



20
25

_state of

CYBERSECURITY

REPORT

AN IN-HOUSE
PERSPECTIVE



ACC Foundation
Association of Corporate Counsel

_table of (contents):



INTRODUCTION	3
KEY FINDINGS	5
STRUCTURE, LEADERSHIP, AND GOVERNANCE	8
RESOURCING AND TECHNOLOGY	20
AWARENESS, TRAINING, AND POLICIES	30
THIRD-PARTY RISK MANAGEMENT	41
PARTICIPANT PROFILE	54
METHODOLOGY	56

_introduction:

The digital age has fundamentally reshaped the risk landscape for organizations, with cybersecurity emerging as a paramount concern. No longer solely a technical issue relegated to IT departments, cybersecurity now presents complex legal, reputational, and operational challenges that demand strategic attention from the highest levels of leadership. This report explores the role of Chief Legal Officers (CLOs) and their legal departments in this complex terrain, revealing a significant shift towards greater legal leadership in cybersecurity strategy, implementation, and oversight.

Based on a survey of 278 in-house legal professionals across 16 countries and 20 industries, the findings paint a clear picture: cybersecurity is no longer just about firewalls and antivirus software; it's about legal liability, regulatory compliance, business continuity, and ultimately, protecting the organization's reputation and bottom line. This necessitates a proactive and informed legal perspective. In-house counsel must recognize that cybersecurity is not simply a technical problem to be solved by IT; it's a strategic imperative that requires their expertise in contract negotiation, regulatory compliance, data privacy, incident response, and risk management. Several key trends highlight this evolving reality:

CLOs are taking charge:

The strategic influence of CLOs in cybersecurity is rapidly expanding. They are increasingly involved in cybersecurity teams, holding leadership roles, and regularly reporting to the board on these critical matters. This growing involvement reflects a crucial understanding: cybersecurity breaches are not just IT issues; they are legal and governance crises waiting to happen.

Dedicated cyber expertise is on the rise:

Legal departments are increasingly prioritizing dedicated cybersecurity expertise by hiring specialized in-house counsel. This investment in cyber talent, often at senior executive levels, demonstrates a commitment to proactive risk management and a recognition of the complex legal landscape surrounding data protection and cybersecurity.

Breach concerns are shifting:

While reputational damage remains a significant concern, organizations are increasingly focused on the legal and operational risks associated with breaches, including liability to data subjects and threats to business continuity. This shift highlights the growing awareness of the multifaceted impact of cyberattacks and the need for comprehensive legal strategies to mitigate these risks.

Training and policies are becoming more robust:

Mandatory cybersecurity training for all employees is now nearly ubiquitous, reflecting a growing understanding of the human element in cybersecurity. Furthermore, legal teams are playing a crucial role in developing and updating key company policies related to data security, emerging technologies like AI, and third-party risk management.

Vendor risk management is maturing:

As organizations increasingly rely on third-party vendors, legal departments are playing a more active role in evaluating vendor cybersecurity practices and managing third-party risks. This heightened scrutiny reflects the understanding that a breach at a vendor can have just as devastating consequences as a direct attack.

The ACC Foundation is pleased to share this report, serving as a call to action for in-house counsel to embrace their expanding role, develop their cybersecurity expertise, and proactively address the legal and regulatory challenges presented by this ever-evolving threat landscape. By taking a leadership role in cybersecurity, in-house counsel can protect their organizations from significant financial, reputational, and legal harm, ensuring business continuity and building a more resilient future.



_Veta T. Richardson
Foundation President
President & CEO
Association of
Corporate Counsel



_Jennifer Chen
Executive Director
ACC Foundation

_key(findings):



The Strategic Influence of CLOs in Cybersecurity Continues to Expand

01

The role of the CLO in cybersecurity is significantly expanding into a more integrated leadership position. While cybersecurity leadership often resides with IT heads, CLOs are increasingly involved in cybersecurity teams (50 percent), holding leadership roles (38 percent), and regularly reporting to the board on cybersecurity matters, with a notable decrease in those who never report (from 28 percent in 2022 to 16 percent in 2025). This shift reflects a growing recognition of the legal and governance implications of cybersecurity, driving a demand for CLO expertise in incident response, strategic planning, and board-level communication.

One-Third of Legal Departments Now Have a Dedicated In-house Cybersecurity Lawyer

02

Legal departments are increasingly prioritizing dedicated cybersecurity expertise, demonstrated by a significant rise in the number of departments with dedicated cyber law expertise (from 22 percent in 2022 to 32 percent in 2025) and a growing interest in adding in-house cyber counsel (with those planning or considering hiring increasing from 13 percent to 18 percent). This trend is further underscored by a shift toward hiring cybersecurity counsel at senior executive levels (from 56 percent to 68 percent), reflecting the increasing strategic importance of cybersecurity. These senior roles often encompass broad responsibility for coordinating cyber law strategy across the entire organization.

03

Top Breach Concerns: Reputation, Liability, and Business Continuity

While reputational damage remains a leading concern (70 percent), though slightly decreased from 81 percent in 2015, liability to data subjects (61 percent) and threats to business continuity (60 percent) have significantly risen as top cybersecurity breach concerns, indicating a growing awareness of legal and operational risks. Loss of proprietary information (44 percent) and regulatory action (43 percent) also remain significant concerns, but to a lesser degree, further highlighting the need for comprehensive cybersecurity strategies that address a wide range of potential impacts beyond just reputational damage.

04

Nearly All Organizations Now Require Mandatory Cybersecurity Training for All Employees

Organizations are increasingly prioritizing employee cybersecurity training, demonstrated by a significant rise in mandatory training (from 62 percent in 2018 to 95 percent in 2025) as well as the introduction of more frequent training (42 percent required annual training in 2018 compared to 63 percent in 2025). The dramatic increase underscores a clear industry-wide shift towards recognizing the critical role of regular, comprehensive cybersecurity education in strengthening security posture and combating evolving threats.

05

Key Company Policies Focus on Data Security and Emerging Technology

Document retention (81 percent), acceptable use (78 percent), and password security (73 percent) remain the most prevalent company policies, reflecting core concerns around data management, resource utilization, and access control. The increasing adoption of “bring your own device” (65 percent) and, notably, the emergence of AI policies (62 percent) highlight organizations’ proactive approach to addressing the security and governance challenges posed by evolving technologies and work styles, emphasizing the crucial role of legal departments in regularly reviewing and updating these policies to maintain effectiveness and compliance.

06

Legal teams Are Gaining Confidence in Vendor Cybersecurity as Evaluation Practices Improve

In-house counsel confidence in vendors' cybersecurity capabilities has modestly improved over time, with those "very confident" rising to 13 percent and those "somewhat confident" remaining high at 70 percent, while those "not at all confident" declining to 13 percent. This increased confidence correlates with a significant increase in organizations now actively evaluating their vendors (from 74 percent to 83 percent) and a rise in the use of rigorous evaluation methods like questionnaires (52 percent) and proof of certification (51 percent), demonstrating a positive trend towards more thorough vendor risk management.

07

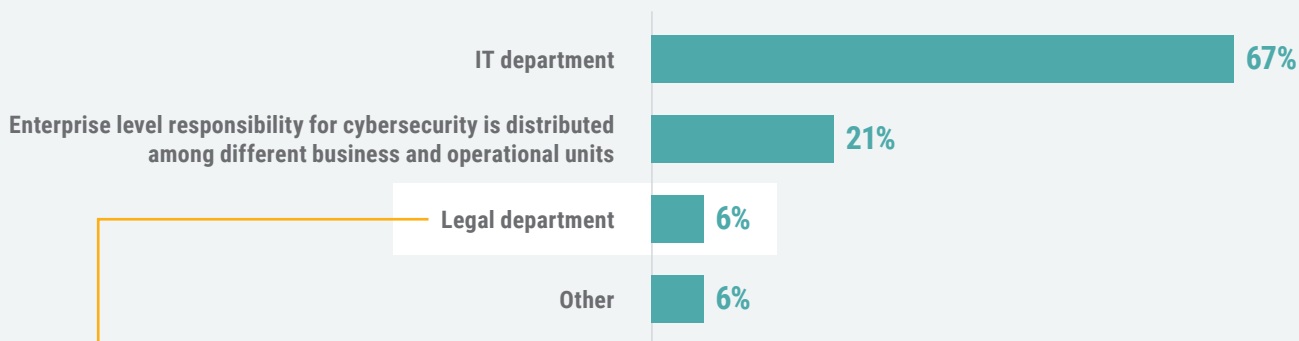
Legal Departments Are Playing an Increasingly Active Role in Third-Party Risk Management

Legal departments are becoming increasingly involved in third-party risk management, with those "often involved" rising from 31 percent to 38 percent and those "sometimes involved" slightly increasing to 40 percent, while the percentage of those "never involved" decreased from 18 percent to 13 percent, demonstrating a growing recognition of the legal department's essential role in mitigating third-party risks and ensuring compliance.

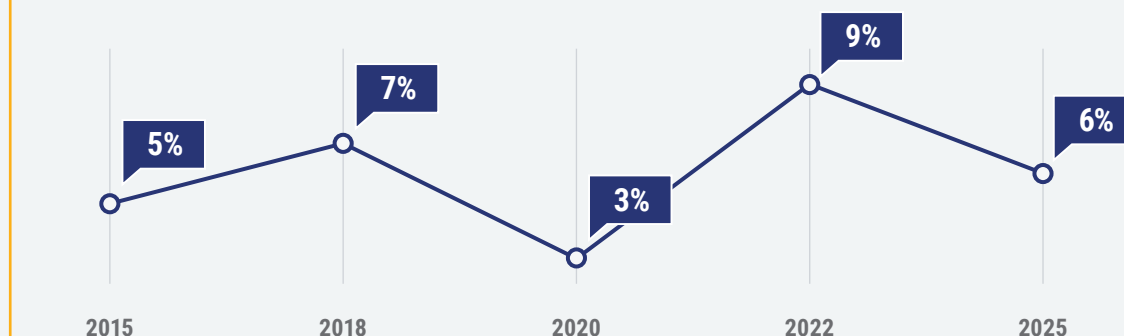
//structure, leadership, and governance

Cybersecurity responsibility overwhelmingly falls to the IT department, according to 67 percent of survey participants. While 21 percent reported a distributed approach, with various business and operational units sharing responsibility, only a small fraction cited the legal department (six percent) or other departments (six percent) as the primary lead. These findings suggest that while IT is generally seen as the central authority for enterprise cybersecurity management, some organizations opt for a more decentralized model. Traditionally, under 10 percent of participants indicate that cybersecurity is primarily housed in the legal department.

Q: Which department or function is primarily responsible for cybersecurity at the enterprise level?



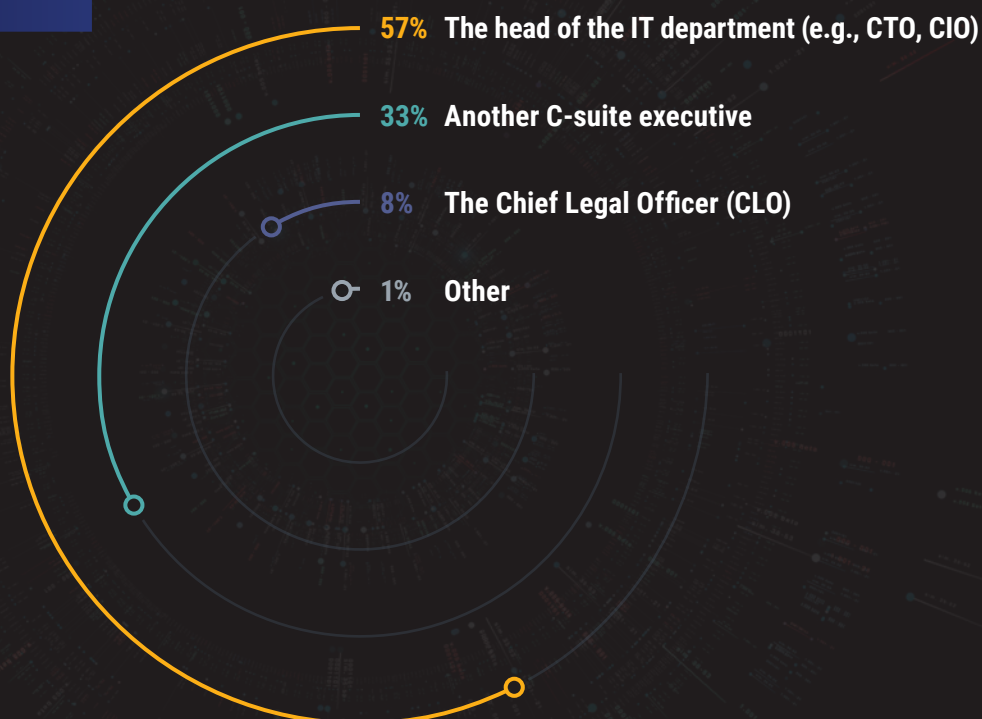
>> Organizations where cybersecurity is primarily housed in Legal



Fifty-seven percent of respondents reported that their head of cybersecurity reports to the head of IT, such as the Chief Technology Officer (CTO) or Chief Information Officer (CIO). One-third indicated that the cybersecurity lead reports to another C-suite executive, including the Chief Information Security Officer (CISO), Chief Operating Officer (COO), Chief Privacy Officer (CPO), or directly to the CEO or President. Only eight percent specified the Chief Legal Officer, and one percent reported other reporting structures.

These findings suggest a common organizational structure where cybersecurity falls under the IT umbrella, perhaps reflecting a perception of cybersecurity as primarily a technical domain. This placement within IT stems from the department's inherent technical expertise, positioning it to manage the day-to-day complexities of cybersecurity. While larger companies tend to place cybersecurity leadership within IT, smaller companies (under US\$100 million) more often have the cybersecurity lead reporting to another C-suite executive. This likely reflects the fact that the head of IT in many smaller organizations does not hold a C-level position.

Q: To whom does the head of cybersecurity ultimately report?

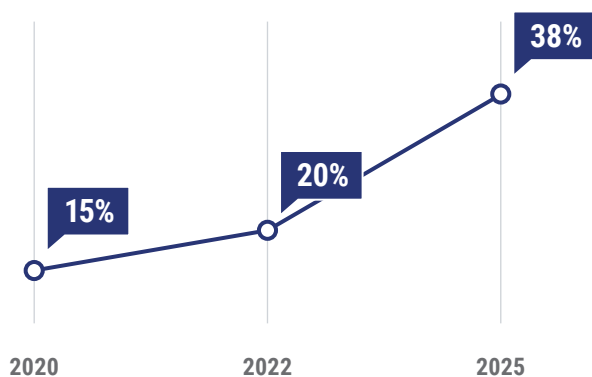


The CLO's responsibilities in cybersecurity have evolved significantly over time. Currently, 38 percent of participants report that the CLO holds a leadership role in cybersecurity in the organization, up from just 15 percent five years ago. Meanwhile, 50 percent of participants say that the CLO is part of a team responsible for cybersecurity at the enterprise level, and just nine percent state that the CLO has no responsibilities in this area. This trend highlights the increasing importance of the CLO's involvement in cybersecurity, reflecting a broader recognition of the legal implications of cybersecurity and the need for comprehensive governance to address these challenges effectively.

Q: What are the CLO's responsibilities regarding cybersecurity?



>> Organizations where the CLO is in a leadership role regarding cybersecurity responsibilities

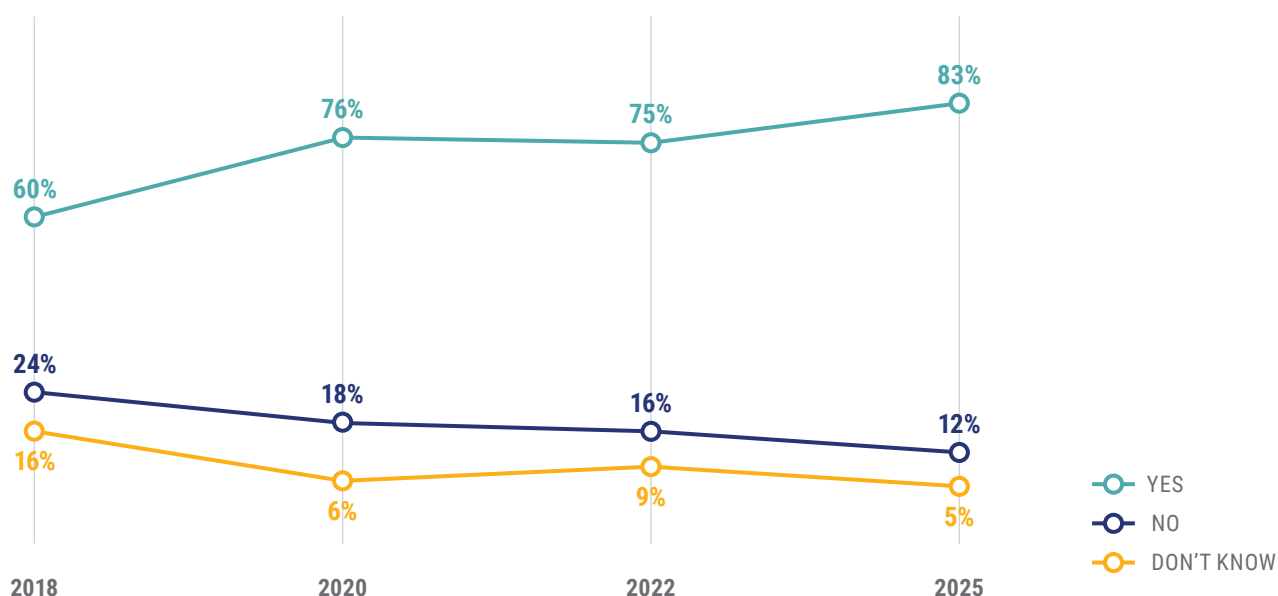


57% of CLOs in companies in the information sector have a leadership role in cybersecurity, followed by professional services (53%), and insurance (47%).

This year's results demonstrate a notable upward trend in the establishment of documented cybersecurity incident response teams within participating organizations over the past several years. In 2018, 60 percent of respondents indicated that their organization had such a team, but the percentage has markedly increased to 83 percent by 2025. Just five percent of participants indicate that they are not sure whether a cybersecurity incident response team exists in their organization, a third of what the percentage was in 2018.

This reinforced presence of a documented response team highlights the growing recognition of the importance of having dedicated resources to address and manage cybersecurity breaches and incidents, reflecting an enhanced focus on cybersecurity preparedness and resilience among organizations.

Q: Does your organization have a documented cybersecurity incident response team (IRT)?



