 | 100.00% |
| Total returns | 2,127 | 4.57% |
| Rejected or screened surveys | 230 | 0.49% |
| Final sample | 1,942 | 4.17% |

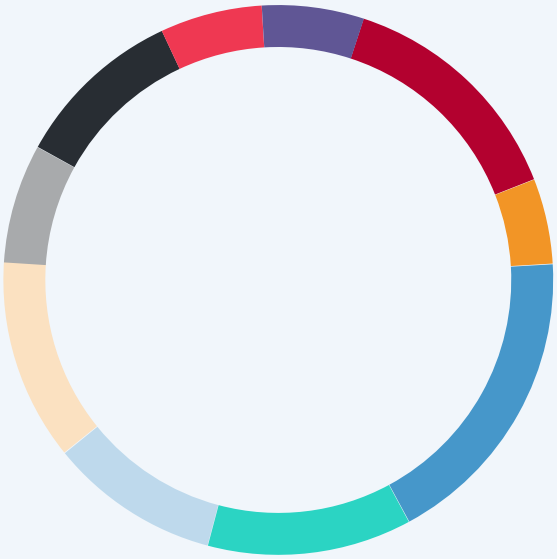
More information about respondents is shown in the charts below.

**Current position within the organization**

- Senior Executive **(6%)**
- Vice President **(6%)**
- Director **(19%)**
- Manager **(14%)**
- Supervisor **(9%)**
- Technician **(8%)**
- Staff **(21%)**
- Contractor **(9%)**
- Other **(8%)**

**Direct reporting channel of respondent or IT security leader**

- CEO/Executive committee **(6%)**
- Chief financial officer **(6%)**
- General Counsel **(14%)**
- Chief privacy officer **(5%)**
- Chief information officer **(18%)**
- Compliance officer **(12%)**
- Human resources VP **(10%)**
- Chief security officer **(12%)**
- Chief risk officer **(7%)**
- Other **(10%)**



**Organizational headcount**

- Less than 500 people **(12%)**
- 501 to 1,000 people **(19%)**
- 1,001 to 5,000 people **(22%)**
- 5,001 to 25,000 people **(21%)**
- 25,001 to 50,000 people **(13%)**
- 25,001 to 75,000 people **(13%)**

# Caveats

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 survey.

**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.

# 04 Appendix

| **Survey response** | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Total sampling frame | 17,118 | 11,005 | 10,505 | 7,900 | 46,528 |
| Total survey returns | 801 | 456 | 636 | 279 | 2,172 |
| Rejected surveys | 68 | 58 | 63 | 41 | 230 |
| Final sample | 733 | 398 | 573 | 238 | 1,942 |
| Response rate | 4.3% | 3.6% | 5.5% | 3.0% | 4.2% |

**Part 1. Screening questions**

| S1. How familiar are you with your organization's approach to managing privileged access abuse, including processes and technologies used to secure third party, vendor and privileged end user access to your network and corporate resources? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Very familiar | 37% | 29% | 45% | 38% | 37% |
| Familiar | 40% | 36% | 34% | 36% | 37% |
| Somewhat familiar | 23% | 35% | 21% | 26% | 26% |
| No familiarity (Stop) | 0% | 0% | 0% | 0% | 0% |
| Total | 100% | 100% | 100% | 100% | 100% |

| S2. How familiar are you with your organization's approach to securing privileged access, including IT admin access to sensitive corporate resources? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Very familiar | 31% | 30% | 35% | 47% | 36% |
| Familiar | 36% | 33% | 29% | 30% | 32% |
| Somewhat familiar | 33% | 37% | 36% | 23% | 32% |
| No familiarity (Stop) | 0% | 0% | 0% | 0% | 0% |
| Total | 100% | 100% | 100% | 100% | 100% |

| S3. What industry does your organization operate in? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Healthcare | 12% | 8% | 11% | 13% | 11% |
| Public sector | 21% | 25% | 23% | 25% | 23% |
| Industrial and manufacturing | 31% | 28% | 35% | 32% | 32% |
| Financial services | 36% | 39% | 31% | 30% | 34% |
| Other industry (Stop) | 0% | 0% | 0% | 0% | 0% |
| Total | 100% | 100% | 100% | 100% | 100% |

