2022

_state of CYBERSECURITY REPORT

ACC Foundation
Association of Corporate Counsel

IN COLLABORATION WITH EY Building a better working world

EY
Building a better working world
Can your company's current cyber defenses keep up with the speed of quantum?
The better the question. The better the answer.
The better the world works.

© 2022 Ernst & Young LLP. All Rights Reserved. ED None

_table of (contents):

_introduction:

The Association of Corporate Counsel (ACC) Foundation, in collaboration with Ernst & Young, LLP, is pleased to present the *2022 State of Cybersecurity Report, An In-house Perspective*. In its fourth edition, this report sheds light on the growing influence that legal departments are having on organization-wide cybersecurity practices and risk reduction strategies.

The results reveal that the legal department continues to play an increasingly important role in enterprise-wide cybersecurity strategy and the Chief Legal Officer (CLO) is often front and center. There is growing cross-functional collaboration among Legal, IT, security and other applicable business units, and one out of five companies now have a dedicated cybersecurity lawyer (often a senior level position) who is sometimes even embedded in the IT department.

The potential reputational damage, liability to data subjects, and effect on business continuity are the top concerns resulting from a data breach and therefore, the results show a significant increase in the number of companies that now require regular cybersecurity training for all staff and thirty-eight percent of companies now expect to increase their cyber-related spend over the coming year.

The data included in this report represents 265 companies across 17 industries and 24 countries, providing a comprehensive understanding of how legal departments of different sizes engage in cybersecurity matters.

The ACC Foundation would like to thank the participants in this study for contributing their valuable expertise as well as the survey advisory board for helping to craft the questions and interpret the results in a way that best reflects the significant changes that have occurred in the cybersecurity landscape over the past two years. We hope the insights included in this report will be useful to law department leaders and in-house legal professionals facing an increase in responsibilities around cybersecurity issues. Finally, we hope the results convey the importance of having legal departments be in a central position to define, influence, and implement cybersecurity policies and risk reduction strategies for their organizations.

_The ACC Foundation/

_acknowledgements:

The ACC Foundation wishes to recognize the following members of the cybersecurity survey project advisory board for their contributions to the development of the *2022 State of Cybersecurity Report*.

John G. Bates
Senior Manager
Ernst & Young LLP

Patrick Huston
Brigadier General (Ret.)
U.S. Army
National Association of
Corporate Directors

Robert Kang
Director & Associate General
Counsel for Cybersecurity
Meta

Nkechi Kanu
Counsel
Crowell & Moring

Ilona Levine
Senior VP, General Counsel &
Corporate Secretary
Internet Society

_key(findings):

01

Cybersecurity Responsibilities Are Increasing for Chief Legal Officers

Cybersecurity reports to the CLO in 38 percent of departments surveyed (15 percent with a direct reporting line and 23 percent with a dotted line). Eighty-four percent of CLOs now have at least some cybersecurity-related responsibilities (up from 76 percent in 2020), whether it be a leadership position, being part of a broader team with cyber responsibilities, or being a part of an incident response team.

02

22 Percent of Companies Now Have A Dedicated Cybersecurity Lawyer

Twenty-two percent of companies now employ an in-house counsel with responsibility for cybersecurity—up 10 percentage points since 2018. In 48 percent of cases, this lawyer is responsible for coordinating cyberlaw strategy across the entire enterprise and in 29 percent of cases, this lawyer is fully embedded in cybersecurity/IT and works directly with technical resources. Fifty-six percent of these lawyers are in senior-level positions.

03

Many Companies Practice Strong Cross-functional Collaboration To Reduce Cyber Risk

Fifty-five percent of those surveyed agree that their organization's IT/cyber department, legal department, and other relevant business units are integrated and work together to reduce cybersecurity risk. There is wide variation across industries with a higher percentage of companies in the IT and educational services sectors reporting cross-functional collaboration (73 percent and 67 percent respectively).

04

The Number of Companies That Now Require Annual Cybersecurity Training For All Employees Has Increased 20 Percentage Points Since 2020

Sixty-three percent of companies now have mandatory annual trainings on cybersecurity for all employees—an increase from 43 percent in 2020. Twenty-seven percent require training on a different interval and just nine percent have no training requirements at all—a reduction from 33 percent in 2018. Among companies that require training, 25 percent customize that training to the specific role or level of security access of individual staff.

05

Just 31 Percent of Legal Departments Say They Are Regularly Involved in Their Company's Third-Party Risk Management (TPRM)

Twenty percent of respondents said their company's TPRM program is able to work with legal to create customized security controls for a low maturity client that is very important for a particular business unit and just 31 percent say their legal department is "often" involved in TPRM. This varies dramatically by industry with legal being more often involved in the finance and insurance industries.

06

38 Percent of Legal Departments Say Their Spend Has Increased As A Result Of Their Approach To Cyber, Compared To One Year Ago

Thirty-eight percent of legal departments now say that their spend has increased as a result of their company's approach to cybersecurity—an increase from just 23 percent who said so in 2015. Fifty percent said this increase was mainly attributed to outside spend (among law firms, ALSPs, and consultants), while 25 percent said the increase was mainly attributed to inside spend (on legal resources exclusively devoted to cybersecurity).

07

Damage To Reputation, Liability To Data Subjects, And Business Continuity Are The Top 3 Areas Of Concern Resulting From A Data Breach

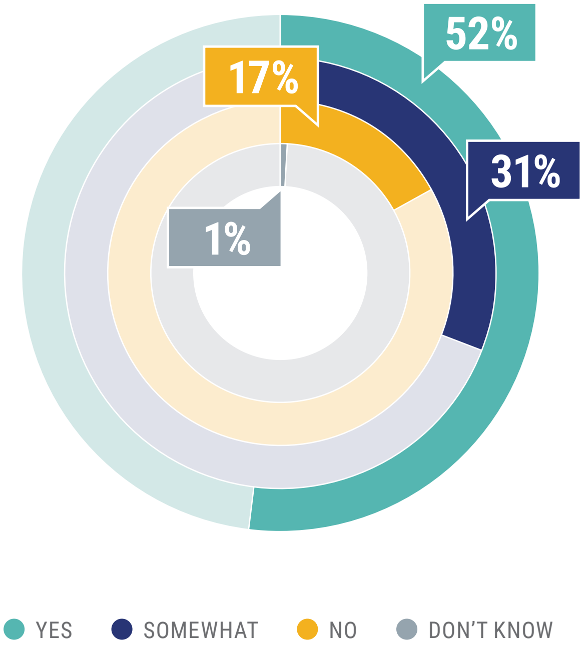
Damage to reputation (77 percent), liability to data subjects (61 percent), and business continuity (51 percent) are the most immediate concerns with regard to a data breach. Issues of least concern include the effect on employee morale, concern among board of directors, executive liability, shareholder activity, and preservation of lawyer-client privilege.

SECTION_01

//the legal department's (role) in "cybersecurity"

Responsibilities for cybersecurity and privacy are clearly divided in a majority of participating organizations. Thirty-one percent indicated that there is somewhat of a distinction between these two areas, and 17 percent responded that responsibilities for cybersecurity and privacy are not differentiated in their organizations.

Q: Is there a clear distinction between responsibilities for cybersecurity and privacy in your organization?

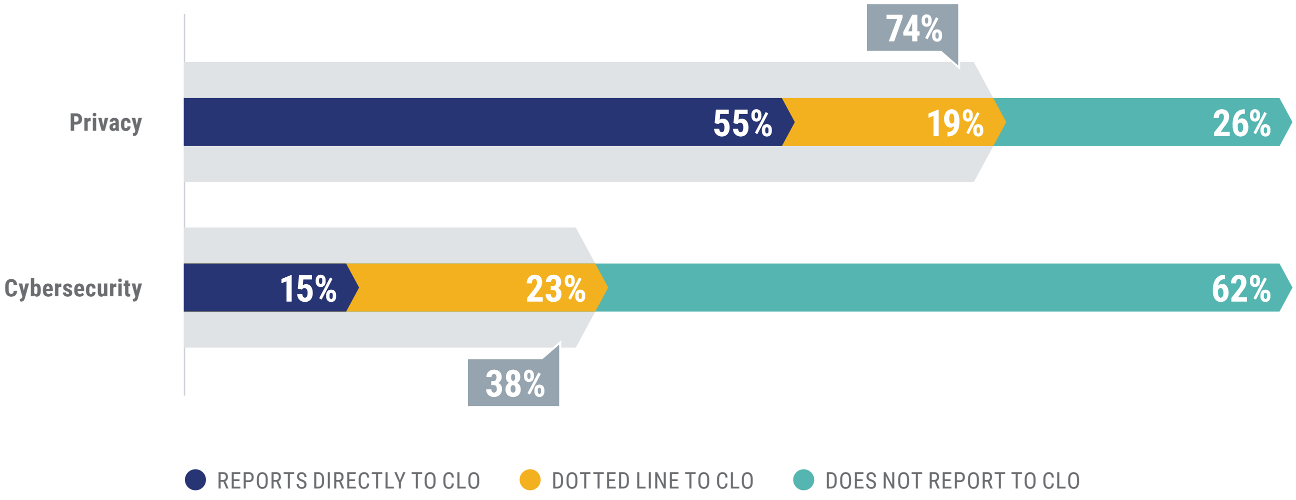


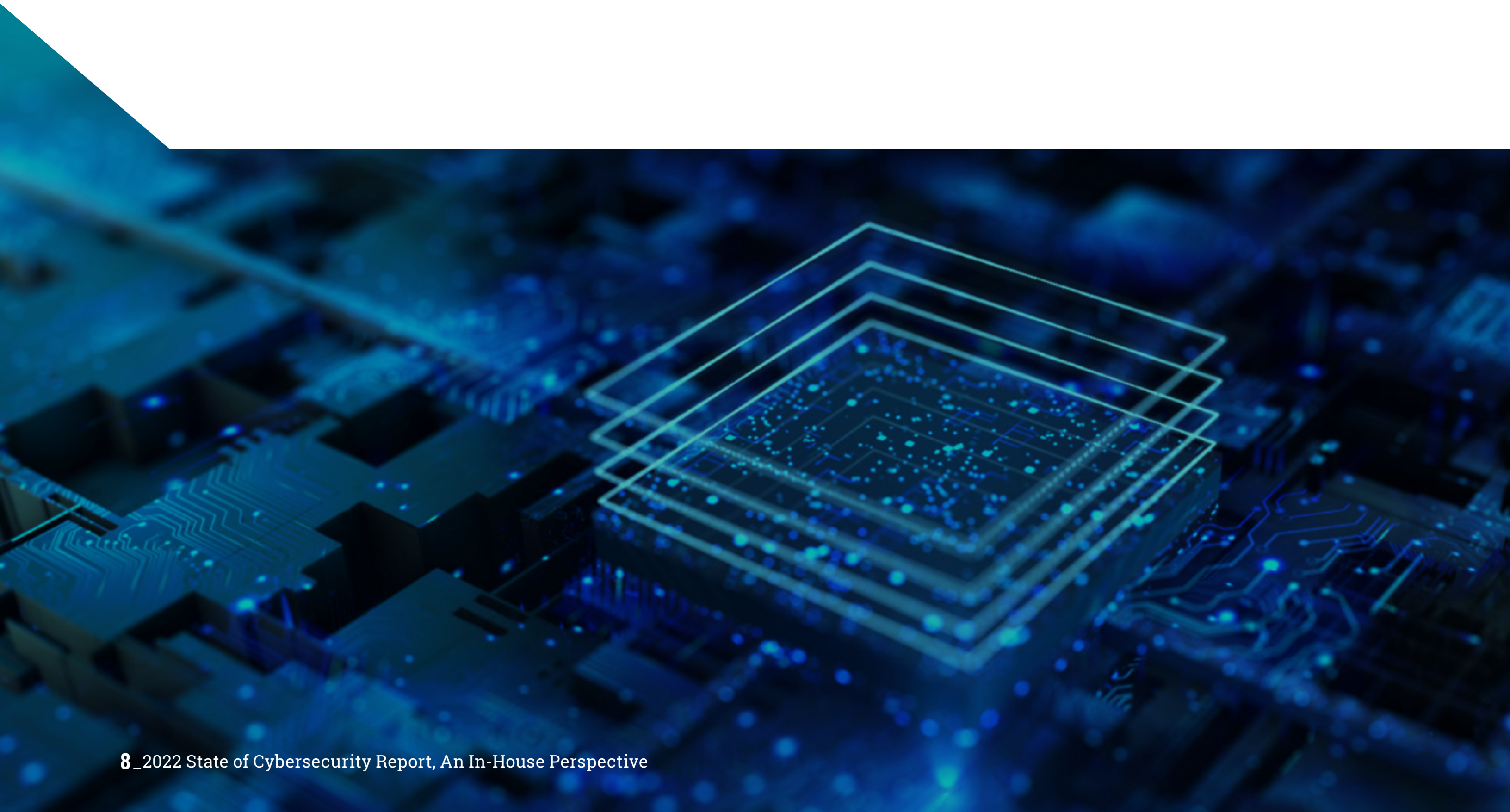
PRIVACY refers to personal data of individuals and concerns itself with the policies and practices pursuant to which those personal data are protected during collection, storage, use, sharing and storage, and destruction.

CYBERSECURITY: The means by which (1) a company's Information Technology systems are protected from unauthorized access; (2) sensitive data (not just personal data) is identified, encrypted, managed, protected from unauthorized access, and privacy policies are enforced. It may also refer to (3) protecting an organization's operational technology systems from unauthorized access (e.g., protecting an automobile company's manufacturing plant or an electric utility's electric grid from unauthorized access).

Chief legal officers and general counsel oversee privacy in greater numbers than cybersecurity. In three-quarters of organizations the CLO oversees privacy, which either reports directly to the CLO (55 percent) or has a dotted line to the top legal officer of the company (19 percent). Conversely, the cybersecurity function reports to the CLO in just 38 percent of organizations — 15 percent indicated that the CLO oversees cybersecurity directly and 23 percent do so through a dotted line. Privacy reporting more often to the CLO than cybersecurity is consistent with the results observed in the previous edition of the survey, though the number of participating organizations where the CLO oversees cybersecurity shows a 20-point increase: from 18 percent to 38 percent.

Q: Do either cybersecurity or privacy ultimately report to the CLO?

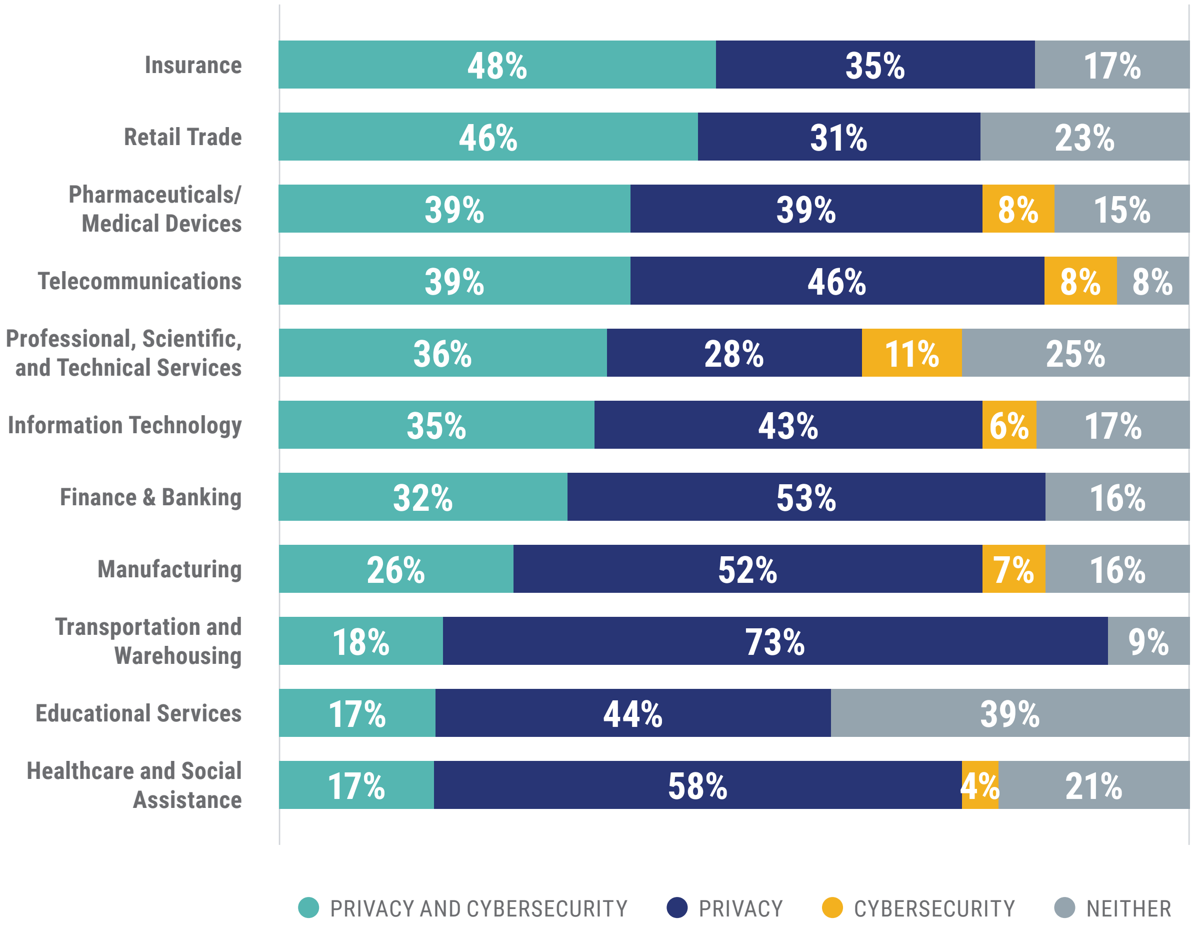




Across industries, many more CLOs oversee cybersecurity and/or privacy than the reported results in 2020. At least 25 percent of companies across all industries reported that year that the CLO did not oversee any of those two functions, while this year's results show that this is only the case in the professional services (25 percent) and educational services (39 percent) industries. Similarly, in 2020 the highest percentage of companies where the CLO oversaw both cybersecurity and privacy was 29 percent in the information technology sector. Most industries reported larger numbers in 2022, namely insurance (48 percent), retail (46 percent), pharmaceuticals (39 percent), telecommunications (39 percent), professional services (36 percent), information technology (35 percent), and financial and banking (32 percent).

//KEY COMPARISON_

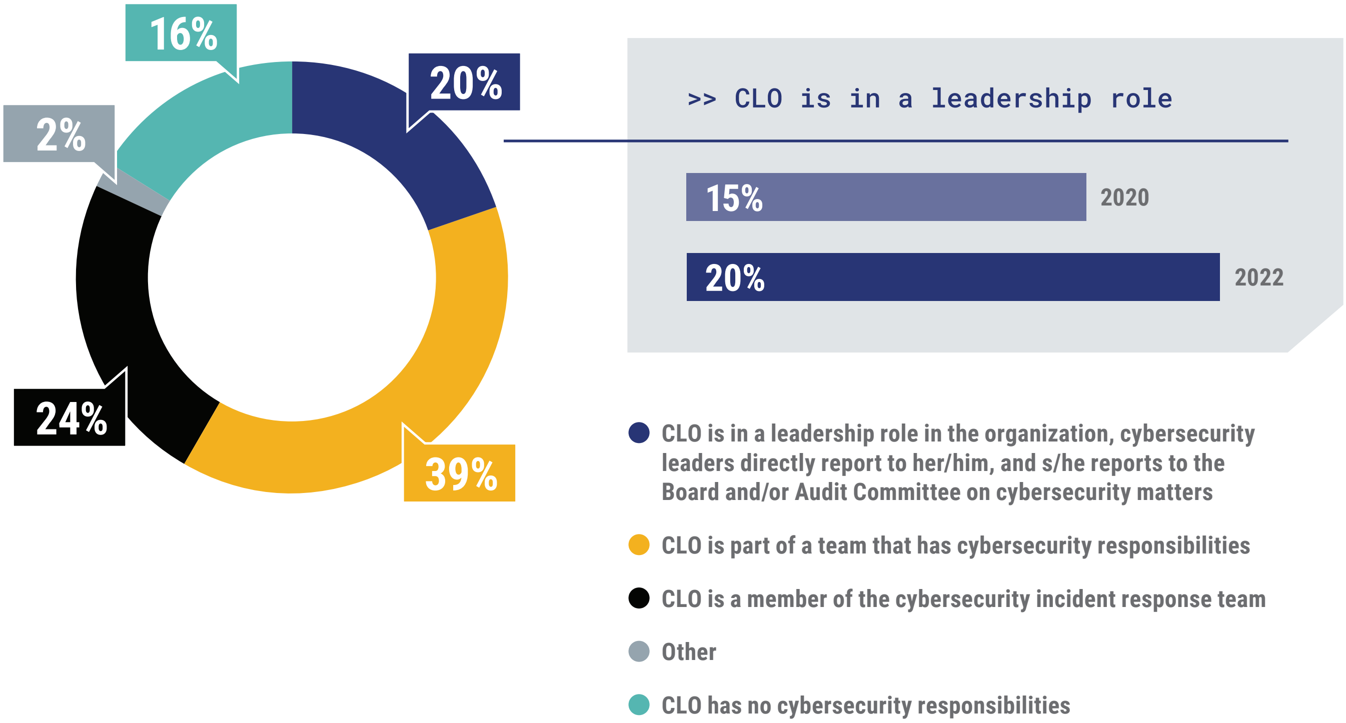
CLO Oversight of Privacy and Cybersecurity [by Industry]



Note: Oversight includes direct reporting to the CLO or dotted line to the CLO. Only industries with 10 or more observations are included.

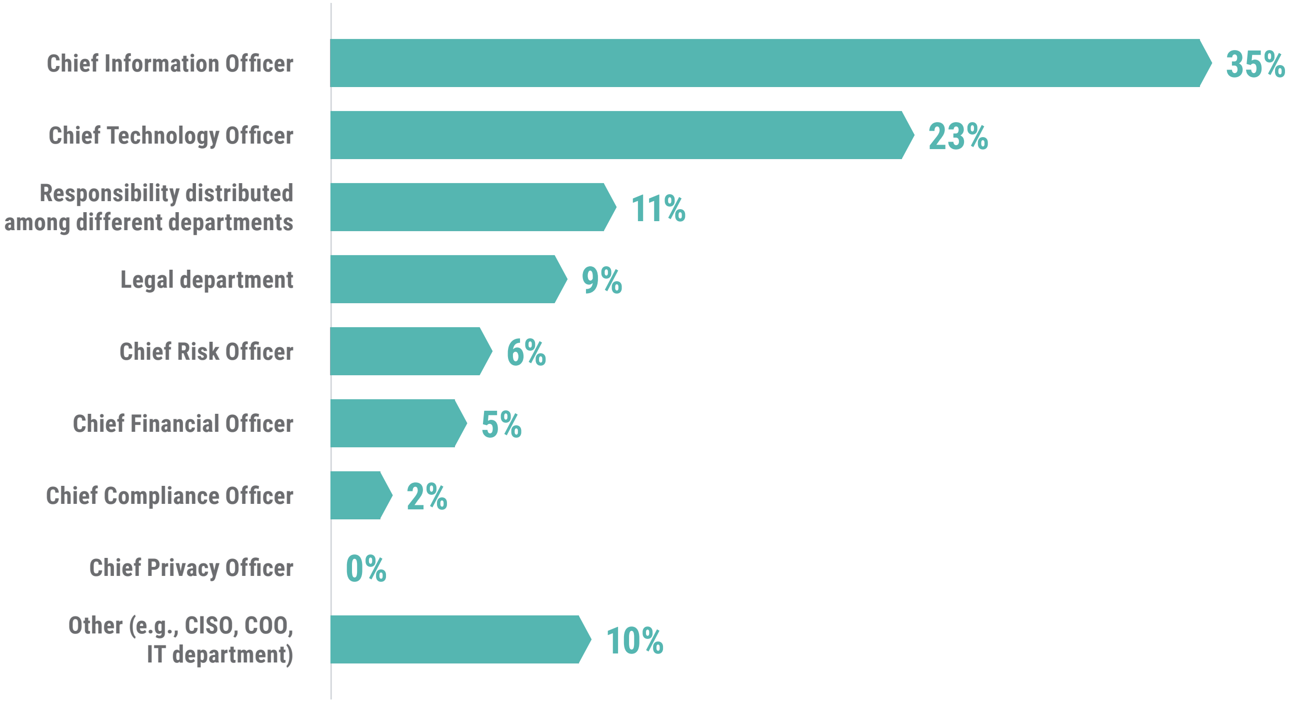
The role of the CLO regarding cybersecurity responsibilities varies significantly across organizations. CLOs are in a defined leadership role, with cybersecurity leaders directly reporting to them, in one-fifth of organizations — a five-point increase compared to 2020. In four out of ten organizations the CLO is part of a team that has cybersecurity responsibilities, and 24 percent of participants reported that their CLO is a member of the cybersecurity response team. Sixteen percent indicated that the CLO has no responsibilities in cybersecurity — 10 points lower than the result observed in 2020. Two percent of respondents indicated other scenarios, such as a lawyer other than the CLO having direct oversight over cybersecurity, or that the function is overseen by the IT department with legal acting in a consulting role.