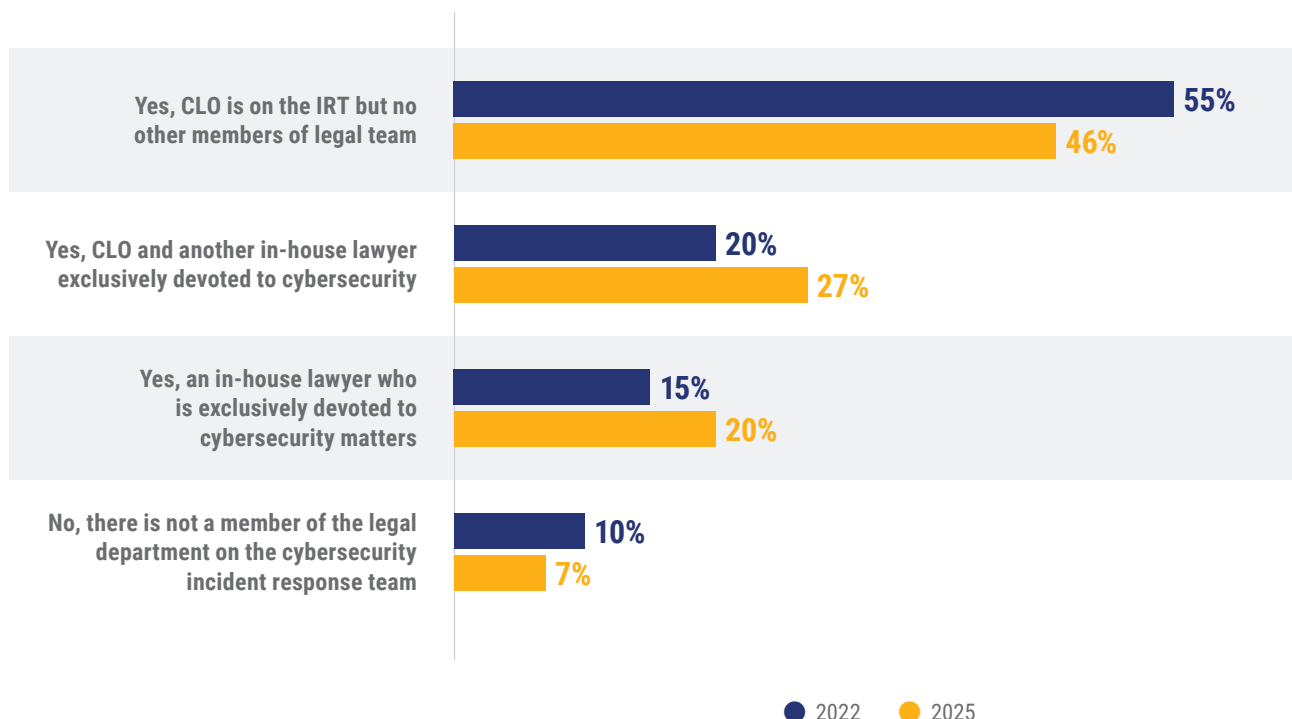
97% of large companies report having a cybersecurity incident response team compared to 69% of small organizations.

In 2022, 55 percent of respondents reported that the CLO was part of the IRT, with no other members of the legal team involved. By 2025, this percentage has decreased to 46 percent. Conversely, the proportion of respondents indicating that both the CLO and another in-house lawyer devoted exclusively to cybersecurity are part of the IRT increased from 20 percent in 2022 to 27 percent in 2025. Additionally, the presence of an in-house lawyer exclusively focused on cybersecurity matters rose from 15 percent in 2022 to 20 percent in 2025. The results point to an increasing integration of legal expertise within cybersecurity incident response teams, reflecting the growing recognition of the importance of legal considerations in managing cybersecurity incidents.

CLOs in small companies are more likely to be part of the IRT than those in large companies, with 98 percent of in-house counsel in single-lawyer departments being in the company's IRT compared to just 12 percent of CLOs in departments with 25 or more in-house counsel. Among this latter group, 47 percent indicate that an in-house counsel exclusively devoted to cybersecurity is a member of the IRT.

Q: Is a member of the legal department on the organization's cybersecurity incident response team [IRT]?

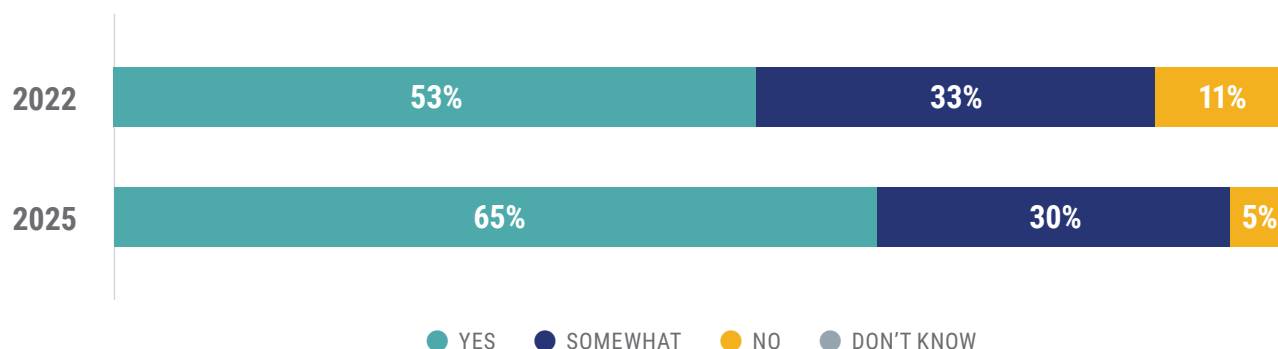
Asked only to those in organizations with a documented cybersecurity IRT.



We observe an encouraging trend towards greater integration and cross-functional collaboration among the IT/cyber department, legal department, and other applicable business departments within organizations to collaboratively reduce cybersecurity risk. In 2022, 53 percent of respondents agreed that these departments worked together to reduce risk, and this percentage increased to 65 percent in 2025. Notably, the percentage of respondents who answered “no” dropped from 11 percent in 2022 to just five percent this year.

The upward trend indicates that organizations are increasingly adopting integrated approaches to cybersecurity, leveraging the expertise of various departments to enhance their overall cybersecurity posture. This implies that companies are becoming more proactive and holistic in their cybersecurity strategies, which is crucial for effectively addressing the complex and evolving nature of cyber threats.

Q: Do you agree with the following statement: “My organization’s IT/cyber department, legal department, and applicable business department(s) generally are integrated and cross-functionally work together to reduce cybersecurity risk”?



A majority of respondents across company sizes report **enhanced collaboration across departments to reduce cybersecurity risk**, though a larger percentage in large companies (73%) report this scenario than in small organizations (57%).

This year's survey reveals interesting trends in how frequently the CLO reports to the board of directors on cybersecurity. The data shows a modest increase in regular reporting, with the percentage of CLOs reporting at every board meeting rising from four percent in 2018 to seven percent in 2025, and the percentage of those reporting on a quarterly basis also increase from 11 percent in 2015 to 18 percent in 2025 (though the highest value was 22 percent in 2018). Meanwhile, annual reporting remained relatively stable, fluctuating between 6 percent and 11 percent over the years (seven percent this year).

Ad hoc (as needed) reporting remains the most common approach, consistently hovering around 35-40 percent across the surveyed years. The main takeaway, however, is the percentage of respondents indicating that the CLO never reports to the board on cybersecurity, which peaked at 28 percent in 2022 but decreased to 16 percent by 2025, a 12-point drop.

The increasing frequency of regular reporting can be attributed to the heightened awareness and emphasis on cybersecurity in corporate governance. As cyber threats become more sophisticated and prevalent, boards are likely demanding more frequent and detailed updates to ensure they are adequately informed and can make strategic decisions to mitigate risks. Additionally, the decline among those who say that they never report on cybersecurity issues indicates that organizations are increasingly valuing the CLO's insights and leadership in cybersecurity, reinforcing a broader trend towards integrating legal perspectives into cybersecurity strategies.

Q: How frequently does the CLO brief the board of directors on cybersecurity?

	2015	2018	2020	2022	2025
At every meeting			4%	5%	7%
Quarterly	11%	22%	15%	13%	18%
Annually	11%	9%	6%	8%	7%
Ad hoc (as needed)	40%	37%	39%	35%	37%
Never	19%	17%	23%	28%	16%
Other	5%	8%	7%	1%	6%
Don't know	14%	7%	6%	9%	10%

Note: The "At every meeting" response option was not offered prior to 2020.

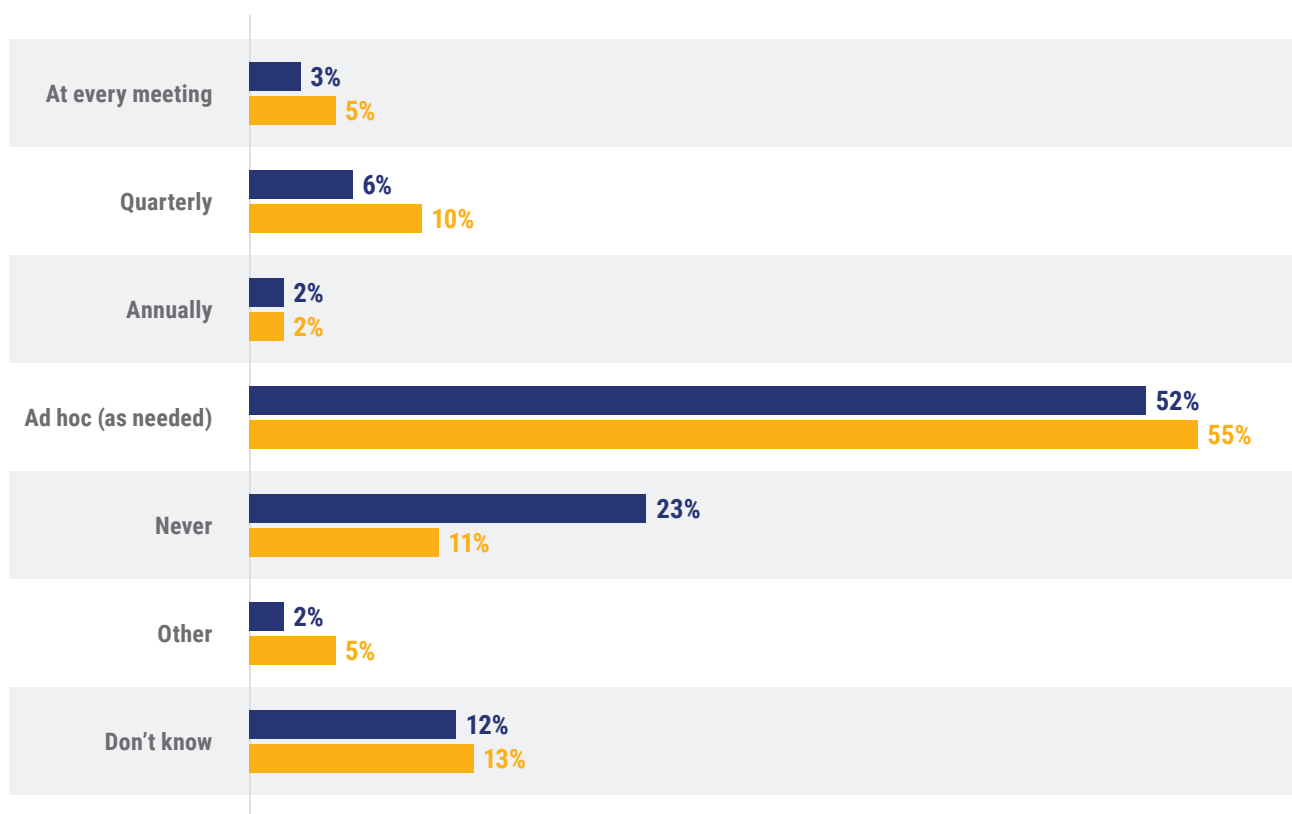
The percentage of respondents reporting that the CLO never briefs the CEO on cybersecurity has decreased significantly from 23 percent in 2022 to just 11 percent in 2025. Although ad hoc briefings remain the most common, with a slight increase from 52 percent in 2022 to 55 percent this year, the proportion of respondents indicating that the CLO regularly briefs the CEO on cybersecurity matters has also increased since 2022 (reporting at every meeting increased from three percent to five percent, and quarterly briefings rose from six percent to 10 percent).

Similarly to the results observed related to board briefings, the data suggests an increasing recognition of the importance of regular and structured communication between the CLO and the CEO on cybersecurity matters. The decline in “never” responses indicates that organizations are prioritizing cybersecurity briefings at the highest executive level, reflecting the growing importance of cybersecurity in overall corporate governance and strategic decision-making.

Q: How frequently does the CLO brief the CEO on cybersecurity?

2022

2025



Just 12% of respondents in the US report that the CLO briefs the CEO on a regular basis (quarterly, at every meeting) compared to 26 percent in non-US organizations.

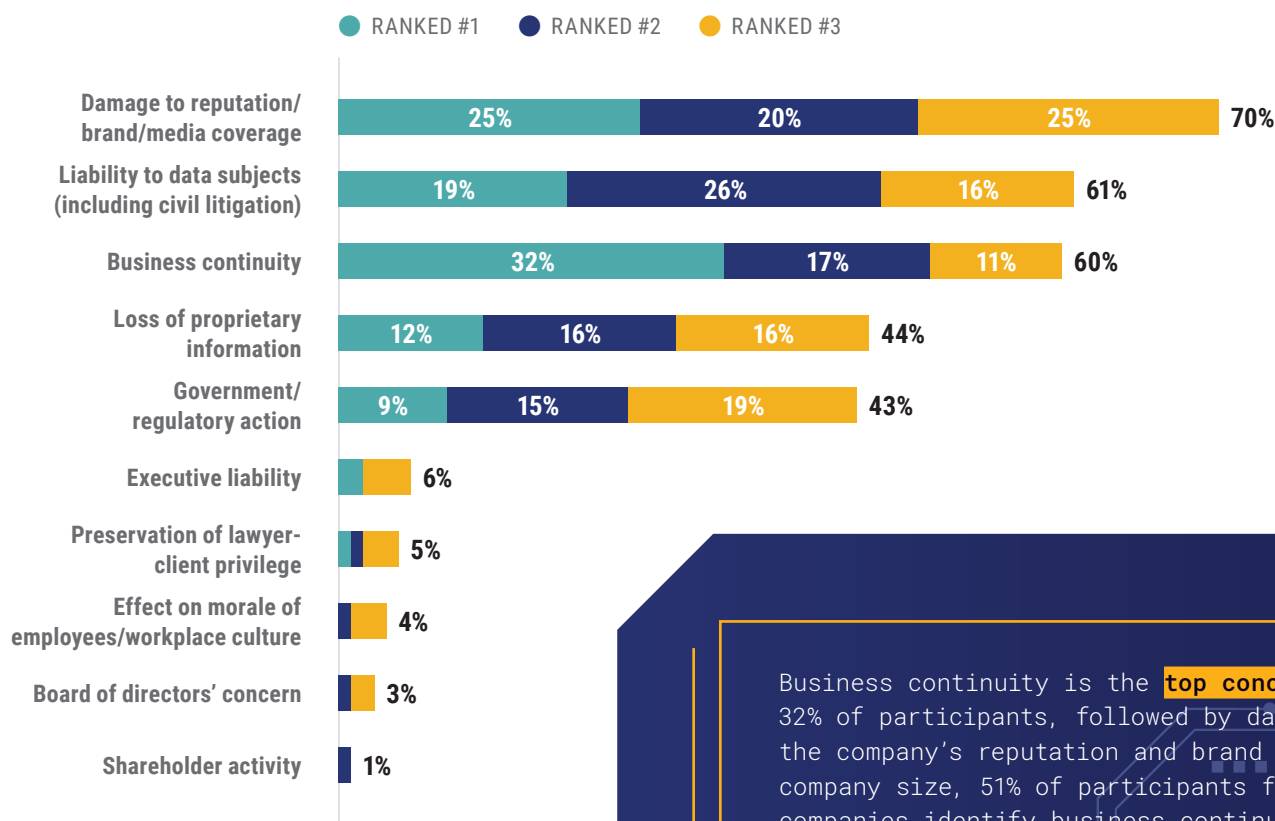
Survey participants identified their top three cybersecurity breach concerns as reputational and brand damage (70 percent), liability to data subjects, including civil litigation (61 percent), and threats to business continuity (60 percent).

The high prioritization of reputational damage reflects the significant impact negative publicity and brand erosion can have on an organization's long-term success and stakeholder trust. Concerns about data subject liability underscore the legal and financial risks associated with data breaches, including potential lawsuits and regulatory penalties. The focus on business continuity highlights the critical need to maintain operational stability and minimize disruptions during a cybersecurity incident.

These top three concerns encompass critical areas impacting an organization's financial health, legal standing, and overall resilience, emphasizing the need for comprehensive cybersecurity strategies. Such strategies must address not only technical defenses but also legal, reputational, and operational considerations.

Beyond the top three, 44 percent of respondents included loss of proprietary information among their top concerns, and 43 percent cited potential government or regulatory action. The remaining potential consequences of a breach were ranked as top concerns by only a small minority of respondents.

Q: Rank your three most immediate concerns with regard to a cybersecurity breach [e.g., what worries you most]?



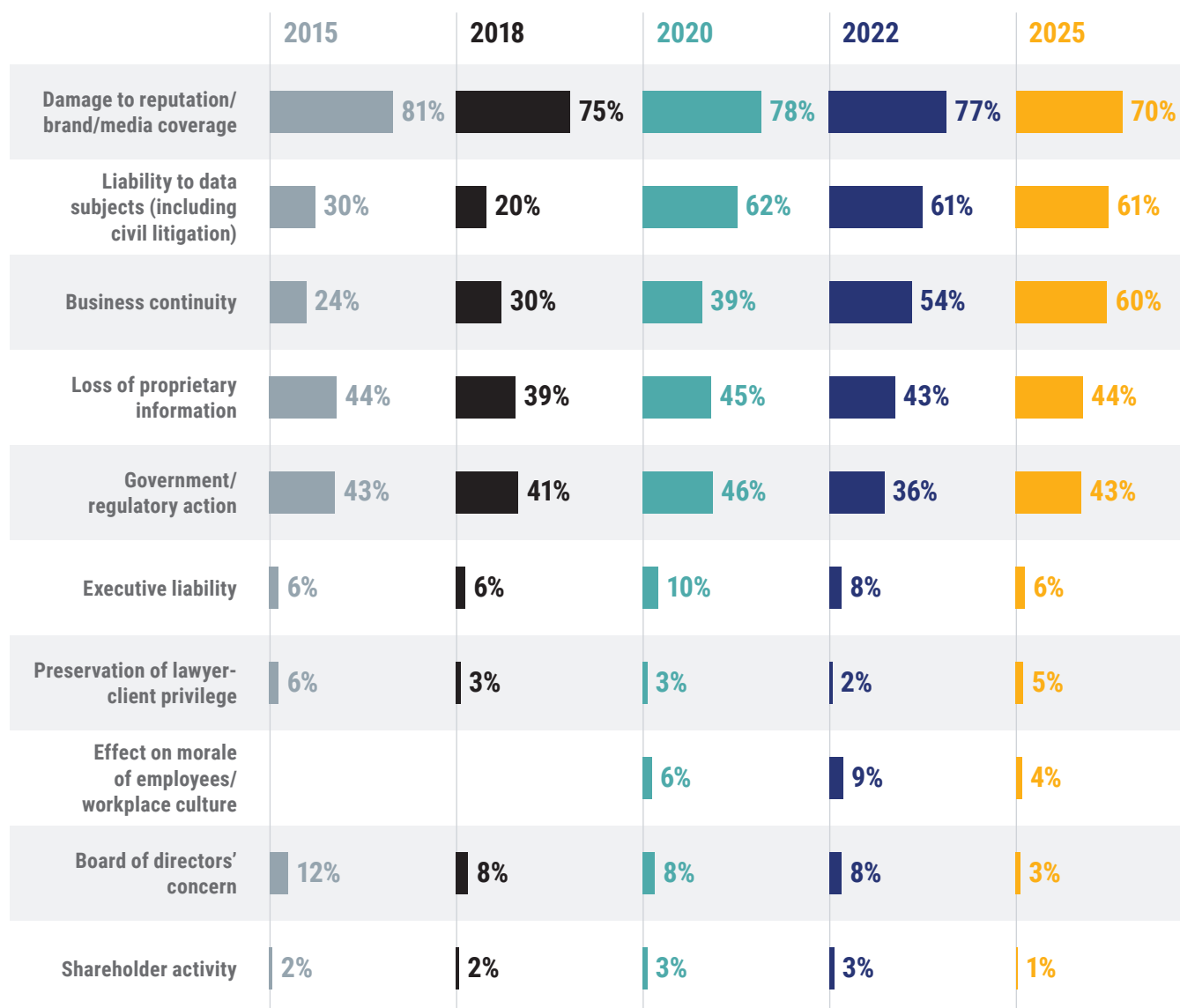
Business continuity is the **top concern** for 32% of participants, followed by damage to the company's reputation and brand at 25%. By company size, 51% of participants from mid-size companies identify business continuity as their first concern following a breach, and 44% in large companies share the same view. In contrast, just 13% of respondents in small organizations ranked business continuity as their top worry resulting from a cybersecurity breach.