**Part 2. Background on reducing privileged access abuse**

| Q1. Does your organization have a VPAM and/or PAM solution as defined above? Please select one choice only. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes, a VPAM and PAM solution (please skip to Q2a) | 40% | 34% | 34% | 29% | 34% |
| Yes, a VPAM solution but not a PAM solution (please skip to Q2a) | 38% | 41% | 43% | 34% | 39% |
| Yes, a PAM solution but not a VPAM solution (please skip to Q2b) | 22% | 25% | 23% | 37% | 27% |
| Neither a VPAM or PAM solution (please skip to Q3) | 0% | 0% | 0% | 0% | 0% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q2a. Using the following 10-point scale, please rate how effective is your organization's **VPAM** solution is in reducing privileged access abuse from 1 = not effective to 10 = highly effective. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 8% | 12% | 9% | 10% | 10% |
| 3 or 4 | 14% | 11% | 13% | 15% | 13% |
| 5 or 6 | 19% | 21% | 26% | 21% | 22% |
| 7 or 8 | 35% | 33% | 32% | 33% | 33% |
| 9 or 10 | 24% | 23% | 20% | 21% | 22% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q2b. Using the following 10-point scale, please rate how effective is your organization's **PAM** solution is in reducing privileged access abuse from 1 = not effective to 10 = highly effective. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 11% | 13% | 12% | 12% | 12% |
| 3 or 4 | 13% | 14% | 15% | 14% | 14% |
| 5 or 6 | 18% | 22% | 23% | 23% | 22% |
| 7 or 8 | 32% | 33% | 30% | 30% | 31% |
| 9 or 10 | 26% | 18% | 20% | 21% | 21% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q3. Does your organization use artificial intelligence (AI) and machine learning (ML) as part of its strategy to reduce privileged access abuse? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 50% | 33% | 41% | 37% | 40% |
| No | 50% | 67% | 59% | 63% | 60% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q4. What are the benefits of using AI and/or ML in your organization's strategy to reduce privilege access abuse? Please select all that apply | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Improves the efficiency of efforts to manage third party and internal privilege access abuse | 59% | 55% | 63% | 57% | 59% |
| Improves the ability to detect third party and internal privilege user risks | 41% | 39% | 39% | 34% | 38% |
| Supports our IT security team dedicated to managing third party and internal privilege access abuse | 53% | 49% | 48% | 50% | 50% |
| Reduces data breaches and cyberattacks involving privileged access abuse | 46% | 41% | 45% | 42% | 44% |
| Reduces human error related to managing third-party and internal privileged access | 63% | 56% | 43% | 41% | 51% |
| Total | 262% | 240% | 238% | 224% | 241% |

| Q5. What best describes the maturity of your organization's strategy to address privileged access risks? Please select one choice only. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Our strategy is applied consistently across the entire organization | 45% | 38% | 50% | 34% | 42% |
| Our strategy is not applied consistently across the entire organization | 24% | 32% | 23% | 27% | 26% |
| Our strategy is ad hoc or informal | 17% | 18% | 19% | 21% | 19% |
| We have no formal strategy for addressing privileged access risks | 14% | 12% | 8% | 18% | 13% |
| Total | 100% | 100% | 100% | 100% | 100% |

**Part 3. Third party and vendor data breach and cyberattack experience**

| Q6. In the past 12 months, did your organization experience a data breach or cyberattack that involved one of your third parties/vendors accessing your organizations' network? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 42% | 51% | 51% | 42% | 47% |
| No (please skip to Q10) | **32%** | 34% | 32% | 35% | 33% |
| Unsure (please skip to Q10) | 26% | 15% | 17% | 23% | 20% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q7. Did the data breach or cyberattack cause the misuse of the organization's sensitive or confidential information, either directly or indirectly? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 45% | 40% | 55% | 39% | 44% |
| No | 24% | 34% | 29% | 32% | 30% |
| Unsure | 31% | 26% | 16% | 29% | 26% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q8. Were these data breaches or cyberattacks the result of a third party having too much privileged access? Too much privileged access can be defined as having access to more applications and information than is needed. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 36% | 32% | 34% | 35% | 34% |
| No | 24% | 32% | 40% | 29% | 31% |
| Unsure | 40% | 36% | 26% | 36% | 35% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q9. What were the consequences of these data breaches and cyberattacks? Please select all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Severed relationships with third party/vendor | 49% | 47% | 55% | 43% | 49% |
| The loss or theft of sensitive and confidential information | 53% | 54% | 55% | 48% | 53% |
| Regulatory fines | 60% | 49% | 47% | 45% | 50% |
| Ransom payment | 39% | 34% | 34% | 32% | 35% |
| Lawsuit | 41% | 37% | 43% | 41% | 41% |
| Loss of business partners | 37% | 44% | 40% | 44% | 41% |
| Loss of customers | 24% | 21% | 24% | 26% | 24% |
| Employee turnover | 27% | 32% | 33% | 32% | 31% |
| Loss of revenue | 22% | 32% | 45% | 45% | 36% |
| Loss of reputation | 21% | 19% | 18% | 15% | 18% |
| Other (please specify) | 8% | 9% | 8% | 5% | 8% |
| Total | 381% | 378% | 402% | 376% | 384% |