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

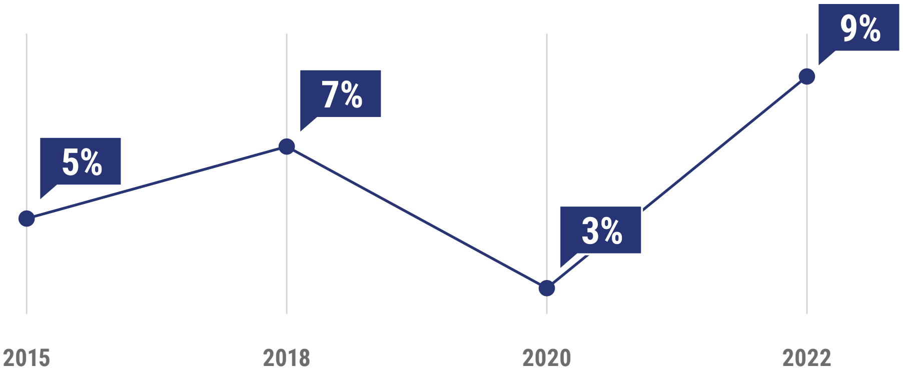


The cybersecurity function is housed in many separate departments within the organization according to survey participants. A plurality (35 percent) of respondents report that cybersecurity is primarily handled by the chief information officer (CIO), 23 percent indicate that it is under the chief technology officer (CTO), 11 percent report that the responsibility for cybersecurity is spread among different departments or business functions, and nine percent indicated that it is primarily housed in the legal department. This is the largest observed percentage of legal departments that house the cybersecurity function since 2015, although it still remains a relatively uncommon practice

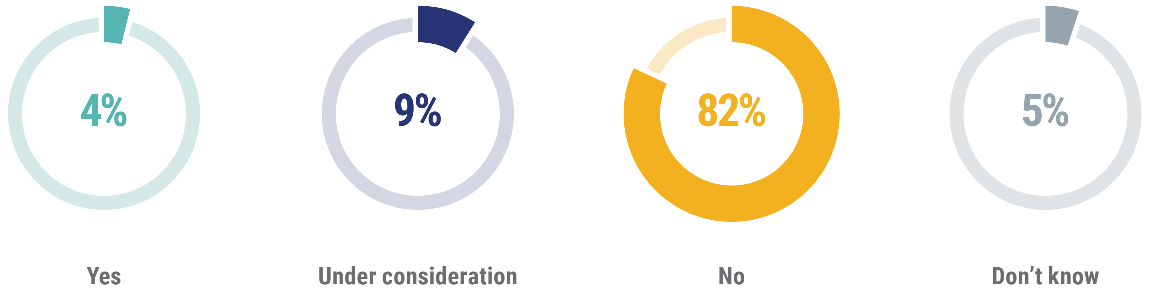
Q: Where is cybersecurity primarily housed at an enterprise-level?



>> Cybersecurity Primarily Housed in Legal



Q: Do you expect to include or add additional in-house counsel exclusively devoted to legal cybersecurity in the next 12–24 months?



Most legal departments (82 percent) do not expect to add an in-house lawyer exclusively dedicated to cybersecurity in the next couple of years. Only 4 percent of participants responded that they intend to do so, with nine percent indicating that this move is under consideration. Five percent of respondents are uncertain.

AMONG $3B+ COMPANIES...

10% will add an attorney dedicated to cybersecurity

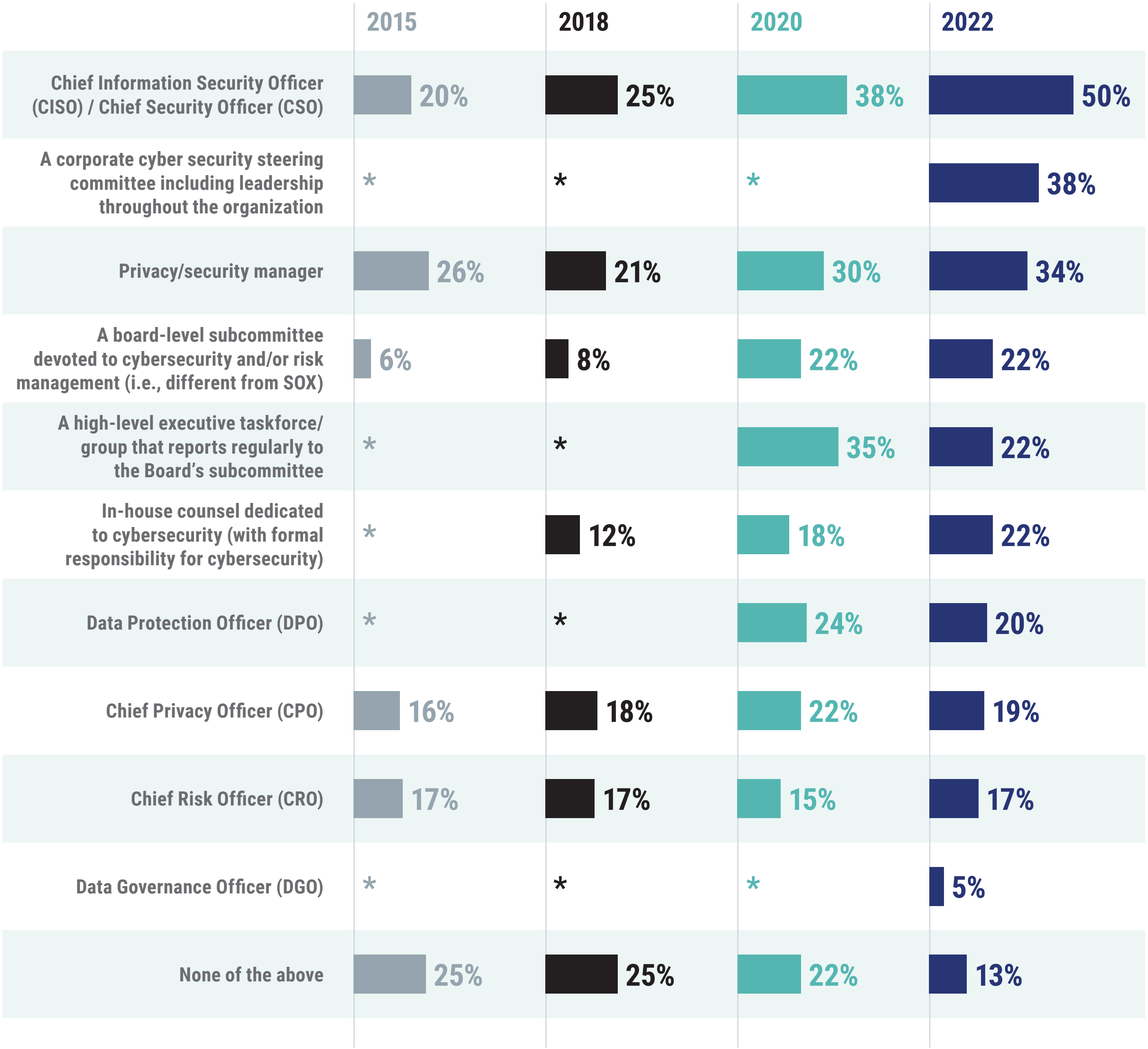
16% are considering it

Participants reported several individuals and committees in their organizations with cybersecurity responsibilities. Half of organizations have a chief information security officer (CISO) or chief security officer (CSO), a position that has progressively become the most common in handling cybersecurity at the organization level — 20 percent of organizations employed a CISO/CSO in 2015, increasing to 25 percent in 2018, 38 percent in 2020, and 50 percent in 2022.

Thirty-eight percent report that the organization has a cybersecurity steering committee, and one-third employ a privacy or security manager — a position that has also become more common since 2015. Twenty-two percent have a board-level subcommittee devoted to cybersecurity — the same percentage observed in 2020 — and also 22 percent indicate that they have a high-level executive taskforce that regularly reports to the board’s subcommittee — 13 points below the result observed in 2020.

Another 22 percent report employing an in-house counsel dedicated to cybersecurity matters, representing a ten-point increase since 2018 and six points since 2020. Thirteen percent of participants report not having any of the listed positions with cybersecurity responsibilities, which represents practically half of the result observed in the previous editions of the survey.

Q: Which of the following does your organization have?



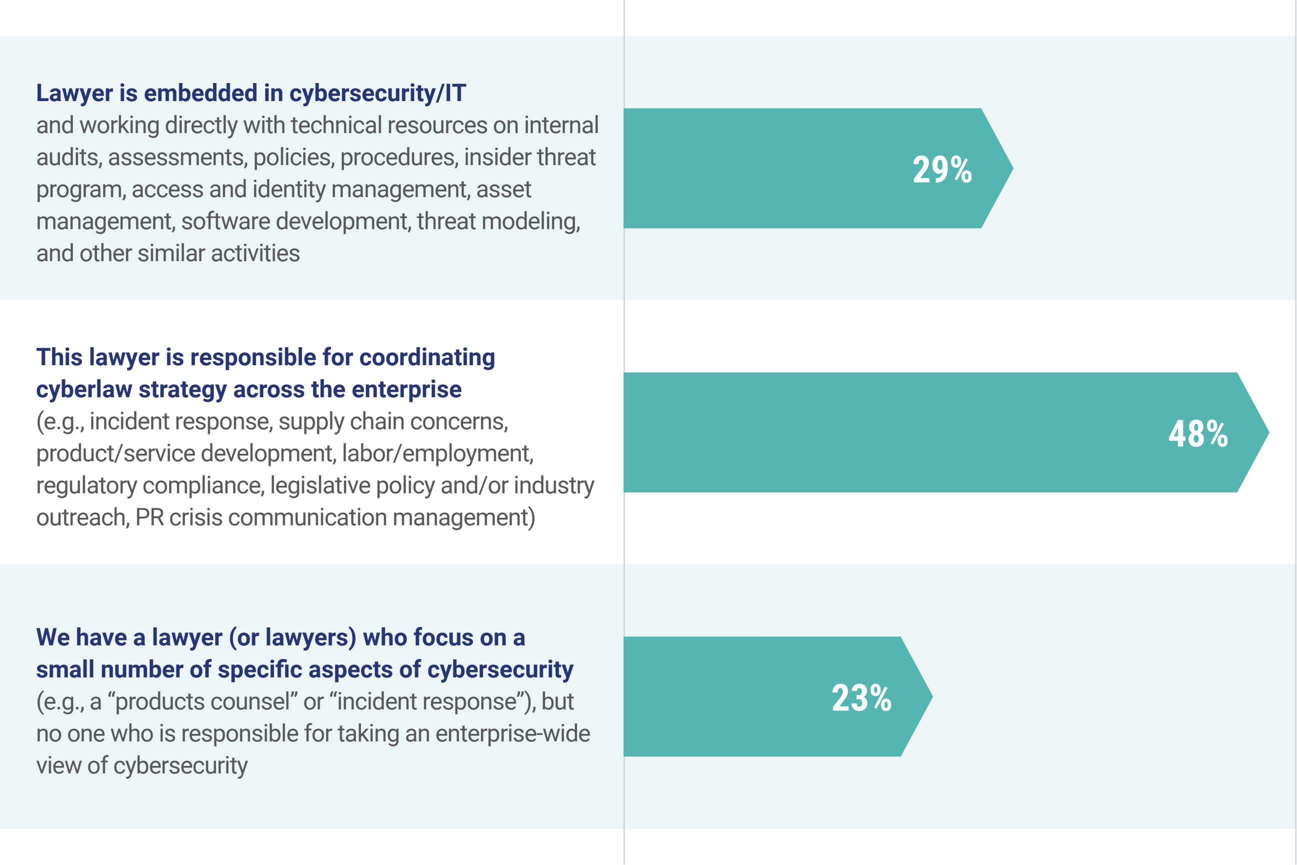
* Response not offered in that year's survey.

42% of large companies with US$3 billion or more in revenue have an in-house counsel dedicated to cybersecurity.

Forty-two percent of companies with a revenue larger than US$3 billion employ an in-house counsel dedicated to cybersecurity, compared to 22 percent for all respondents. Smaller companies tend to employ a dedicated cybersecurity lawyer less frequently, with 18 percent of companies with a revenue under US$100 million doing so.

Practically half of the departments that have an in-house counsel dedicated to cybersecurity task this individual with responsibilities involving the coordination of the cybersecurity strategy across the organization. In twenty-nine percent of organizations this in-house attorney is embedded in the cybersecurity and/or IT teams and works directly with the technical resources on several tasks, while in the remaining 23 percent of organizations the cybersecurity-focused in-house counsel is dedicated to a small number of specific aspects or tasks.

Q: If you have an in-house counsel dedicated to cybersecurity, please describe his/her duties.



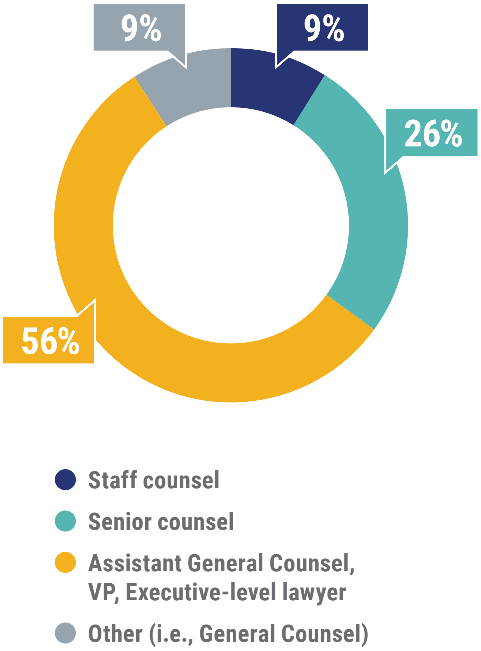
Lawyer is embedded in cybersecurity/IT and working directly with technical resources on internal audits, assessments, policies, procedures, insider threat program, access and identity management, asset management, software development, threat modeling, and other similar activities

This lawyer is responsible for coordinating cyberlaw strategy across the enterprise (e.g., incident response, supply chain concerns, product/service development, labor/employment, regulatory compliance, legislative policy and/or industry outreach, PR crisis communication management)

We have a lawyer (or lawyers) who focus on a small number of specific aspects of cybersecurity (e.g., a “products counsel” or “incident response”), but no one who is responsible for taking an enterprise-wide view of cybersecurity

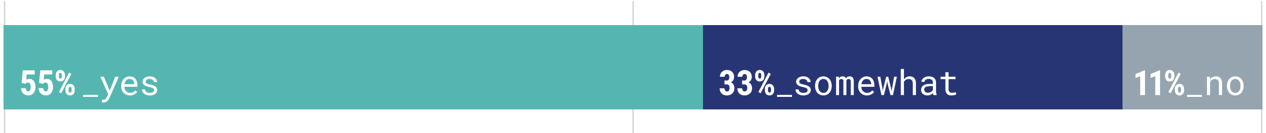
Q: What level of seniority is your dedicated in-house cyber counsel? If you have more than one such attorney, please provide the seniority level of the most highly-ranked attorney.

The lawyer dedicated to cybersecurity matters is most often an executive-level lawyer, vice-president, or assistant general counsel, according to 56 percent of participants — the same percentage observed in 2020. This attorney is at the senior counsel level in 26 percent of organizations, and nine percent report that the cybersecurity-dedicated attorney is at the staff counsel level. In nine percent of organizations, another type of lawyer handles cybersecurity — in most reported of such cases, this is the general counsel in small legal departments, including one-lawyer departments.



Q: Would you say the following is true: "My organization's IT/cyber department, legal department, and applicable business/compliance department(s) generally are integrated and cross-functionally work together to reduce cybersecurity risk"?

For example, in your organization, member(s) of legal department are regularly working directly with IT and Security resources on cyber security program, risk register, corrective action plans, internal audits, technical controls, policies, etc.



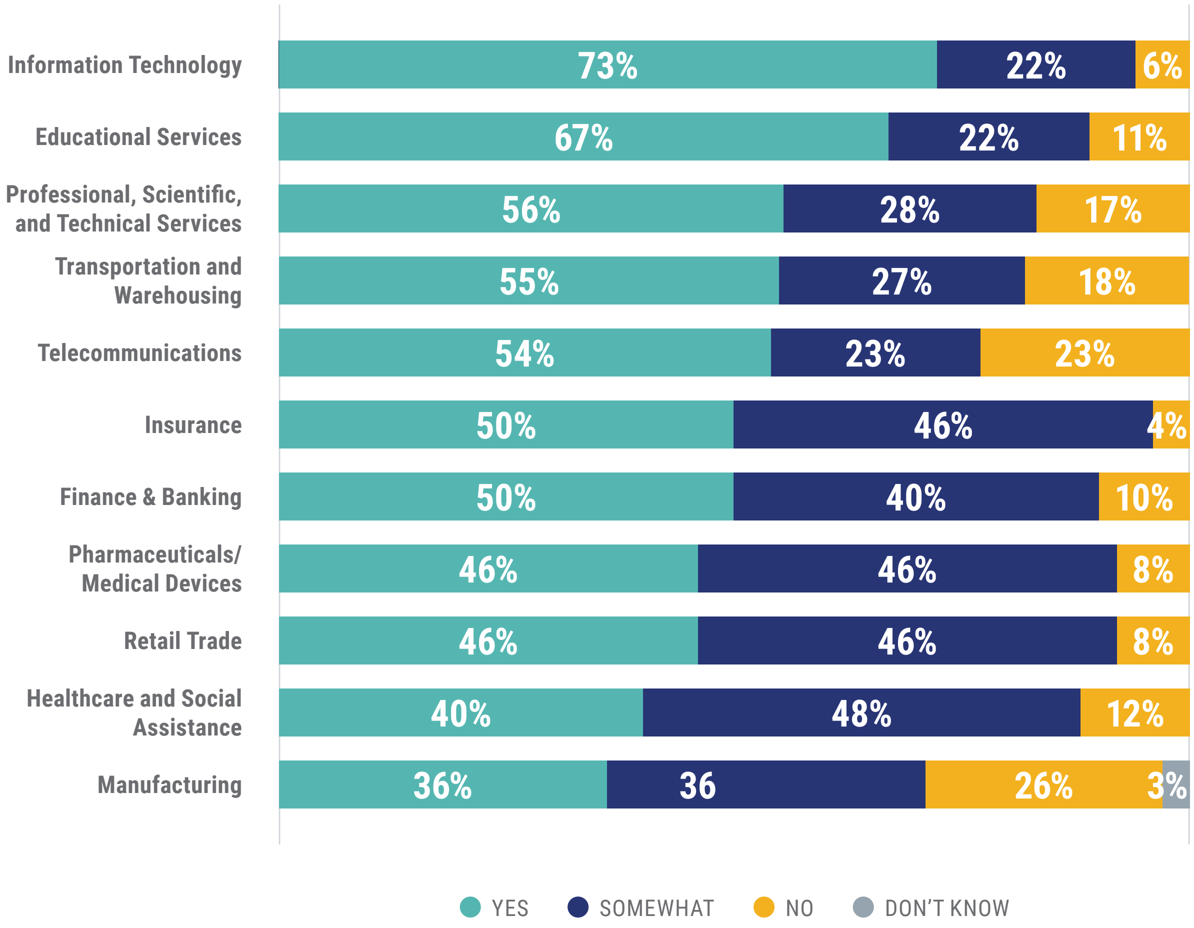
A majority of respondents reported that in their organization the IT, cybersecurity, legal, and other relevant departments are integrated and work together to reduce cybersecurity risk. Fifty-five percent agree with the scenario described in the statement above, while an additional 33 percent agree to it somewhat. Only one in ten respondents report that these key departments are not integrated or do not work together to mitigate cybersecurity risks.

There is wide variation across industry sectors on the degree to which there is cross-functional collaboration to reduce cybersecurity risks. Companies in information technology are those that show the highest levels of collaboration (73 percent), followed by education (67 percent), professional services (56 percent), transportation (55 percent), and finance and banking (50 percent), and insurance (50 percent).

Under half of respondents in pharmaceuticals/medical devices, retail, and healthcare reported that different departments work together, though close to half of participants in these industries reported at least some level of cooperation. Manufacturing companies rank last with only 36 percent saying that departments work together to address cybersecurity risk and one in four saying that there is no cooperation.

//KEY COMPARISON_

Departments are integrated and work together to reduce risk [by industry]

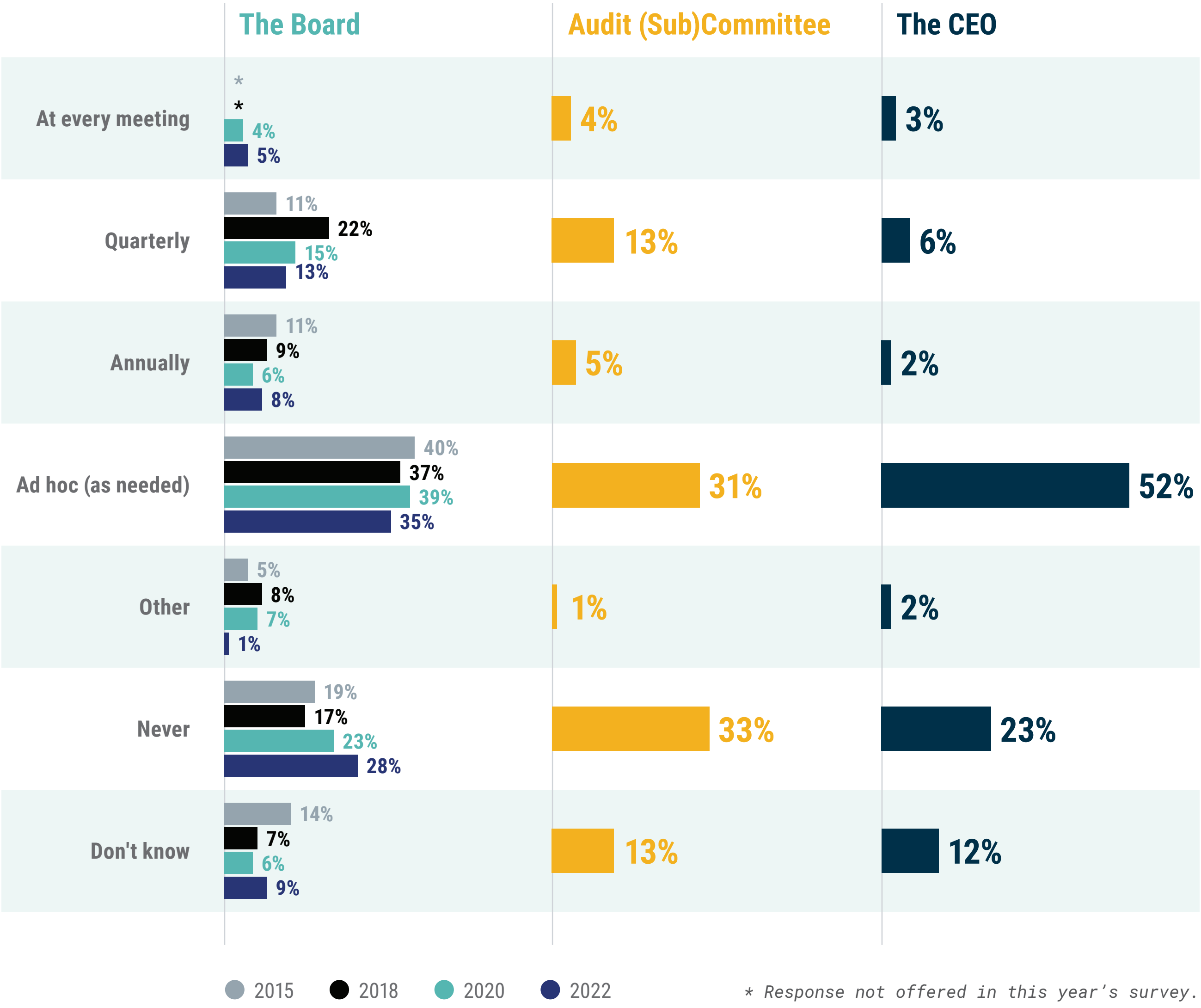


Note: Only companies with 10 or more observations are listed.

Survey participants provided insights on the frequency that the CLO reports on cybersecurity matters to the board of directors, the audit (sub)committee on cybersecurity, and the CEO. The most common reporting cadence is ad hoc or as needed, with 35 percent reporting to the board in such a manner, 31 percent do the same to the audit committee, and a majority of 52 percent report on cybersecurity to the CEO when required.