Over the years, damage to the company's reputation and brand remains the most pressing concern, although its importance has receded from 81 percent in 2015 to 70 percent in 2025, indicating a moderate rebalancing in dangers of a cybersecurity breach. Liability to data subjects and the possibility of facing litigation have seen a significant rise, peaking at 62 percent in 2020 and stabilizing at 61 percent through 2025, reflecting growing awareness of legal risks.

Concerns on business continuity have steadily increased in importance as well from 24 percent in 2015 to 60 percent in 2025, emphasizing the critical need for operational stability. Concerns over loss of proprietary information and government or regulatory action have remained relatively stable, suggesting consistent recognition of these risks among participants.

These trends reflect a broader and more nuanced understanding of cybersecurity risks, with increasing emphasis on legal implications, operational resilience, and the multifaceted impact of breaches on organizations.

>> Concerns selected among the three most important



Q: What specific AI-powered cyber threats are you most concerned about, and why?

Survey participants provided valuable insights on what AI-powered cyber threats are most concerning and have the potential to damage corporate interests, and we have identified the following five concerns:

01

AI-Enhanced Phishing and Social Engineering

AI significantly amplifies the effectiveness of phishing and social engineering attacks by creating highly personalized and convincing messages, including voice and video impersonations. This makes it harder for individuals to distinguish genuine communication from malicious attempts.

"AI has increased the plausibility of phishing attacks, increasing our susceptibility to them. In addition, as our company grows and becomes more well-known, I am concerned about voice and video cloning of our CEO and CFO being used to initiate fraudulent transfers."

02

Data Breaches and Confidentiality Leaks

AI can be used to extract and disseminate sensitive data, including personal information, proprietary information, and trade secrets. This can lead to financial losses, reputational damage, and legal liabilities. The use of AI tools themselves can also be a vector for data leakage.

"Leakage of confidential information, including our customer's data, through use of AI platforms."

03

Ransomware and Disruptive Attacks

AI-powered ransomware attacks can be more sophisticated and difficult to defend against, potentially leading to significant business disruption, financial losses, and operational downtime. AI can also be used to identify vulnerabilities and develop exploits, increasing the risk of successful attacks.

"Ransomware attacks are of most concern because they have the potential to create the largest business interruption and customer relations threats."

04

Impersonation and Fraud

AI facilitates impersonation by creating convincing deepfakes and mimicking voices, enabling fraudulent activities like unauthorized transfers, identity theft, and manipulation of employees.

"Impersonation of C-suite executives with criminals directing employees to take actions detrimental to the company and our clients."

05

Lack of Awareness and Understanding

Many organizations and individuals lack sufficient understanding of AI-powered cyber threats, making them more vulnerable to attacks. The rapid advancement of AI technology makes it challenging to keep up with the evolving threat landscape. There is also concern about the unknown threats that AI could bring.

"I am actually concerned about the fact that I don't know enough about specific AI-powered cyber threats to be concerned about any particular ones."

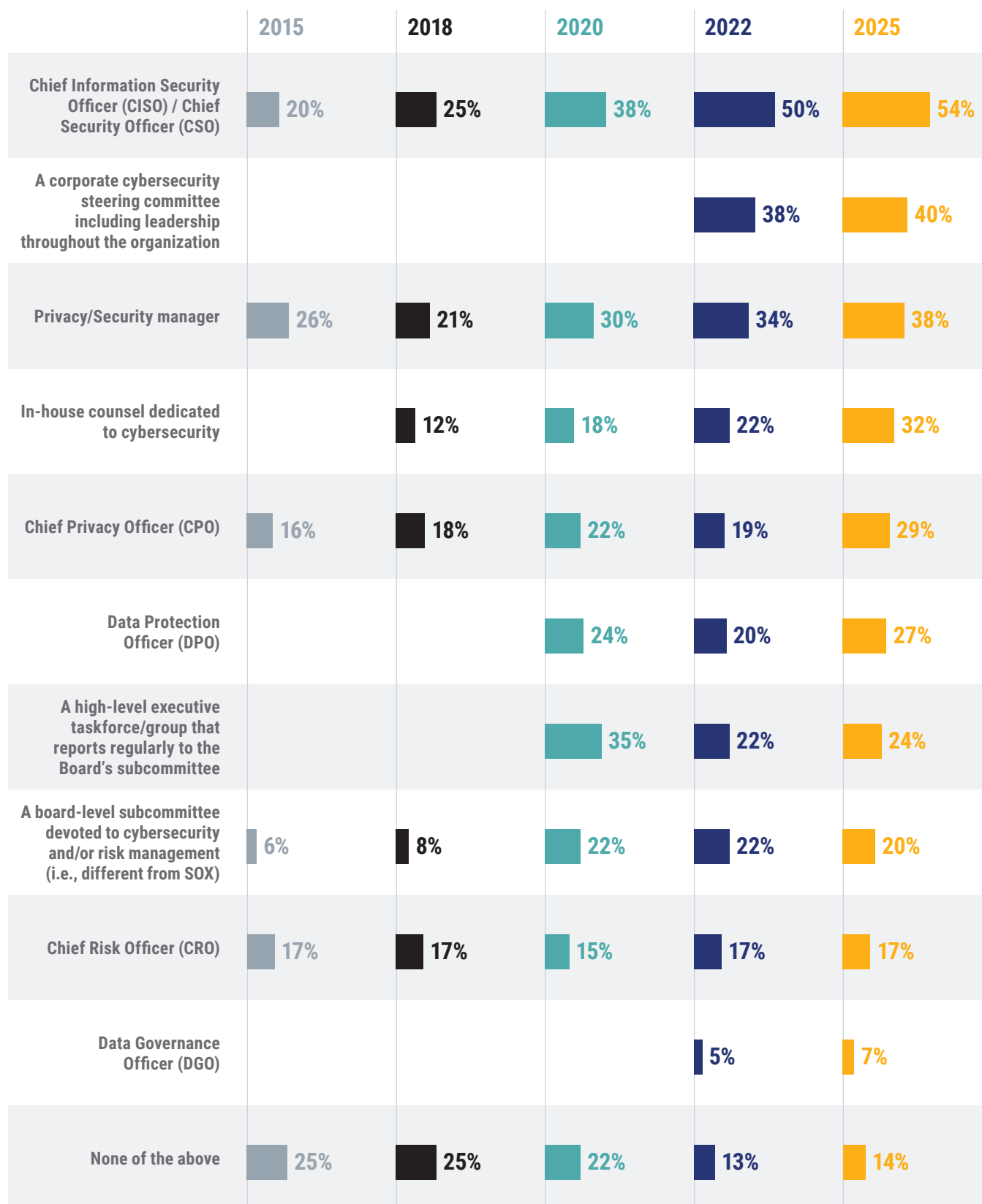
//resourcing [and] technology

An analysis of the resources allocated to cybersecurity since 2015 shows a clear trend towards increased organizational focus on tackling cybersecurity risks. The percentage of organizations with a chief information security officer (CISO) or chief security officer (CSO) has steadily risen from 20 percent in 2015 to 54 percent in 2025, highlighting the growing importance of dedicated cybersecurity leadership.

Similarly, the specific, specialized role of privacy/security manager has become more common, increasing from 26 percent to 38 percent over the same period. Most notably, the presence of in-house counsel dedicated to cybersecurity has also grown significantly, from 12 percent in 2018 to 32 percent in 2025, reflecting the need for specialized legal expertise in handling cybersecurity matters and incident response. Finally, the establishment of corporate cybersecurity steering committees and high-level executive taskforces has also become more prevalent, emphasizing the importance of cross-functional collaboration and governance in cybersecurity.

This trend reflects a growing recognition of robust cybersecurity strategies and governance as crucial for success in today's business environment. However, a significant disparity exists between large and small organizations. While large companies are typically well-resourced to fill these specialized positions, 31 percent of small companies reported lacking dedicated cybersecurity resources, compared to only three percent of large organizations. This gap leaves smaller businesses particularly vulnerable.

Q: Which of the following does your organization have?



Legal departments are increasingly recognizing the need for dedicated cybersecurity expertise. The survey results indicate a modest but notable rise in the intent to hire in-house cybersecurity counsel. While only four percent of respondents in 2022 planned to add such a role, with another nine percent considering it, those numbers have risen to seven percent planning to hire and 11 percent considering it in 2025. This means nearly one in five legal departments are now actively considering adding a cybersecurity specialist to their in-house team.

The number of respondents unsure about their plans has also increased, from five percent in 2022 to 14 percent currently. This suggests that while more departments are recognizing the importance of this expertise, they are also grappling with the complexities of implementation. Simultaneously, the proportion of respondents definitively stating they *would not* add such a role has decreased by 14 percentage points, further underscoring the growing awareness of the crucial link between legal counsel and effective cybersecurity risk management.

Q: Do you expect to add additional in-house counsel exclusively devoted to legal cybersecurity in the next two years?

● YES ● UNDER CONSIDERATION ● NO ● DON'T KNOW

2022



2025

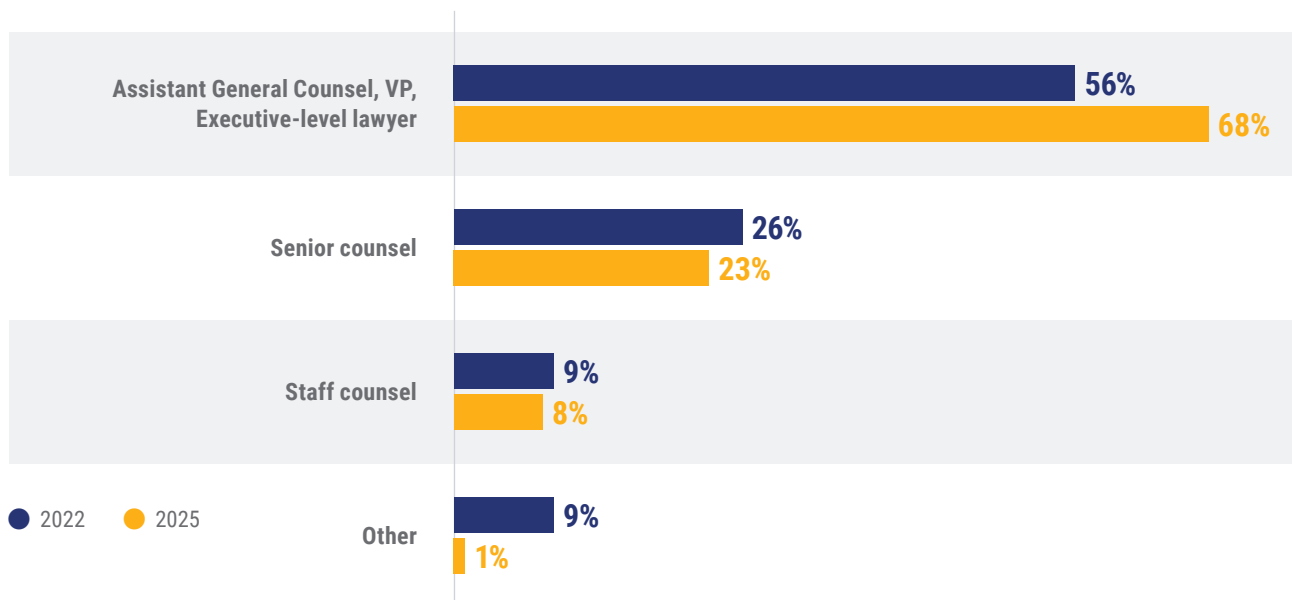


Most in-house lawyers exclusively devoted to cybersecurity issues are of high seniority, with the proportion of assistant general counsel, vice president-level, or other executive-level lawyers rising from 56 percent in 2022 to 68 percent in 2025. The percentage of senior counsel has slightly decreased from 26 percent to 23 percent, while the share of those who are at the staff counsel level remains practically unchanged at around eight and nine percent.

The enhanced presence of executive-level lawyers who are mostly dedicated to cybersecurity management likely stems from an increasing recognition of the importance of cybersecurity within organizations. Higher-ranking positions such as assistant general counsel and vice president are likely chosen due to extensive legal experience, subject matter expertise, and the ability to influence strategic decisions, ensuring that cybersecurity considerations are integrated at the highest levels of the company. Senior in-house counsel are also valued for their specialized expertise and capability to handle complex cybersecurity issues, providing crucial support to executive leadership.

**Q: What level of seniority is your dedicated in-house cyber counsel?
[If you have more than one such lawyer, please provide the seniority level of the most highly ranked lawyer.]**

Only asked to those who reported having an in-house counsel dedicated to cybersecurity.



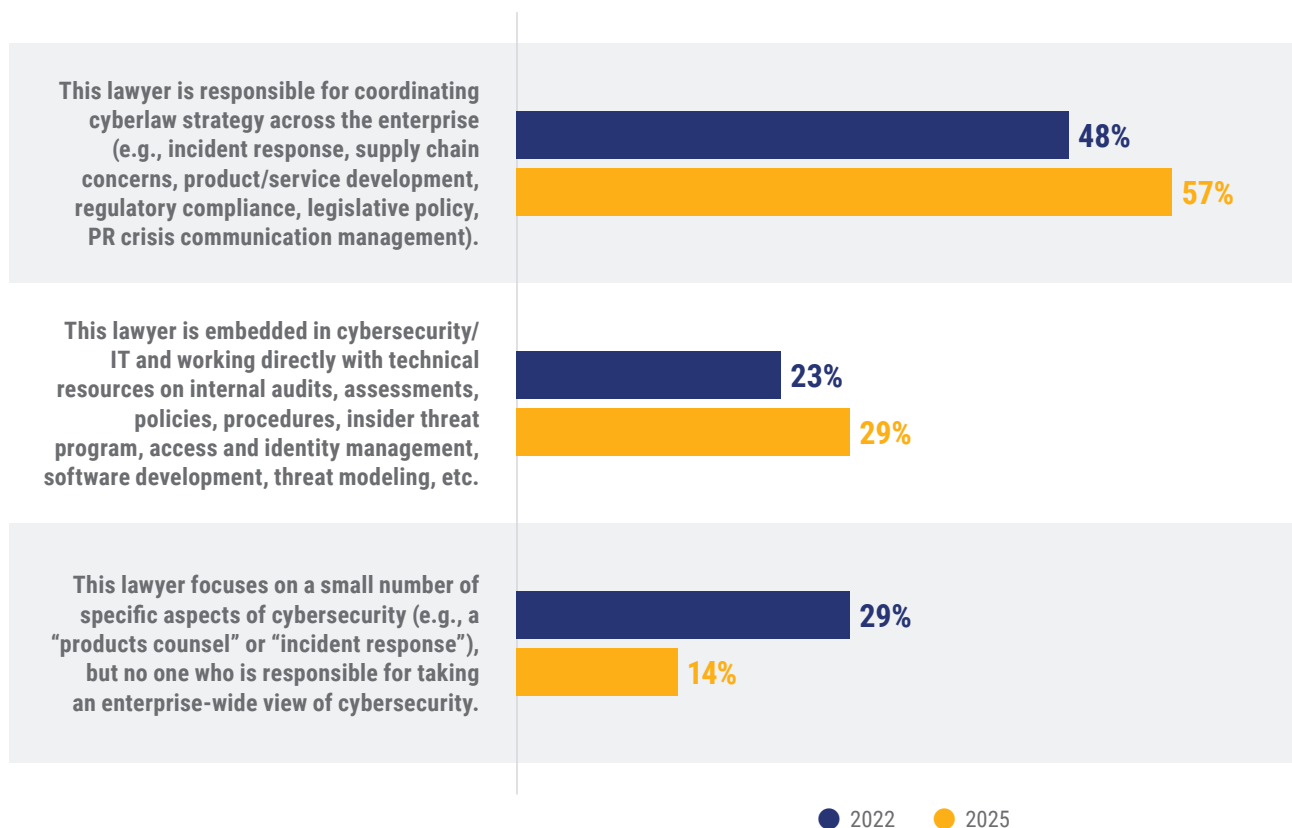
In-house counsel dedicated to cybersecurity are **most likely to be executive-level lawyers** in organizations in the insurance (90%), finance and banking (86%), and information (82%) sectors.

Among organizations that have a dedicated in-house counsel to cybersecurity, most employ an in-house counsel who is responsible for coordinating cyberlaw strategies across the company, reflecting a growing emphasis on a comprehensive, enterprise-wide cybersecurity approach. In 2025, 57 percent of respondents reported that these are the duties of the dedicated cybersecurity counsel, up from just under the 50-percent mark three years ago.

The proportion of cybersecurity lawyers who are embedded within IT teams and who work directly with technical resources have also increased from 23 percent in 2022 to 29 percent in 2025. Consequently, the percentage of lawyers focusing on a small number of specific aspects of cybersecurity without an enterprise-wide view halved since 2022, from 29 percent to 14 percent. This shift highlights a trend towards more integrated collaboration between legal and technical departments to effectively respond to cybersecurity challenges.

Q: Please describe this lawyer's duties:

Only asked to those who reported having an in-house counsel dedicated to cybersecurity.