| Q10. How many third parties and vendors have access to your organization's network? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| None | 12% | 7% | 8% | 11% | 9% |
| Less than 5 | 14% | 18% | 13% | 18% | 16% |
| 5 to 10 | 14% | 12% | 14% | 11% | 13% |
| 11 to 20 | 17% | 17% | 19% | 17% | 18% |
| 21 to 30 | 20% | 20% | 21% | 22% | 21% |
| 31 to 40 | 11% | 10% | 12% | 11% | 11% |
| 41 to 50 | 8% | 11% | 9% | 6% | 9% |
| More than 50 | 4% | 6% | 4% | 4% | 5% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated average | 19.0 | 20.8 | 20.1 | 18.7 | 19.7 |

**The cost of third party and privileged access abuse data breaches and cyberattacks**

| Q11. In the past 12 months, approximately how much did it cost to restore access to third party and privileged access user? Please consider the costs associated with detecting, responding and recovering to a third-party data breach and privileged access abuse. This includes subsequent technical support including forensic investigations, incident response activities, help desk and customer service operations. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Less than $10,000 | 12% | 15% | 8% | 15% | 13% |
| $10,000 to $25,000 | 12% | 11% | 11% | 23% | 14% |
| $25,001 to $50,000 | 23% | 23% | 25% | 21% | 23% |
| $50,001 to $100,000 | 20% | 23% | 23% | 18% | 21% |
| $100,001 to $250,000 | 21% | 19% | 21% | 17% | 19% |
| More than $250,000 | 12% | 9% | 12% | 6% | 10% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated average | $96,075 | $86,550 | $98,700 | $72,400 | $87,556 |

| Q12. Do you anticipate data breaches caused by third parties will increase, decrease or stay at the same level over the next 12 to 24 months? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Increase | 45% | 41% | 38% | 36% | 40% |
| Decrease | 35% | 35% | 32% | 43% | 36% |
| Stay the same | 20% | 24% | 30% | 21% | 24% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q13. Approximately, how many hours each week are spent **analyzing and investigating** the security of third party and privileged access? Please estimate the aggregate hours of the IT security team. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Less than 5 | 10% | 13% | 11% | 12% | 11% |
| 5 to 10 | 9% | 8% | 10% | 12% | 10% |
| 11 to 25 | 12% | 11% | 15% | 13% | 13% |
| 26 to 50 | 14% | 19% | 15% | 14% | 16% |
| 51 to 100 | 17% | 14% | 12% | 18% | 15% |
| 101 to 250 | 20% | 15% | 12% | 15% | 15% |
| 251 to 500 | 10% | 11% | 14% | 12% | 12% |
| More than 500 | 8% | 9% | 11% | 4% | 8% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated average | 135.7 | 135.4 | 149.7 | 114.7 | 134.0 |

**Part 4. Attributions about third parties' and vendors' privileged access**

| Q14a. The number of cybersecurity incidents and data breaches involving third parties and vendors is increasing. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 31% | 26% | 27% | 25% | 27% |
| Agree | 21% | 21% | 20% | 21% | 21% |
| Unsure | 14% | 15% | 20% | 16% | 16% |
| Disagree | 12% | 17% | 16% | 18% | 16% |
| Strongly disagree | 22% | 21% | 17% | 20% | 20% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q14b. My organization's IT/IT security function makes ensuring the security of third parties' and vendors' remote access to its network a priority. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 23% | 21% | 23% | 24% | 23% |
| Agree | 24% | 25% | 23% | 23% | 24% |
| Unsure | 16% | 26% | 21% | 19% | 20% |
| Disagree | 11% | 8% | 15% | 14% | 12% |
| Strongly disagree | 26% | 20% | 18% | 20% | 21% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q14c. Managing third party permissions and remote access to our network can be overwhelming and a drain on our internal resources. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 25% | 22% | 21% | 21% | 22% |
| Agree | 21% | 22% | 22% | 23% | 22% |
| Unsure | 25% | 15% | 21% | 20% | 20% |
| Disagree | 20% | 18% | 22% | 16% | 19% |
| Strongly disagree | 9% | 23% | 14% | 20% | 17% |
| Total | 100% | 100% | 100% | 100% | 100% |