A minority of respondents indicated that the CLO never reports on cybersecurity to the above three key stakeholders. Twenty-eight percent responded that the CLO never reports to the board on cybersecurity — the highest percentage since 2015; one-third of CLOs never report to the audit or cybersecurity committee, and 23 percent never report to the CEO on cybersecurity matters. A small number of respondents indicated that the CLO reports to the board, the audit/cybersecurity committee, and the CEO periodically — annually, quarterly, or at every meeting — and around one in ten are not sure of the reporting frequency.

Q: How frequently does the CLO brief the...
...board of directors on cybersecurity?
...Audit Committee/Subcommittee on cybersecurity?
...CEO on cybersecurity?



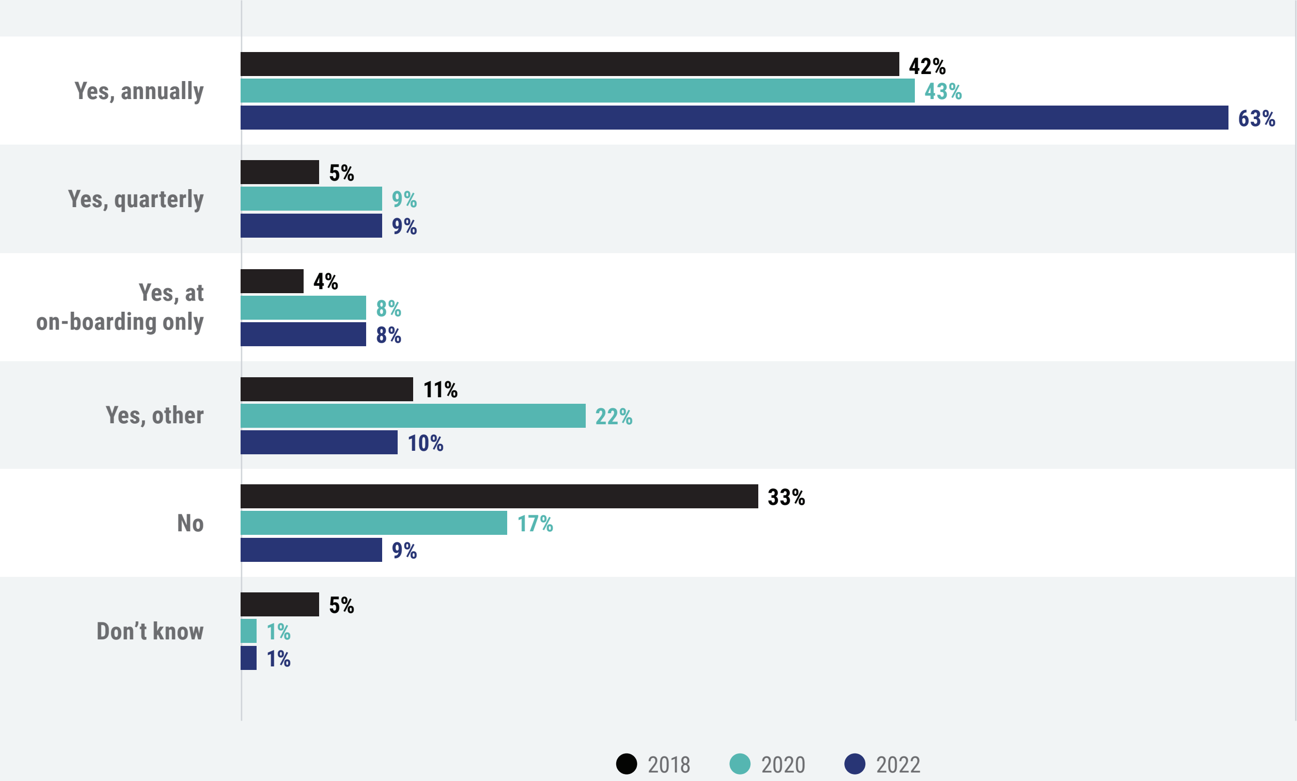
* Response not offered in this year's survey.

SECTION_ 02

//policies [and] practices

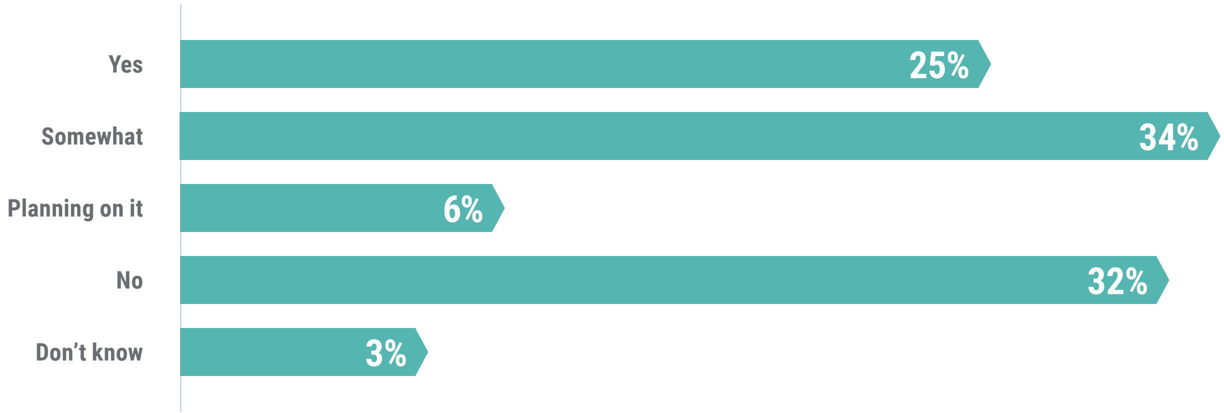
Cybersecurity training for employees is mandatory in nine out of 10 participating organizations. Only nine percent indicated that employees are not required to receive cybersecurity training, compared to 17 percent in 2020 and 33 percent in 2018. Sixty-three percent require mandatory training on an annual basis — a 20-point increase compared to 2020 — and an additional nine percent provide mandatory training each quarter. Eight percent of respondents indicated that cybersecurity training is provided at on-boarding only. Ten percent of organizations require training in a different frequency, such as twice a year, every month, or continuously throughout the year without a fixed schedule.

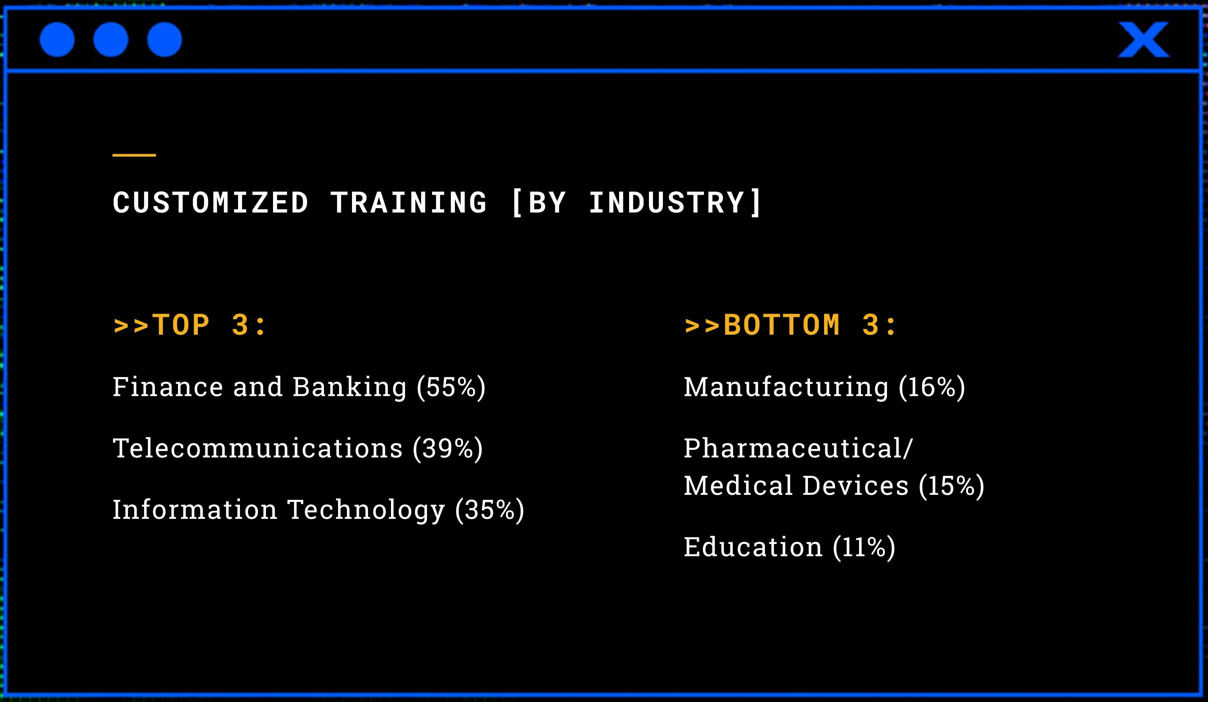
Q: Does your organization have mandatory training on cybersecurity for all employees?



Training for employees on cybersecurity is customized to the individual's role or level of access to sensitive data in 25 percent of organizations, while an additional 34 percent indicate that training is somewhat specific to an individual's role. By industry, only organizations in finance and banking cross the 50 percent mark in providing tailored cybersecurity training to employees. Six percent of participants are planning to customize mandatory training in the near future. Around one-third of organizations do not provide customized cybersecurity training to the employees' positions and data access levels.

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





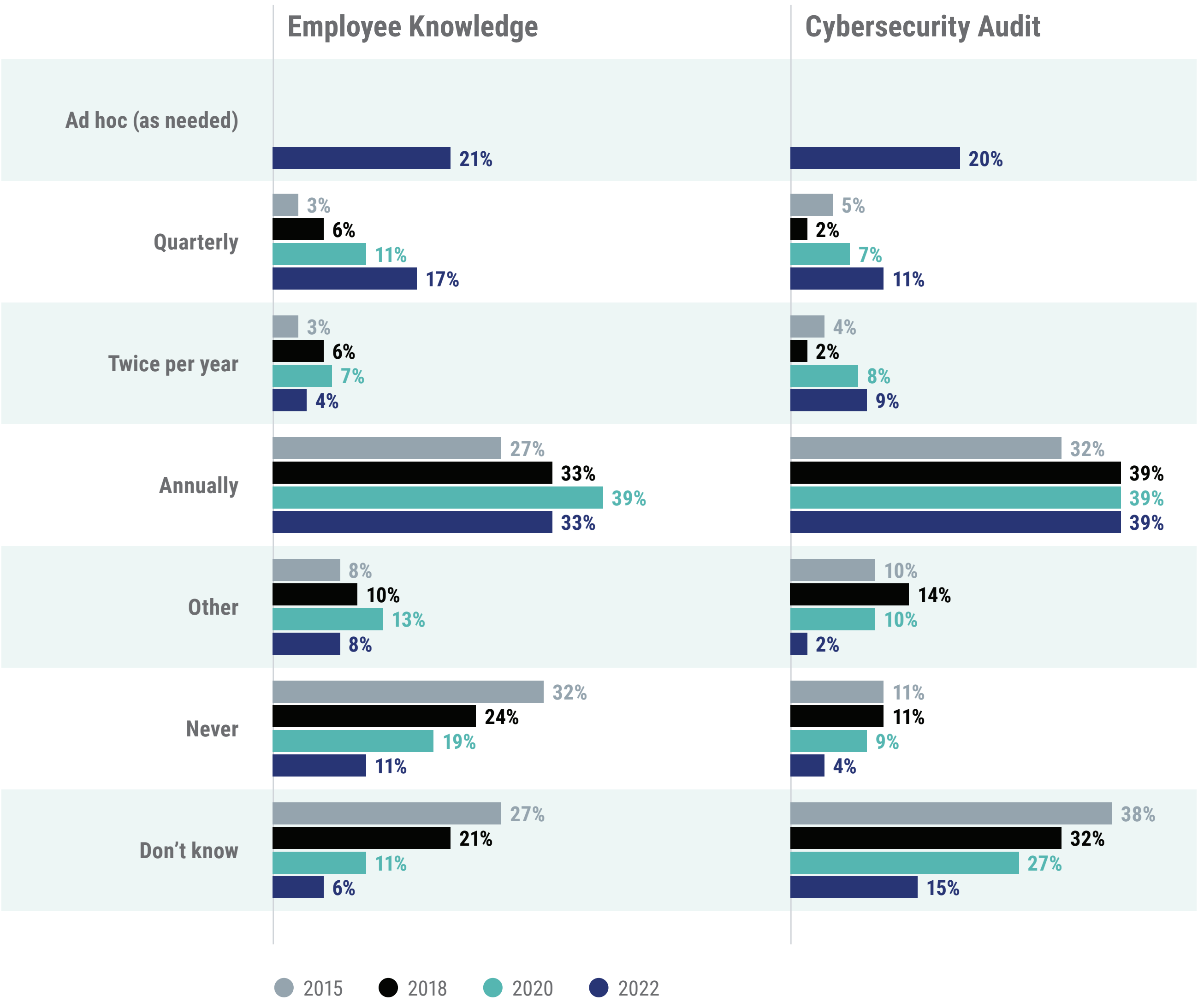
CUSTOMIZED TRAINING [BY INDUSTRY]

>>TOP 3:	>>BOTTOM 3:
Finance and Banking (55%)	Manufacturing (16%)
Telecommunications (39%)	Pharmaceutical/ Medical Devices (15%)
Information Technology (35%)	Education (11%)

Respondents also indicated how often the organizations test employees' knowledge on best cybersecurity practices. One-third of organizations evaluate cybersecurity knowledge every year, and an additional 17 percent do so on a quarterly basis. Twenty-one percent do not test knowledge on a regular basis but do so ad hoc, four percent test employees twice a year, and eight percent use other formats, such as monthly or even more regularly — with email phishing tests being one of the most common evaluation tools. Only 11 percent reported never testing employee knowledge on cybersecurity, which represents a steady decline since the 32 percent observed in 2015.

In terms of conducting an organization-wide cybersecurity audit, four in 10 organizations do so annually, 11 percent do it quarterly, and an additional nine percent conduct an audit twice a year. Twenty percent of participants report that audits are only conducted on an ad hoc basis, and just four percent indicated that their organization never carries out a cybersecurity audit — down from 11 percent in 2018 and nine percent in 2020. Fifteen percent of respondents do not know how often they are conducted, a result that also shows a steady decline from the 38 percent observed in 2015.

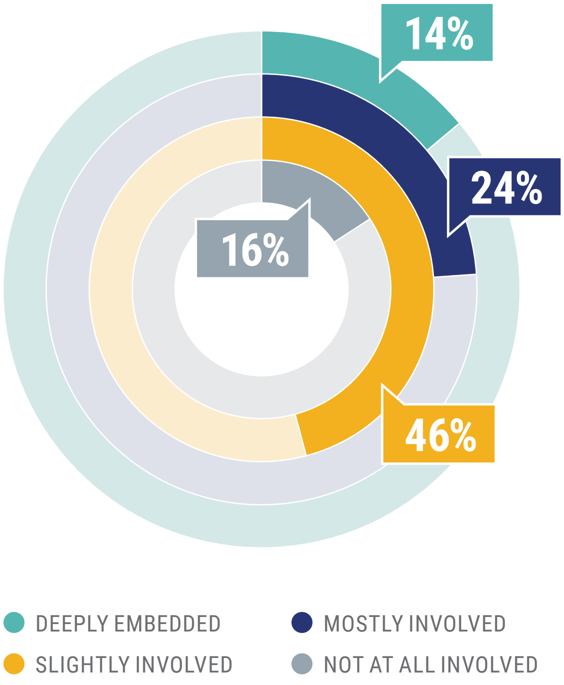
Q: How often does your organization...
...evaluate employee knowledge of cyber safety practices/data policies?
...conduct a cybersecurity audit of part(s) of the organization?



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

Among the organizations that conduct cybersecurity audits, a plurality of participants (46 percent) indicate that the legal department is only slightly involved. Four in ten participants indicate that the legal department is either mostly involved (24 percent) or deeply embedded (14 percent) in the cybersecurity audit process. Sixteen percent, on the other hand, report that legal is not involved at all in cybersecurity audits.

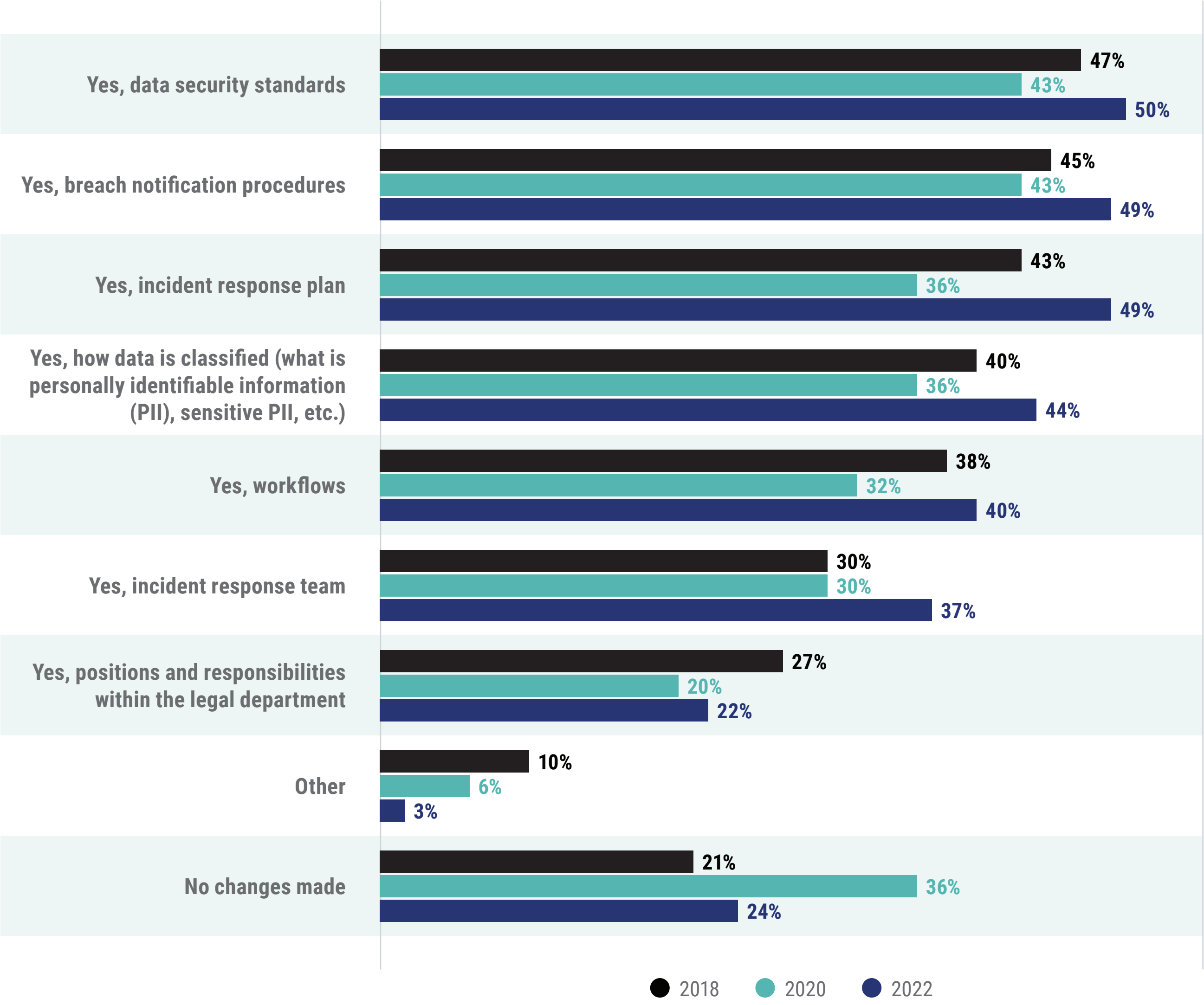
Note: Asked if conducted cybersecurity audits "ad hoc", "quarterly", "twice per year", or "annually".



Around half of participants have made several changes as a result of data privacy regulations, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the New York SHIELD Act. Fifty percent report changing data security standards, 49 percent updated breach notification procedures, and another 49 percent changed the organization's incident response plan. Forty-four percent made changes on how personal data is classified, 40 percent updated workflows, and another 37 percent made changes on the incident response team.

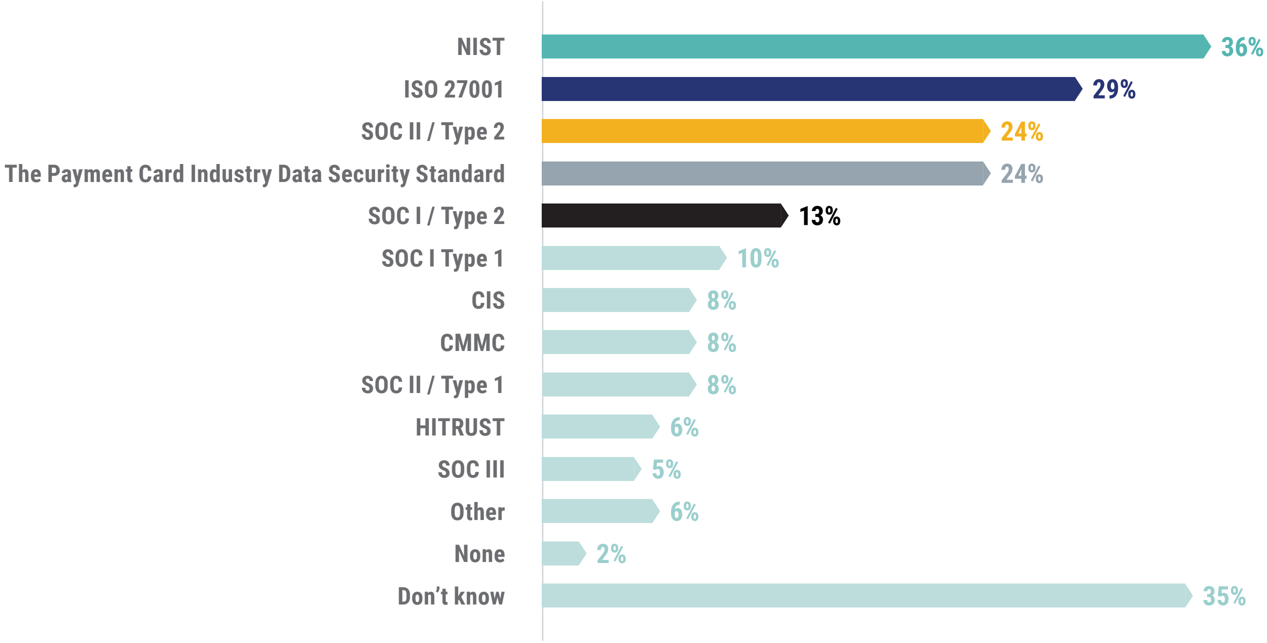
A higher percentage of respondents made all the above changes compared with the results observed in both 2018 and 2020, though this question in those years only explicitly referred to the European Union's GDPR regulation. Twenty-two percent made changes to positions and responsibilities within legal as a result of data privacy and protection regulations, while 24 percent made no changes — 36 percent made no changes in 2020 as a result of GDPR, which had already been in effect for around two years.

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

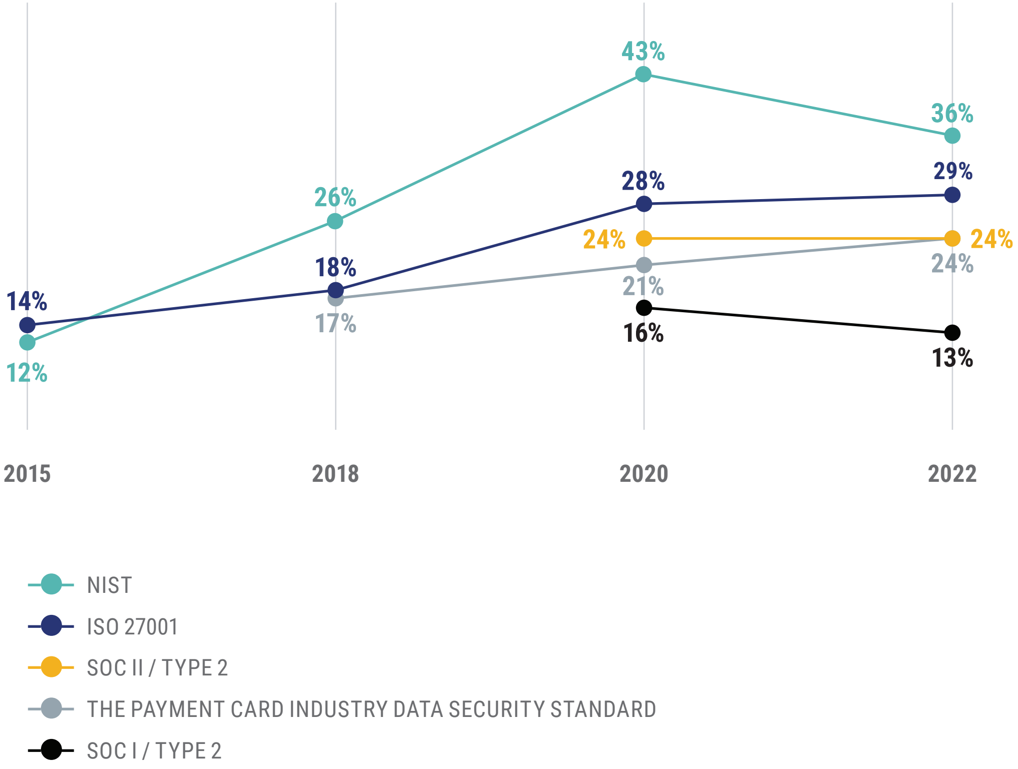


When asked about the cybersecurity standards use by the organization, 35 percent of participants are not sure and, though substantial, this percentage has decreased considerably since 2015 (61 percent) and remained stable in comparison to 2020 (36 percent). The most common standard used is the National Institute of Standards and Technology (36 percent), followed by ISO 27001 (29 percent), SOC II / Type 2 (24 percent), the Payment Card Industry Data Security Standard (also 24 percent), and the SOC I / Type 2 standard (13 percent). A trendline with the percentage of participants that use those five standards since 2015 shows a general upward trajectory in usage, especially related to NIST, ISO 27001, and the Payment Card Industry Data Security Standard. Two percent of respondents indicated that their organization does not use any cybersecurity standard.