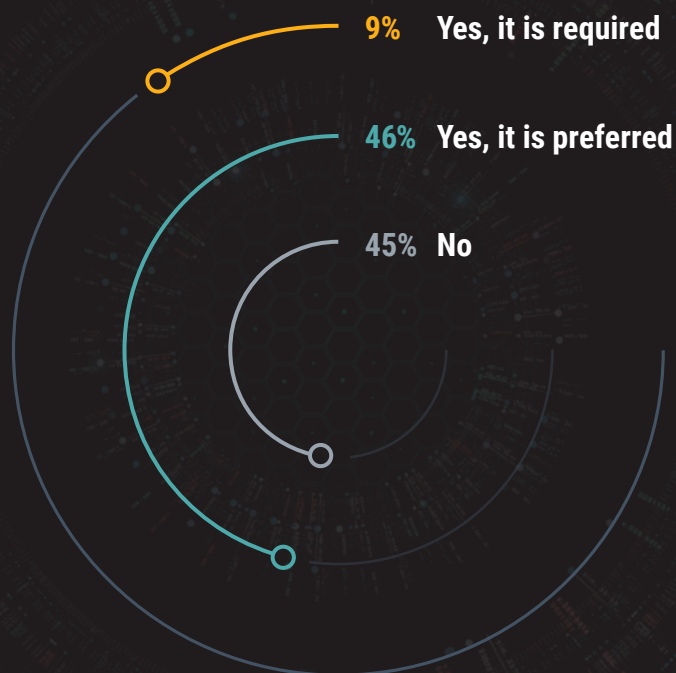


When hiring in-house counsel dedicated to cybersecurity, a majority of legal department leaders prefer lawyers with cybersecurity certifications. Forty-six percent of respondents say that having a cybersecurity certification, such as Certified in Cybersecurity (CC), Certified Information Systems Security Professional (CISSP), and Certified Information Security Manager (CISM), is preferred, and an additional nine percent of respondents indicate that having a cybersecurity certification is required in order to get a position as a dedicated cybersecurity in-house counsel. The remaining 45 percent of respondents among those who either have a dedicated cybersecurity lawyer or are considering hiring one in the coming months indicate that they do not seek such certifications for these roles.

While the results show a preference overall for certified professionals, a nearly equal proportion of organizations likely rely on other factors such as experience or internal training programs to ensure their legal teams are well-equipped to handle cybersecurity challenges. The emphasis on certifications by most of those that employ a cybersecurity in-house counsel (or seek to hire one) indicates a growing recognition of the importance of specialized knowledge in managing complex cybersecurity issues effectively.

Q: When hiring new cyber counsel, does your organization seek counsel with an operational cybersecurity certification (e.g., CC, CISSP, CISM)?

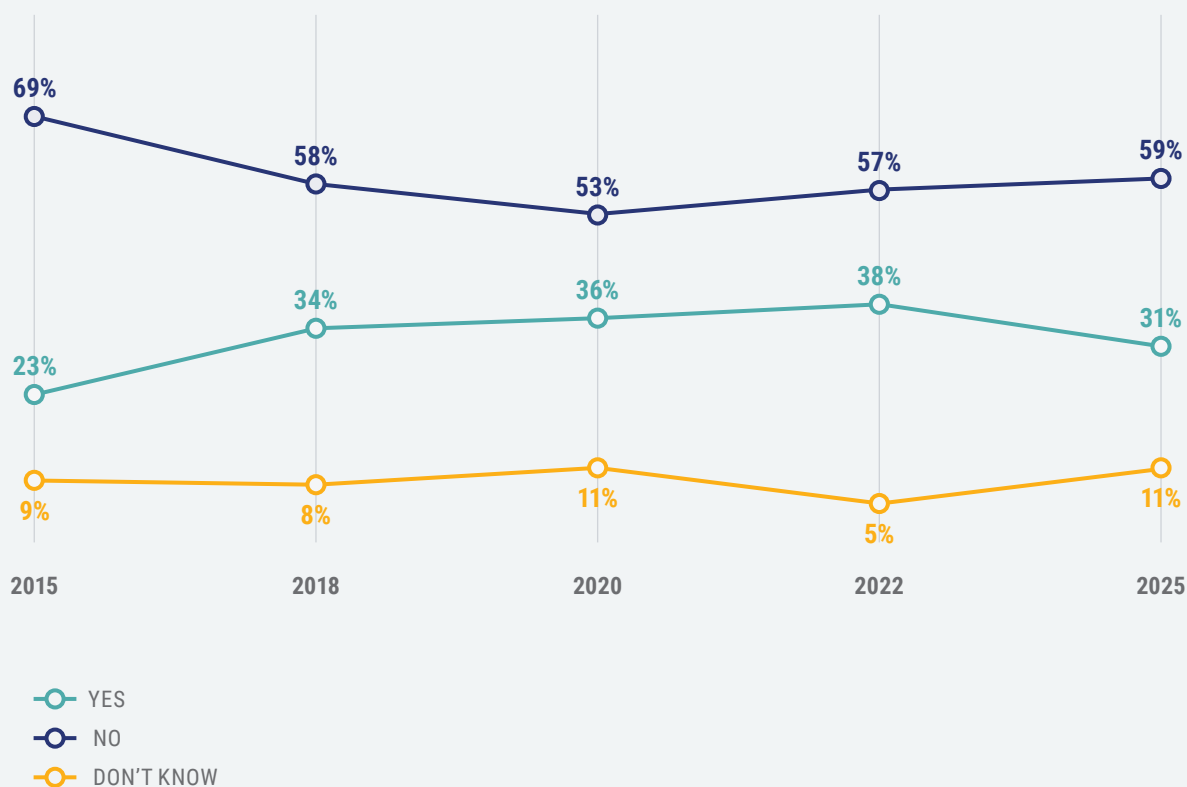
Asked only to those who have an in-house counsel dedicated to cybersecurity or are intending or considering hiring one such specialist in the next two years.



Considering the last 10 years, the survey data reveals a clear upward trend in the percentage of participants reporting increased legal department expenses due to their company's approach to cybersecurity, peaking at 38 percent in 2022, a 15-point jump compared to the 23 percent value observed in 2015. However, there is a notable drop to 31 percent in this year's survey.

While there has been a consistent growth in legal expenses attributable to cybersecurity over the years, possibly due to heightened regulatory requirements and more frequent cybersecurity incidents, the decline in 2025 might indicate improved efficiency and cost-management strategies within legal departments, or a shift in how cybersecurity responsibilities and costs are being managed within organizations. Overall, the data highlights the growing financial impact of cybersecurity on legal departments, stressing the importance of strategic planning and resource allocation in managing these expenses.

Q: Compared with one year ago, has your law department spend increased as a result of your organization's approach to cybersecurity?



The respondents who reported an increase in legal department expenses were asked to clarify whether the increase in costs was mainly allocated to inside spend, outside spend, or equally split between these two categories. The majority have consistently reported that increased costs are mainly due to outside spend, with this category fluctuating but generally high, starting at 54 percent in 2015, dropping to 39-40 percent in 2018 and 2020, and then rising again to 50 percent in 2022 and 52 percent in 2025. This suggests a continued reliance on external expertise such as law firms, alternative legal service providers, and consultants for handling cybersecurity issues.

In contrast, the proportion of respondents citing mainly inside spend rose to a peak of 36 percent in 2020 but has since declined significantly to 14 percent by 2025. This trend suggests that, while there was an initial push to build internal cybersecurity legal resources and expertise, organizations may have found it more sustainable or efficient to revert to external support.

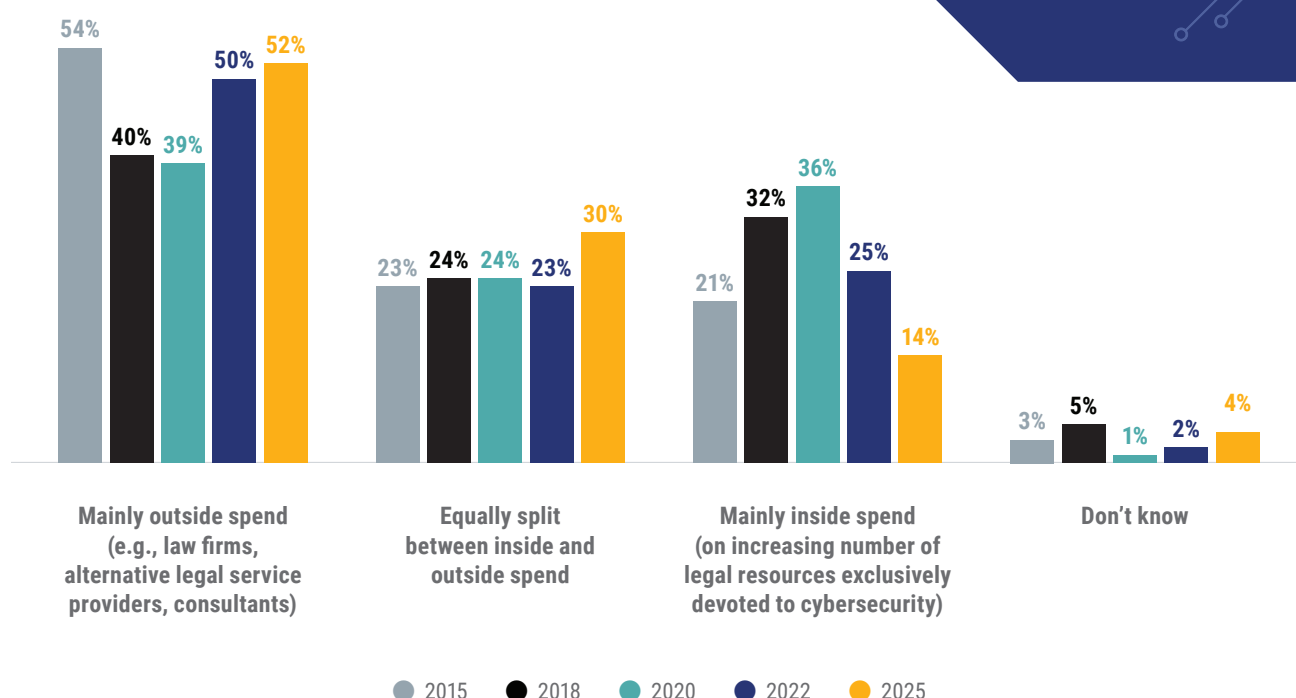
The percentage of respondents reporting an equal split between inside and outside spend has increased from 23 percent in 2015 to 30 percent in 2025, reflecting a balanced approach where organizations leverage both internal and external resources for additional legal costs related to cybersecurity.

Overall, the notable increase in additional outside spending in recent years is likely driven by the growing complexity and specialization required in cybersecurity legal matters. Organizations may find it more advantageous to rely on external expertise for specialized tasks while maintaining some internal capabilities for ongoing needs.

Q: Please describe the increase in spend:

Asked only to those who reported an increase in legal department spend as a result of the organization's approach to cybersecurity.

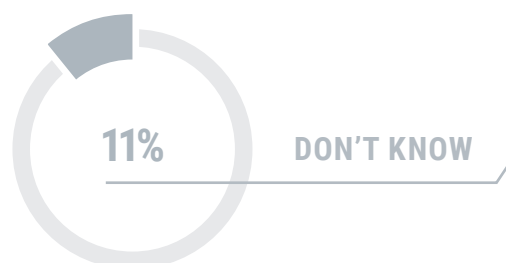
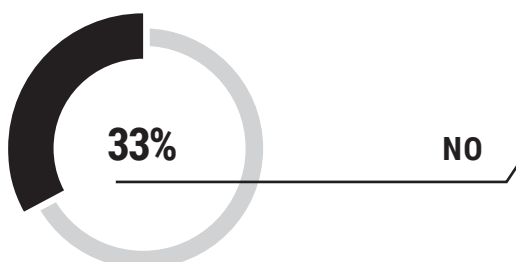
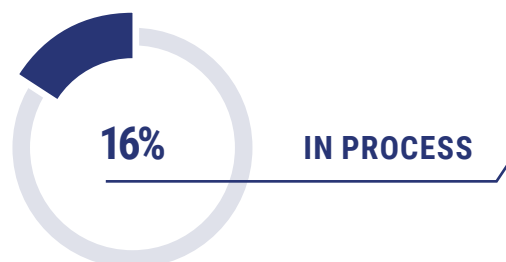
Large companies with more than US\$3 billion in revenue tend to allocate additional legal spend related to cybersecurity more evenly between inside and outside spend (42%), while just 31% say the increase in costs is mainly due to outside spend.



Q: Has your organization implemented a Governance, Risk, and Compliance (GRC) solution to document, address, and follow up on vendor cybersecurity risks?

The result show varied levels of implementation of Governance, Risk, and Compliance (GRC) solutions for managing vendor cybersecurity risks among organizations. As of 2025, only 17 percent of respondents confirmed that their organization has implemented a GRC solution, while an additional 16 percent are in the process of doing so, and 23 percent are considering it. A significant portion, 33 percent, reported that their organization has not implemented a GRC solution.

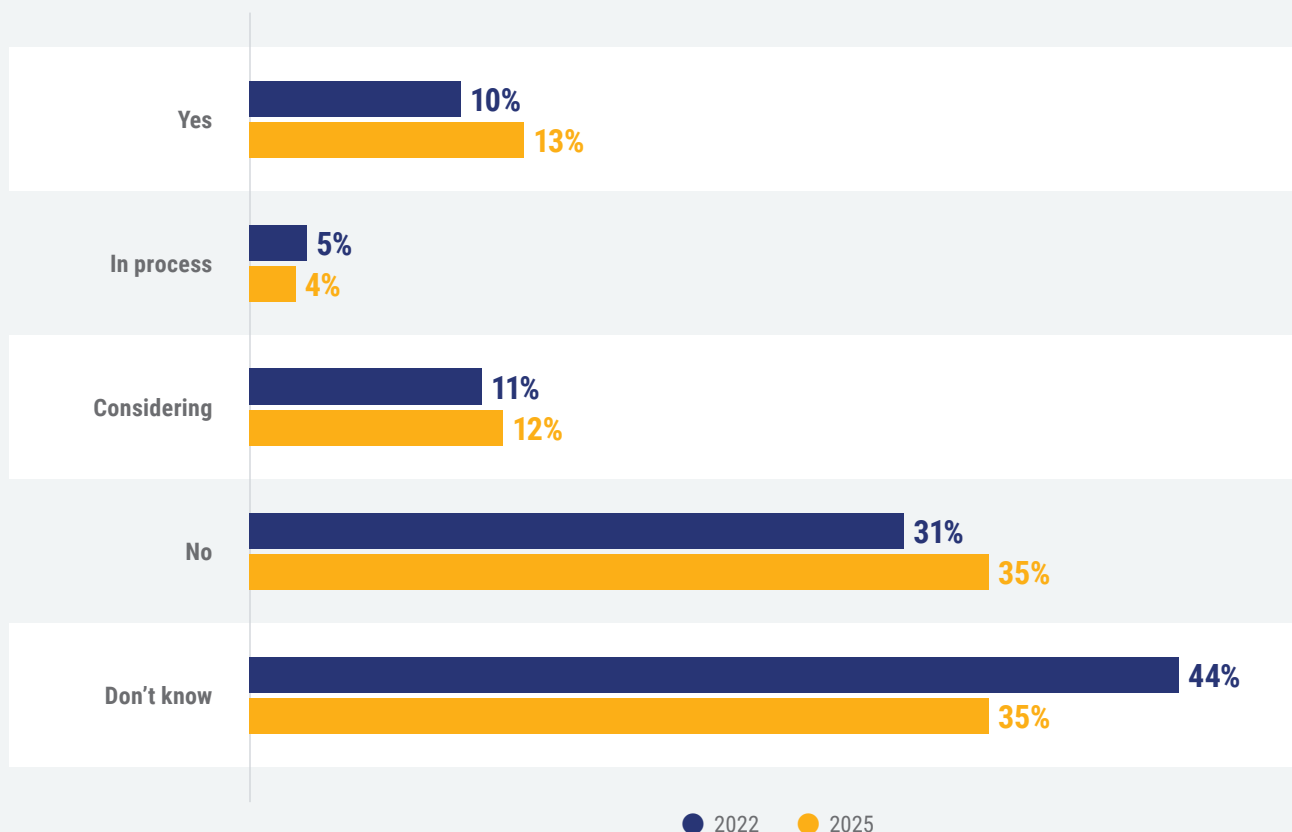
While GRC solutions are gaining traction, their adoption is still in its early stages for many organizations. The relatively low percentage of fully implemented solutions may indicate the complexity, cost, and resource demands associated with these systems. However, the fact that a combined 56 percent of respondents are either implementing, considering, or have already implemented GRC solutions demonstrates a clear trend toward comprehensive vendor cybersecurity risk management. This increasing adoption aligns with the core capabilities of GRC solutions, which offer structured frameworks for documenting, addressing, and mitigating cybersecurity risks, ultimately strengthening an organization's overall risk management posture.



The results show a modest increase in the implementation of Security Orchestration, Automation, and Response (SOAR) technology within legal departments, with 13 percent of respondents this year confirming its implementation, up from 10 percent in 2022. Additionally, a consistent percentage of departments are considering SOAR (11-12 percent), while those in the process of implementation have slightly decreased from five percent to four percent. Notably, the percentage who do not know whether their department has implemented SOAR has decreased from 44 percent in 2022 to 35 percent in 2025, suggesting growing awareness and consideration of SOAR technologies. However, the proportion of legal departments not implementing SOAR has increased from 31 percent to 35 percent.

These results imply that while there is a gradual adoption of SOAR technology within legal departments, a significant portion remains either unaware or hesitant about its implementation. These have implications for legal departments as they are missing out on the potential for enhanced incident response capabilities, improved efficiency, and better management of cybersecurity risks through automation and orchestration. However, the slow adoption rate also suggests that there may be barriers such as cost, complexity, or lack of awareness of SOAR benefits that first need to be addressed in order to encourage broader implementation.

Q: Has your organization implemented a Security Orchestration, Automation and Response (SOAR) technology?



//awareness, training, and policies

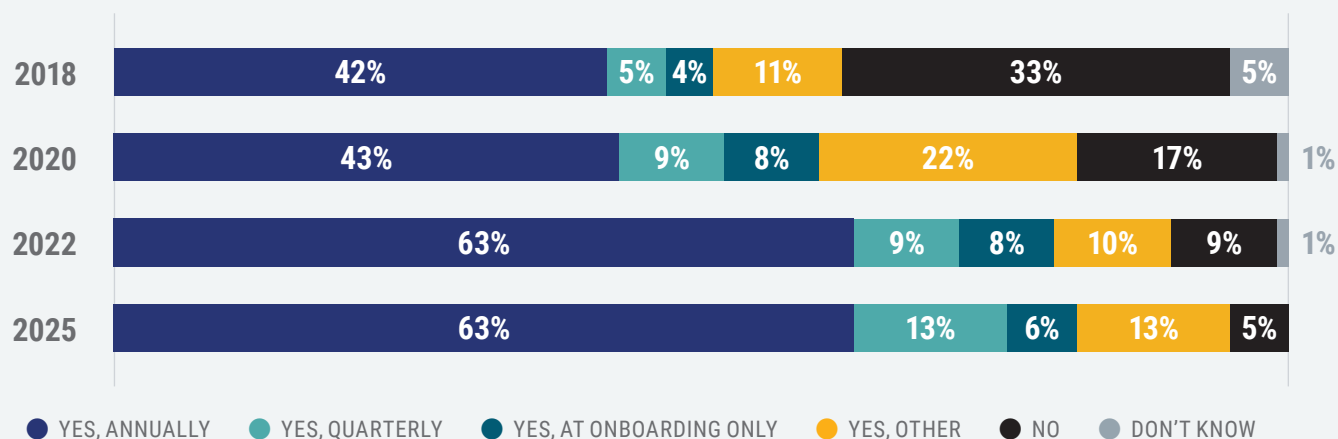
Employee cybersecurity training is becoming a priority for organizations. The survey data reveal a significant increase in mandatory annual training, rising from 42 percent in 2018 to 63 percent in both 2022 and 2025. Quarterly training has also seen a substantial jump, from just five percent in 2018 to 13 percent in 2025. While onboarding-only training has remained relatively consistent at around six to eight percent, other training scenarios (including monthly sessions, ad-hoc training, frequent microlearning exercises, and needs-based or incident-triggered training) peaked at 22 percent in 2020 and have now stabilized at 13 percent in 2025.