| 14d. Third parties' remote access to our network is becoming our organization's weakest attack surface. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 31% | 26% | 27% | 25% | 27% |
| Agree | 21% | 21% | 20% | 21% | 21% |
| Unsure | 14% | 15% | 20% | 16% | 16% |
| Disagree | 12% | 17% | 16% | 18% | 16% |
| Strongly disagree | 22% | 21% | 17% | 20% | 20% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q14e. Our organization provides third parties with enough access and nothing more to perform their designated responsibilities and nothing more. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 25% | 27% | 25% | 23% | 25% |
| Agree | 22% | 23% | 22% | 30% | 24% |
| Unsure | 12% | 20% | 25% | 17% | 19% |
| Disagree | 24% | 10% | 22% | 12% | 17% |
| Strongly disagree | 17% | 20% | 6% | 18% | 15% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q14f. Our organization has visibility into the level of access and permissions internal and external users have. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 27% | 26% | 21% | 25% | 25% |
| Agree | 22% | 21% | 25% | 21% | 22% |
| Unsure | 26% | 15% | 23% | 16% | 20% |
| Disagree | 12% | 17% | 16% | 18% | 16% |
| Strongly disagree | 13% | 21% | 15% | 20% | 17% |
| Total | 100% | 100% | 100% | 100% | 100% |

**Part 5. The challenges of reducing cyberattacks and data breaches caused by third parties and vendors**

| Q15. What are the most significant barriers to reducing third-party and privileged access risks? Please select your top three choices only. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Insufficient resources or budget | 65% | 46% | 27% | 25% | 41% |
| Insufficient visibility of people and business processes | 42% | 36% | 37% | 32% | 37% |
| Insufficient assessment of risks | 35% | 36% | 44% | 46% | 40% |
| Difficulty in hiring and training which leads to a lack of skilled or expert personnel | 40% | 37% | 36% | 48% | 40% |
| Lack of leadership | 22% | 42% | 47% | 42% | 38% |
| Lack of oversight or governance | 54% | 53% | 47% | 45% | 50% |
| Complexity of compliance and regulatory requirements | 35% | 45% | 59% | 55% | 48% |
| Other (Please specify) | 7% | 5% | 3% | 7% | 6% |
| Total | 300% | 300% | 300% | 300% | 300% |

| Q16. Please check all steps taken to **ensure appropriate access** to high-value data assets. Please check all that apply | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Enhanced physical controls (i.e., restricted control areas) | 34% | 44% | 29% | 33% | 35% |
| Restriction of network access | 45% | 45% | 49% | 37% | 44% |
| Enhanced identity and access management techniques | 23% | 26% | 33% | 34% | 29% |
| Ensure access entitlement is appropriate to the job function | 36% | 50% | 43% | 32% | 40% |
| Network segmentation/isolation | 54% | 67% | 51% | 60% | 58% |
| Remove access credentials when appropriate | 45% | 66% | 56% | 55% | 56% |
| Verification of a third party's need to have network access | 67% | 56% | 57% | 45% | 56% |
| Education of privileged users | 45% | 56% | 44% | 34% | 45% |
| Other (Please specify) | 6% | 5% | 6% | 4% | 5% |
| Total | 355% | 415% | 368% | 334% | 368% |

| Q17. Does your organization have a comprehensive inventory of all third parties with access to its network? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes, please skip to Q19 | 54% | 45% | 56% | 46% | 50% |
| No | 38% | 46% | 35% | 46% | 41% |
| Unsure | 8% | 9% | 9% | 8% | 9% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q18. If no or unsure, why? Please check all that apply | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Lack of resources to track third parties | 43% | 41% | 45% | 50% | 45% |
| No centralized control over third-party relationships | 39% | 38% | 42% | 27% | 37% |
| Complexity in third-party relationships | 21% | 24% | 23% | 41% | 27% |
| Cannot keep track due to frequent turnover in third parties | 19% | 21% | 16% | 33% | 22% |
| Not a priority | 15% | 21% | 16% | 15% | 17% |
| Other (please specify) | 6% | 8% | 9% | 6% | 7% |
| Total | 143% | 153% | 151% | 172% | 155% |