Q: What standard or standards does your organization currently use to address cybersecurity? *(Select all that apply)*

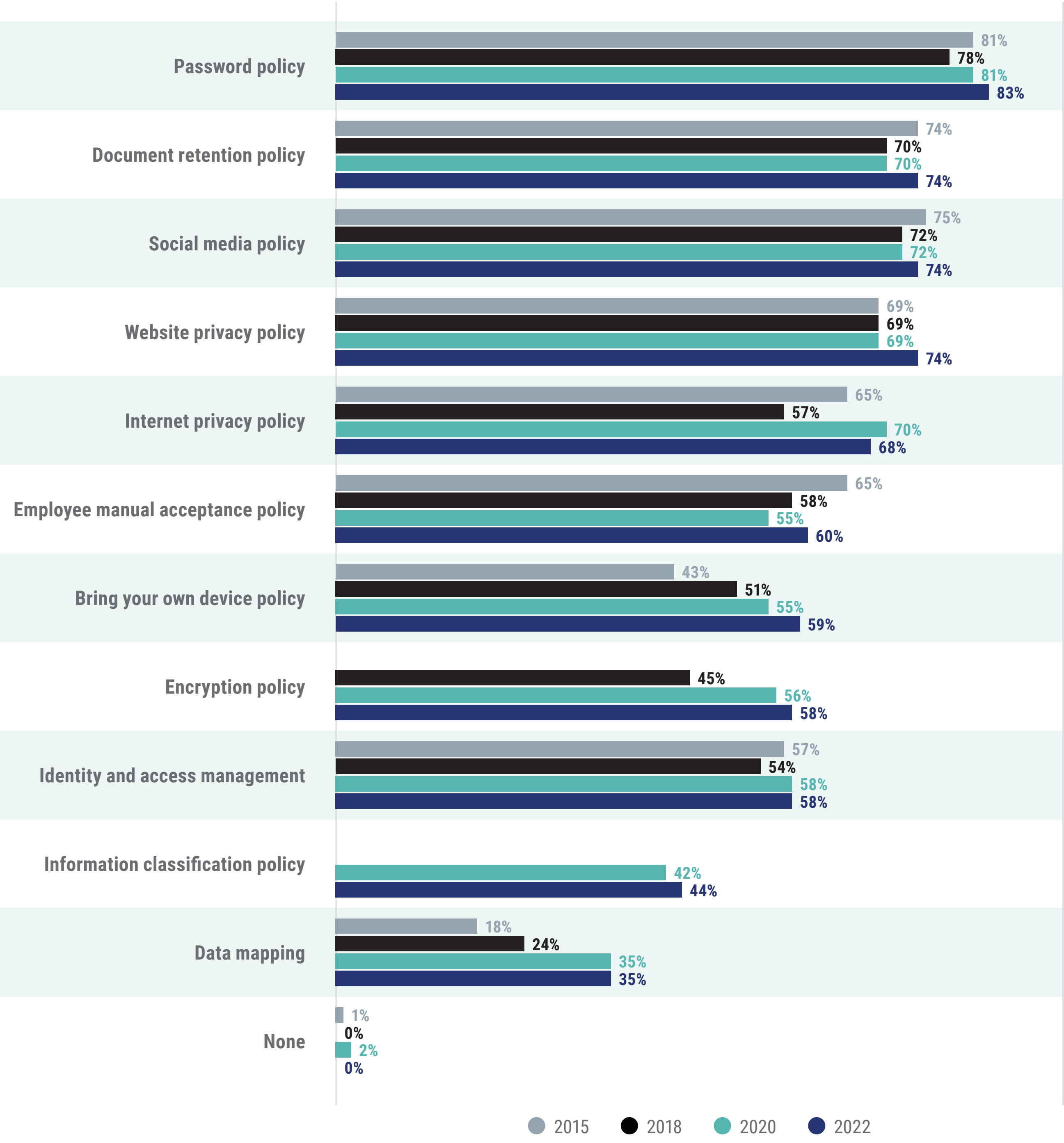


>> Most Used Cybersecurity Standards Trend

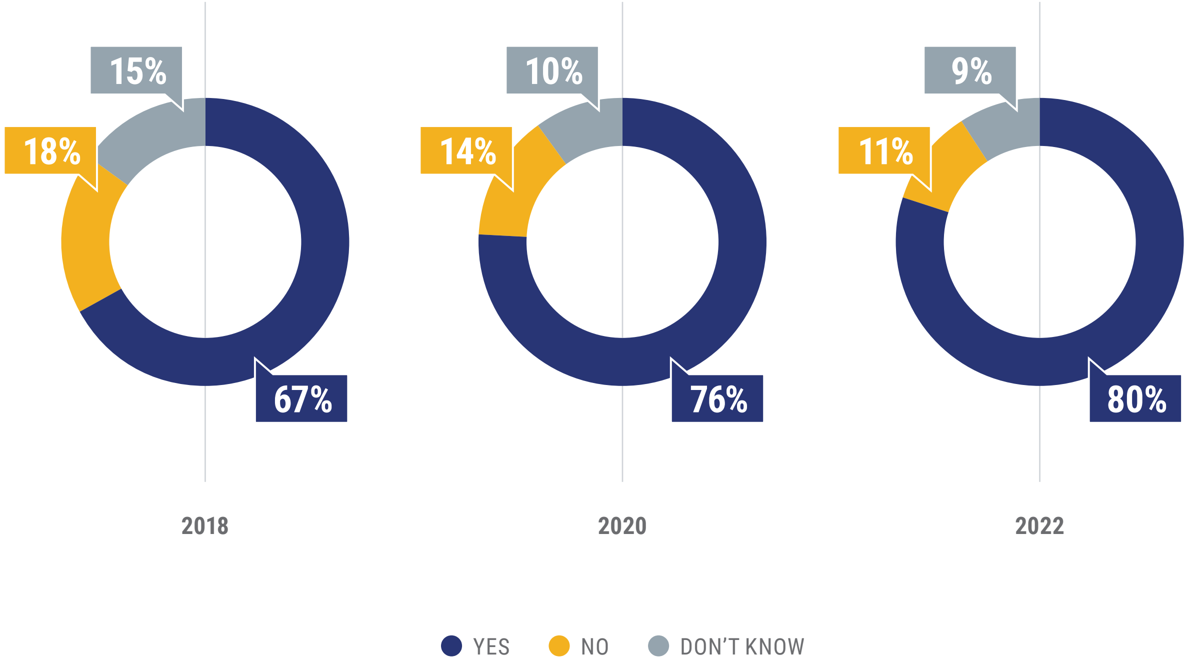


Participating organizations do have several written policies in place designed to mitigate cybersecurity risks. No dramatic changes are observed when analyzing the patterns over time. A solid majority of participants have written policies related to passwords (83 percent); document retention, social media, and website privacy (all three with 74 percent); internet privacy (68 percent); employee manual acceptance (60 percent); bring your own device (59 percent) — a policy that has become more common over time; encryption, and identity and access management (both 58 percent). Under half of participants reported having written policies on information classification (44 percent) and data mapping (35 percent).

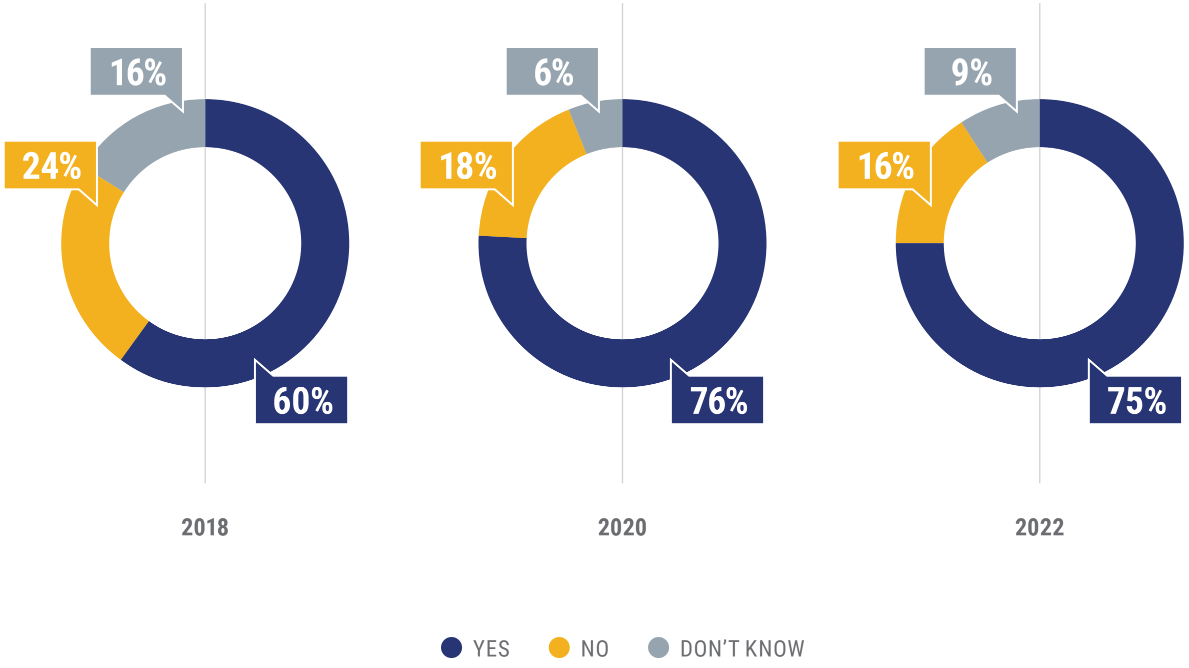
Q: Does your organization have any of the following written policies in place? *(Select all that apply)*



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

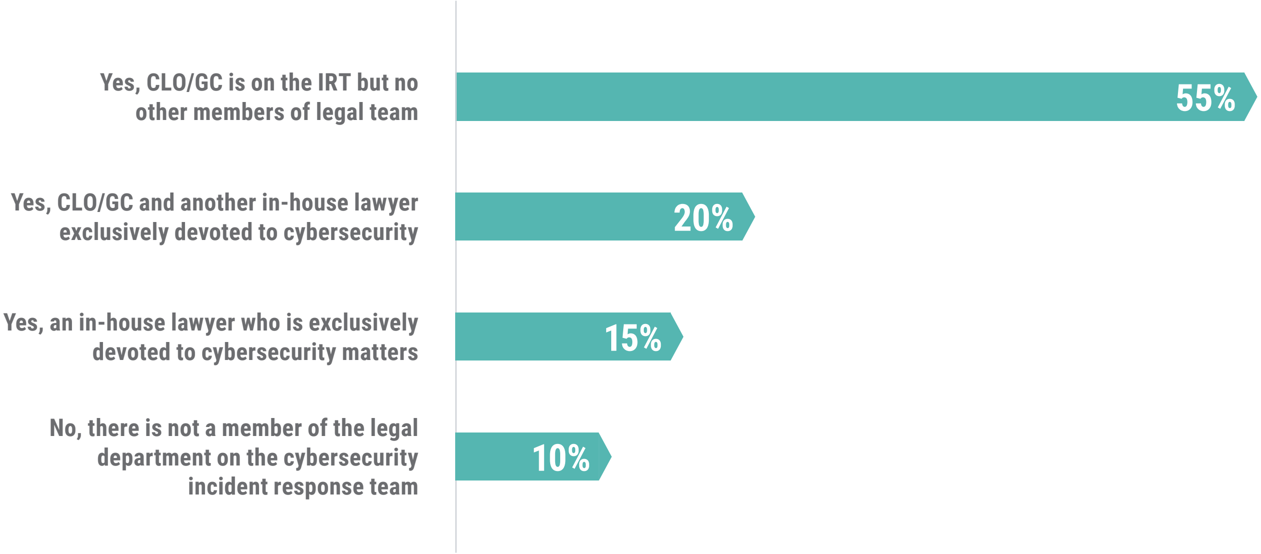


Q: Does your organization have a documented cybersecurity incident response team (IRT)?

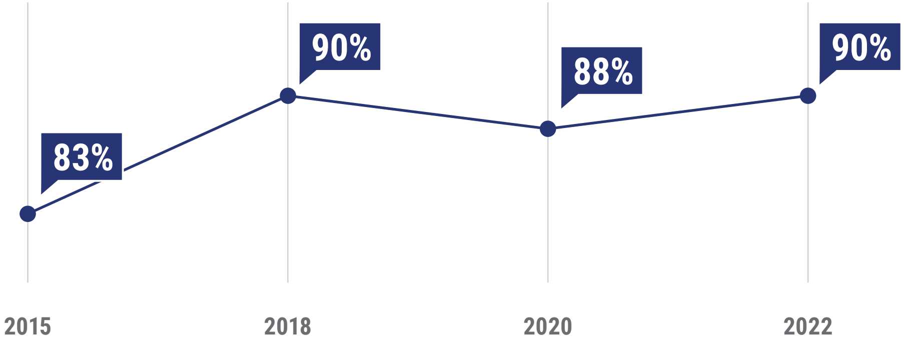


In nine out of 10 organizations a member of the legal department is part of the organization's cybersecurity incident response team (IRT). This result has remained stable since 2018. Fifty-five percent of participants report that the CLO or GC is part of the IRT, but no other attorneys are. In 20 percent of organizations the CLO/GC and another in-house lawyer — who is devoted exclusively to cybersecurity — are members of the IRT. In the remaining 15 percent of organizations, the CLO/GC is not part of the IRT, but the cybersecurity-dedicated in-house attorney is.

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



>> Percentage of Organizations Where a Legal Department Member is Part of the IRT



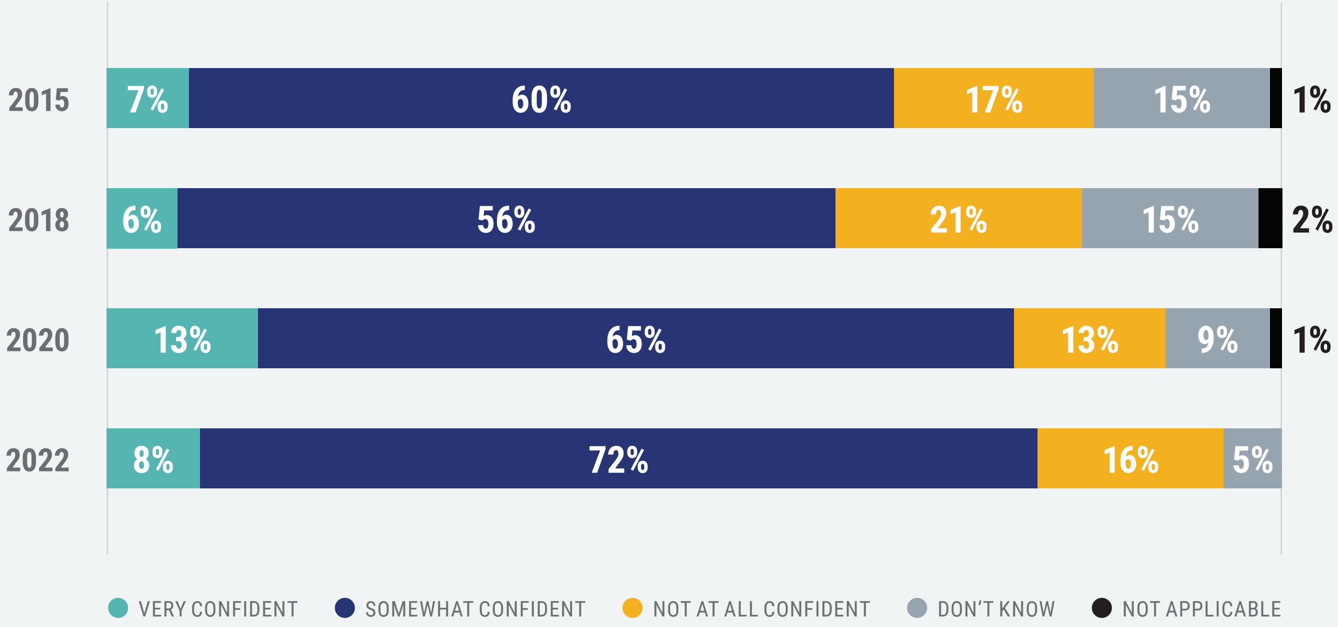
Note: Only asked if organization has a documented cybersecurity incident response team.

SECTION_ 03

//risk management

Four in five participants are at least somewhat confident — though just eight percent are very confident — that vendors are keeping the organization protected from cybersecurity risks. This result is similar to those observed in 2020 (78 percent), and considerably higher than the confidence in vendors recorded in 2018 (62 percent). Sixteen percent of participants are not at all confident about their vendors keeping the organization safe, and just five percent of participants do not know — the share of respondents that did not know has been cut by two-thirds since 2018.

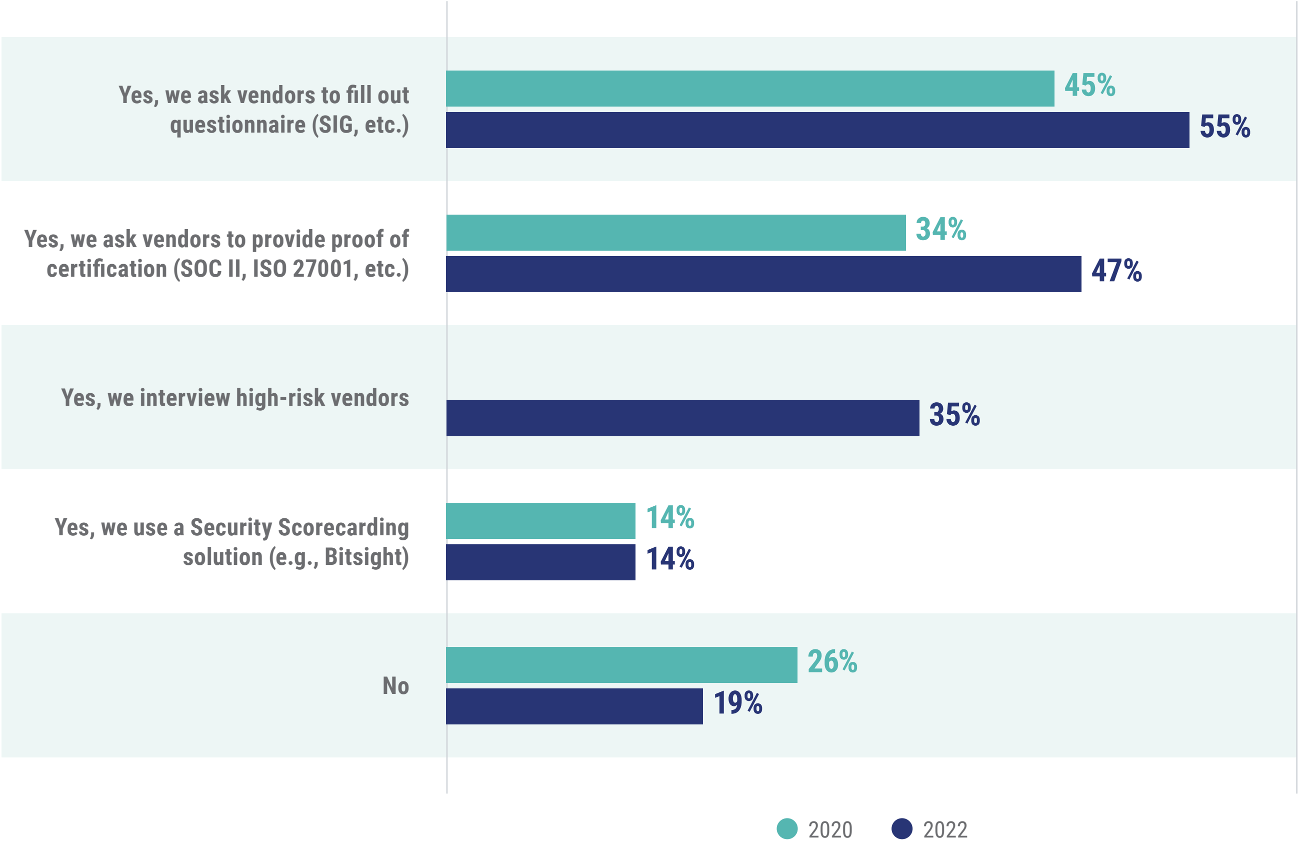
Q: How confident are you that your vendors protect you from cybersecurity risks?



Most participants indicated that they evaluate their vendors in order to assess whether they pose any cybersecurity risks to the organization. Eighty-one percent do so, compared to 74 percent two years ago. A majority of 55 percent ask vendors to fill out a questionnaire, and almost half (47 percent) require vendors to provide proof of cybersecurity certification. These numbers are 10 points and 13 points higher, respectively, compared to the results observed in 2020. Thirty-five percent interview high-risk vendors about cybersecurity issues, and 14 percent use a Security Scorecarding solution.

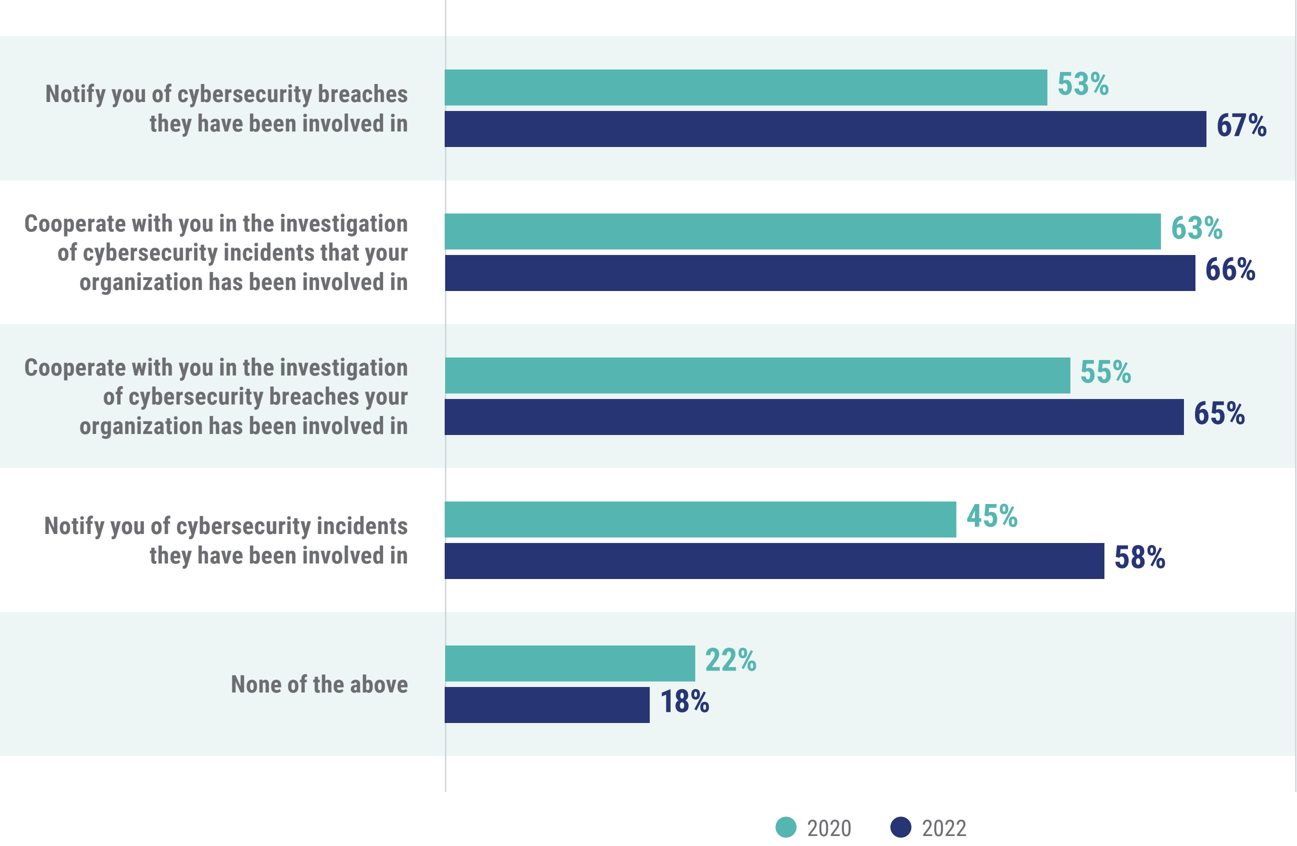
Q: Does your organization evaluate vendors for cyber risk?