Perhaps most telling is the dramatic reduction in companies offering *no* mandatory cybersecurity training, falling from 33 percent in 2018 to a mere five percent in 2025. Furthermore, the proportion of respondents unaware of their company's training programs has dropped to zero, indicating a significant improvement in communication and awareness. These trends demonstrate a clear shift towards recognizing the critical role of regular, comprehensive cybersecurity training in building a robust security posture and fostering employee resilience against evolving threats.

80% of large companies

require mandatory training for employees on cybersecurity either quarterly or annually, while 68% of small companies do the same.

Q: Does your organization have mandatory training on cybersecurity for all employees?



While organizations acknowledge the importance of role-specific cybersecurity training, implementation lags behind recognition. In 2022, 25 percent of respondents reported providing fully personalized training, a figure that has since decreased to 20 percent in 2025. However, the proportion of companies offering *some* level of customized training has increased from 34 percent in 2022 to 39 percent in 2025, suggesting a partial, albeit incomplete, move towards tailored programs.

Overall, the percentage of participants reporting at least some degree of role-based customization (59 percent) has remained relatively static. This stability underscores a general understanding that different roles and levels of access require specialized cybersecurity knowledge. However, the fact that roughly one-third of respondents still report a lack of role-specific training highlights the need for significant improvement in this area. This persistent gap since 2022 represents a missed opportunity to enhance cybersecurity preparedness by ensuring training is directly relevant to individual employee responsibilities and potential vulnerabilities.

Q: Does your organization customize security training to the individual role or level of access to sensitive data or systems?

● YES ● SOMEWHAT ● PLANNING ON IT ● NO ● DON'T KNOW

2022

25%

34%

6%

32%

3%

2025

20%

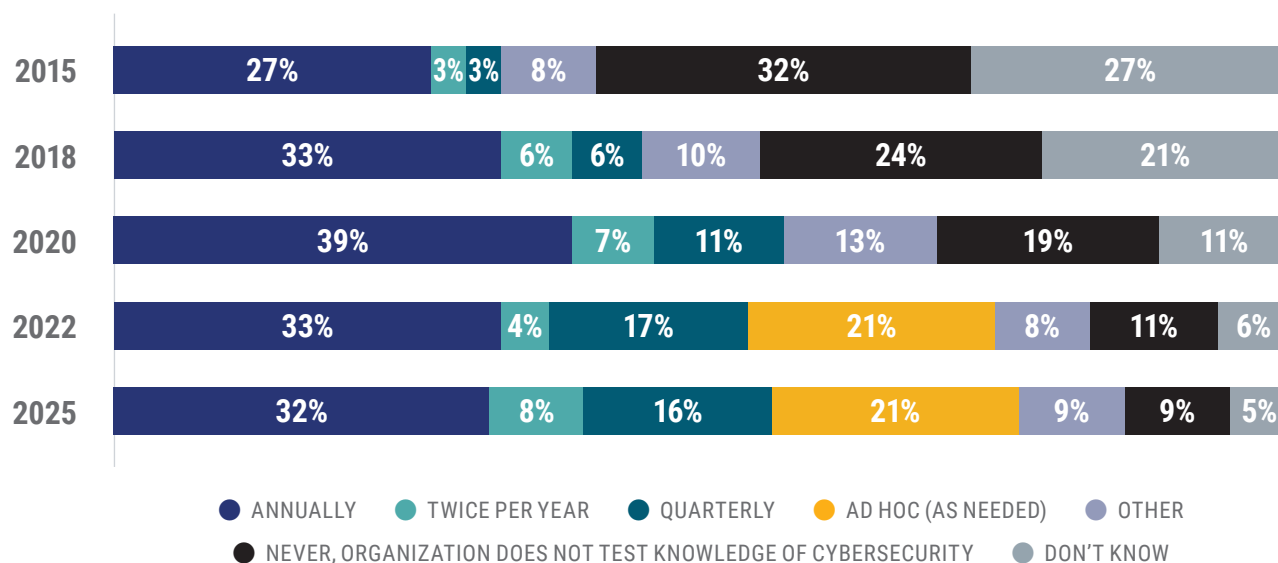
39%

5%

33%

3%

Q: How often does your organization evaluate employee knowledge of cyber safety practices/data policies?



Note: The "Ad hoc (as needed)" response option was not offered prior to 2020.

The survey results indicate a consolidation of the practice of evaluating employee knowledge of cybersecurity safety practices and data policies over the past decade. The percentage of companies conducting annual evaluations rose from 27 percent in 2015 to 39 percent in 2020 and stabilized around 32-33 percent since 2022. Quarterly evaluations have seen a significant increase, rising from just three percent in 2015 to 17 percent by 2025. The implementation of ad hoc evaluations remains steady at 21 percent since first considered in 2022.

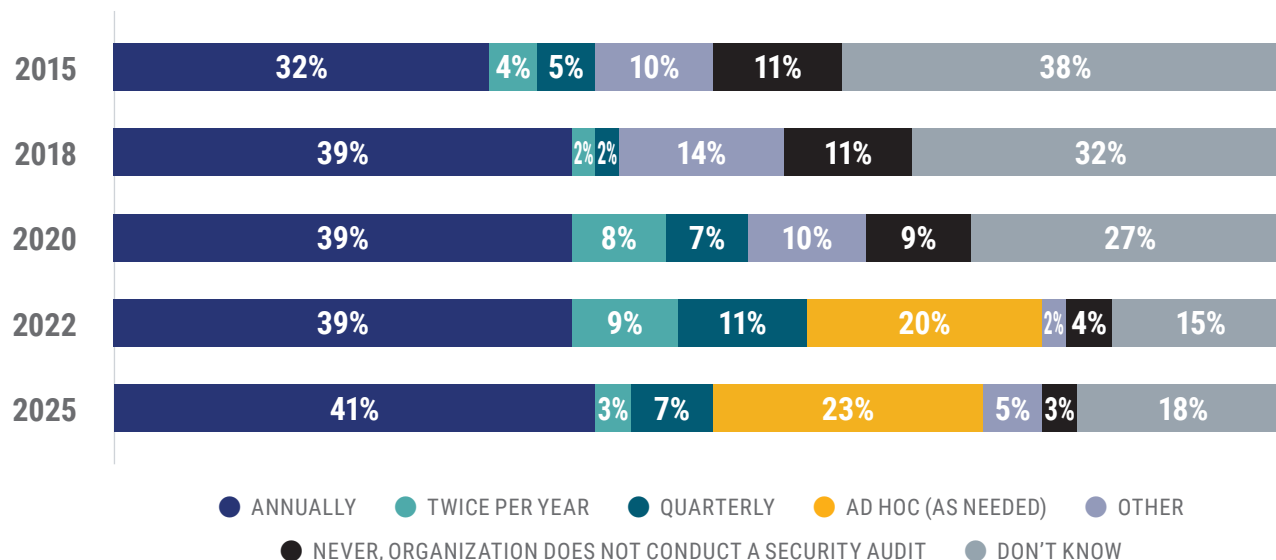
As a result of the increased focus on periodic evaluations, the proportion of organizations that never test employee knowledge has decreased markedly from 32 percent in 2015 to just nine percent in 2025. Furthermore, the number of respondents unsure about their organization's testing practices has declined from a substantial 27 percent to five percent in 10 years.

The data clearly show a growing recognition of the importance of regular and varied evaluations to ensure that employees are knowledgeable about cybersecurity practices. The increasing frequency of evaluations, particularly quarterly and twice per year, indicates a proactive approach to maintaining cybersecurity awareness and competence. For legal departments, this implies a need for ongoing collaboration with cybersecurity and training teams to develop and implement effective evaluation strategies, ensuring compliance and reducing the risk of cyber incidents through well-informed employees.

18% of companies

under US\$100 million in revenue never evaluate employee knowledge on cyber safety practices.

Q: How often does your organization conduct a cybersecurity audit of part(s) of the organization?



Note: The "Ad hoc (as needed)" response option was not offered prior to 2020.

The percentage of companies conducting at least an annual cybersecurity audit has increased from 32 percent in 2015 to 41 percent in 2025. The frequency of quarterly audits also rose, peaking at 11 percent in 2022 before slightly declining to seven percent in 2025. Ad hoc audits, first reported in 2022, saw a slight increase from 20 percent to 23 percent in 2025. Interestingly, there has been a noticeable decrease in companies that never conduct security audits, from 11 percent in 2015 to just three percent in 2025, and the percentage of respondents who are not aware of the frequency of cybersecurity audits has also declined, which clearly demonstrates an increased awareness and transparency regarding cybersecurity practices within organizations.

Companies are placing greater importance on regular and structured cybersecurity audits to identify and mitigate potential risks. The slight decline in the number of organizations conducting audits more regularly than on an annual basis may indicate a preference to conducting audits less often, either annually or every other year (as reported by some participants as other frequencies), or when the need arises.

24% of respondents in large companies do not know how often their organization conducts cybersecurity audits, compared to just 14% of those in small organizations. This may indicate a relatively lower involvement of Legal in cybersecurity audits, which may be undertaken by other departments in large organizations, such as IT, privacy, etc.

Q: If so, how is Legal involved in reoccurring internal cybersecurity audits?

Asked only to those who conduct cybersecurity audits on an annual, semi-annual, quarterly, or ad-hoc basis.

● DEEPLY EMBEDDED ● MOSTLY INVOLVED ● SLIGHTLY INVOLVED ● NOT INVOLVED AT ALL

2022

14%

24%

46%

16%

2025

9%

31%

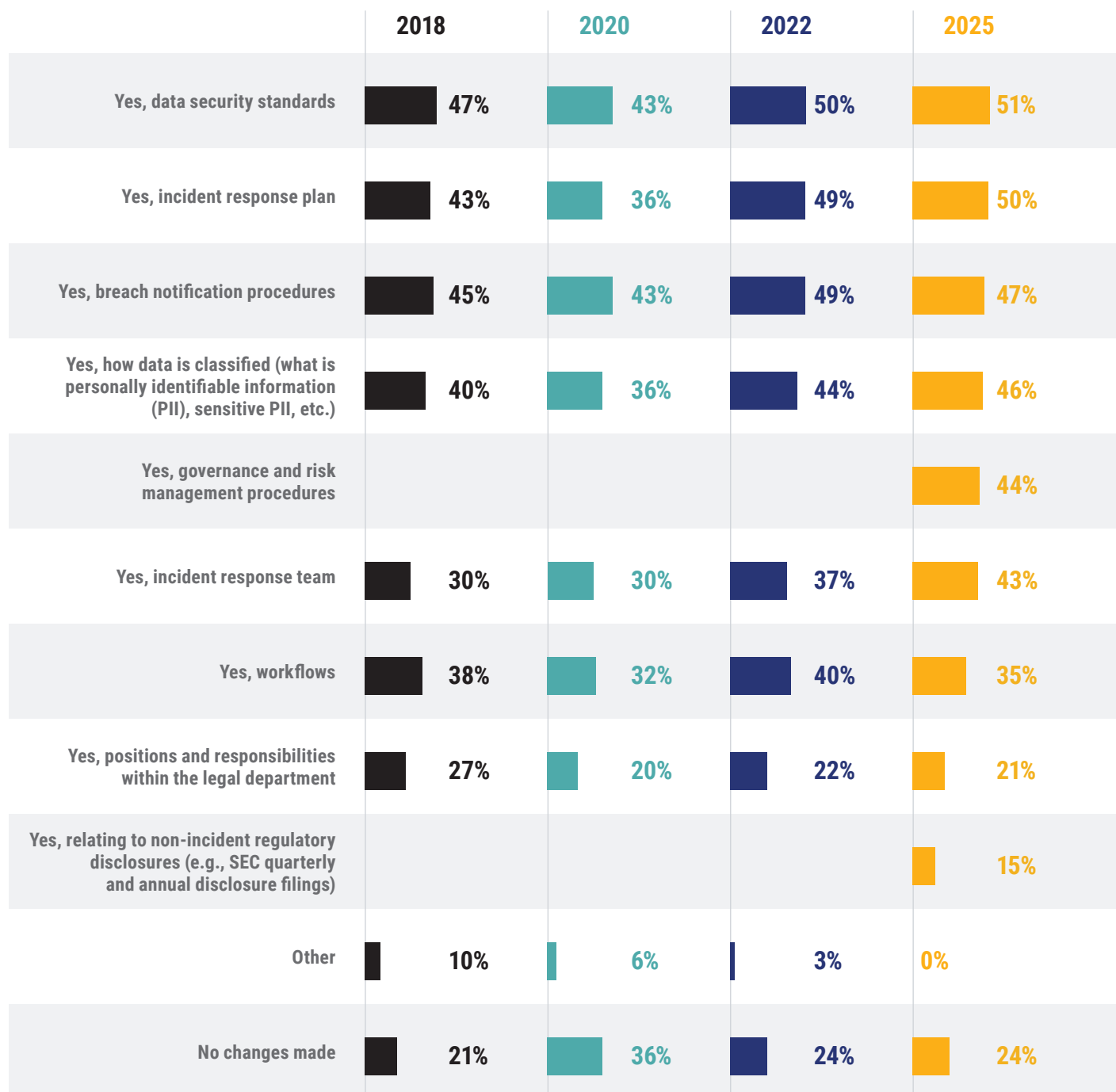
46%


13%

The percentage of respondents indicating that the legal department is deeply embedded in cybersecurity audits decreased from 14 percent in 2022 to nine percent in 2025, while those reporting that the legal department is mostly involved increased from 24 percent to 31 percent. The proportion of legal departments that are slightly involved remained stable at 46 percent, while those not involved at all in their organizations' cybersecurity audits decreased slightly.

Although there are fewer legal departments that are deeply embedded in cybersecurity audits, there is an overall increase in substantial involvement, as evidenced by the rise among those who indicate that legal is mostly involved. This modest progress could indicate a more balanced approach where legal departments play a significant yet collaborative role in audits rather than leading them entirely. The increased involvement of legal departments in cybersecurity audits can enhance compliance, risk management, and strategic oversight, ensuring that legal considerations are adequately integrated into cybersecurity practices to the benefit of the whole organization.

Q: Have you made changes to any of the following as a result of the General Data Protection Regulation (SEC cybersecurity regulations, GDPR)/CCPA/CCPR, NY DFS, NY SHIELD, or similar regulations?





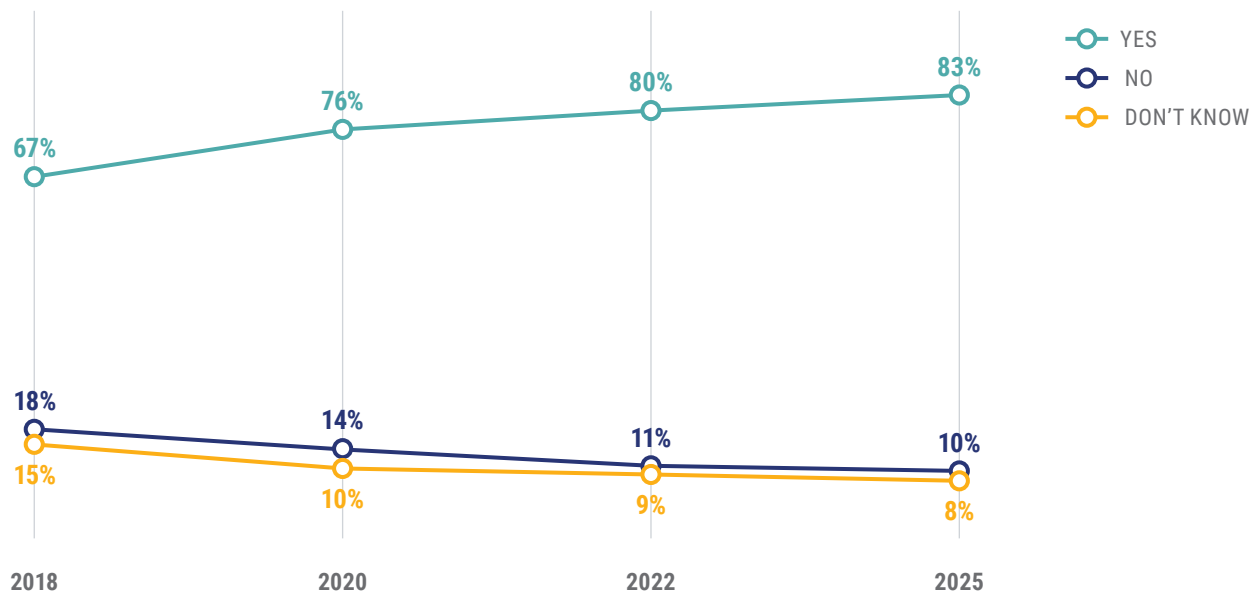
Changes to data security standards (51%) and the incident response plan (51%) are the most common actions taken by US companies as a result of data privacy regulations. For non-US companies, however, the most common actions are changes to the breach notification procedures (62%) and to governance and risk management procedures (55%).

A significant number of organizations have implemented changes in response to data privacy regulations from 2018 to 2025. The data indicates a consistent and increasing focus on enhancing data security standards, incident response plans, and breach notification procedures, with the number of those who made changes to specific items rising to around 50-51 percent by 2025. Changes in the classification of personally identifiable information (PII) also saw an upward trend, reaching 46 percent of participating organizations in 2025. Categories that were added to the list this year, such as governance and risk management procedures (44 percent) and non-incident regulatory disclosures (15 percent), show emerging attention as part of broader risk management and compliance efforts.

Other areas that have seen growth include changes related to incident response teams and workflows, suggesting an emphasis on improving operational readiness. However, changes in positions and responsibilities within the legal department have remained relatively stable around 20-27 percent, which may suggest a cautious approach to structural shifts within legal teams.

Given these results, the lessons for legal departments may be to proactively enhance their data security and incident response frameworks, ensuring compliance with evolving regulations. By regularly updating procedures, classifications, and teams, legal departments can mitigate risks and stay ahead of regulatory demands. Additionally, fostering collaboration with other departments will be crucial to holistically address and manage data privacy challenges across the entire organization.

