Cyber Threats:

Measuring Awareness, Assessing Preparation

A FOX ROTHSCHILD SURVEY OF C-LEVEL EXECUTIVES

Fox Rothschild LLP
ATTORNEYS AT LAW

Executives Recognize the Menace of Cyber Threats, Yet Preparation and Defense Remain Woefully Inadequate

EXECUTIVE SUMMARY

BY FAILING TO PREPARE, many companies have prepared to fail when it comes to thwarting cyberattacks. Fox Rothschild's survey of corporate leaders reveals endemic misperceptions about what is necessary for privacy and data security protections in the age of phishing and ransomware.

The survey, conducted in the fourth quarter of 2017, discovered an alarming lack of preparedness at a time when companies are facing daily privacy and data security threats. The key findings: while a majority of U.S. executives appreciate the gravity of the threat of a cybersecurity breach – and that it is now a perpetual risk – few are taking adequate steps to protect their companies.

"People generally think, 'We're doing enough to protect ourselves,' or even, 'It won't happen to us because we don't have the kind of data that cyber thieves want,'" says Mark McCreary, Fox Rothschild's Chief Privacy Officer. "That could not be further from the truth. Statistics show the risk of an attack or accidental breach is real, and that companies not only need to put defenses in place, but also must prepare to respond effectively should a data loss occur."

"Alternatively, others recognize the threat but throw their hands in the air, thinking nothing they do is really going to make a difference if they're attacked," notes Elizabeth Litten, Fox Rothschild's HIPAA Privacy & Security Officer.

More than half of the C-level executives surveyed reported that their companies are at "high" or "very high" risk for a breach. However, nearly one-third said they don't provide any cybersecurity training to their employees, and a majority assessed their budgets as inadequate to manage a breach response.

"The black hat hackers are typically faster, more motivated, have no rules and are a few steps ahead of the white hats," said one survey participant. "Keeping our security position strong needs to always be a focus within the organization. One slip is all that is needed to become vulnerable."

"People generally think, 'We're doing enough to protect ourselves,' or even, 'It won't happen to us because we don't have the kind of data that cyber thieves want,'" says Mark McCreary, Fox Rothschild's Chief Privacy Officer.

Cyber insurance coverage was common among respondents, but the survey found that executives lack a solid grasp of the policies' limitations. This is yet another example of appreciating the threat but failing to marshal the resources required to safeguard the organization.

More than a quarter of companies surveyed do not furnish any cybersecurity and data privacy reports to their boards of directors. Such negligence is potentially disastrous. Board members should, at a minimum, receive quarterly updates on data security – and more frequently if something material changes – from an informed, qualified C-level executive who is fluent and knowledgeable about cyber issues.

"Many companies think it's sufficient to have a well-funded information technology department, or even someone considered an expert in charge of cybersecurity," says McCreary. "But not every IT department, regardless of the size of its budget, is equipped to manage table-top risk exercises, sophisticated software and other aspects of breach prevention and response. Likewise, not every alleged expert is a veteran IT executive with a comprehensive understanding of how to truly safeguard the company's data and systems."

EXECUTIVE SUMMARY

"One slip is all that is needed to become vulnerable."

Indeed, in their responses and interviews, many survey respondents reported that they had appointed a C-level executive – often the chief information officer – to oversee data security, and most said they dedicate up to 10 percent of their IT budgets to cybersecurity. But those efforts may amount to little more than checking off boxes on a list if the individuals lack the credentials and skill sets to perform in these roles. In our experience, many CIOs do not possess, nor have they developed, the cybersecurity expertise required to defend against and respond to breaches.

And rather than a ceiling, 10 percent should be the starting point for an IT budget dedicated to security because even seasoned experts need the proper team and tools to build an adequate cybersecurity bulwark. "We have a lean team on cyber, and that's because our budget is lean," one respondent complained. "We know it's a risk."

"With the exception of a year with a major hardware or software upgrade, 10 percent of an IT budget dedicated to system security strikes me as a bare minimum," says McCreary. "There are so many efforts and strategies that can and should go into data loss prevention that can easily exceed 10 percent of an organization's IT budget."

Other executives, the survey revealed, are startlingly uninformed about the value of their companies' data. One respondent stated: "We don't have much worth stealing."