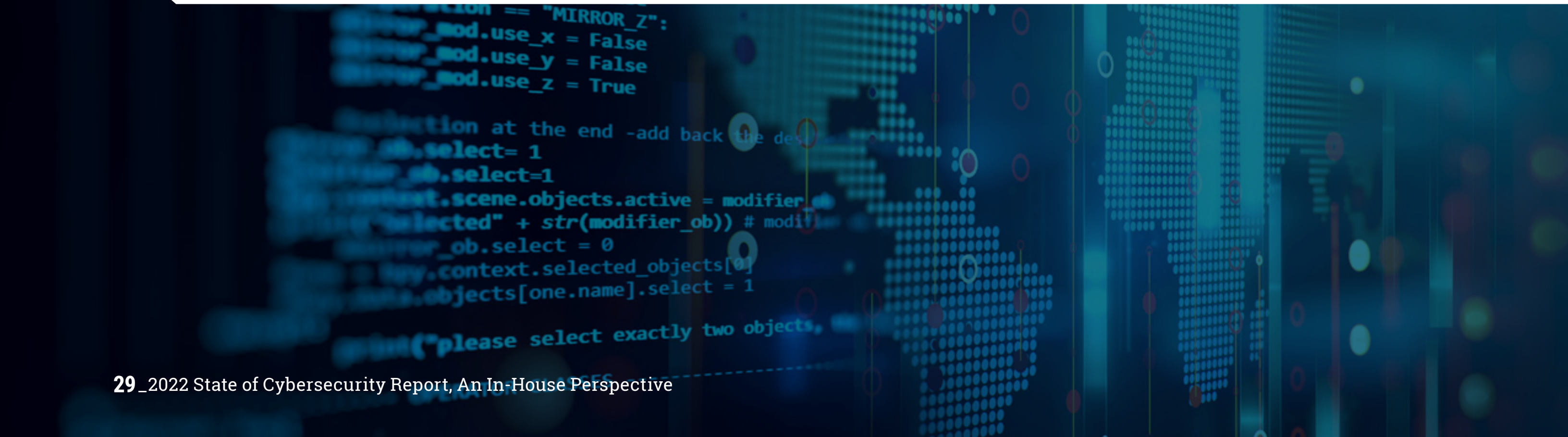
(Select all that apply)



Similarly, 82 percent of organizations require third-party vendors to obtain some contractual obligations regarding notifications and cooperate in investigations related to cybersecurity incidents and breaches. This is four points higher than the result recorded in 2020. Two-thirds of participants require vendors to notify the organizations of any cybersecurity breaches the have been involved in, and to cooperate in the investigation of cybersecurity incidents and breaches that the respondent's organization has been involved in. Additionally, 58 percent require that vendors notify their organizations of any cybersecurity incidents the vendors have been involved in.

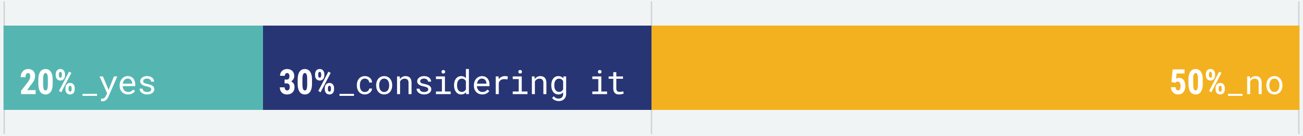
Q: Do you contractually require your third-party vendors to do any of the following? *(Select all that apply)*





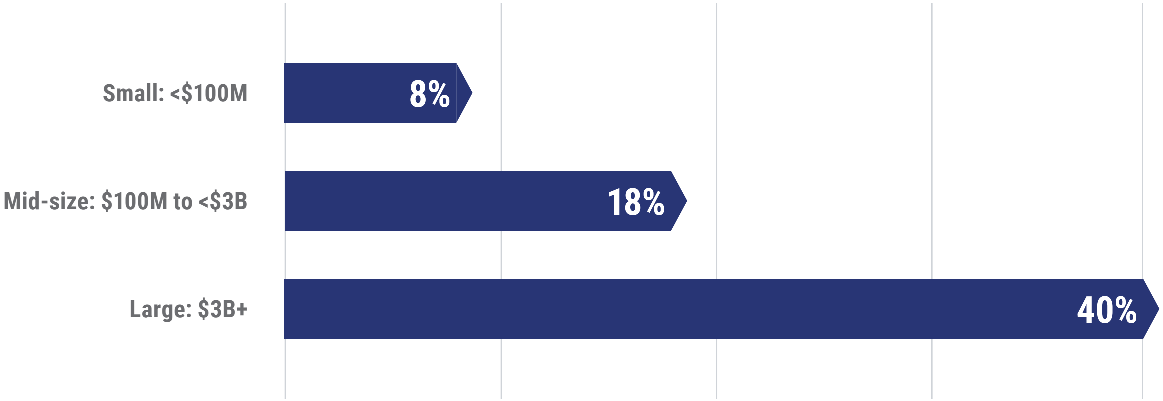
Two in ten organizations use a Governance, Risk, and Compliance (GRC) solution to document, address, and follow up on vendor cybersecurity risks, three in ten are considering implementing a GRC solution, and five in ten stated that they do not intend to do so at the moment. Large companies are more likely to use a GRC solution (40 percent), compared to mid-sized (18 percent) and smaller organizations (eight percent).

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



//KEY COMPARISON_

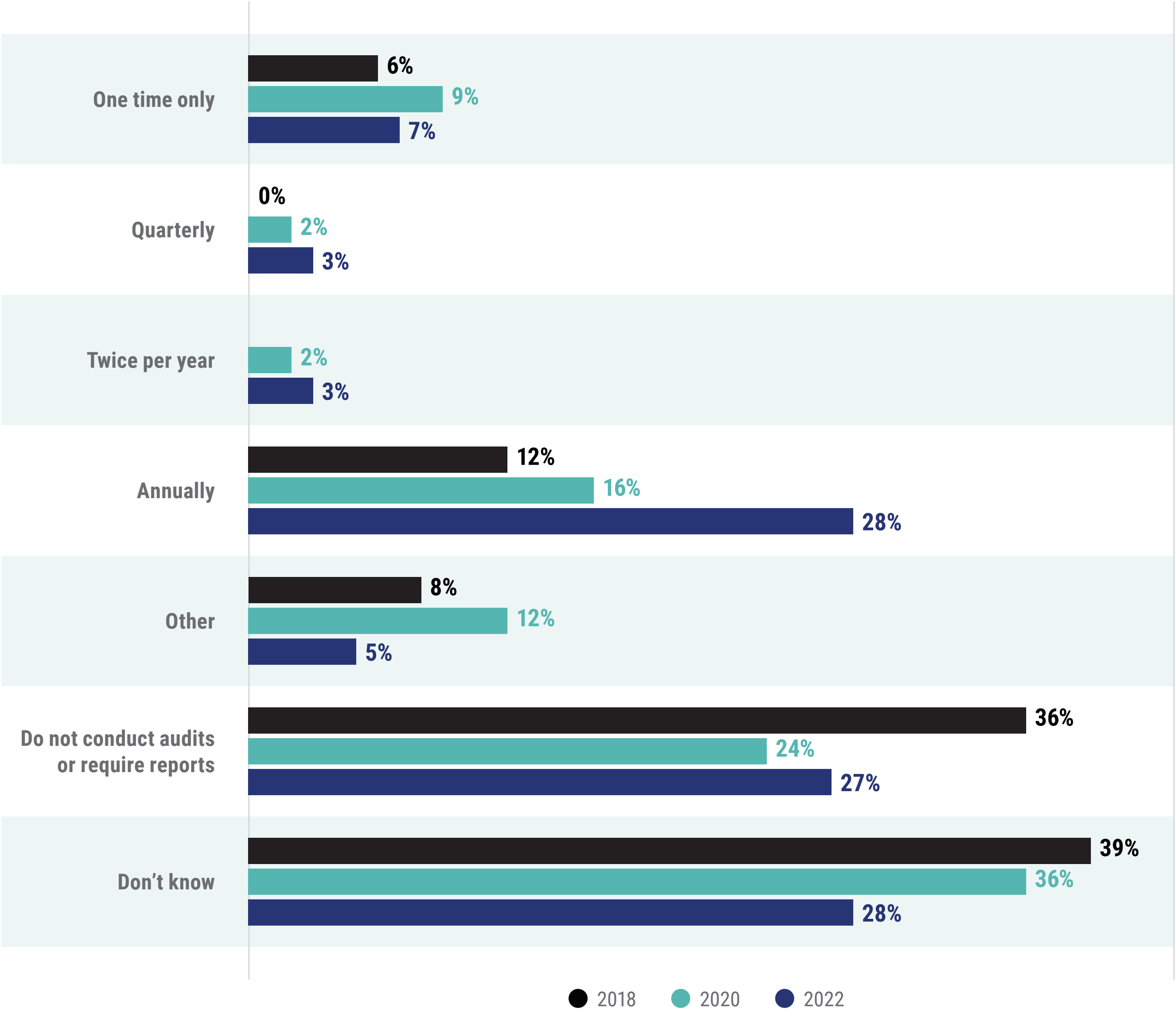
Usage of a Governance, Risk, and Compliance (GRC) solution [by company size]



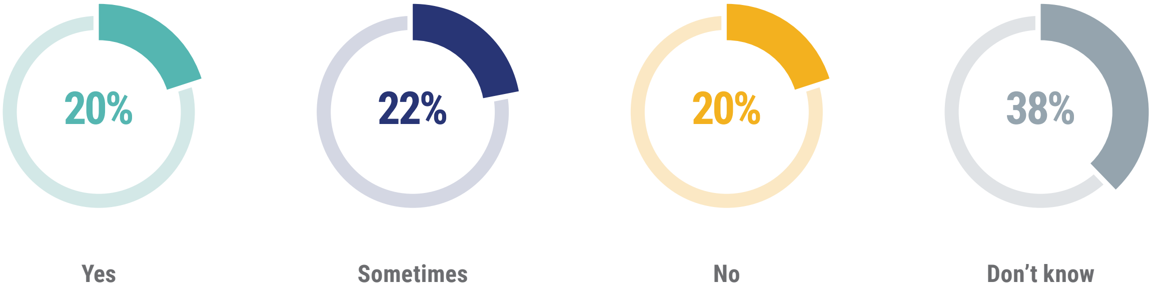
Under half of organizations conduct security audits of high-risk vendors to mitigate cybersecurity challenges. Twenty-eight percent conduct annual audits, a 12-point increase since 2020 and more than doubling the result from 2018. Just three percent of organizations conduct audits twice per year and three percent do so quarterly. Seven percent of organizations audit high-risk vendors one time only.

Around one in four organizations (27 percent) do not conduct cybersecurity audits, a result slightly higher than the one observed in 2020 but considerably smaller than the 2018 result (36 percent). Another 28 percent of participants were not sure whether their organization audited high-risk vendors, with an eight-point reduction compared to 2020.

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



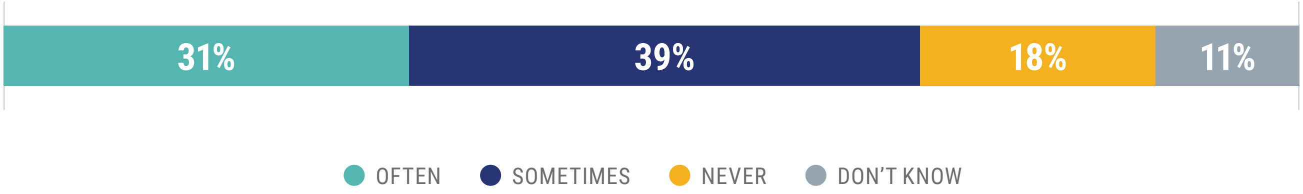
Q: Is your third-party risk management program able to work with legal to create customized security controls for a low maturity client that is very important for a particular business unit?



One in five respondents indicated that the legal department works with the company's third-party risk management program to create customized security controls, while 22 percent of departments do so sometimes. Another 20 percent reported that legal does not collaborate with the risk management program.

Seven in ten participants reported that legal is sometimes involved in third-party risk management, with 31 percent saying that legal is often involved and 39 percent stating that the in-house team is sometimes involved in managing cybersecurity risks related to third parties. Eighteen percent, on the other hand, say that legal is not involved.

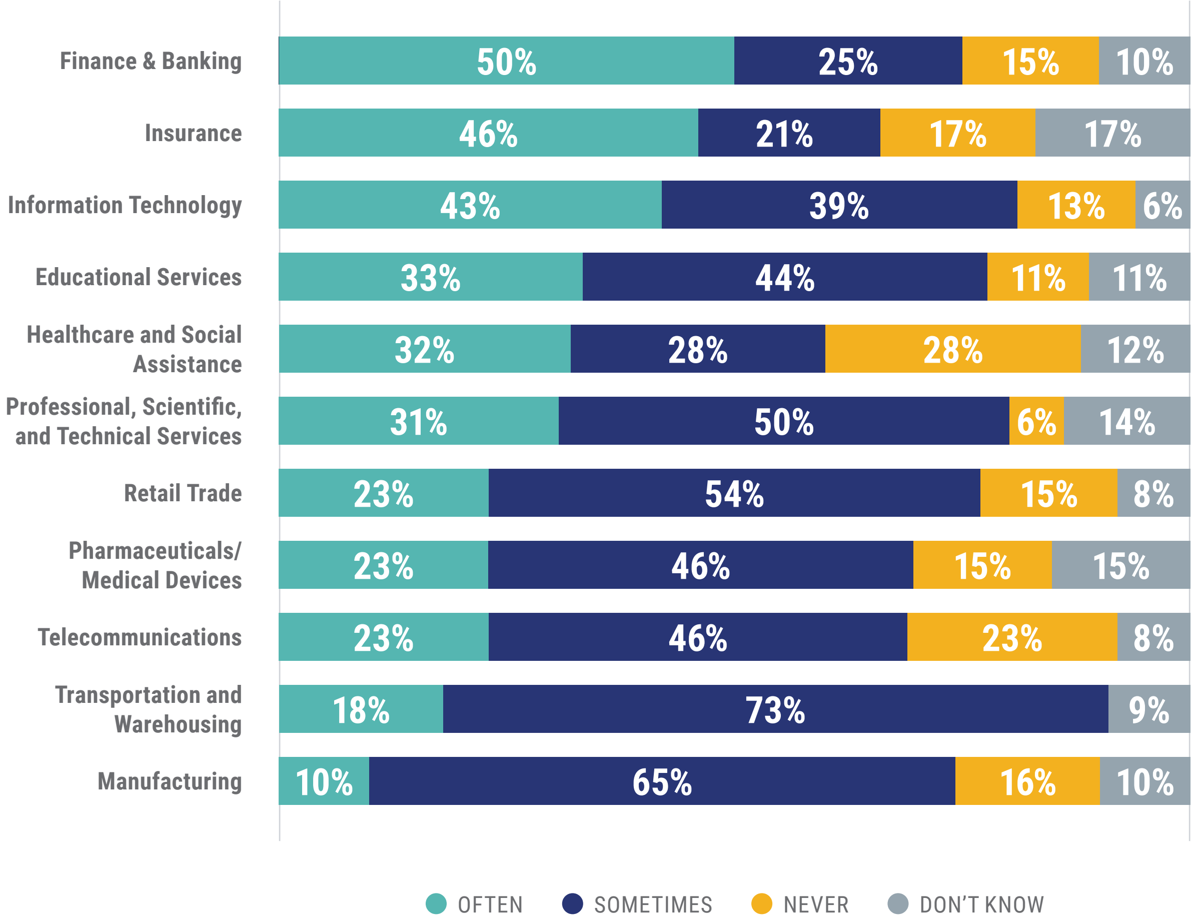
Q: How involved is the legal department in Third-Party Risk Management (TPRM)?



Half of legal departments in the finance and banking sectors are often involved in third-party risk management, while 46 percent of those in insurance companies and 43 percent in information technology organizations are also often involved. Conversely, only 18 percent of legal departments in transportation and just one in ten in manufacturing companies say that they are often involved in TPRM.

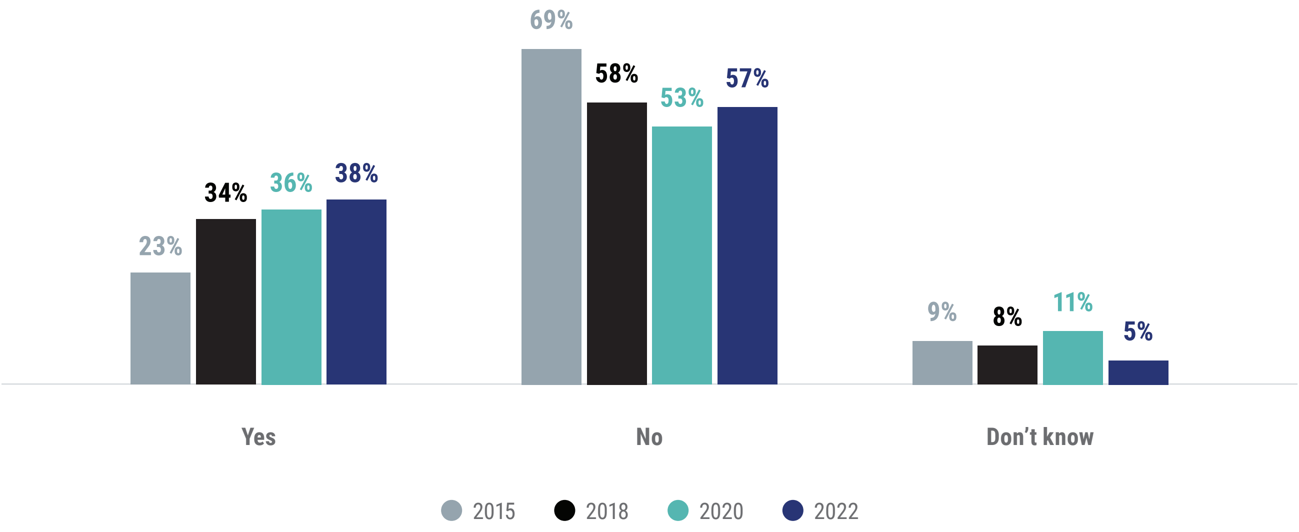
//KEY COMPARISON_

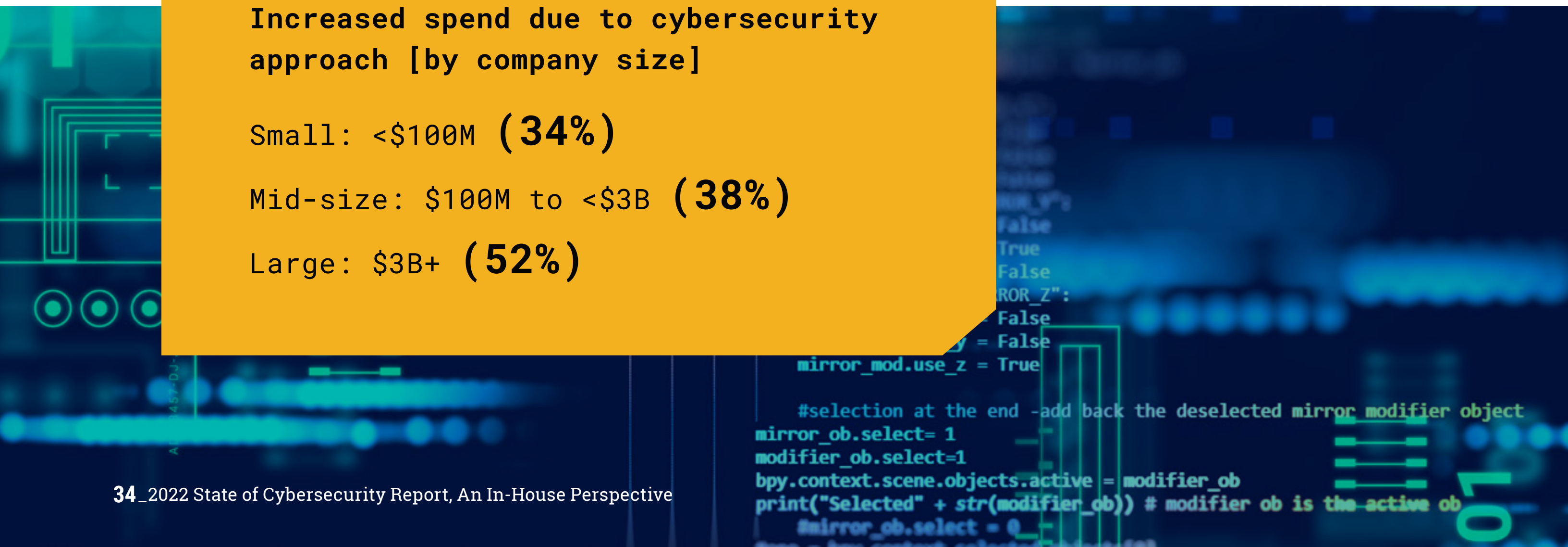
Legal department involvement in Third-Party Risk Management (TPRM) [by industry]



A majority of legal departments (57 percent) indicateed that legal department spending did not increase the previous year as a result of the organization’s approach to cybersecurity. This is four points higher than the result recorded in 2020, but significantly lower (12 points) than the 2015 value of 69 percent. Thirty-eight percent of departments indicated that legal expenses did increase because of cybersecurity — a result consistent with the values observed since 2018 and showing a slight trend upward. The results for both an increase and no increase in legal spend go up compared to the 2020 edition of the survey because of the lower share of respondents who were uncertain how cybersecurity impacted legal spend last year — five percent compared to 11 percent in 2020.

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




mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob

Increased spend due to cybersecurity approach [by company size]

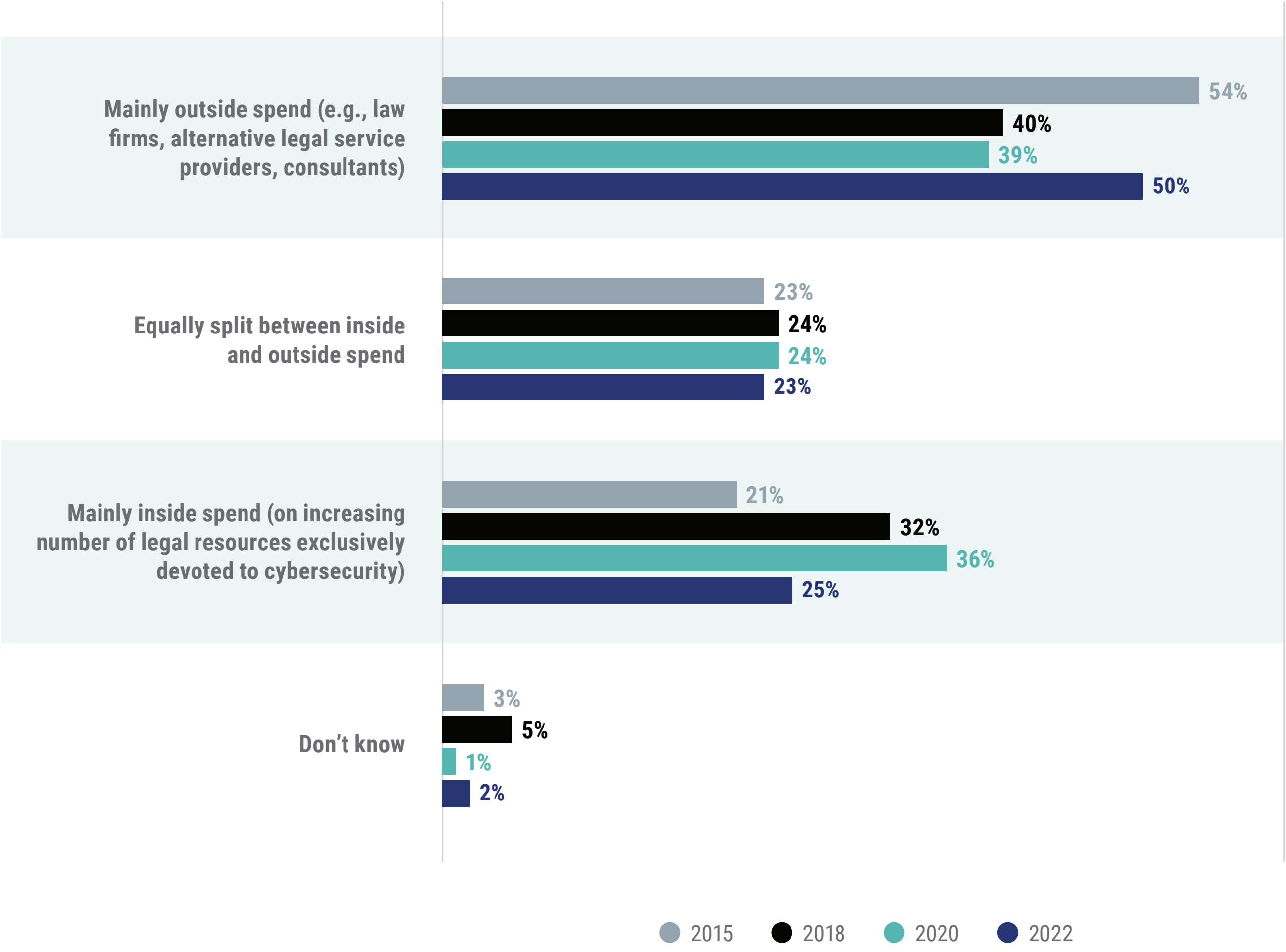
Small: <$100M **(34%)**

Mid-size: $100M to <$3B **(38%)**

Large: $3B+ **(52%)**

Those departments that reported increased legal expenses as a result of the organization's cybersecurity approach indicated that additional spend is mainly allocated outside to law firms, other service providers, and consultants. Fifty percent of those with an increased legal budget allocated the additional funds mainly outside — a 10-point increase compared to 2020 and approaching the 54 percent value registered in 2015. Consequently, those who allocated additional funds mainly in-house show a smaller share of 25 percent of participants with an 11-point reduction compared to the number recorded in 2020. The remaining respondents — around one-quarter — indicated that additional legal funds were allocated equally between outside and inside resources, showing consistency with the survey results since 2015.