| Q19. Which part of your organization is **most** responsible for managing and granting access to third parties and vendors? Please select one choice only. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Information technology | 15% | 15% | 16% | 19% | 16% |
| Information security | 15% | 16% | 22% | 19% | 18% |
| Compliance/general counsel | 19% | 17% | 16% | 16% | 17% |
| Internal audit | 13% | 16% | 13% | 17% | 15% |
| Human resources | 12% | 11% | 13% | 9% | 11% |
| Risk management | 11% | 11% | 7% | 7% | 9% |
| Lines of business | 15% | 15% | 13% | 13% | 14% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q20a. Using the following 10-point scale, please rate how effective your organization is in **mitigating remote access** third-party risks. (1 = not effective to 10 = highly effective) | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 9% | 8% | 11% | 12% | 10% |
| 3 or 4 | 13% | 12% | 15% | 14% | 13% |
| 5 or 6 | 21% | 23% | 23% | 20% | 22% |
| 7 or 8 | 33% | 32% | 32% | 31% | 32% |
| 9 or 10 | 24% | 25% | 19% | 23% | 23% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q20b. Using the following 10-point scale, please rate how effective your organization is in **detecting remote access** third-party risks. (1 = not effective to 10 = highly effective) | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 9% | 13% | 9% | 10% | 10% |
| 3 or 4 | 12% | 10% | 13% | 15% | 12% |
| 5 or 6 | 21% | 23% | 26% | 21% | 23% |
| 7 or 8 | 33% | 33% | 32% | 33% | 33% |
| 9 or 10 | 25% | 21% | 20% | 21% | 22% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q20c. Using the following 10-point scale, please rate your organization's effectiveness in **preventing** third parties from sharing credentials in the form of usernames and/or passwords. 1 = not effective to 10 = highly effective) | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 10% | 12% | 8% | 10% | 10% |
| 3 or 4 | 12% | 11% | 14% | 14% | 13% |
| 5 or 6 | 20% | 21% | 23% | 20% | 21% |
| 7 or 8 | 33% | 33% | 29% | 32% | 32% |
| 9 or 10 | 25% | 23% | 26% | 24% | 24% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q20d. Using the following 10-point scale, please rate the effectiveness of your organization in **controlling** third-party access to your network. 1 = not effective to 10 = highly effective) | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 8% | 14% | 10% | 11% | 11% |
| 3 or 4 | 13% | 12% | 12% | 16% | 13% |
| 5 or 6 | 21% | 23% | 26% | 20% | 23% |
| 7 or 8 | 34% | 31% | 32% | 31% | 32% |
| 9 or 10 | 24% | 20% | 20% | 22% | 21% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q20e. Using the following 10-point scale, please rate the effectiveness of your third parties in achieving compliance with security and privacy regulations that affect your organization. 1 = not effective to 10 = highly effective) | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| 1 or 2 | 11% | 12% | 11% | 8% | 11% |
| 3 or 4 | 12% | 13% | 12% | 14% | 13% |
| 5 or 6 | 17% | 22% | 23% | 22% | 21% |
| 7 or 8 | 35% | 31% | 31% | 32% | 32% |
| 9 or 10 | 25% | 22% | 23% | 24% | 23% |
| Total | 100% | 100% | 100% | 100% | 100% |

**Part 6. Reducing internal privileged access management risks**

| Q21. Did your organization experience data breaches or cyberattacks involving internal users with privileged access to your organization's network? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 46% | 43% | 50% | 36% | 44% |
| No (please skip to Q25a) | 50% | 49% | 41% | 54% | 48% |
| Unsure | 4% | 8% | 9% | 10% | 8% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q22. Did the data breach or cyberattack cause the misuse of the organization's sensitive or confidential information, either directly or indirectly? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 44% | 41% | 49% | 29% | 41% |
| No | 50% | 52% | 42% | 44% | 47% |
| Unsure | 6% | 7% | 9% | 27% | 12% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q23. Were these data breaches or cyberattacks caused by giving too much privileged access to internal users? Too much privileged access can be defined as giving access to more applications and information than is needed. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 51% | 47% | 54% | 27% | 45% |
| No | 43% | 46% | 40% | 46% | 44% |
| Unsure | 6% | 7% | 6% | 27% | 11% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q24. What were the consequences of these attacks? Please select all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| The loss or theft of sensitive and confidential information | 64% | 54% | 39% | 53% | 53% |
| Regulatory fines | 32% | 23% | 31% | 32% | 30% |
| Ransom payment | 24% | 26% | 25% | 23% | 25% |
| Lawsuit | 23% | 21% | 26% | 26% | 24% |
| Loss of business partners | 47% | 55% | 57% | 44% | 51% |
| Loss of customers | 36% | 32% | 24% | 26% | 30% |
| Employee turnover | 45% | 41% | 43% | 42% | 43% |
| Loss of revenue | 34% | 43% | 33% | 43% | 38% |
| Loss of reputation | 43% | 41% | 45% | 46% | 44% |
| Other (please specify) | 5% | 6% | 4% | 5% | 5% |
| Total | 353% | 342% | 327% | 340% | 341% |