In reality, every business – no matter the industry – possesses valuable data. This common misperception can lead to devastating consequences. Hackers don't necessarily target organizations for a particular type of data. Cyber criminals cast expansive nets that probe for vulnerabilities and weaknesses. It is quite common for a cyber criminal to be dealing with a victim company and have no idea of the size or sophistication of the company. These criminals are adept at converting nearly any proprietary data into cash, either by selling it on the black market or demanding ransom.

A successful attack can hold a company hostage, severely disrupting operations and doing lasting damage to public trust. When businesses are brought to their knees because their computer systems are disabled, they will pay.

Companies at a particularly high level of cybersecurity risk are those that collect sensitive data involving personal or financial information. Health care businesses across the board – not just large hospital systems or doctors' groups – are acutely vulnerable.

"Hackers target even small physician practices and other similarly sized organizations," says Litten. "The reaction is often 'Why us?' and the answer is simply that they have either data the hackers want – such as health information or financial information – or data the hackers know is essential to conduct the company's business. Hackers steal and sell data, or encrypt it and extort ransom payments in return for decryption. Cybersecurity preparedness is essential for every organization, no matter its size."

Keep reading for key highlights and analysis from Fox Rothschild's 2018 report "Cyber Threats: Measuring Awareness, Assessing Preparation."

KEY FINDINGS

UNDERSTANDING THE SOURCE AND IMPACT OF DATA AND PRIVACY BREACHES

- At 71 percent, external hacks are the chief source of concern among respondents. This closely paces the 75 percent who indicated they have been targeted by a phishing attack in the last five years. "Everyone is at risk," one survey respondent said. "We are part of everyone."
- Business interruption is the most significant impact of a breach noted by respondents. However, many seemed to underappreciate the risk and potential threats posed by state-sponsored attacks from a foreign entity.

A TELLING BLIND SPOT: EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

- While half of survey participants noted they share data across borders, only 44 percent said their companies will be in compliance with the European Union's General Data Protection Regulation (GDPR) when it takes effect on May 25, 2018.
- Many U.S. companies do not grasp the true reach of GDPR, even those that consider themselves informed and prepared for its implementation. "There are executives who don't realize or fully appreciate how their businesses will be impacted by GDPR," says Litten. "They don't fathom the severity of the financial penalties for noncompliance and are inadvertently leaving their companies open to substantial risk as a result of that ignorance."

TRAINING ENOUGH PEOPLE OFTEN ENOUGH

- Although 68 percent of respondents train their employees on cybersecurity issues – an encouraging sign – only 14 percent reported that they train directors. An aware and informed staff is viewed by 46 percent as boosting a company's privacy efforts, but 52 percent perceive executive and board awareness as more critical. "Potentially anyone, from executives to staff, can click on a phishing email," says McCreary.
- Annual training is adequate only if it includes an element of periodic testing. Companies that conduct regular training believe the risk of a breach justifies the productivity lost from time spent on employee training. Statistics show rank-and-file employees inadvertently cause most data breaches and security weaknesses and thus are most in need of regular training and periodic testing to ensure the training is effective.

KEY FINDINGS

CYBERSECURITY INSURANCE IS POPULAR, BUT POORLY UNDERSTOOD

- A full 70 percent of respondents carry cyber liability insurance, and nearly four out of five in that group have never filed a claim. The percentage of those who report having this insurance is significantly higher than in other surveys. This could reflect a high degree of sophistication among this audience, but it might also indicate that some respondents incorrectly assume cyber matters are covered under other existing commercial policies, such as directors' and officers' liability insurance and errors and omissions insurance.

- More than half of survey respondents worked with a broker to obtain a policy. Advisers can assist in a variety of ways, by ensuring that employee error isn't excluded from coverage, that sublimits will cover potential fines and that companies know which costs related to business interruption will be covered. "Working with a broker or with legal counsel ensures that you have a much more effective policy in place – one that will offer broader and better coverage for your company's needs," McCreary says.

- In one interview, a software firm's general counsel volunteered that his company had recently filed an insurance claim on a relatively minor breach as a way to test the limits of the policy and the insurer's approach to breach claims. "It's unknown territory," he said. "We figured there's only one way to find out how strong our policy really is."

SPEND ON THE RIGHT THINGS

- Most companies are not spending enough of their IT budget on cybersecurity and data privacy programs. Two-thirds of companies reported spending 10 percent or less of their IT budgets on cyber programs. More alarming is the fact that about half of the respondents (47 percent) believe that their budget is sufficient to adequately manage a breach response.