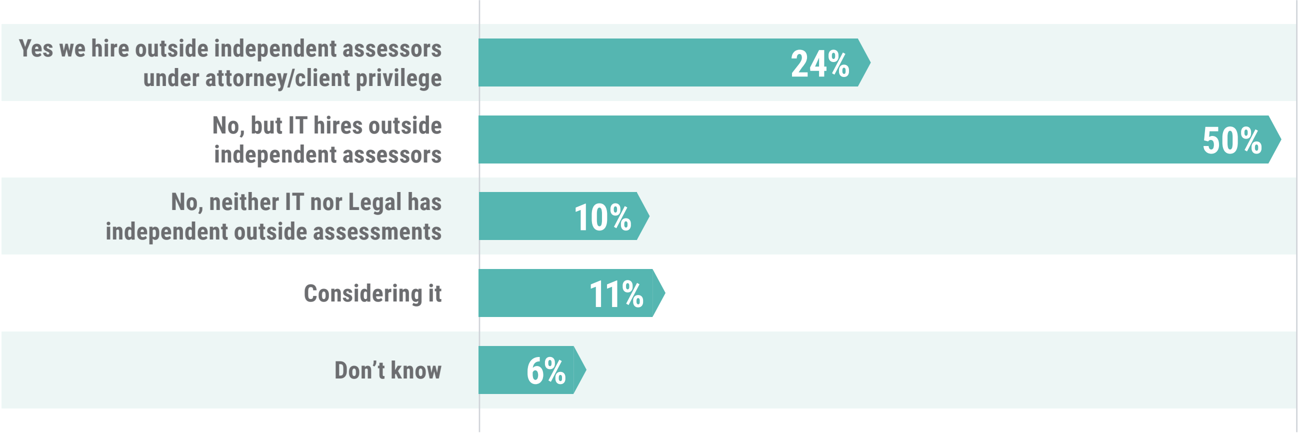
Q: Please describe the increase in spend:



Note: Only asked to those who reported an increase in legal spend.

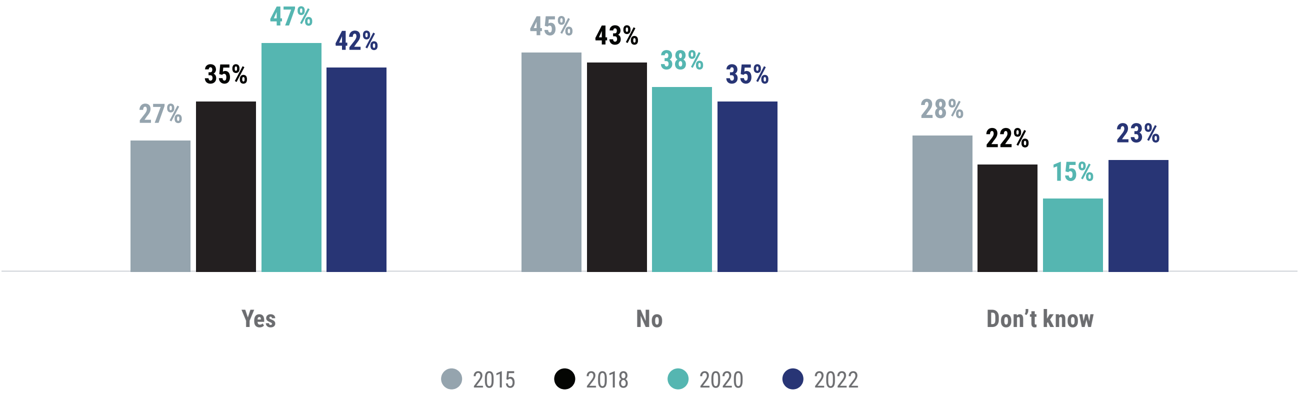
Three in four departments indicated that the organization hires outside assessors or auditors to conduct independent reviews of cybersecurity maturity under attorney-client privilege. Twenty-four percent of participants said that the legal department is responsible for hiring those external auditors, while half reported that the IT department handles this process. Among the remaining participants, 11 percent are considering hiring external cybersecurity auditors, and 10 percent said that neither legal nor the IT department commission these outside assessments.

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



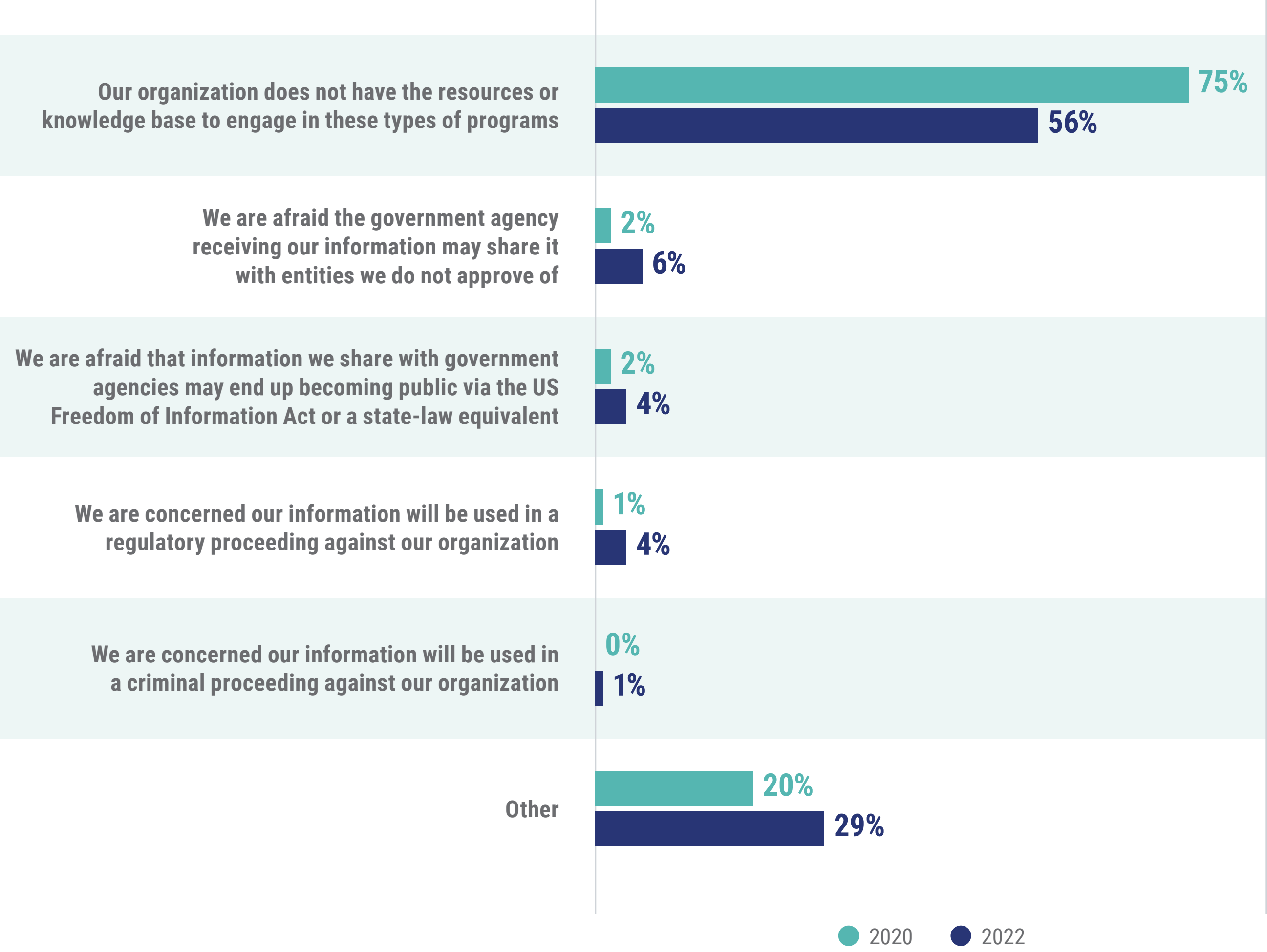
About four in ten departments indicated that their organization collaborates proactively with law enforcement or other government agencies to address cybersecurity risks, and 35 percent said that there is no collaboration. The trend suggests that the number of organizations that do not collaborate with law enforcement is decreasing while the number of participants that reportedly collaborate with governments on cybersecurity is increasing. However, both values record lower percentages compared to 2020 because of the notable increase in respondents that do not know whether the organization collaborates with law enforcement and governmental agencies — 23 percent, up from 15 percent in the last edition of the survey.

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



Most organizations that do not collaborate with law enforcement and government agencies argue that they do not have the resources or knowledge to engage with these programs, though the percentage of organizations that claim this has decreased by 20 points compared to the 2020 result — 56 percent, down from 75 percent. Six percent are afraid the government agencies may share the information with other entities, four percent are concerned that the shared data may become public, four percent are wary that the information shared with the government may be used against the organization in a regulatory proceeding, and one percent indicate that they do not want information shared to be used against the company in criminal proceedings. Each of these concerns scored higher than in 2020 but represent only 15 percent of organizations when combined.

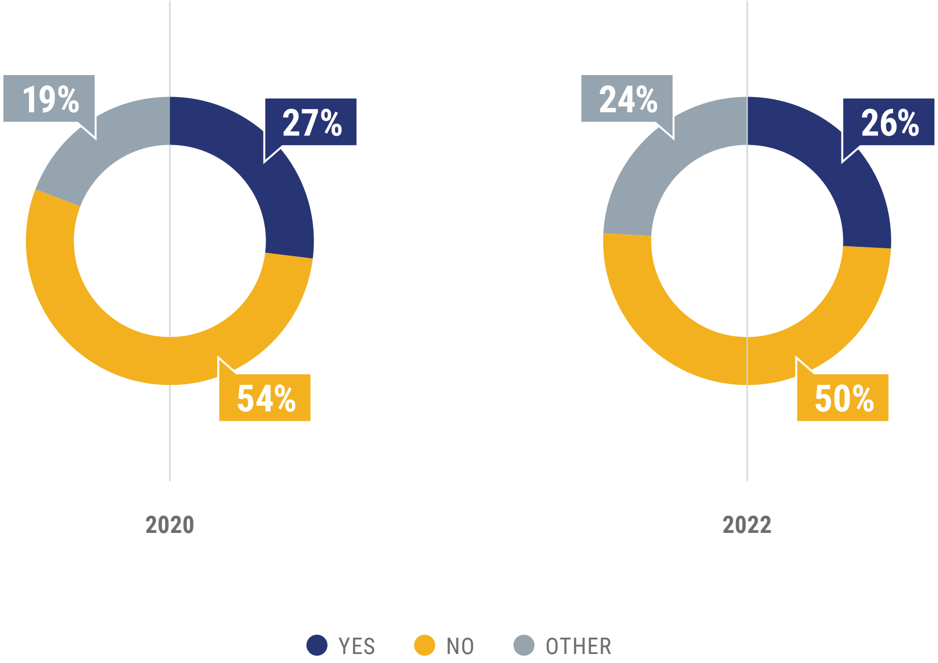
Q: Please explain why your organization does not collaborate proactively with law enforcement or other government agencies to address cybersecurity risks:

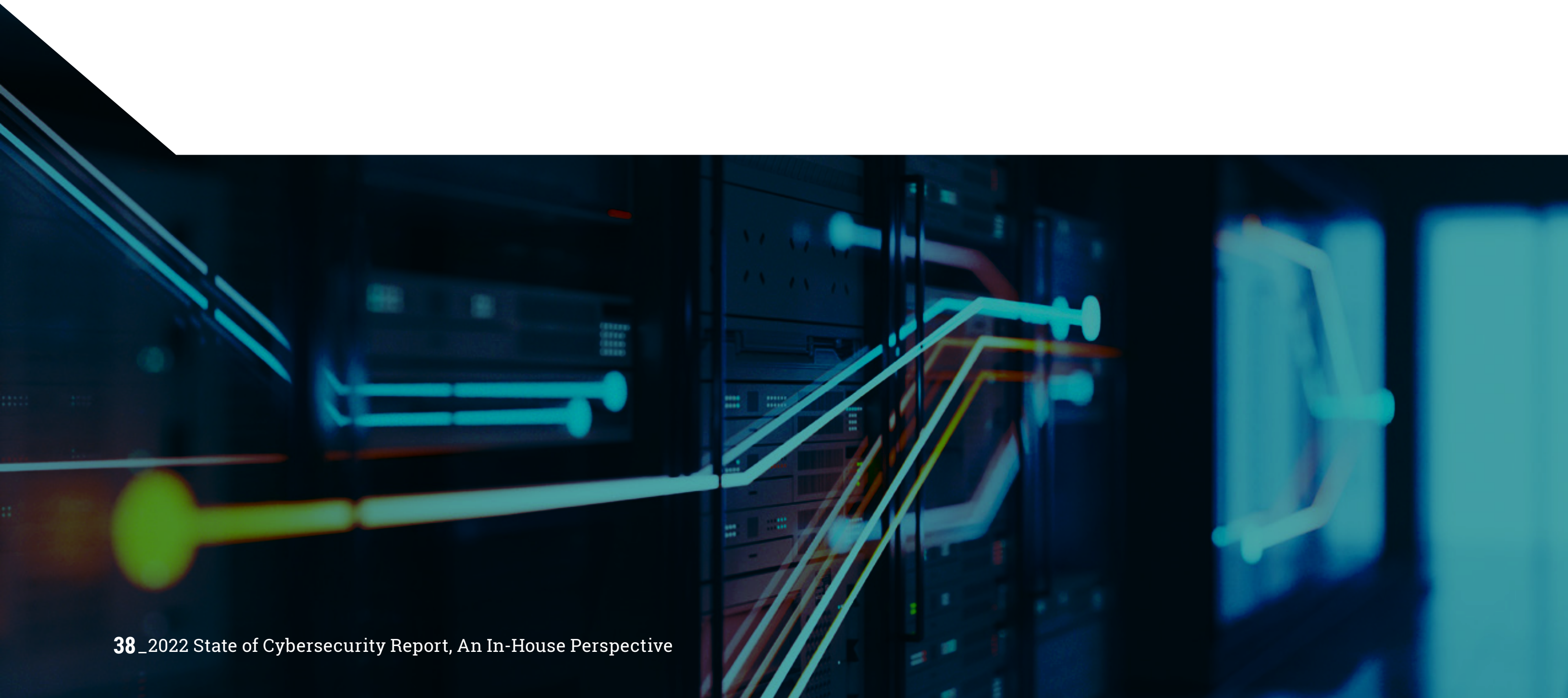


Note: Asked only to those who do not collaborate proactively with law enforcement.

When further inquired about governmental collaboration, half of participants indicated that they are not necessarily more inclined to collaborate with a nonregulatory agency compared to a regulatory agency. Just one in four said they would be more inclined to cooperate with nonregulatory agencies, and the other one-quarter selected other, unspecified considerations.

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)?

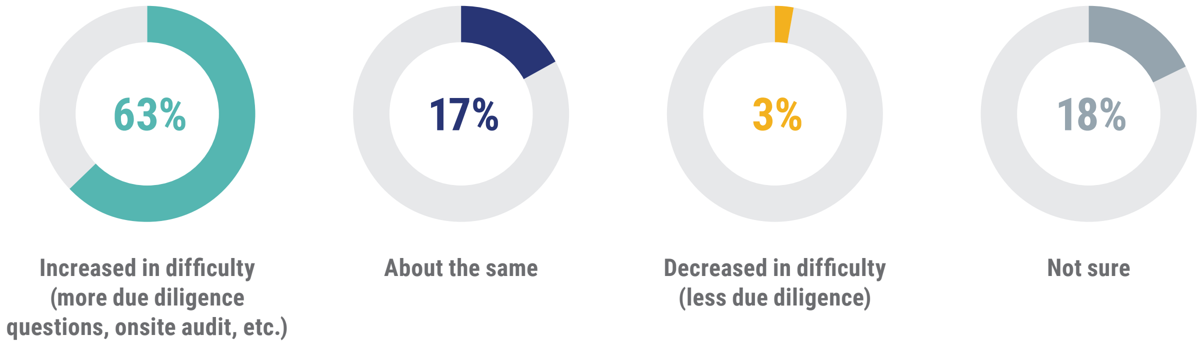




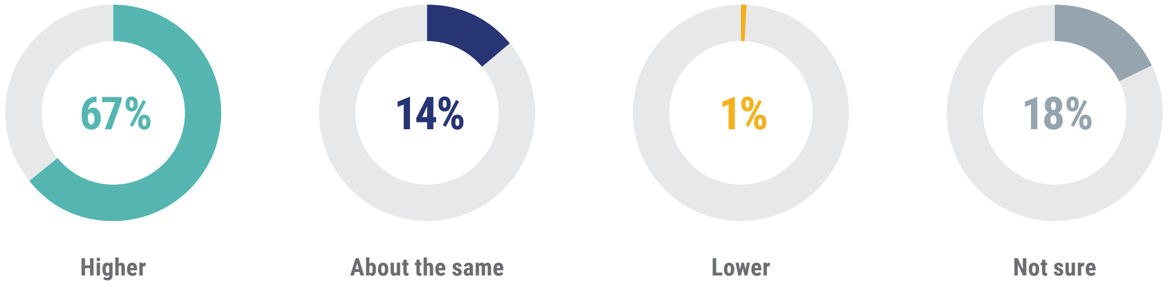
Participants were asked to consider their last review or application process for cybersecurity and technology errors and omissions (E&O) insurance policies. Around two-thirds reported that the application or review process increased in difficulty (63 percent) and costs (67 percent), while only 17 percent said that the resulting insurance policy coverage was higher than in the preceding period. Forty-three percent reported that the new (or most recent) insurance coverage is about the same, and 20 percent said that they received lower coverage. Another 20 percent were unsure about whether the new E&O insurance coverage is higher or lower than before the last review.

Q: Consider the last review and/or procurement of cyber/tech E&O insurance policies:

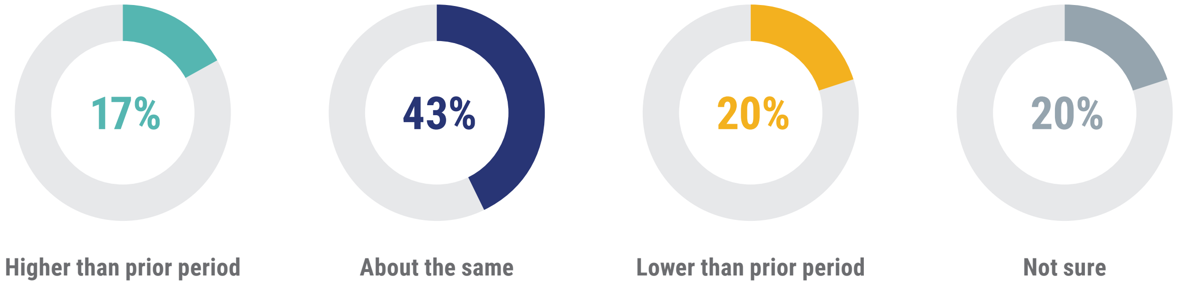
>> Application process:



>> Policy cost was:



>> Policy Coverage was:



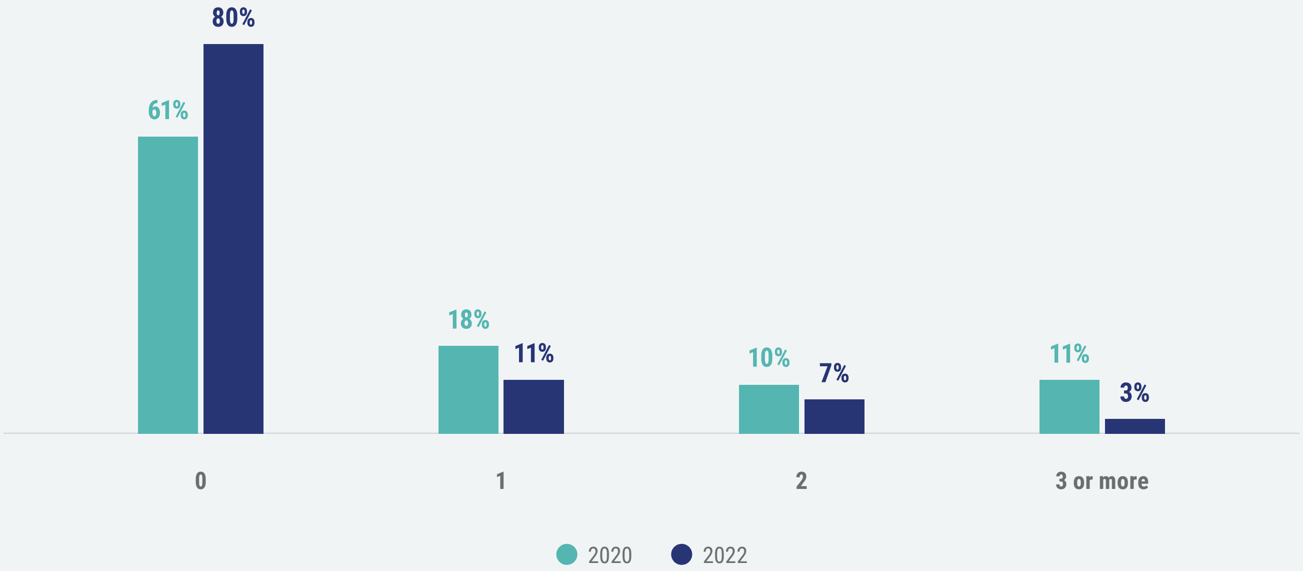
SECTION_04

//breach and incident response:

Four in five participants reported that their organization did not experience any data breaches in the last twelve months, a 20-point drop compared to the result observed in 2020. Eleven percent suffered one data breach, seven percent experienced two, and three percent suffered three or more data breaches in the last year.

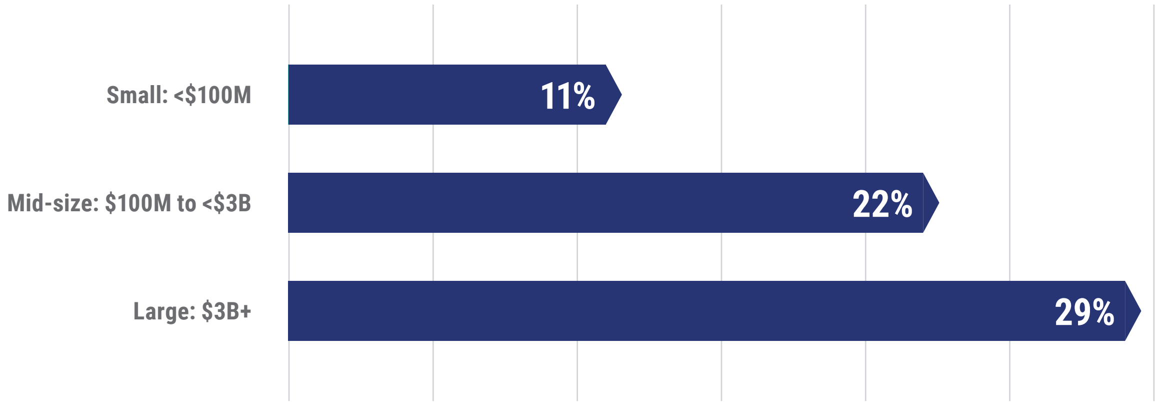
DATA BREACH: A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Q: In the past 12 months, how many data breaches has your organization experienced?