| Q25a. Managing internal privileged access permissions and remote access to our network can be overwhelming and a drain on our internal resources. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 25% | 23% | 25% | 26% | 25% |
| Agree | 23% | 26% | 21% | 22% | 23% |
| Unsure | 14% | 26% | 19% | 15% | 19% |
| Disagree | 11% | 15% | 20% | 14% | 15% |
| Strongly disagree | 27% | 10% | 15% | 23% | 19% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q25b. Our organization is able to provide employees with enough privileged access and nothing more to perform their designated responsibilities and nothing more. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Strongly agree | 24% | 24% | 22% | 21% | 23% |
| Agree | 26% | 21% | 25% | 25% | 24% |
| Unsure | 20% | 23% | 19% | 16% | 20% |
| Disagree | 9% | 8% | 14% | 15% | 12% |
| Strongly disagree | 21% | 24% | 20% | 23% | 22% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q26. How many employees have privileged access rights? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| None | 21% | 11% | 3% | 5% | 10% |
| Less than 5 | 13% | 17% | 12% | 14% | 14% |
| 5 to 10 | 12% | 13% | 24% | 16% | 16% |
| 11 to 20 | 13% | 5% | 14% | 23% | 14% |
| 21 to 30 | 16% | 13% | 17% | 16% | 15% |
| 31 to 40 | 15% | 25% | 20% | 14% | 18% |
| 41 to 50 | 6% | 14% | 7% | 7% | 9% |
| More than 50 | 4% | 2% | 3% | 5% | 4% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated average | 17.6 | 21.8 | 20.5 | 20.1 | 20.0 |

| Q27a. Does your organization have a comprehensive inventory of all privileged internal users with access to its network? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 55% | 42% | 58% | 32% | 47% |
| No | 39% | 52% | 35% | 46% | 43% |
| Unsure | 6% | 6% | 7% | 22% | 10% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q27b. If no or unsure, why? Please check all that apply | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Lack of resources to track internal user privileges | 43% | 39% | 54% | 27% | 41% |
| No centralized control over internal user privileges | 47% | 37% | 44% | 47% | 44% |
| Complexity of multiple internal tech platforms | 55% | 46% | 55% | 54% | 53% |
| Cannot keep track due to frequent employee turnover | 23% | 32% | 42% | 38% | 34% |
| Not a priority | 28% | 39% | 16% | 27% | 28% |
| Other (please specify) | 6% | 8% | 5% | 7% | 7% |
| Total | 202% | 201% | 216% | 200% | 205% |

| Q28. How does your organization protect itself from privileged access user abuse? Please select all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Performs thorough background checks before issuance of privileged credentials | 56% | 54% | 62% | 56% | 57% |
| Conducts manual oversight by supervisors and managers | 61% | 56% | 58% | 45% | 55% |
| Monitors and reviews provisioning systems | 56% | 54% | 38% | 37% | 46% |
| Reviews and acts upon threat intelligence | 45% | 46% | 55% | 45% | 48% |
| Deploys IAM policy monitoring tools | 44% | 47% | 56% | 51% | 50% |
| Conducts regular privileged user training programs | 37% | 39% | 47% | 39% | 41% |
| Other (please specify) | 7% | 3% | 4% | 5% | 5% |
| Total | 306% | 299% | 320% | 278% | 301% |

| Q29. Do you expect the risk of privileged user abuse to increase, decrease or stay at the same level over the next 12 to 24 months? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Increase | 34% | 29% | 34% | 38% | 34% |
| Stay the same | 32% | 37% | 37% | 27% | 33% |
| Decrease | 34% | 34% | 29% | 35% | 33% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q30. How does your organization determine if an action taken by a privileged user is truly a threat? Select all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Monitors and reviews log files | 36% | 34% | 35% | 57% | 41% |
| Conducts manual oversight by supervisors and managers | 45% | 46% | 45% | 45% | 45% |
| Deploys SIEM and/or other network intelligence tools | 57% | 55% | 53% | 55% | 55% |
| Utilizes big data analytics to identify suspicious insider activities | 61% | 59% | 56% | 47% | 56% |
| Deploys PAM tooling capabilities like session monitoring | 54% | 54% | 47% | 48% | 51% |
| Deploys non-PAM security technologies | 38% | 61% | 58% | 53% | 53% |
| Performs endpoint monitoring | 43% | 46% | 44% | 43% | 44% |
| Other (please specify) | 5% | 6% | 7% | 8% | 7% |
| Total | 339% | 361% | 345% | 356% | 350% |

| Q31. What are the main problems your organization faces in granting and enforcing privileged user access rights? Please select your top five choices. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Takes too long to grant access to privileged users (not meeting our SLAs with the business) | 63% | 63% | 63% | 56% | 61% |
| Too expensive to monitor and control all privileged users | 62% | 59% | 64% | 57% | 61% |
| Too much staff required to monitor and control all privileged users | 54% | 50% | 65% | 56% | 56% |
| Cannot apply access policy controls at point of change request | 67% | 71% | 59% | 70% | 67% |
| Granting access to privileged users is staggered (not granted at the same time) | 54% | 60% | 64% | 65% | 61% |
| Cannot keep pace with the number of access change requests that come in on a regular basis | 55% | 56% | 63% | 56% | 58% |
| Lack of a consistent approval process for access and a way to handle exceptions | 49% | 37% | 23% | 47% | 39% |
| Difficult to audit and validate privileged user access changes | 33% | 28% | 26% | 29% | 29% |
| Burdensome process for business users requesting access | 25% | 25% | 21% | 21% | 23% |
| No common language exists for how access is requested that will work for both IT and the business | 31% | 45% | 44% | 37% | 39% |
| Other (please specify) | 7% | 6% | 8% | 6% | 7% |
| Total | 500% | 500% | 500% | 500% | 500% |