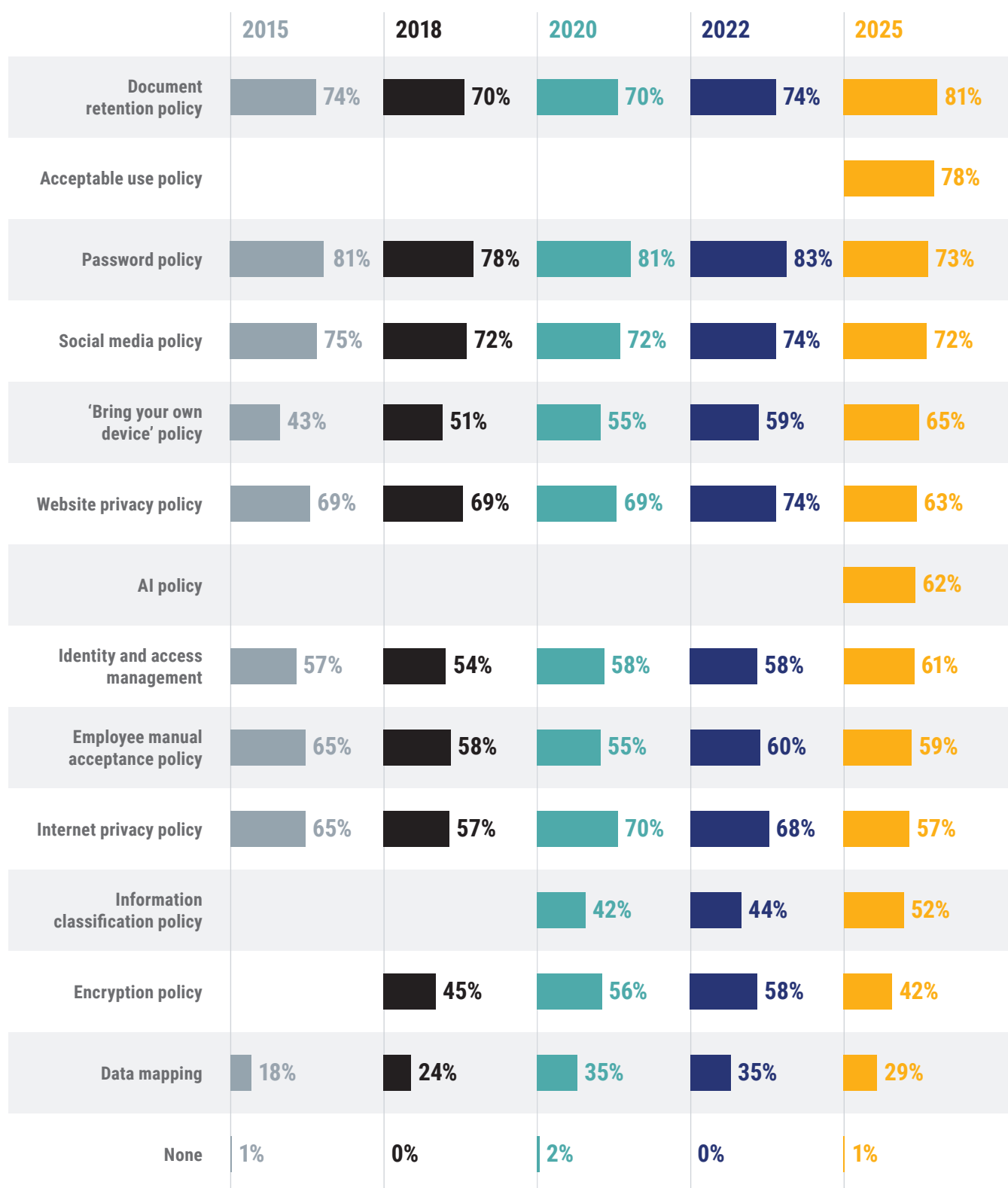
Q: Does your organization have a written cybersecurity incident response plan?




The results reveal a positive and steady increase in the percentage of organizations with a written cybersecurity incident response plan over time, rising from 67 percent in 2018 to 83 percent in 2025. This may be due to the growing awareness and prioritization of structured response strategies to handle cybersecurity incidents. The reasons behind this positive trend likely include heightened regulatory requirements, increased frequency and sophistication of cyberattacks, and a broader understanding of the importance of having a well-defined response plan to minimize damage resulting from cybersecurity incidents and ensure compliance. For legal departments, this means a greater emphasis on collaborating with cybersecurity teams to develop and maintain comprehensive incident response plans that align with evolving best practices and regulatory standards.

94% of large companies with US\$3 billion or more in annual revenue have a cybersecurity incident response plan, but just 67% of small companies with up to US\$100 million in revenue have one.

Q: Does your organization have any of the following written policies in place?





While 62% of participants say their organization has an AI policy, **76 percent of large companies report having this policy in place** compared to under half of small organizations.

The most common company policies are related to document retention (81 percent), acceptable use (78 percent), and password security (73 percent). These policies are essential for ensuring that sensitive information is managed appropriately, that employees understand the acceptable use of company resources, and that strong passwords are maintained to protect against unauthorized access.

The trend over time indicates a steady increase in the adoption of document retention policies, emphasizing the growing importance of managing and preserving information in compliance with legal and regulatory requirements. The consistent presence of password policies at the top of the list highlights the ongoing focus on securing access to systems and data. The significant adoption of “bring your own device” policies (65 percent this year) reflect the increasing prevalence of mobile and remote work, requiring clear guidelines to secure personal devices used for work purposes. The introduction of AI policies (62 percent) in 2025 recognizes the need to govern the use of artificial intelligence within organizations.

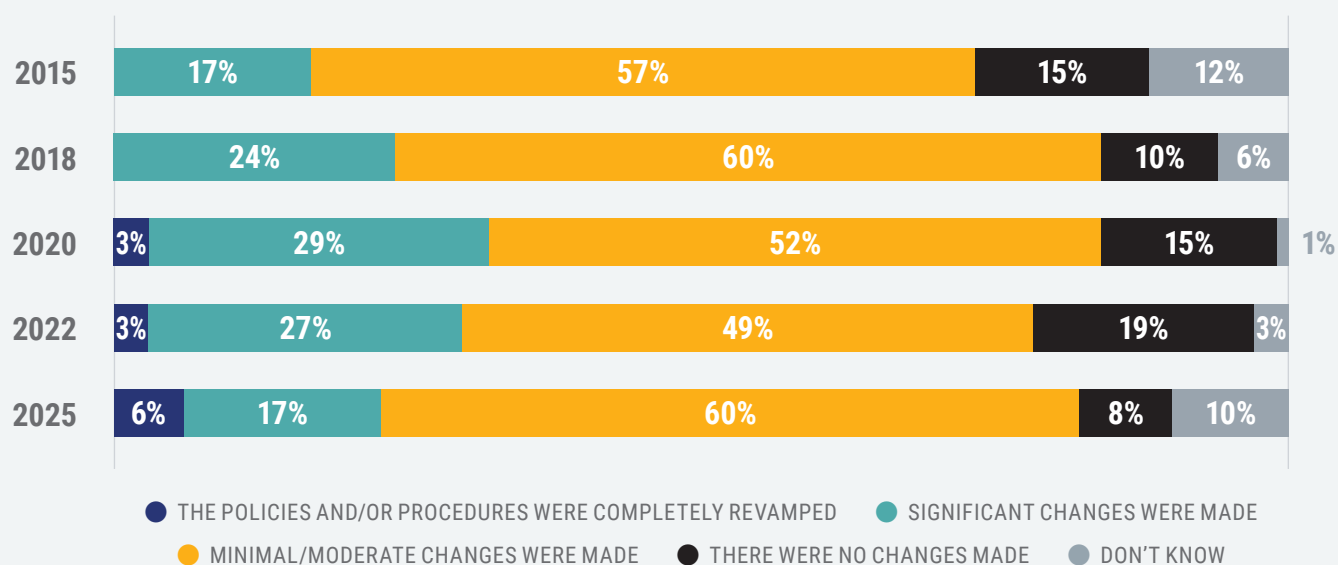
This evolving landscape reflects a comprehensive approach to cybersecurity and data governance. Organizations are increasingly implementing structured policies to address emerging risks and meet evolving regulatory demands. Legal departments play a vital role in this process and should regularly review and update these policies to ensure their continued effectiveness and alignment with the latest industry standards and legal requirements.

Organizations' responses to cybersecurity breaches vary considerably. While only a small percentage (six percent in 2025) report completely overhauling their policies and procedures after a breach (though this number has seen a modest increase), a larger proportion (17 percent in 2025, down from a peak of 29 percent in 2020) made significant changes. The number of organizations making *no* changes after a breach has decreased significantly, reaching just eight percent in 2025, though this figure has fluctuated over time. Finally, the percentage of respondents unsure about the extent of changes implemented remains low, though with some variation.

The fact that most organizations opt for minimal to moderate changes in the company's security policies when responding to a data breach could be a result of the growing maturity of cybersecurity programs. Over time, organizations have likely matured in their cybersecurity practices, having already implemented significant changes in response to earlier breaches. As a result, subsequent breaches may only require fine-tuning or incremental improvements rather than overhauls. By adopting a continuous improvement approach, companies are likely to reduce the need for drastic changes after each incident, leading to more moderate adjustments instead. Finally, as regulations and industry standards evolve, organizations may have already aligned their policies and procedures with these requirements. Therefore, post-breach changes might focus more on compliance tweaks and updates rather than major overhauls.

Q: Describe the degree of change (if any) made to your organization's security policies or procedures following the most recent breach.

Asked only to those in organizations that have experienced at least one cybersecurity breach in the past year.

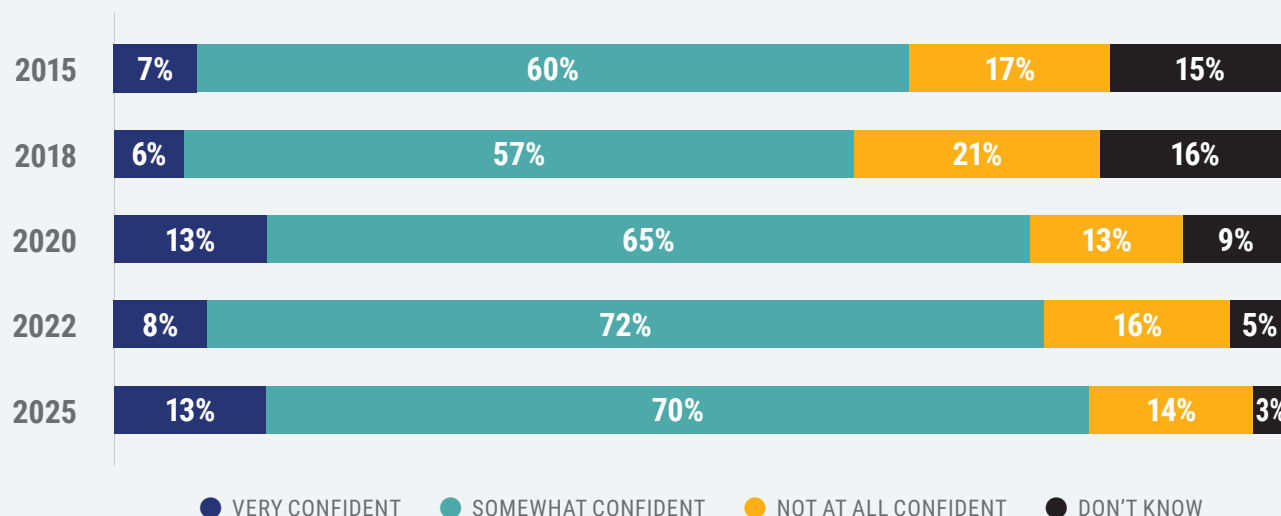


//third-party risk management

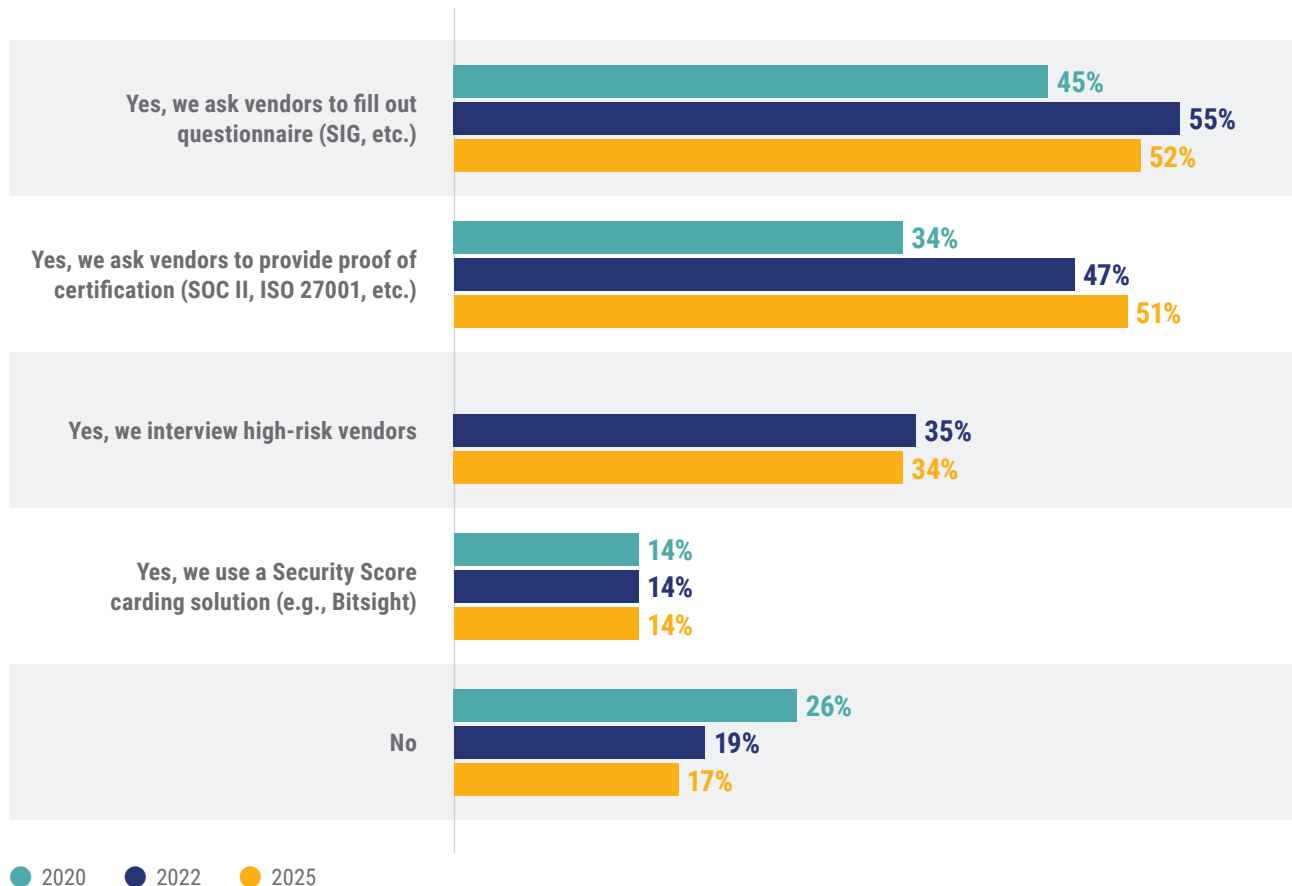
Since 2015 the confidence levels of in-house counsel in their vendors' ability to protect the company from cybersecurity risks have shown a modest positive trend. The percentage of participants who are very confident has fluctuated, starting at seven percent in 2015 and growing to 13 percent in 2025. Those who are somewhat confident have generally increased in numbers, from 60 percent in 2015 to a high of 72 percent in 2022 before slightly decreasing to 70 percent this year.

Respondents who are not at all confident in their vendors' ability to protect them from cybersecurity risks have decreased from a high of 21 percent in 2018 to a low of 13 percent in both in 2025, and those who were not confident to provide an answer have also markedly decreased over the years from 15 percent in 2015 to just three percent in 2025. Overall, the results suggest that while there is still some uncertainty and lack of confidence among in-house counsel regarding third-party vendor management in handling cybersecurity risks, there is a general trend towards increased confidence over time.

Q: How confident are you that your vendors protect you from cybersecurity risks?



Q: Does your organization evaluate vendors for cyber risk?



The practices used by organizations to evaluate vendors for cybersecurity risks have shown some interesting trends. The percentage of organizations asking vendors to fill out questionnaires has increased from 45 percent in 2020 to a peak of 55 percent in 2022 before slightly decreasing to 52 percent in 2025. Similarly, requiring proof of certification has seen a steady increase from 34 percent in 2020 to 51 percent in 2025. Interviewing high-risk vendors was introduced as an option in 2022 and has remained relatively stable at around 34-35 percent. The use of security score carding solutions has remained constant at 14 percent over the years.

Most notably, the percentage of organizations not evaluating vendors at all has decreased from 26 percent in 2020 to 17 percent in 2025, a nine-point drop. We observe a clear growing, positive trend towards more rigorous vendor evaluation methods over time. The most common practices, such as questionnaires and proof of certification, used by more than half of participating companies, are likely the most used because they provide structured and verifiable information about the vendors' cybersecurity practices.

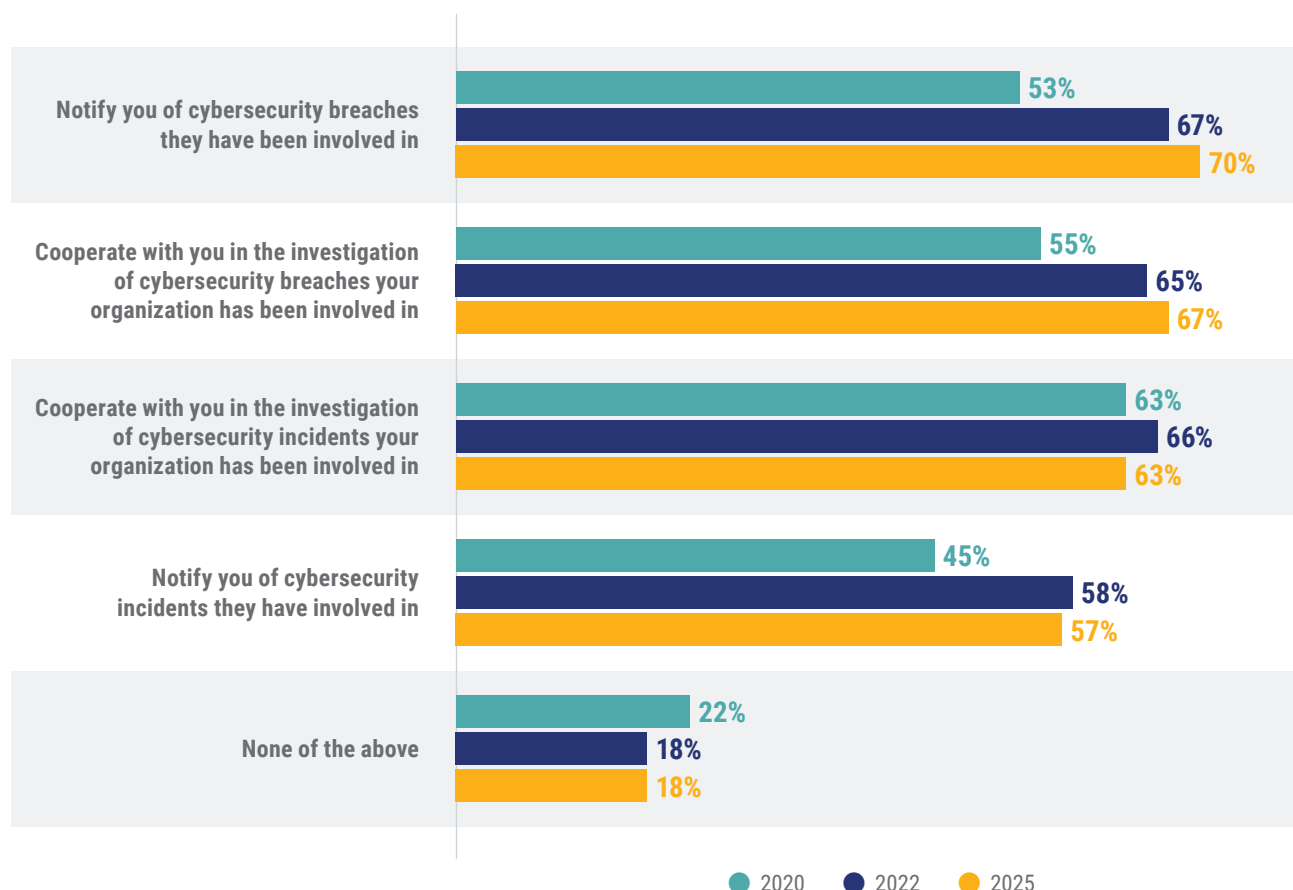
All participating organizations in the finance, information, and insurance industries evaluate vendors for cybersecurity risk, with more than six-in-ten asking for either questionnaires or certifications, or both. In contrast, 33% of participants in manufacturing and 30% in professional services say they do not evaluate vendors for cybersecurity risk.