//KEY COMPARISON_

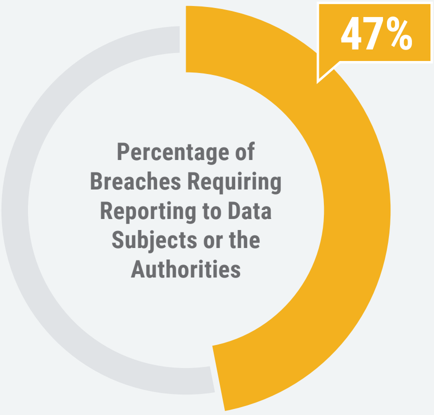
Experienced a data breach [by company size]



Q: How many were of a level or type requiring reporting to data subjects or the authorities?

Almost half of the data breaches suffered by survey participants were of a level requiring reporting to the affected subjects or the authorities.

Note: Only asked to those who reported at least one data breach. Value represents the average for companies that experienced at least one data breach.

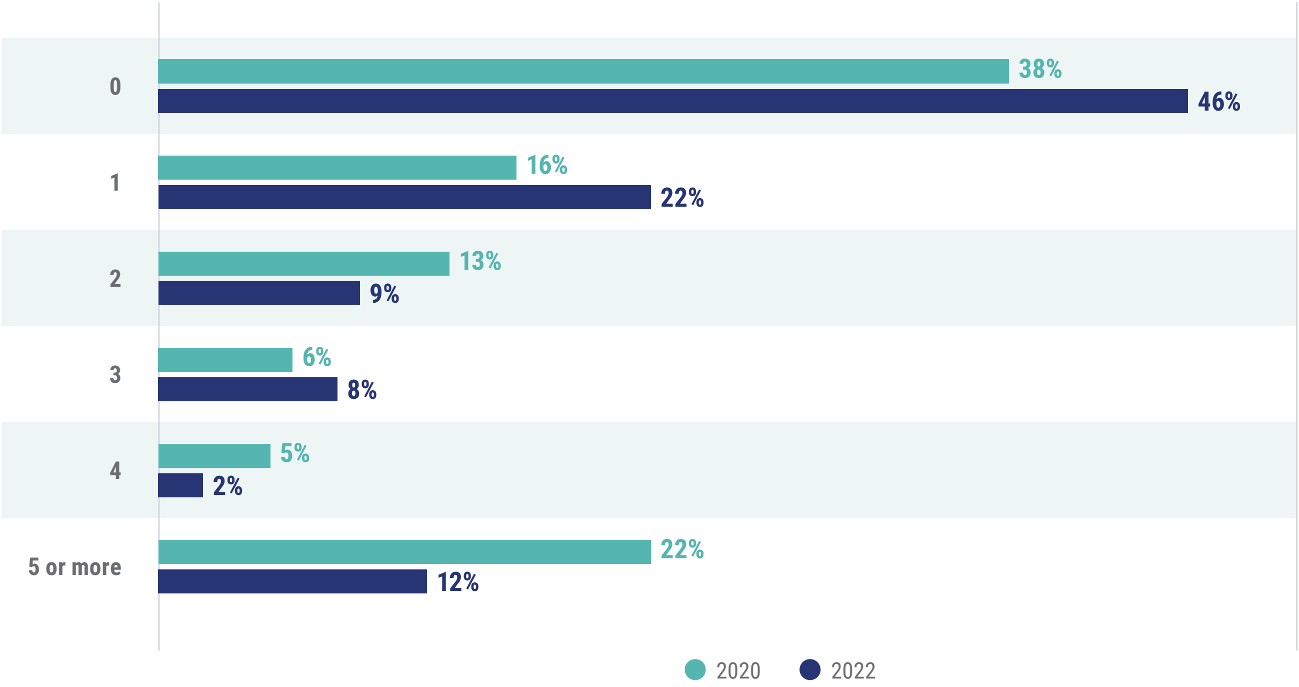


Cybersecurity incidents are more common, with 54 percent of organizations reporting at least one such incident in the last year — eight percent lower than in 2020. Twenty-two percent of participants experienced one cyber incident last year, nine percent reported two, eight percent suffered three, four percent, two, and twelve percent of organizations had to respond to five or more cybersecurity incidents. Compared to 2020, the median number of incidents experienced by participants remains stable at one per year, while the average is significantly lower — nine incidents per organization per year compared to around 24 in 2020.

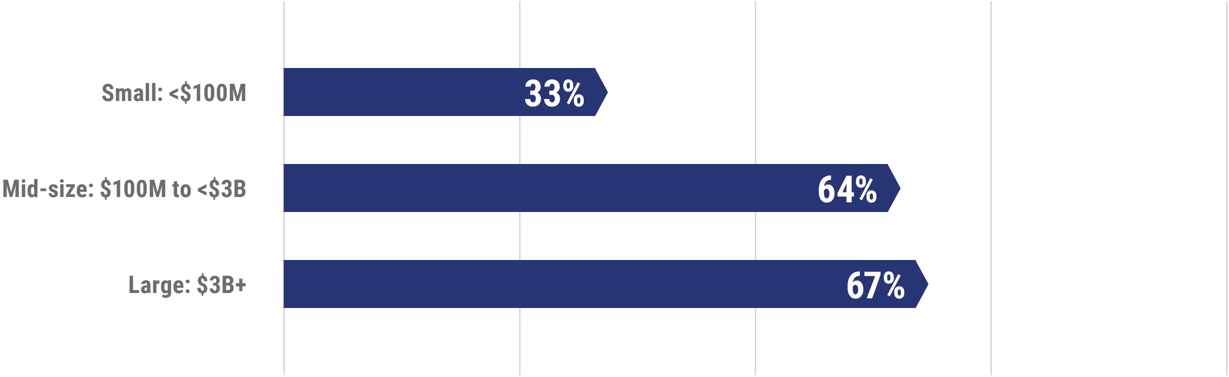
CYBER INCIDENT: A cyber incident is a breach or attempted breach of security that did not result in or lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Q: In the past 12 months, how many cyber incidents has your organization experienced?

>> Number of incidents experienced:

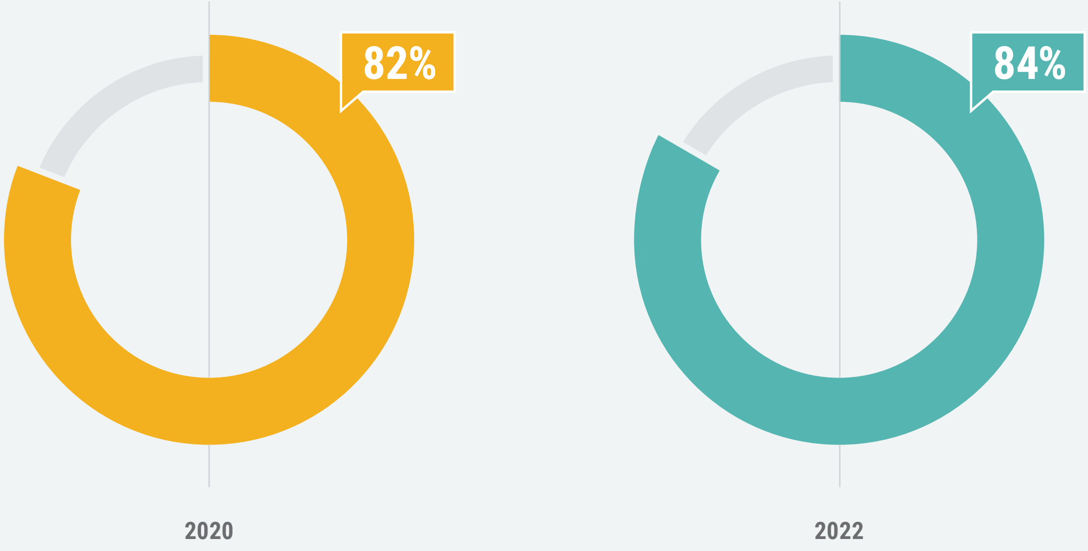


>> Experienced a cybersecurity incident [by company size]:



Though reporting a lower number of annual incidents overall compared to 2020, a slightly higher percentage of participants state that their organizations keep a register of cybersecurity incidents and their resolution — 84 percent compared to 82 percent in the previous edition of the survey.

Q: Do you keep a register of cyber incidents and their resolution?

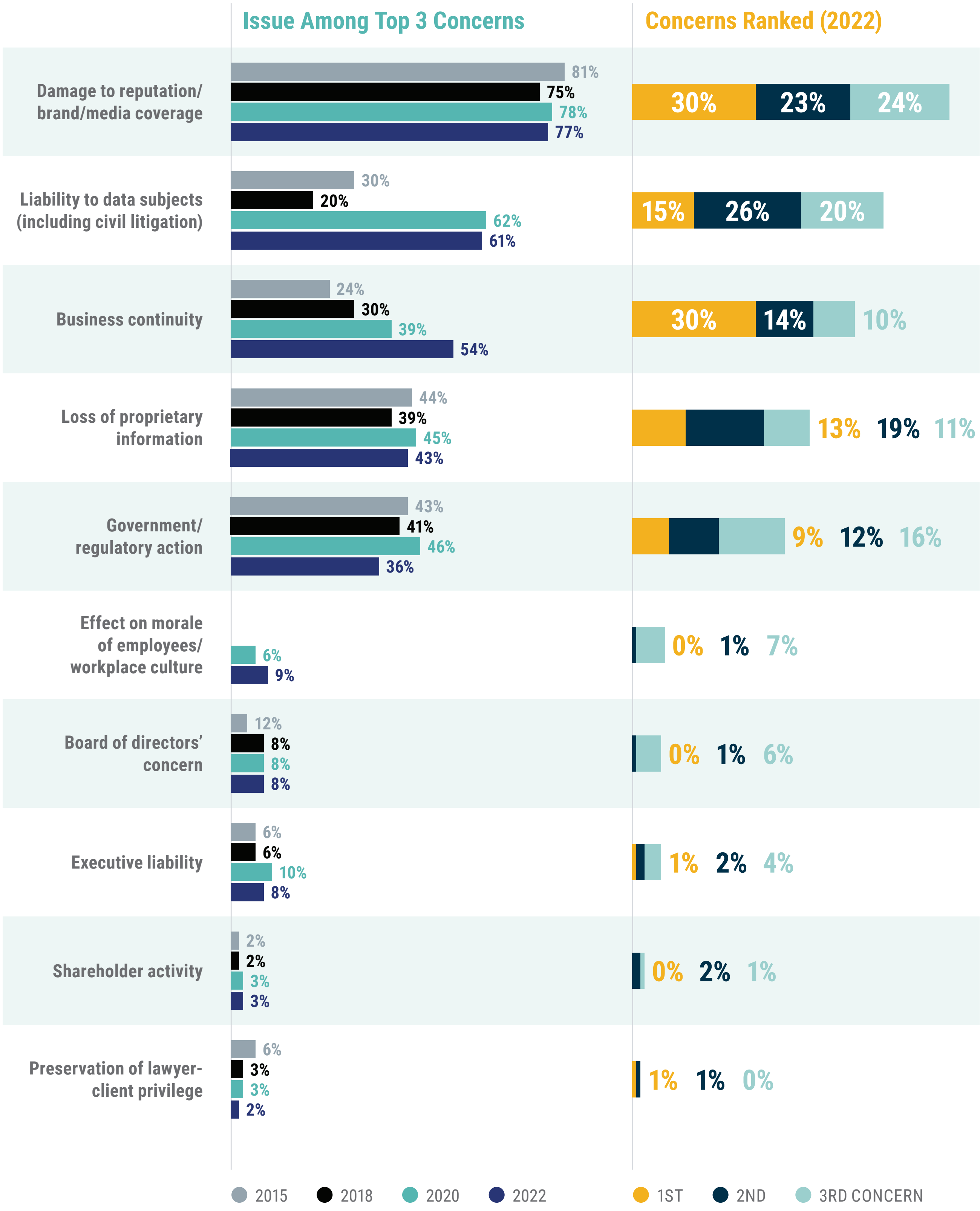


Note: Only asked to those who reported at least one cyber incident. Percentage of "yes" responses reported.

The consequences of a data breach that most worry participants are the damage to the company's brand, reputation, and the negative media coverage, according to 77 percent of participants. Reputational damage has consistently ranked as the top concern resulting from a data breach since 2015. Six in ten participants are wary that a data breach may expose the organization to civil litigation due to liabilities involving the data subjects, and a majority are also concerned about the impact that a data breach could have on business continuity.

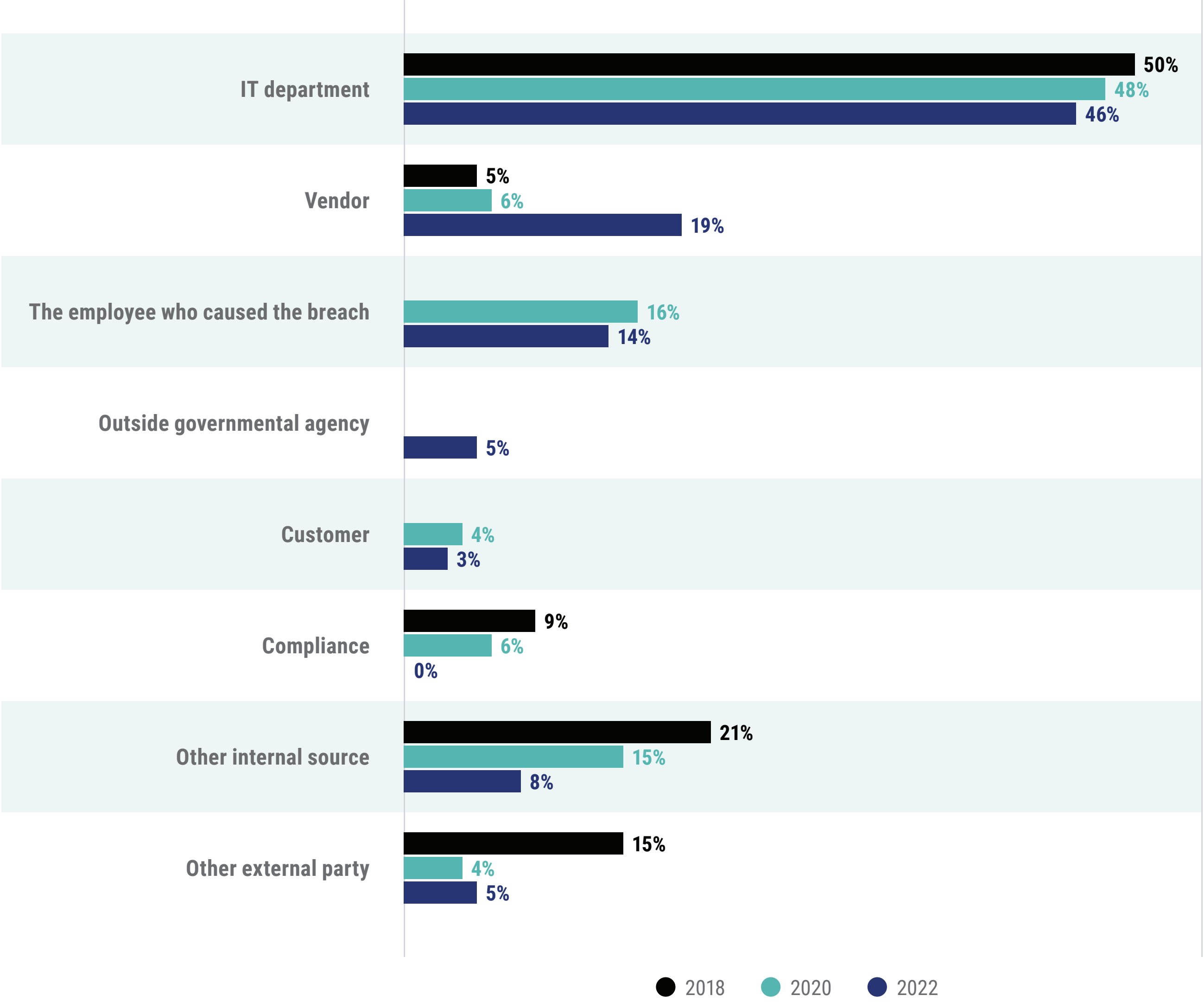
This concern has gained importance steadily since 2015 (a 30-point increase) and three in ten participants rated it as the most immediate concern. Additionally, forty-three percent of participants listed the loss of proprietary information as a top risk from data breaches, and 36 percent fear government or regulatory action against the company — though this concern seems to be receding in importance, with a 10-point decrease compared to 2020. Other less pressing concerns, according to participants, involve the effect on employees' morale (nine percent), the impact of the data breach on the board of directors (eight percent), the liability of company executives (eight percent), shareholder activity (three percent), and the preservation of lawyer-client privilege (two percent).

Q: Rank your three most immediate concerns with regard to a data breach (e.g., what worries you most)?



Participants that reported experiencing a data breach in the last year provided insight on how cybersecurity stakeholders learned about it. About half of participants say that the IT department reported the breach (46 percent), while 19 percent point out that a vendor was the actor that sounded the alarm — a result that tripled those observed in 2018 and 2020. In fourteen percent of cases the employee that caused the breach was the individual to report it, eight percent of breaches were reported by another internal source, five percent were reported by an outside governmental agency, an additional five percent were reported by another external party, and three percent of breaches were reported by a customer.

Q: How did you learn of the most recent breach?

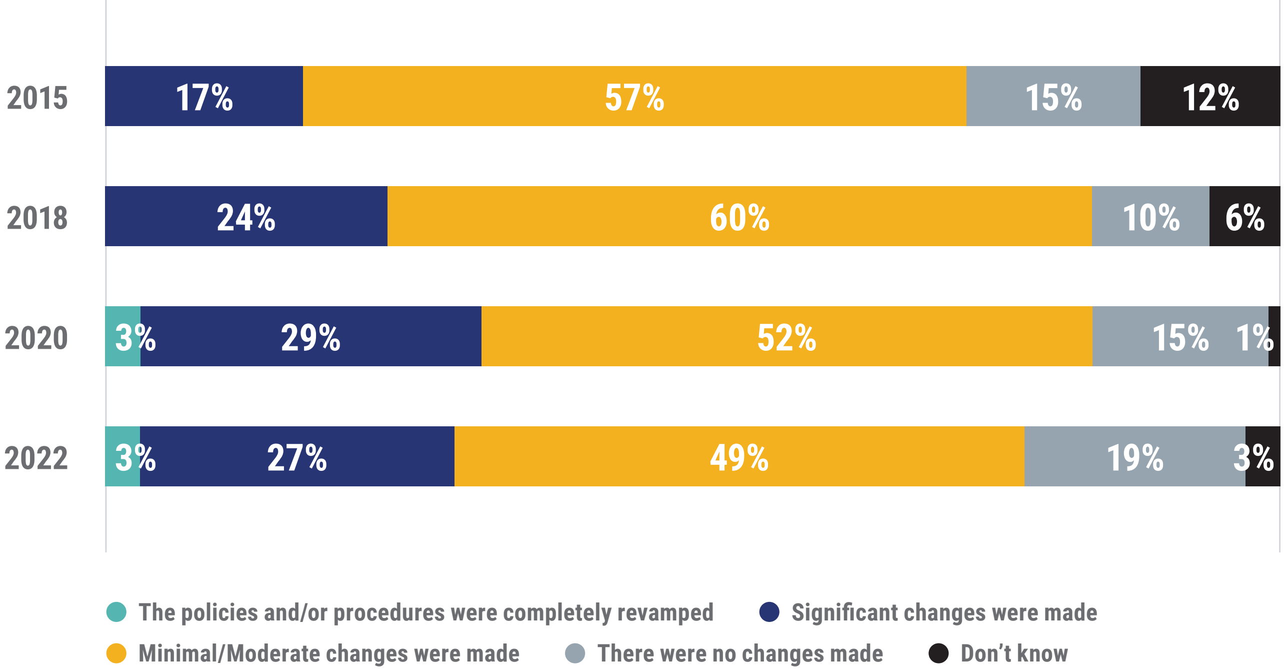


Note: Only asked to those who experienced at least one data breach.

Three in ten organizations that suffered a data breach in the last year made significant changes to the cybersecurity policies and procedures as a result of the breach, with a small minority of companies deciding to completely revamp those processes. This result is comparable to the 2020 result and points to a moderate increase in the number of companies that made significant changes following a data breach observed since 2015.

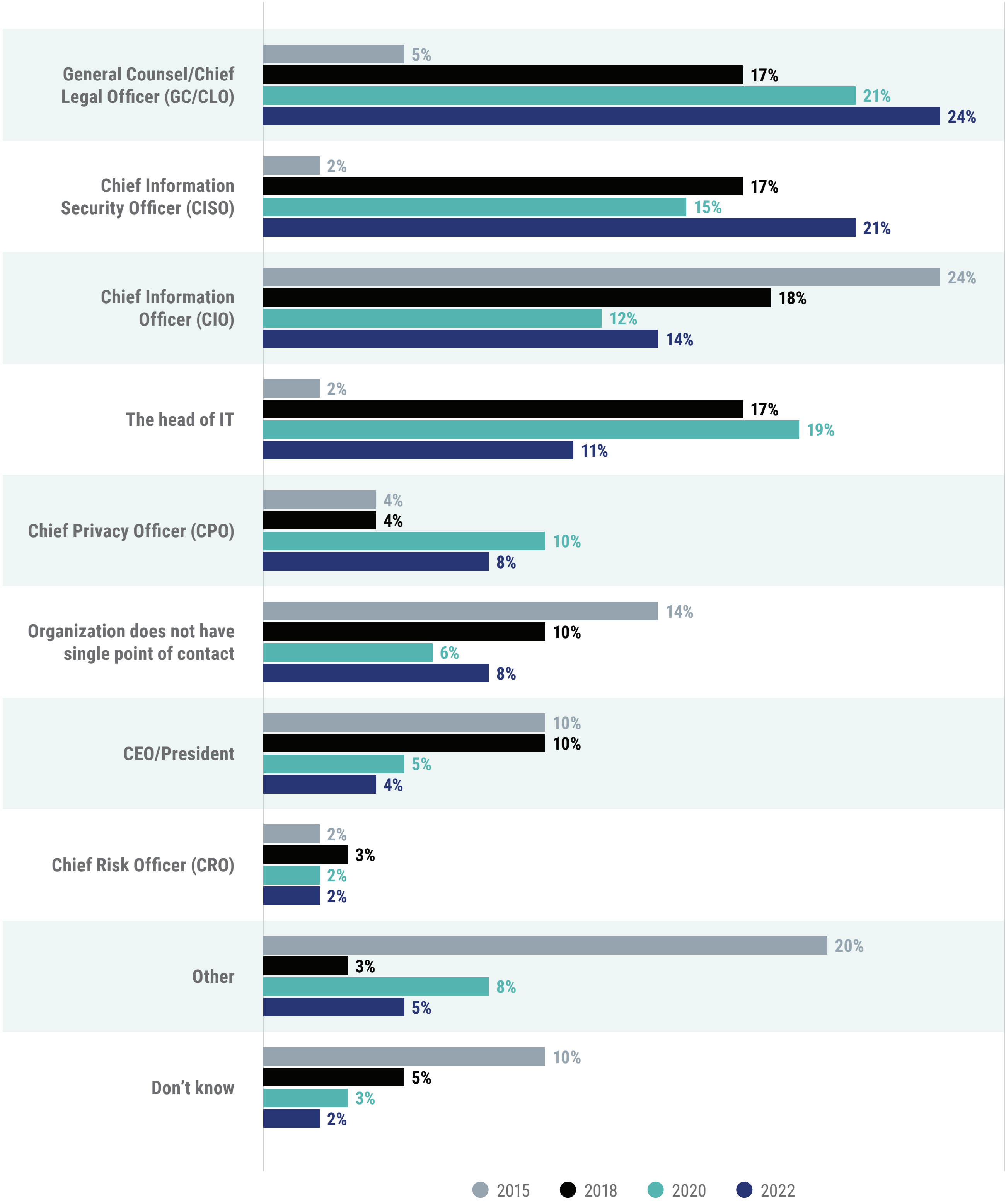
Practically half of organizations (49 percent) that suffered a breach made minimal to moderate changes, and one in five made none. While this is the highest percentage observed since 2015 related to inaction following a data breach, it could relate to companies having already made significant changes to their cybersecurity policies and procedures.