**Part 7. Security in the third-party ecosystem**

| Q32a. Do you evaluate the security and privacy practices of all third parties before you engage them in a business relationship that requires providing access to sensitive or confidential information? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 51% | 47% | 38% | 45% | 45% |
| No (please skip to Q33) | 49% | 53% | 62% | 55% | 55% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q32b. If yes, how do you perform this evaluation? Please check all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Review written policies and procedures | 54% | 52% | 47% | 46% | 50% |
| Acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices | 51% | 45% | 51% | 48% | 49% |
| Obtain indemnification from the third party in the event of a data breach | 44% | 38% | 45% | 37% | 41% |
| Conduct an assessment of the third party's security and privacy practices | 52% | 47% | 56% | 43% | 50% |
| Obtain a self-assessment conducted by the third party | 44% | 51% | 34% | 35% | 41% |
| Obtain references from other organizations that engage the third party | 31% | 29% | 27% | 33% | 30% |
| Obtain evidence of security certification such as NIST ISO 2700/27002 or SOC. | 15% | 16% | 21% | 22% | 19% |
| Other (please specify) | 8% | 5% | 9% | 6% | 7% |
| Total | 299% | 283% | 290% | 270% | 286% |

| Q33. If no, why don't you perform an evaluation? Please check all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| We don't have the internal resources to check or verify | 61% | 59% | 61% | 61% | 61% |
| We have confidence in the third party's ability to secure information | 63% | 58% | 63% | 63% | 62% |
| We rely on the business reputation of the third-party | 58% | 55% | 58% | 58% | 57% |
| We have insurance that limits our liability in the event of a data breach | 47% | 44% | 49% | 47% | 47% |
| The third party is subject to data protection regulations that are intended to protect our information | 43% | 41% | 43% | 43% | 43% |
| The third party is subject to contractual terms | 39% | 32% | 32% | 32% | 34% |
| The data shared with the third party is not considered sensitive or confidential | 41% | 34% | 36% | 31% | 36% |
| Total | 352% | 323% | 342% | 335% | 338% |

| Q34a. Are third parties with access to your organization's sensitive and confidential information monitored? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 52% | 41% | 38% | 33% | 41% |
| No (please skip to Q35) | 48% | 59% | 62% | 67% | 59% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q34b. If yes, does your organization automate the monitoring of third parties? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Yes | 56% | 43% | 38% | 44% | 45% |
| No | 44% | 57% | 62% | 56% | 55% |
| Total | 100% | 100% | 100% | 100% | 100% |

| Q35. If no, why doesn't your organization monitor the third parties' access to its sensitive and confidential information? Please check all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| We don't have the internal resources to check or verify | 59% | 48% | 38% | 29% | 44% |
| We have confidence in the third party's ability to secure information | 63% | 61% | 57% | 56% | 59% |
| We rely on the business reputation of the third party | 44% | 56% | 47% | 32% | 45% |
| We have insurance that limits our liability in the event of a data breach | 41% | 44% | 35% | 23% | 36% |
| The third party is subject to data protection regulations that are intended to protect our information | 34% | 29% | 31% | 27% | 30% |
| The third party is subject to contractual terms | 27% | 23% | 23% | 31% | 26% |
| The data shared with the third party is not considered sensitive or confidential | 25% | 26% | 26% | 24% | 25% |
| The third party will not allow us to independently monitor or verify their security and privacy activities | 19% | 24% | 12% | 25% | 20% |
| Other (please specify) | 7% | 9% | 8% | 9% | 8% |
| Total | 319% | 320% | 277% | 256% | 293% |