The results also indicate a trend towards more stringent contractual requirements for vendors regarding cybersecurity practices. The percentage of organizations requiring vendors to notify them of cybersecurity breaches has increased from 53 percent in 2020 to 70 percent in 2025. Similarly, the requirement for vendors to cooperate in the investigation of cybersecurity breaches has risen from 55 percent in 2020 to 67 percent. The requirement for vendors to cooperate in the investigation of cybersecurity incidents has remained relatively stable, ranging from 63 percent to 66 percent. The requirement for vendors to notify organizations of cybersecurity incidents has also increased from 45 percent in 2020 to 57 percent in 2025. Finally, the percentage of organizations not imposing any of these requirements has stabilized at 18 percent, a four-point decrease since 2020.

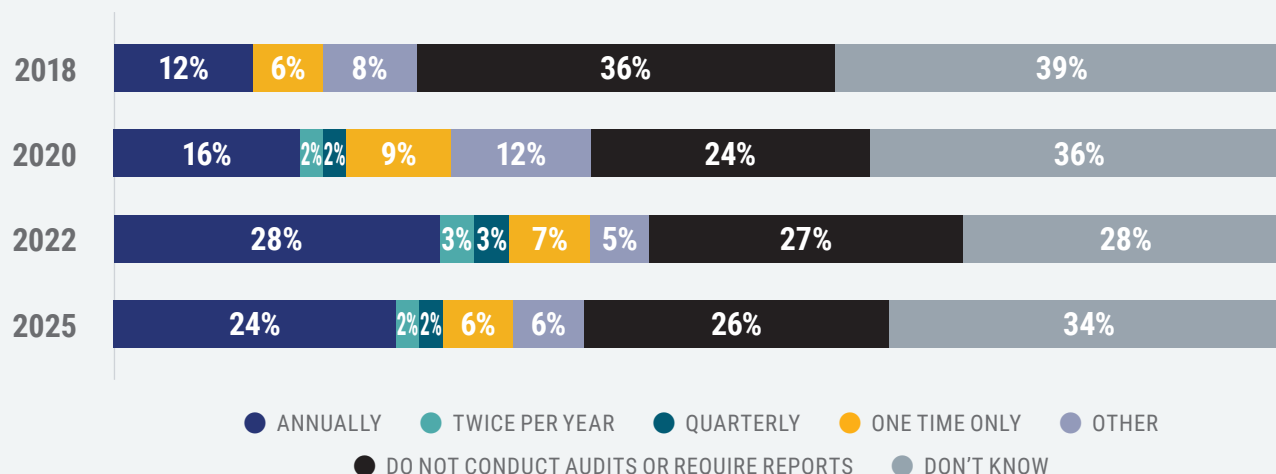
Requiring vendors to notify and cooperate with organizations on breaches and incidents aligns with cybersecurity best practices, which emphasize the importance of timely breach notification and cooperation in investigations to mitigate risks and enhance the organization's incident response capabilities.

35% of participants in small companies say that they do not require vendors to notify them or cooperate with them in the investigation of cybersecurity breaches and incidents.

Q: Do you contractually require your third-party vendors to do any of the following?



Q: How frequently, if at all, does your organization conduct security audits of your high-risk vendors?



Note: The "Twice per year" response option was not offered in 2018.

The results suggest a trend towards more frequent and structured security audits of high-risk vendors since 2018, though this year's results show a moderate step back compared to the last survey in 2022. While there is a growing recognition of the importance of regular security assessments in mitigating cybersecurity risks and ensuring vendor compliance with security standards, under half of participating organizations audit their high-risk vendors, only slightly more than one-quarter conduct audits regularly.

While annual security audits have become more common, their frequency remains a concern. The percentage of organizations conducting them annually rose from 12 percent in 2018 to a peak of 28 percent in 2022, before slightly declining to 24 percent in 2025. Less frequent audits, such as semi-annual or quarterly, remain rare (around two to three percent). One-time audits are also infrequent, representing a relatively stable six to nine percent of organizations. Other audit triggers, including ad-hoc audits and audits tied to vendor contract renewals, account for six percent of organizations. Although the proportion of organizations conducting *no* audits or requiring no reports has decreased from 36 percent in 2018 to just over a quarter in recent years, a worrying trend is the increasing number of respondents (34 percent in 2025) who are *unaware* of their organization's audit frequency. While this is lower than the 2018 peak of 39 percent, it represents a six-point increase since 2022 and suggests a potential disconnect between security practices and employee awareness.

The survey results from 2022 to 2025 reveal an increasing involvement of legal departments in third-party risk management. The percentage of legal departments often involved rose from 31 percent to 38 percent, while those respondents that say that legal is sometimes involved saw a slight increase from 39 percent to 40 percent. Accordingly, the percentage of legal departments that never participate in third-party risk management decreased by five points, from 18 percent to 13 percent, and those unsure about their involvement also declined. These trends show a growing recognition of the legal department's crucial role in managing third-party risks, as their expertise can ensure compliance with legal and regulatory standards, reduce potential liabilities, and safeguard the organization's reputation.

Legal departments in **large companies are more often involved** in third-party risk management (49%) than departments in small organizations (29%).

Q: How involved is the legal department in Third-Party Risk Management [TPRM]?

● OFTEN ● SOMETIMES ● NEVER ● DON'T KNOW

2022

31%

39%

18%

11%

2025

38%

40%

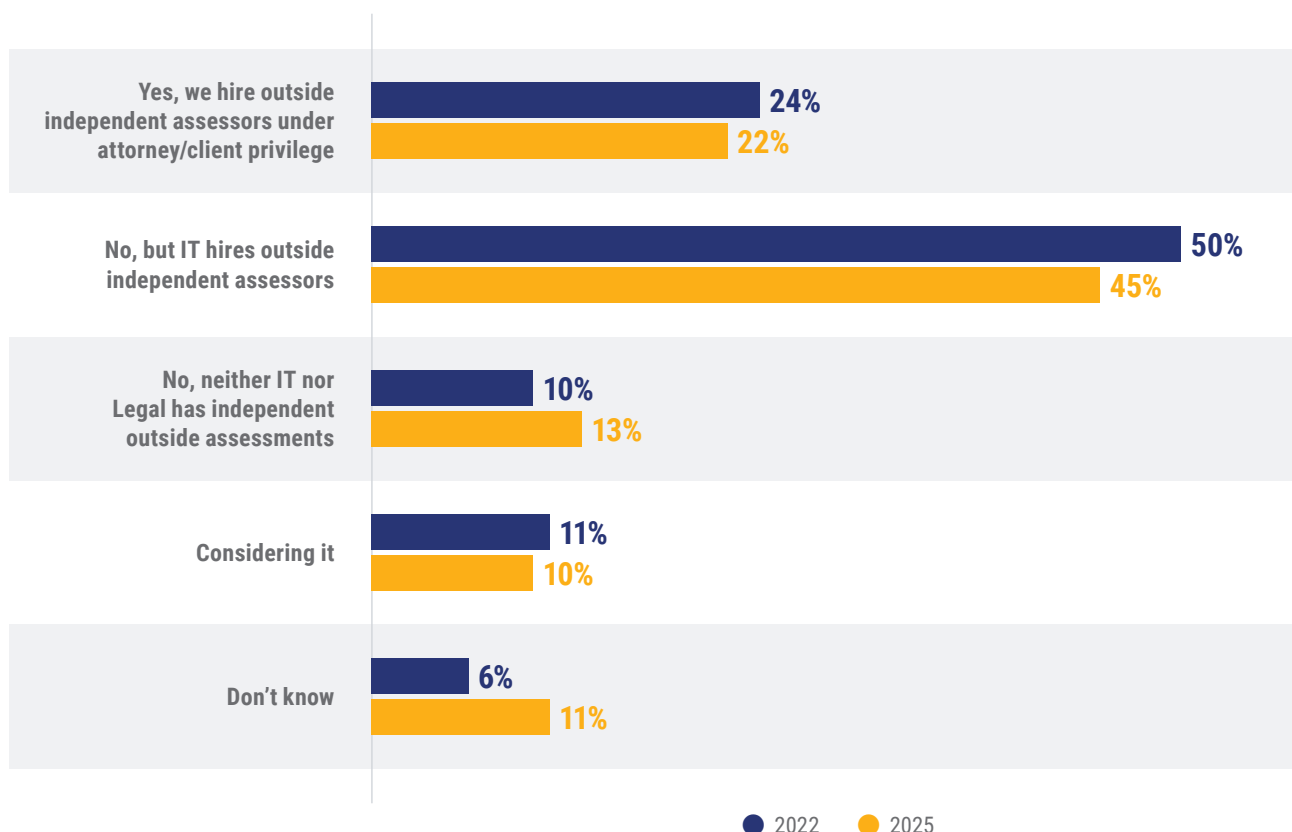
13%

9%

This year's survey shows a slight decrease in the percentage of legal departments hiring outside cybersecurity assessors under attorney-client privilege, dropping from 24 percent in 2022 to 22 percent in 2025. Similarly, there is a reduction in the number of participants who report that IT departments hire outside assessors, from 50 percent to 45 percent. The percentage of organizations where neither IT nor the legal department conducts independent assessments increased from 10 percent to 13 percent. Ten percent say they are considering hiring outside auditors, while those who are not aware practically doubled.

Although the change since 2022 is modest, this result may signal some uncertainty or lack of clarity within organizations regarding their cybersecurity assessment practices. The involvement of outside assessors under attorney-client privilege is crucial as it enhances the confidentiality and protection of sensitive cybersecurity findings, allowing organizations to address vulnerabilities without the risk of exposure in legal proceedings. The decrease in external assessments could potentially impact the organization's ability to maintain robust cybersecurity defenses and respond effectively to emerging threats. Thus, it is essential for organizations to ensure clear and informed decision-making processes around cybersecurity assessments to sustain and improve their cybersecurity maturity.

Q: Does the legal department hire outside cybersecurity assessors/auditors to conduct independent reviews of their organization's cybersecurity maturity under attorney-client privilege?



The results point to a growing commitment among legal departments to engage external forensics experts for thorough and unbiased reviews of cybersecurity incidents, with a slight increase in the percentage of legal departments that hire outside experts to conduct independent reviews of cybersecurity incidents, from 28 percent to 31 percent. Those departments that engage in this practice occasionally have declined, however, from 21 percent to 17 percent, while those that are considering it increased marginally from 10 percent to 11 percent. The percentage of legal departments that do not hire outside experts decreased from 28 percent to 26 percent, and those who do not know saw a slight increase from 14 percent to 15 percent. Overall, these results remain largely the same compared to 2022.

Q: Does the legal department or outside counsel hire forensics experts to conduct independent reviews of a cybersecurity incident?

● YES ● SOMETIMES ● CONSIDERING IT ● NO ● DON'T KNOW

2022



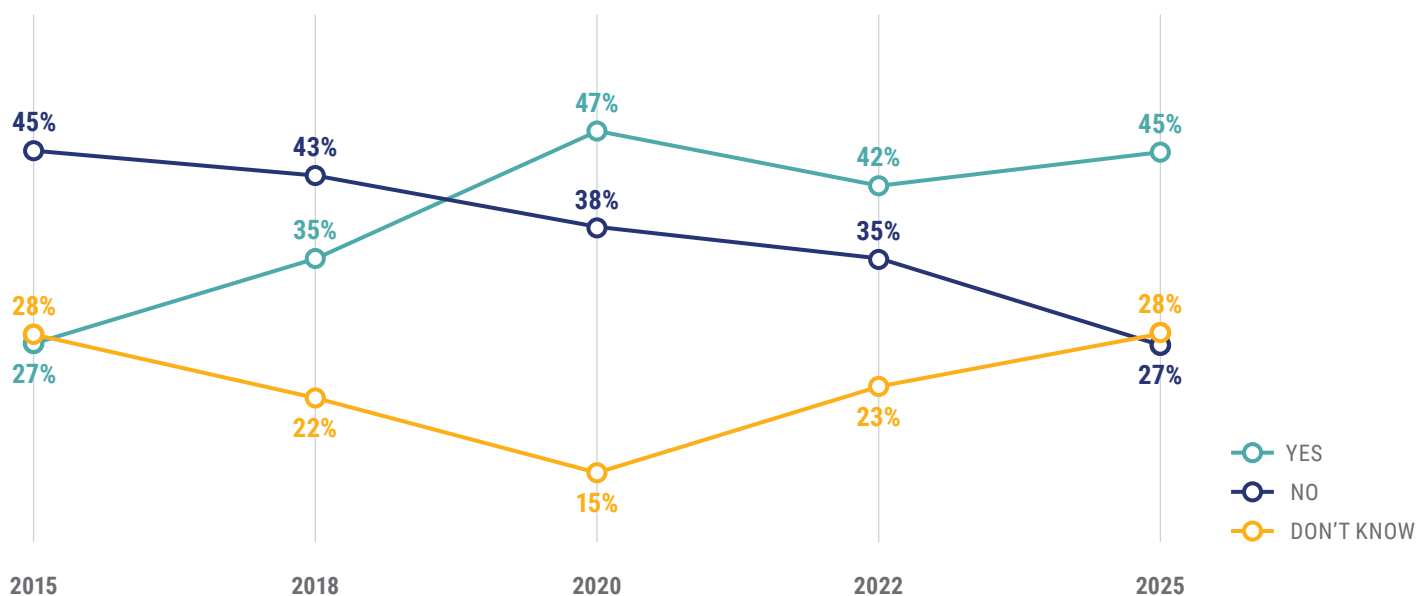
2025



The percentage of organizations that proactively collaborate with law enforcement or other governmental agencies to address cybersecurity risks has increased significantly since 2015, peaking at 47 percent in 2020, and remaining stable at 45 percent in 2025. Conversely, the percentage of organizations that do not collaborate decreased steadily from 45 percent in 2015 to 27 percent.

This trend may suggest a growing recognition of the importance of involving law enforcement and governmental agencies in managing cybersecurity risks, possibly due to escalating cyber threats and regulatory pressures. However, the fluctuating values of the “do not know” responses and a consistent portion of non-collaborating organizations could indicate persistent uncertainty or hesitation in formalizing such collaborations. Proactive collaboration can enhance an organization’s cybersecurity posture by leveraging external expertise and resources to address evolving cyber threats effectively. But there are barriers that can explain the lack of collaboration, including concerns over confidentiality, fear of reputational damage, or perceived bureaucracy in dealing with governmental agencies.

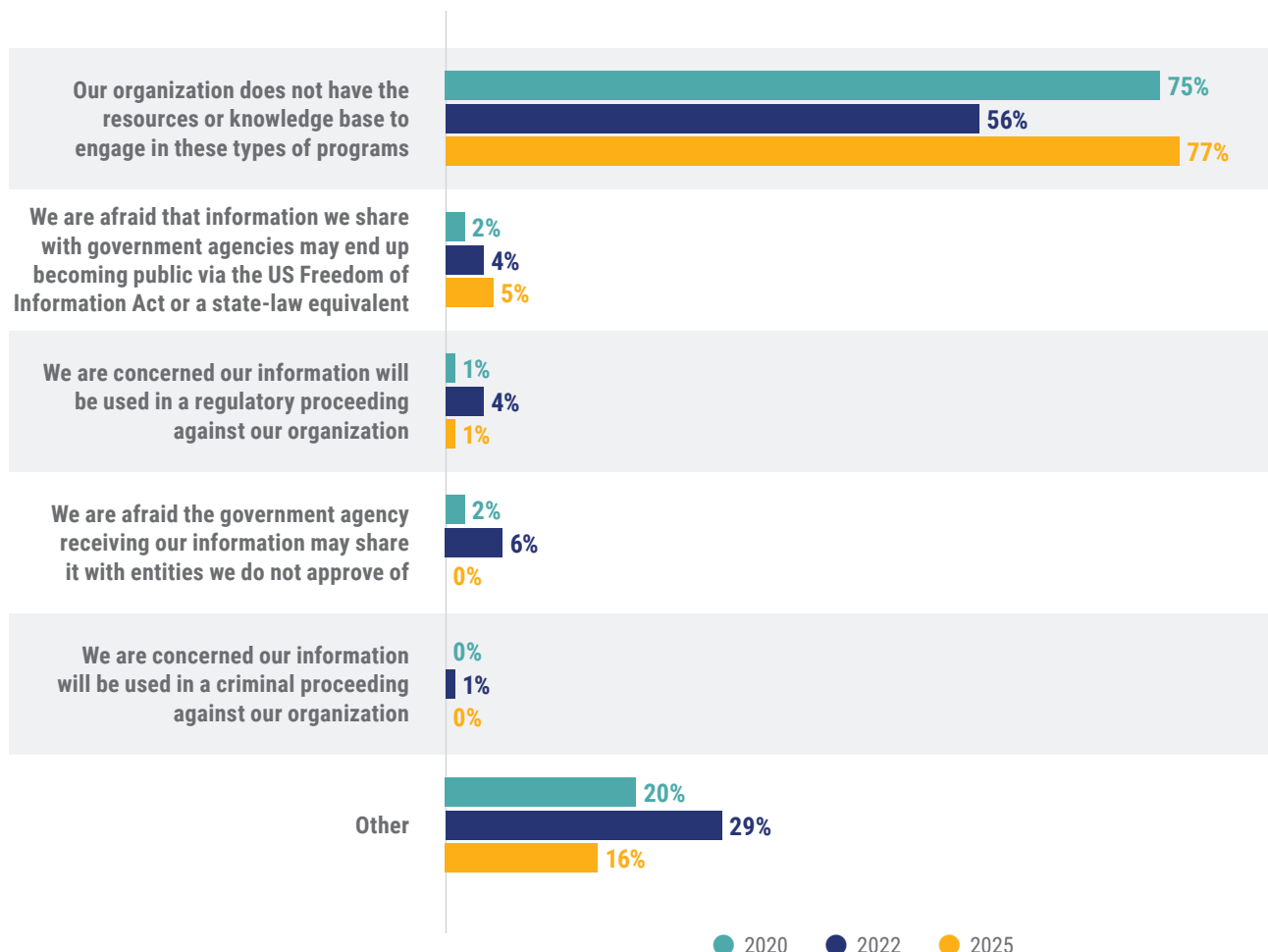
Q: Does your organization collaborate proactively with law enforcement [member of InfraGard, etc.] or other governmental agencies to address cybersecurity risks?



Organizations based in the US are more inclined to collaborate with law enforcement and government agencies (51%) than non-US organizations (44%).

Q: Please explain why your organization does not collaborate proactively with law enforcement or other government agencies to address cybersecurity risks.