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



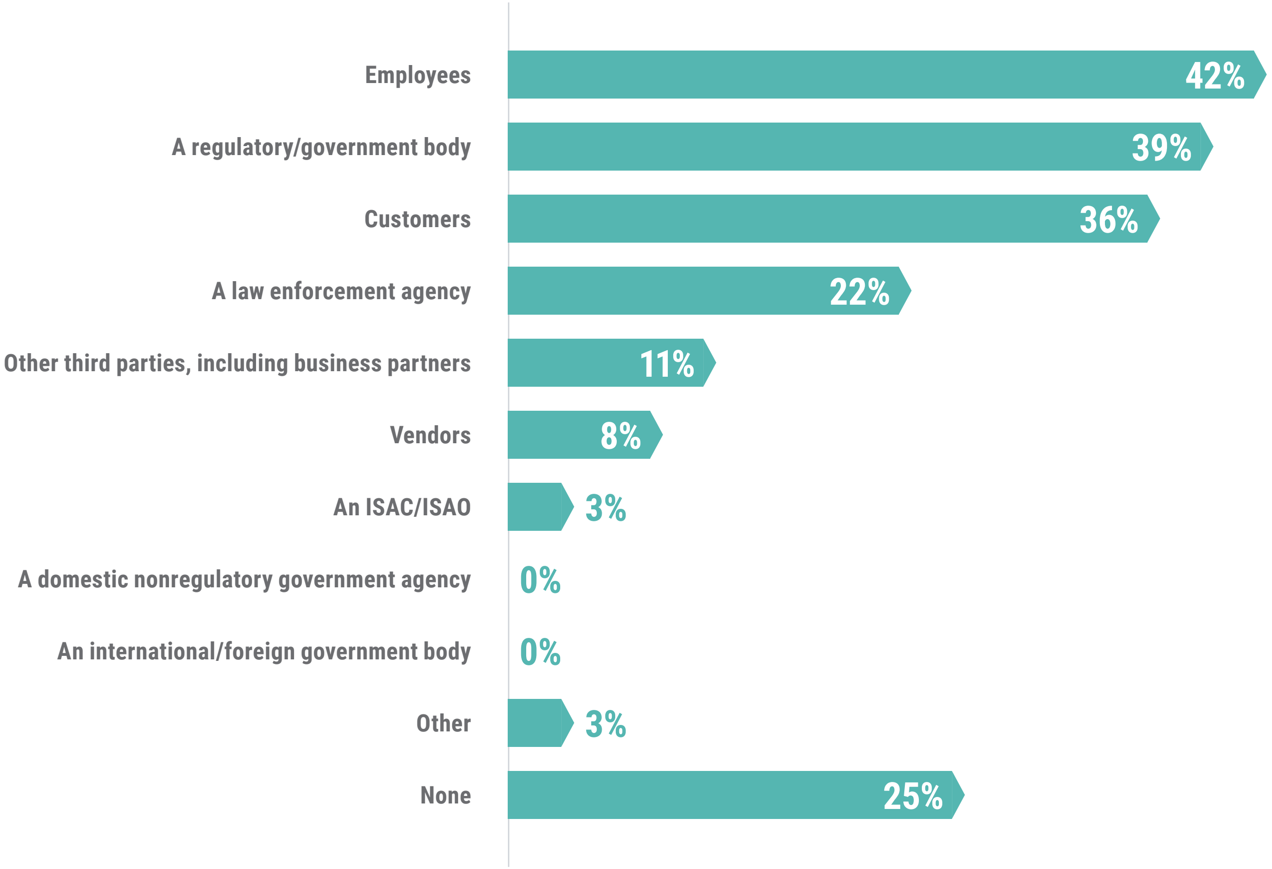
The chief legal officer is primarily responsible for coordinating the response to a breach that involves the theft of personal data. Practically one in four participants said the CLO plays this role in their organization, a percentage that has increased every year since 2015. In 21 percent of organizations the responsible officer is the CISO — with a six-point increase compared to 2020 — while the chief information officer coordinates this type of breach response in 14 percent of organizations. The head of IT is responsible in 11 percent of organizations — decreasing from 19 percent observed in 2020 — and the chief privacy officer is responsible in eight percent of companies. An additional eight percent reported that their organization does not have a single point of contact, and other positions that play this role include the company's CEO or president (four percent), the chief risk officer (two percent), or other positions (five percent) — which, in some cases, are a cybersecurity- or privacy-focused in-house counsel.

Q: Who in your organization is primarily responsible for coordinating the response to a personal data breach (involving theft of personal data)?



Twenty-five percent of participants who suffered a data breach admitted that the organization did not notify anybody about the breach. Employees were notified in 42 percent of cases, a regulatory or government body in 39 percent, and 36 percent of companies that suffered a breach notified customers. Twenty-two percent reported the breach to a law enforcement agency, 11 percent did the same to third parties, including business partners, and eight percent notified their vendors about the breach.

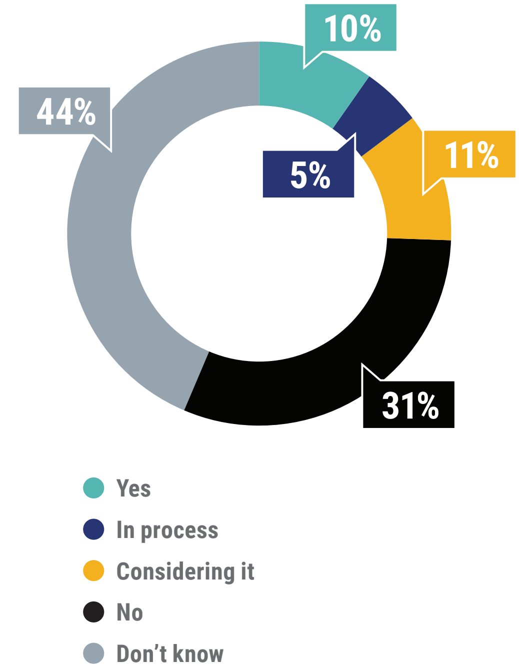
Q: In relation to the most recent breach you experienced, did your organization notify any of the following:



Note: Only asked to those who experienced at least one data breach.

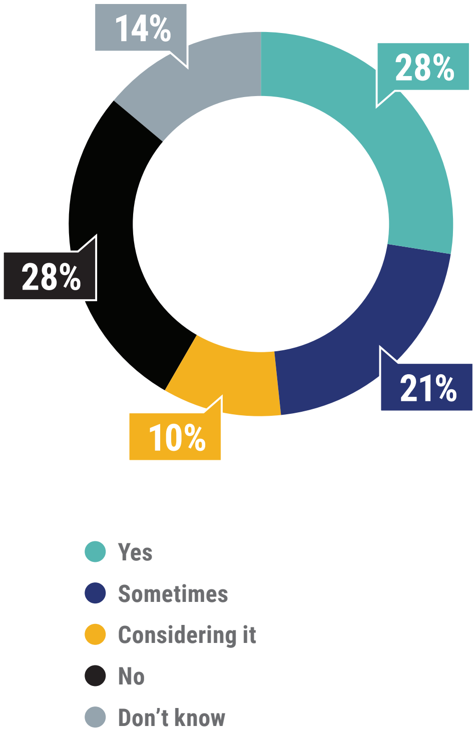
Q: Has your organization implemented a Security Orchestration, Automation and Response (SOAR) technology?

Only one-quarter of respondents is engaging to some extent with security orchestration, automation, and response (SOAR) technology, with ten percent of organizations having implemented such a tool, an additional five percent saying that implementation is being processed, and 11 percent considering adapting this tool. Three in ten have not implemented SOAR technology and close to half of participants do not know if this technology is employed by their organization.

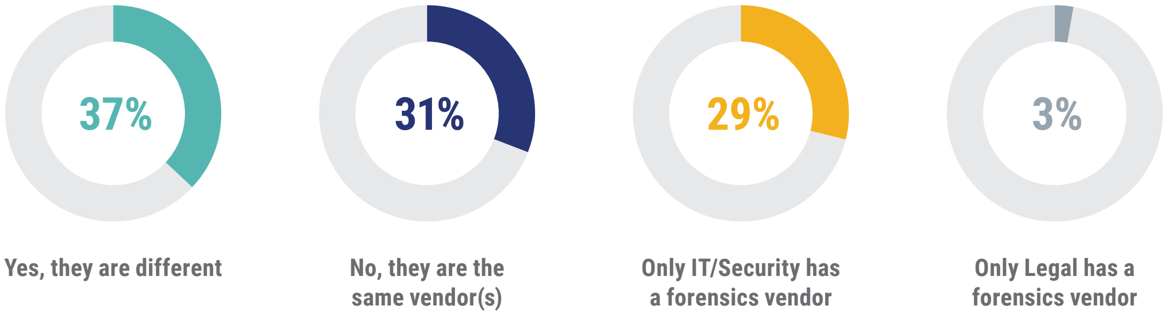


Q: Does the legal department or outside counsel hire forensics experts to conduct independent reviews of a cybersecurity incident?

Almost half of participants reported that either the legal department or outside counsel hire cybersecurity forensics experts to conduct independent reviews of incidents experienced by the organization. Twenty-eight percent reported that this action is taken regularly and 21 percent reported engaging with forensics experts sometimes. An additional ten percent indicated that they are considering taking those measures following future cybersecurity incidents. Twenty-eight percent do not conduct independent reviews of cybersecurity incidents.



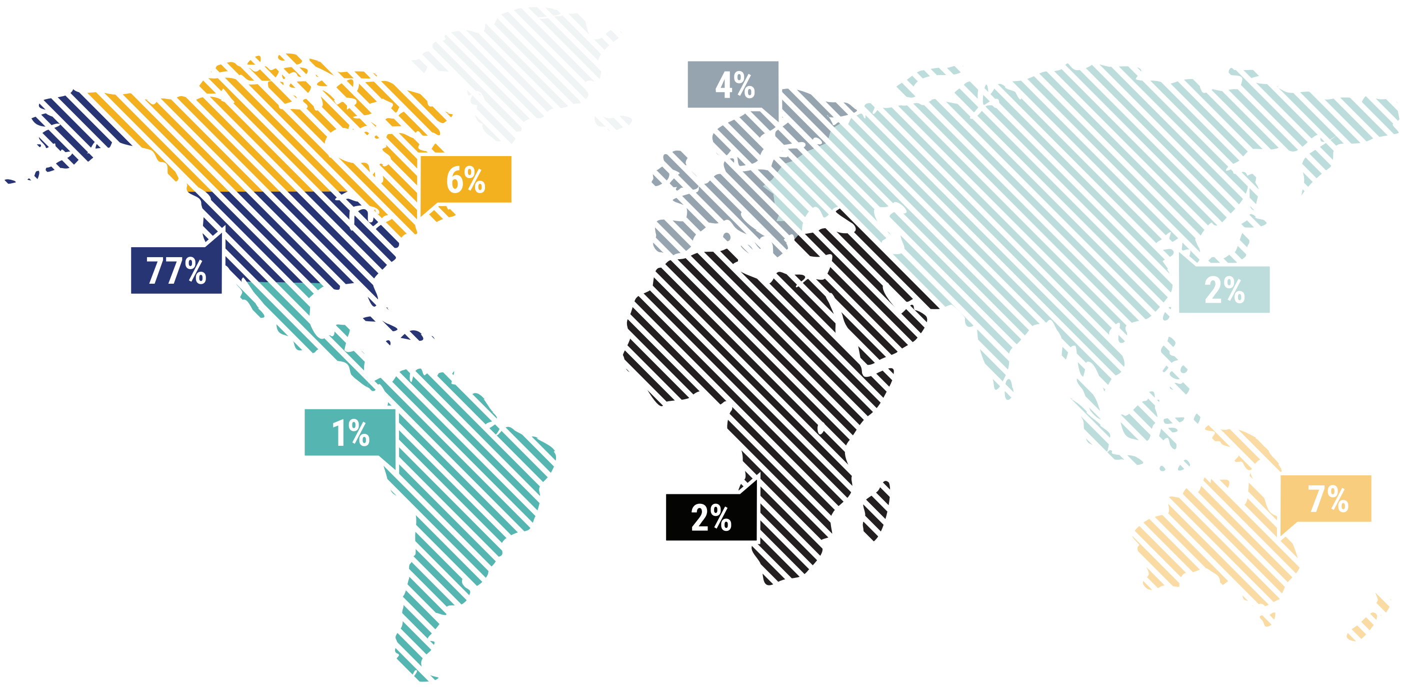
Q: Is the Legal forensics vendor different from the IT/ Security forensics vendor?

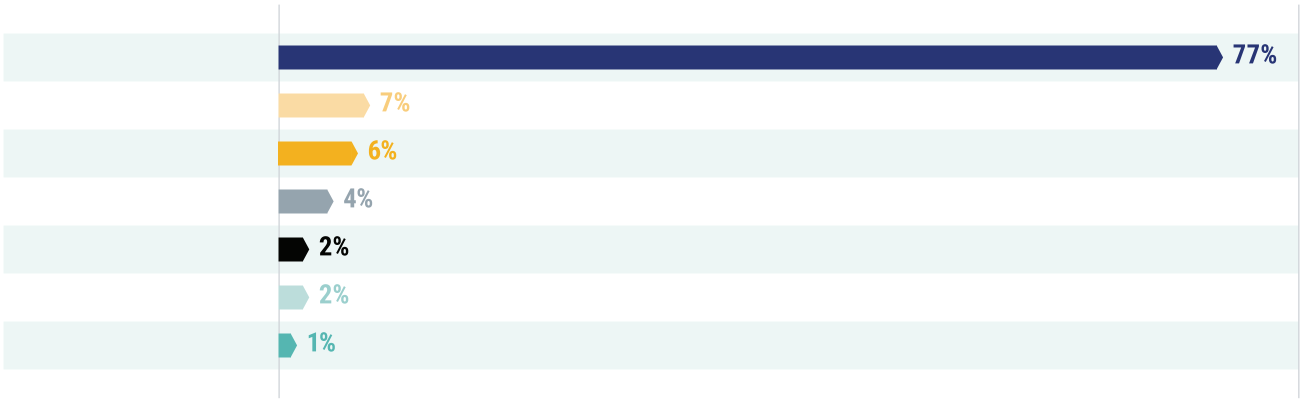


Those who engage with forensics vendors reported varied types of engagements in relation to the forensics providers for the legal and the IT departments. Thirty-seven percent have different forensics vendors for legal and IT, while 31 percent reported that the vendors servicing the needs of both departments are the same. In 29 percent of organizations only the IT department has a forensics vendor, and in a small minority (three percent) of cases it is the legal department alone that engages with a forensics vendor.

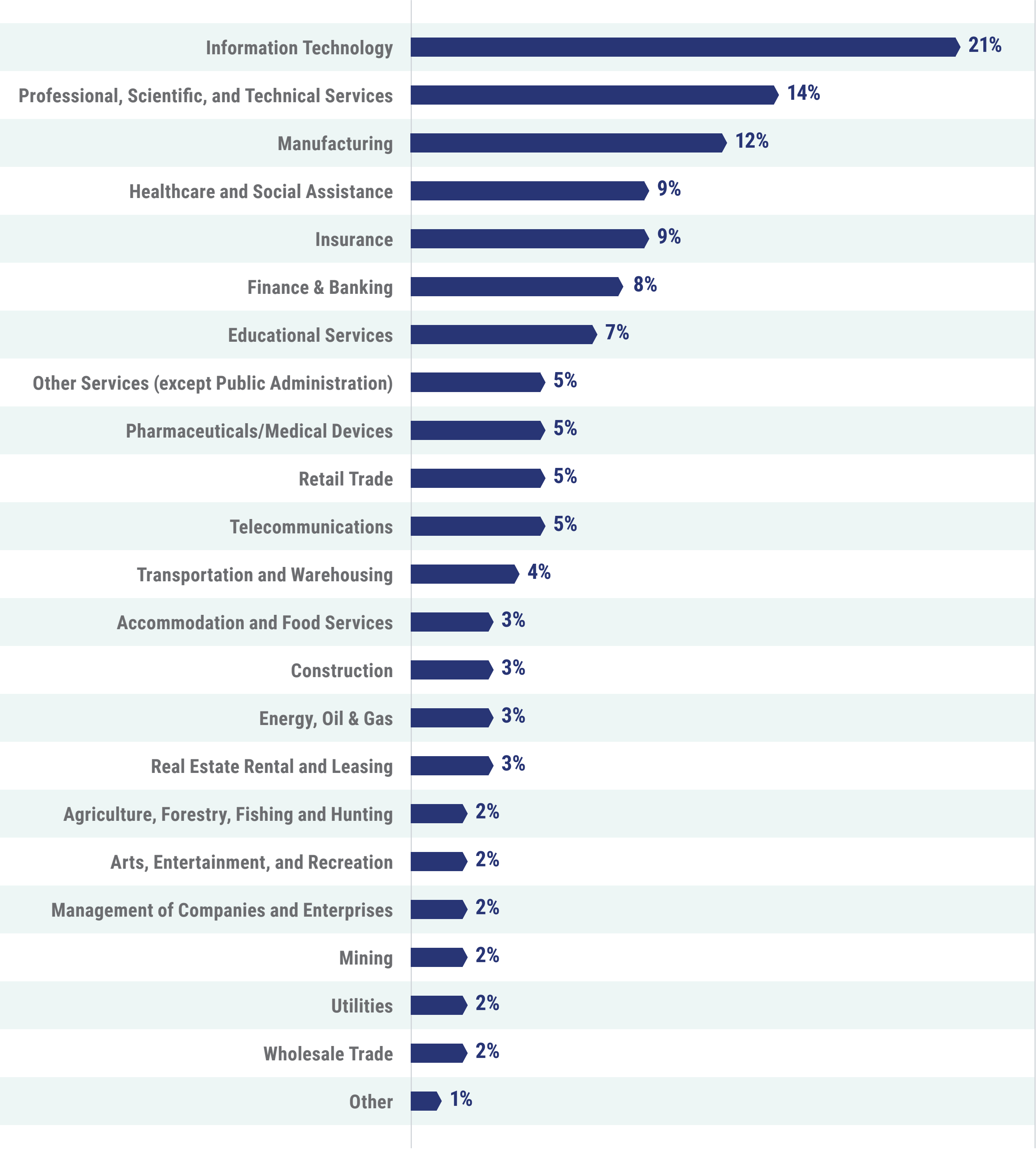
//participant profile_

Global Region

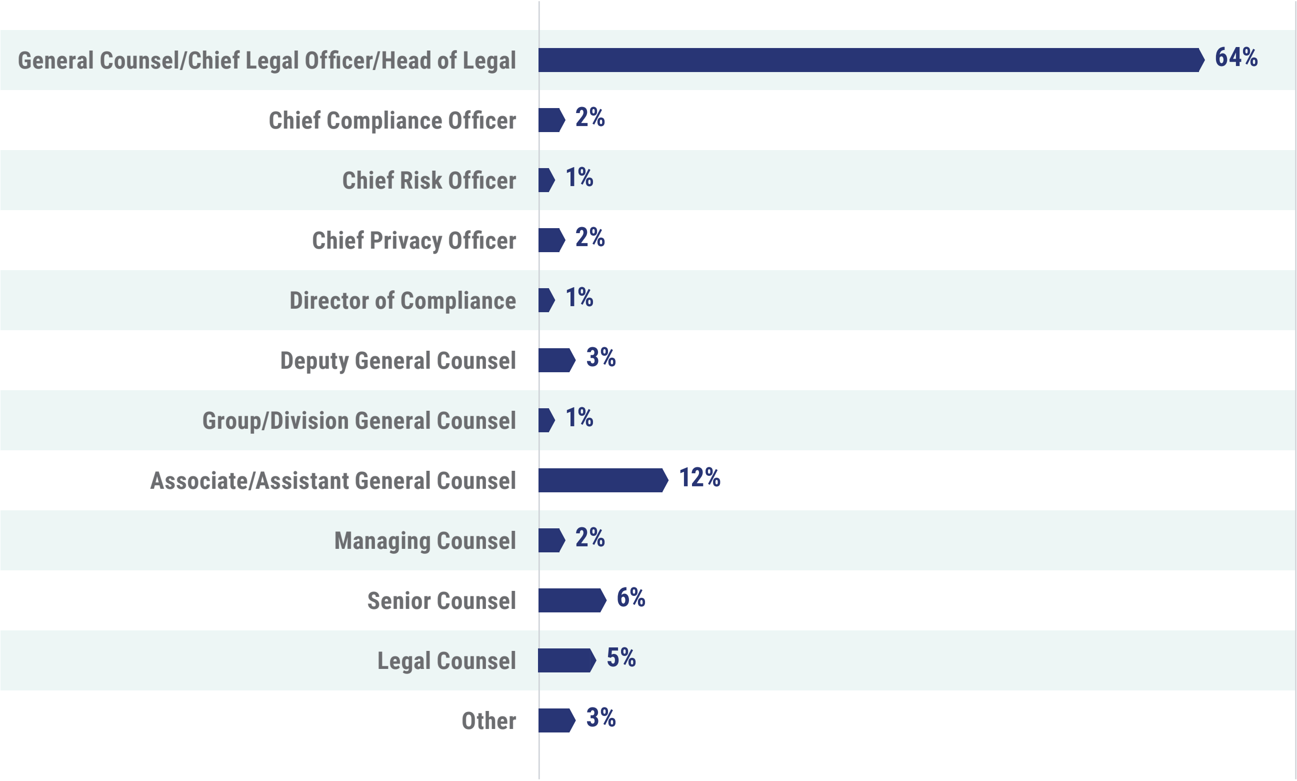




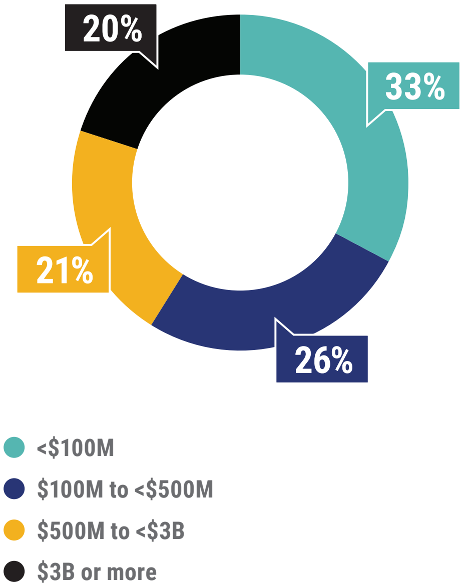
Industry


Information Technology 21%
Professional, Scientific, and Technical Services 14%
Manufacturing 12%
Healthcare and Social Assistance 9%
Insurance 9%
Finance & Banking 8%
Educational Services 7%
Other Services (except Public Administration) 5%
Pharmaceuticals/Medical Devices 5%
Retail Trade 5%
Telecommunications 5%
Transportation and Warehousing 4%
Accommodation and Food Services 3%
Construction 3%
Energy, Oil & Gas 3%
Real Estate Rental and Leasing 3%
Agriculture, Forestry, Fishing and Hunting 2%
Arts, Entertainment, and Recreation 2%
Management of Companies and Enterprises 2%
Mining 2%
Utilities 2%
Wholesale Trade 2%
Other 1%

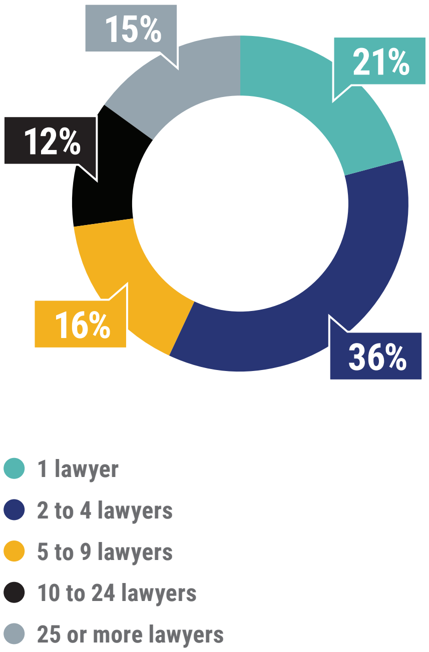
Job Title



Company Revenue



Number of Lawyers



_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 June 14, 2022, and closed on July 29, 2022. 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 265 legal department decision-makers participated. Apart from targeted email messages, opportunities to participate were also sent through LinkedIn campaigns and on relevant ACC Networks forums.

ANONYMITY

Survey responses were completely anonymous. 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.

ABOUT ACC AND THE ACC FOUNDATION

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 45,000 members employed by over 10,000 organizations in 85 countries, the ACC Foundation 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.

The report was sponsored by Ernst & Young Consulting.

ACC Foundation
Association of Corporate Counsel

IN COLLABORATION WITH

EY Building a better working world

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

© 2022 ACC Foundation, All Rights Reserved.
This report and the information contained herein are copyrighted by the Association of Corporate Counsel.
All additional requests for use must comply with ACC copyright policy located at
acc.com/about/privacy-policies/copyright.

When using information from this report, the following language must appear:
Reprinted with permission from the Association of Corporate Counsel 2022. All Rights Reserved.