| Q36. To ensure third parties' compliance with privacy and security regulations, does your organization take any of the following steps? Please check all that apply. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Identify and categorize third-party vendor and partner access needs | 58% | 55% | 49% | 58% | 55% |
| Perform access assessments for each vendor and partner | 62% | 59% | 45% | 63% | 57% |
| No vendor-supplied security parameters or default passwords | 55% | 48% | 52% | 49% | 51% |
| Implement least privileged access | 41% | 52% | 45% | 43% | 45% |
| Insist on unique user access credentials | 48% | 49% | 44% | 53% | 49% |
| Encrypt transmissions for all open or public networks | 45% | 51% | 45% | 45% | 47% |
| Track and monitor all access to network resources and critical data | 39% | 36% | 34% | 34% | 36% |
| Capture detailed audit logs of each support session | 36% | 36% | 36% | 36% | 36% |
| Install and maintain a firewall configuration to protect data | 34% | 40% | 38% | 36% | 37% |
| Develop secure application and system implementation | 41% | 44% | 37% | 39% | 40% |
| Protect all systems against malware and regularly monitor anti-virus protections | 36% | 27% | 33% | 29% | 31% |
| Restrict physical access | 34% | 35% | 45% | 46% | 40% |
| Other (please specify) | 9% | 6% | 9% | 8% | 8% |
| Total | 538% | 538% | 512% | 539% | 532% |

**Part 8. Budget and investment in the cybersecurity infrastructure**

| Q37. What range best describes your organization's **annual IT security budget**? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Less than $1 million | 6% | 5% | 4% | 9% | 6% |
| $1 to $10 million | 9% | 8% | 7% | 9% | 8% |
| $11 to $25 million | 11% | 9% | 12% | 13% | 11% |
| $26 to $50 million | 13% | 11% | 14% | 13% | 13% |
| $51 to $100 million | 14% | 15% | 15% | 14% | 15% |
| $101 to $250 million | 21% | 22% | 25% | 16% | 21% |
| $251 to $500 million | 13% | 19% | 14% | 13% | 15% |
| More than $500 million | 13% | 11% | 9% | 13% | 11% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated average | $174,945,000 | $187,765,000 | $164,885,000 | $166,570,000 | $170,791,250 |

| Q38. What percentage of your company's annual IT security budget is dedicated to reducing third-party and vendor risks and securing privileged access. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| None | 0% | 0% | 0% | 0% | 0% |
| Less than 5% | 9% | 8% | 8% | 9% | 9% |
| 5% to 10% | 12% | 13% | 11% | 18% | 13% |
| 11% to 15% | 14% | 15% | 13% | 13% | 14% |
| 16% to 20% | 17% | 12% | 12% | 16% | 14% |
| 21% to 30% | 20% | 21% | 23% | 12% | 19% |
| 31% to 50% | 16% | 15% | 21% | 13% | 16% |
| More than 50% | 12% | 16% | 12% | 19% | 15% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated average | 24% | 26% | 26% | 25% | 25% |

**Part 9. Demographics and organizational characteristics**

| D1. What organizational level best describes your current position? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Senior Executive | 6% | 5% | 5% | 7% | 6% |
| Vice president | 5% | 7% | 8% | 5% | 6% |
| Director | 21% | 19% | 17% | 20% | 19% |
| Manager | 15% | 13% | 12% | 14% | 14% |
| Supervisor | 8% | 9% | 9% | 9% | 9% |
| Technician | 9% | 8% | 9% | 8% | 8% |
| Staff | 21% | 22% | 22% | 19% | 21% |
| Contractor | 9% | 8% | 9% | 9% | 9% |
| Other | 6% | 9% | 9% | 9% | 8% |
| Total | 100% | 100% | 100% | 100% | 100% |

| D2. Check the **Primary Person** you or your IT security leader reports to within the organization. | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| CEO/executive Committee | 6% | 5% | 7% | 5% | 6% |
| Chief financial officer | 7% | 5% | 6% | 5% | 6% |
| General counsel | 13% | 16% | 13% | 15% | 14% |
| Chief privacy officer | 5% | 5% | 5% | 5% | 5% |
| Chief information officer | 18% | 18% | 18% | 18% | 18% |
| Compliance officer | 12% | 13% | 11% | 12% | 12% |
| Human resources VP | 9% | 10% | 10% | 13% | 10% |
| Chief security officer | 12% | 10% | 12% | 12% | 12% |
| Chief risk officer | 8% | 8% | 8% | 4% | 7% |
| Other | 10% | 10% | 10% | 11% | 10% |
| Total | 100% | 100% | 100% | 100% | 100% |

| D3. What is the worldwide headcount of your organization? | US | UK | DE | AU | Consolidated |
|---|---|---|---|---|---|
| Less than 500 people | 12% | 11% | 10% | 13% | 12% |
| 501 to 1,000 people | 19% | 20% | 16% | 21% | 19% |
| 1,001 to 5,000 people | 21% | 21% | 23% | 22% | 22% |
| 5,001 to 25,000 people | 23% | 23% | 23% | 16% | 21% |
| 25,001 to 75,000 people | 13% | 13% | 13% | 14% | 13% |
| More than 75,000 people | 12% | 12% | 15% | 14% | 13% |
| Total | 100% | 100% | 100% | 100% | 100% |