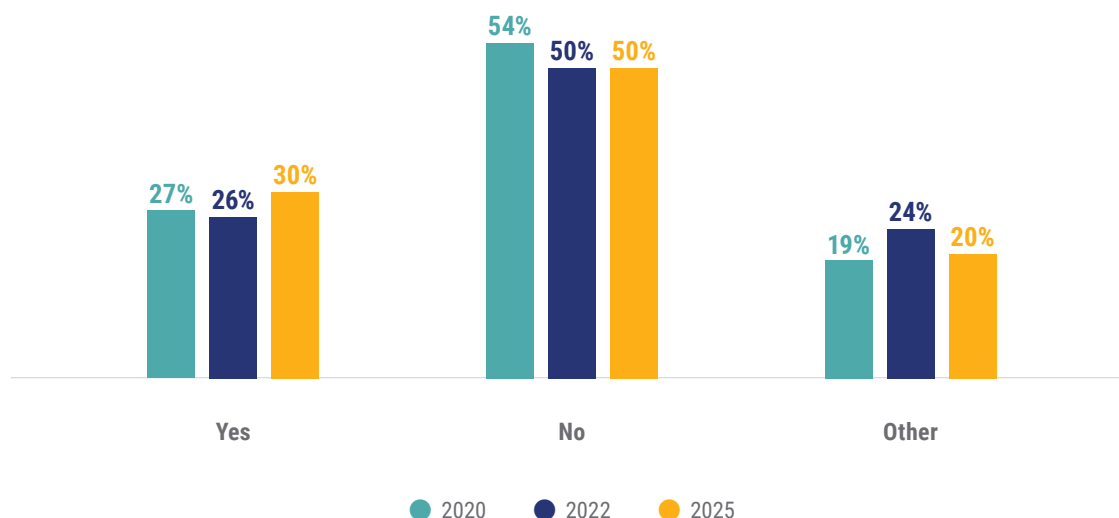
Asked only to those whose organizations do not collaborate proactively with law enforcement agencies or other governmental agencies.



The results clearly show that the primary reason for organizations choosing not to collaborate with law enforcement or governmental agencies on addressing cybersecurity risks is the lack of resources or knowledge base to engage in such programs, with 75 percent in 2020, 56 percent in 2022, and a notable increase to 77 percent in 2025. This fluctuation, particularly the significant drop in 2022 and subsequent rise, may indicate temporary efforts to address resource constraints or knowledge gaps, which were not sustained. Additionally, there is a modest increase in concerns about information shared with government agencies becoming public (two percent in 2020 to five percent in 2025) and the potential for information misuse in regulatory proceedings (one percent to four percent in 2022, returning to one percent in 2025). Fears of unauthorized information sharing peaked in 2022 (six percent) but dropped to zero in 2025.

The main takeaway is that resource limitations and knowledge gaps are persistent barriers to collaboration. Addressing resources and knowledge constraints, along with building trust in the confidentiality and use of shared information, could encourage more organizations to collaborate with governmental agencies on cybersecurity risks.

Q: Is your organization more inclined to collaborate proactively with a nonregulatory agency, such as the US Department of Homeland Security, versus a regulatory agency, such as the US Federal Trade Commission (or non-US equivalent body)?



The survey results indicate a slight increase in organizations' willingness to collaborate with a nonregulatory government agency on cybersecurity matters, with a rise from 27 percent in 2020 to 30 percent in 2025. The percentage of organizations not willing to collaborate has remained relatively stable, decreasing slightly from 54 percent to 50 percent. Participants who indicated that other situations apply show some fluctuation, peaking at 24 percent in 2022 before returning to 20 percent in 2025.

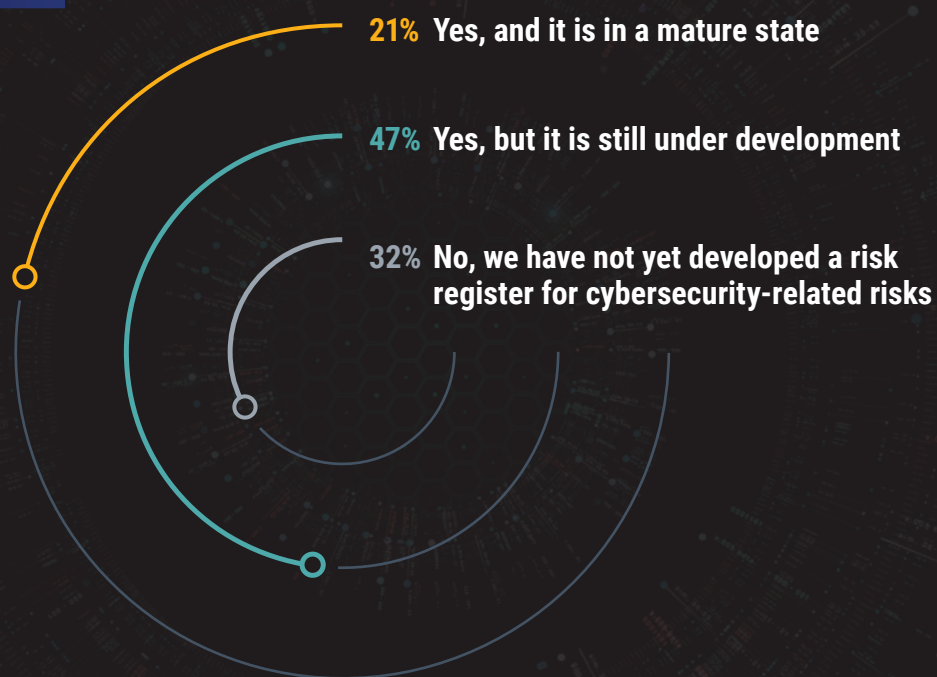
Companies may be more inclined to collaborate with nonregulatory agencies because these agencies are perceived as partners in enhancing national security rather than enforcing compliance and penalizing non-compliance. Nonregulatory agencies may offer more support and resources without the fear of regulatory actions, fostering a collaborative environment. On the other hand, regulatory agencies are associated with oversight and enforcement, which can deter organizations from sharing information due to concerns about potential legal or regulatory repercussions. Half of the participating organizations, nonetheless, may still be unwilling to collaborate with a nonregulatory agency due to concerns about the confidentiality of shared information and potential indirect repercussions, such as reputational damage or future regulatory scrutiny.

Participants in the information industry are least likely to collaborate with a nonregulatory agency (61%).

Sixty-eight percent of organizations have taken steps toward developing a comprehensive risk register for cybersecurity risks, with 21 percent having a mature register and 47 percent reporting that a register is under development. The remaining 32 percent of organizations have not yet developed a cybersecurity risk register.

This indicates a positive trend toward recognizing the importance of systematically identifying and managing cybersecurity risks, but there are still many organizations that have not fully embraced this practice. The development of a comprehensive risk register is essential for proactively addressing potential threats, ensuring better risk management, and enhancing overall cybersecurity resilience. Organizations with mature risk registers are likely better equipped to identify vulnerabilities, allocate resources effectively, and implement mitigation strategies. Those still developing their registers should prioritize this task to ensure they are well-prepared for evolving cybersecurity challenges.

Q: Has your organization developed a comprehensive risk register for cybersecurity risks?





Q: Please share any best practices or most important lessons learned that may help others manage cybersecurity risk in their organizations.

We have distilled the 10 most important lessons learned from survey participants in their experience managing cybersecurity risks in their organization to create a brief checklist that will assist legal departments in their efforts to enhance safety and make cybersecurity an enterprise-wide priority:

01

Align Policies and Procedures:

Ensure documented policies and standards match operational procedures and implement ongoing monitoring and testing against cyber controls.

03

Proactive Cyber Insurance Awareness:

Understand the coverage details of your cyber insurance to manage risks effectively.

02

Annual Tabletop Exercises:

Conduct regular tabletop exercises, including those managed by outside vendors, to test incident response plans and train key stakeholders.

04

Cross-Department Collaboration:

Foster collaboration between IT, Legal, and other departments, ensuring cybersecurity is a shared responsibility and managed jointly.

05

**Comprehensive
Employee Training:**

Implement frequent, tailored cybersecurity training for all employees, emphasizing that cybersecurity is everyone's responsibility.

06

**Phased Cybersecurity
Maturity Plans:**

Develop a multi-phase plan to improve cybersecurity maturity, focusing on containing a significant portion of risk in each phase.

07

Engage External Experts:

Hire cybersecurity consultants for dark-web monitoring, vulnerability scanning, and penetration testing, and involve outside counsel when necessary.

08

Breach Preparedness:

Have a breach coach, develop incident response plans for both InfoSec professionals and cross-functional leaders, and run regular tabletop exercises at multiple organizational levels.

09

**Enterprise-Wide
Cooperation:**

Promote enterprise-wide, cross-functional cooperation and collaboration to enhance cybersecurity initiatives and address risks comprehensively.

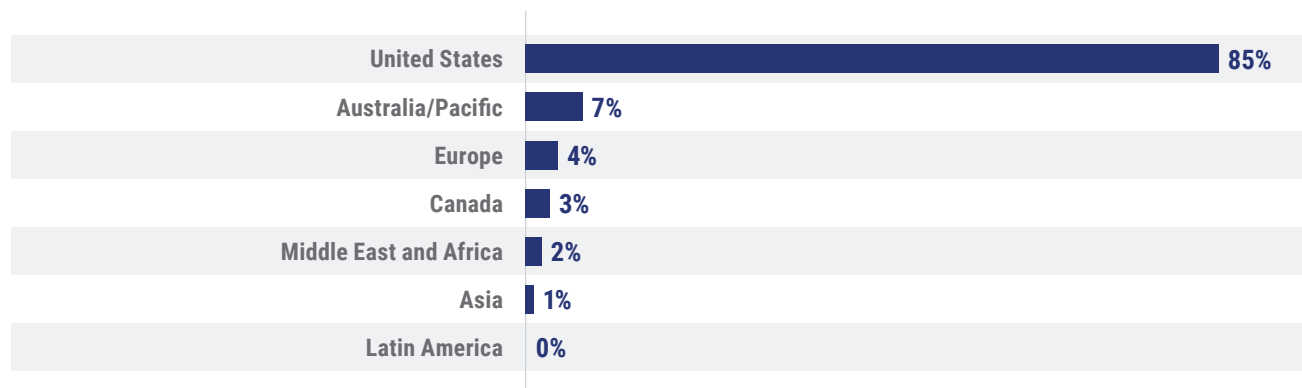
10

Resource Allocation:

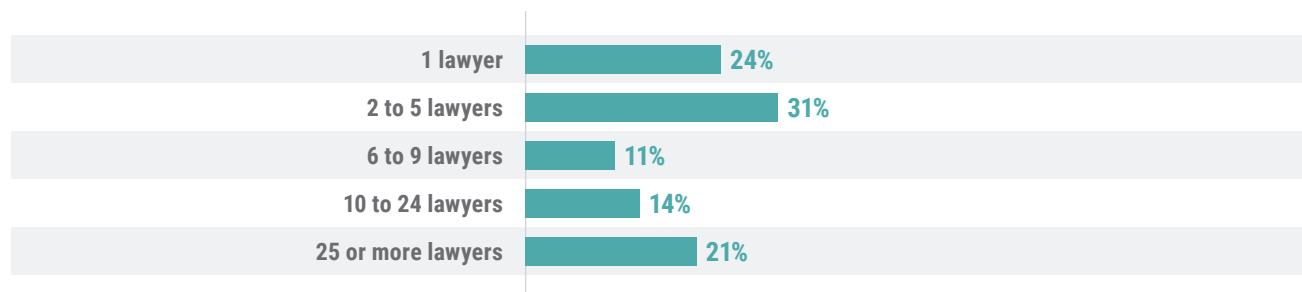
Ensure adequate resources and budget for proactive cybersecurity measures, recognizing the evolving nature of threats and the importance of continuous security improvements.

_participant profile

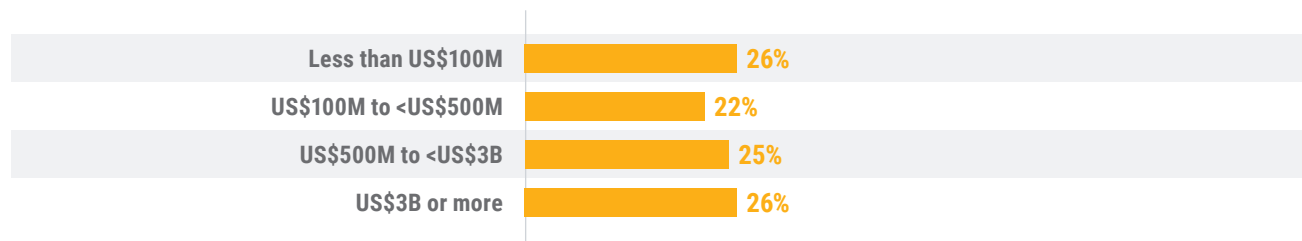
Global Region



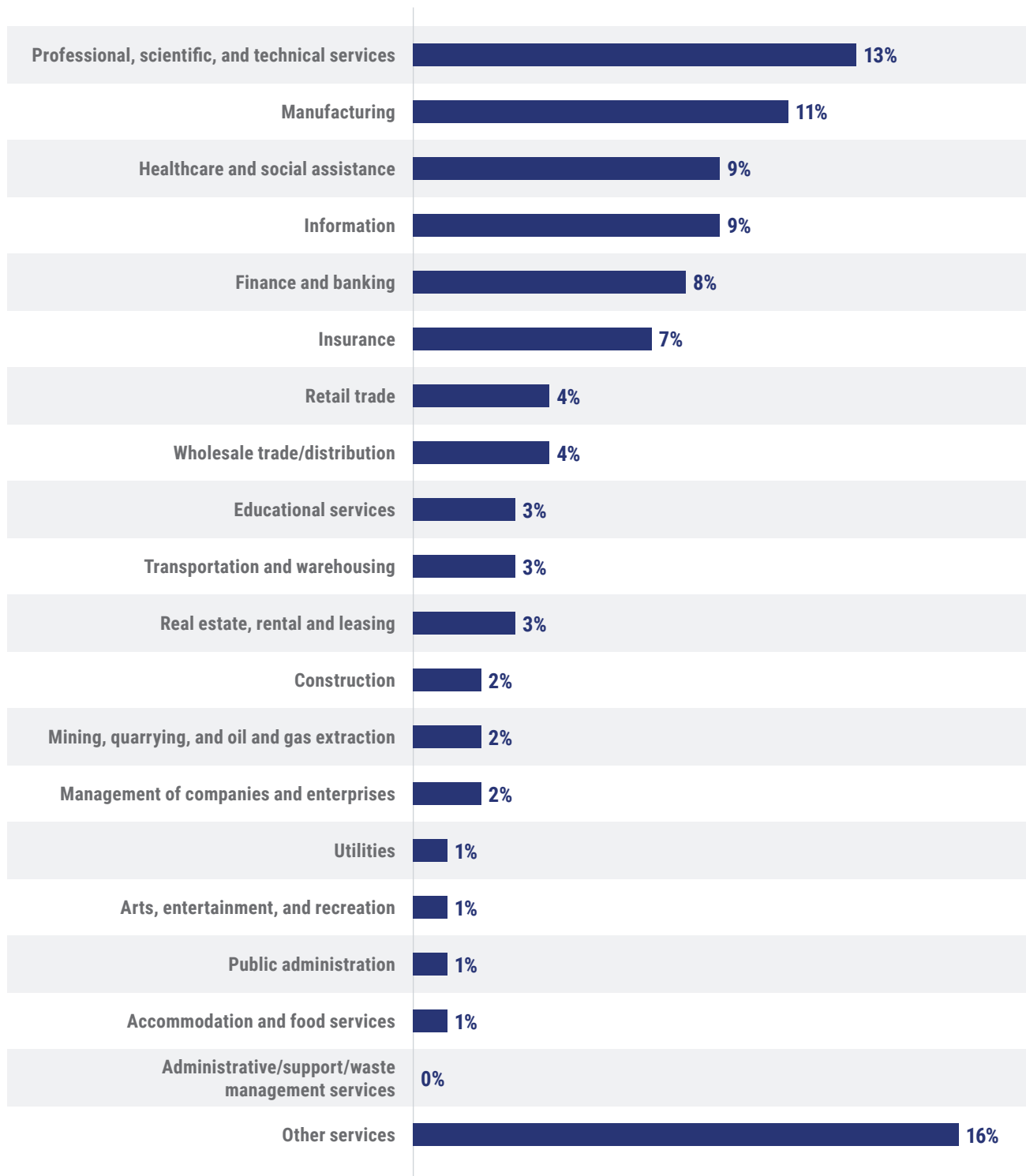
Number of Lawyers



Number of Lawyers



Industry



_methodology

Survey instrument_

The survey questionnaire was offered through an online survey platform. Personalized survey links were sent by email to the target population, which allowed participants to save their responses and fill out the questionnaire in more than one sitting, if needed.

Fielding period_

The survey opened on November 14, 2024, and closed on January 3, 2025. Reminder emails were sent weekly.

Target population_

We targeted ACC members worldwide who are the decision-makers in their respective legal departments. To further expand our reach, we also sent participation invites through other ACC Foundation contacts.

Participation_

A total of 278 legal department decision-makers participated. Apart from targeted email messages, opportunities to participate were also sent through LinkedIn campaigns and on relevant ACC online communities.

Anonymity_

Survey responses were confidential. No information is linked in any way to an individual respondent. The results are provided only at the aggregate level, and respondents' quotes from write-in responses were carefully reviewed and edited, if appropriate, to remove any identifiable information related to respondents or their organizations.

Data accuracy_

Not all respondents answered all questions. The percentages provided are based on the number of valid responses received for each individual question. Many survey questions offered the opportunity to select multiple response options. In those cases, percentages may not total to 100 percent. In some instances, percentages may add up slightly above or below 100 percent due to rounding.

The Association of Corporate Counsel (ACC) is a global legal association that promotes the common professional and business interests of in-house counsel who work for corporations, associations and other organizations through information, education, networking opportunities and advocacy initiatives. With more than 48,000 members employed by over 12,000 organizations in 117 countries, ACC connects its members to the people and resources necessary for both personal and professional growth. By in-house counsel, for in-house counsel.® To learn more about ACC Research & Insights, please contact ACC Research at +1 202.293.4103 or visit: acc.com/surveys.

The ACC Foundation – a 501(c)(3) non-profit organization – supports the efforts of the Association of Corporate Counsel, serving the needs of the in-house bar through the dissemination of research and surveys, leadership and professional development opportunities, and support of diversity and pro-bono initiatives.

The ACC Foundation partners with corporations, law firms, legal service providers and bar associations to assist in the furtherance of these goals.

This report and the information contained herein are copyrighted by the Association of Corporate Counsel (ACC). Any use thereof, in whole or in part, must comply with ACC's copyright policy located at acc.com/about/privacy-policies/copyright and applicable copyright protection laws. Any use or uploading into external applications, websites, bots or software is prohibited, including those that make use of artificial intelligence infrastructure or software (e.g., generative AI, machine learning, deep learning or large language models).

When using extracts from this report, the following language must appear: "Reprinted with permission from the Association of Corporate Counsel 2025. All Rights Reserved." Request permission for re-use from www.copyright.com. Or contact ACC directly at acc@acc.com.

ACC HEADQUARTERS OFFICE

1001 G St., NW, Suite 300W
Washington, DC 20001 USA
Tel +1 202.293.4103
acc-foundation.com

ACC Foundation
Association of Corporate Counsel