- That's particularly shocking given that the average cost of a data breach is about $6 million.

- "I believe the resources being put into waging cyberattacks are greater than the resources put against attacks," a survey participant emphasized. "My greatest concern is complacency."

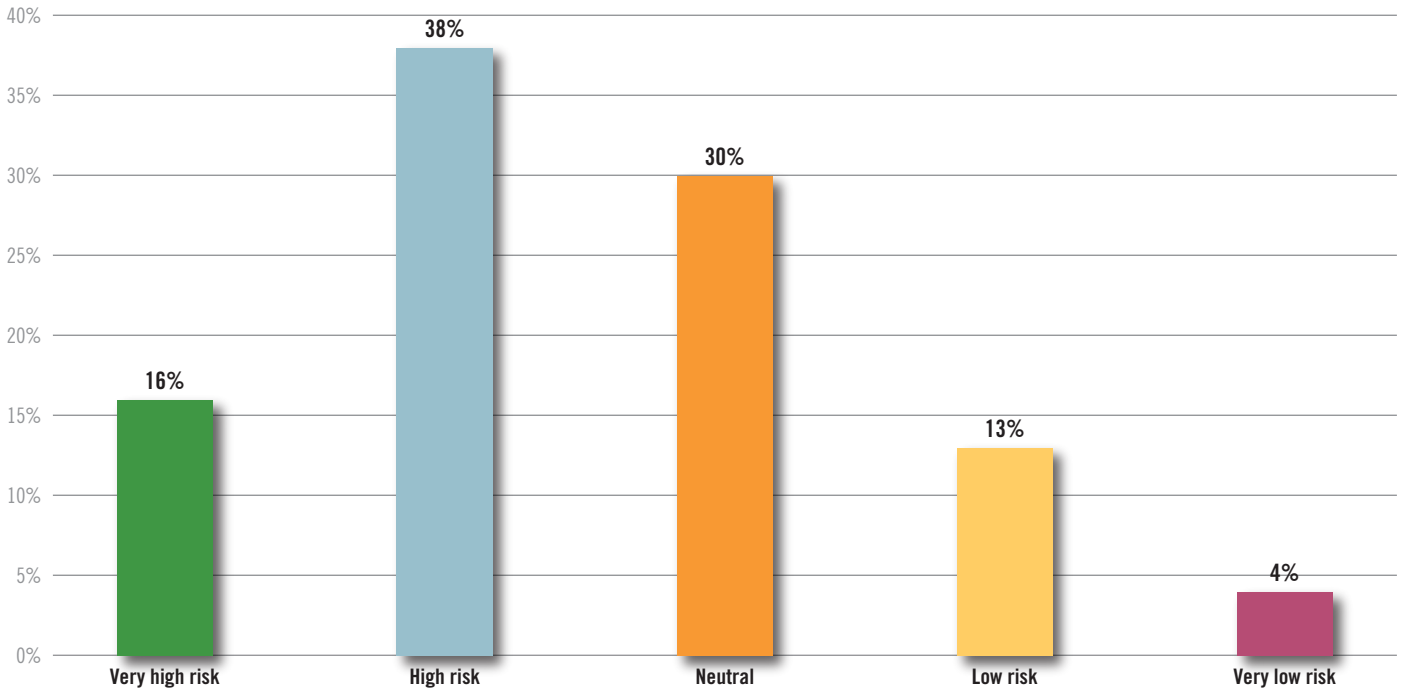
- "With the exception of a year with a major hardware or software upgrade, 10 percent of an IT budget dedicated to system security strikes me as a bare minimum," says McCreary.

Percentages in certain questions exceed 100 percent because respondents were asked to check all that apply. Due to rounding, percentages used in some questions may not add up to 100 percent.

FULL RESULTS

RISKS – UNDERSTOOD AND OTHERWISE

What do you perceive as the current level of risk for your company's cybersecurity and data privacy environment?



"The size of the business and the type of data it keeps – or doesn't keep – can offer a false sense of comfort," says Litten. "We cannot stress enough that everyone is at risk."

Companies appear evenly split over whether they perceive themselves as high risk for cybersecurity and data privacy threats or not. Nearly a fifth view their risk as low or very low. Some respondents indicated that because they don't retain customer data, they believe their breach risk is significantly lower. In verbatim comments and interviews, many said they felt safer because they aren't the kind of consumer brands whose breaches have made headlines, while others saw themselves as too small to target.

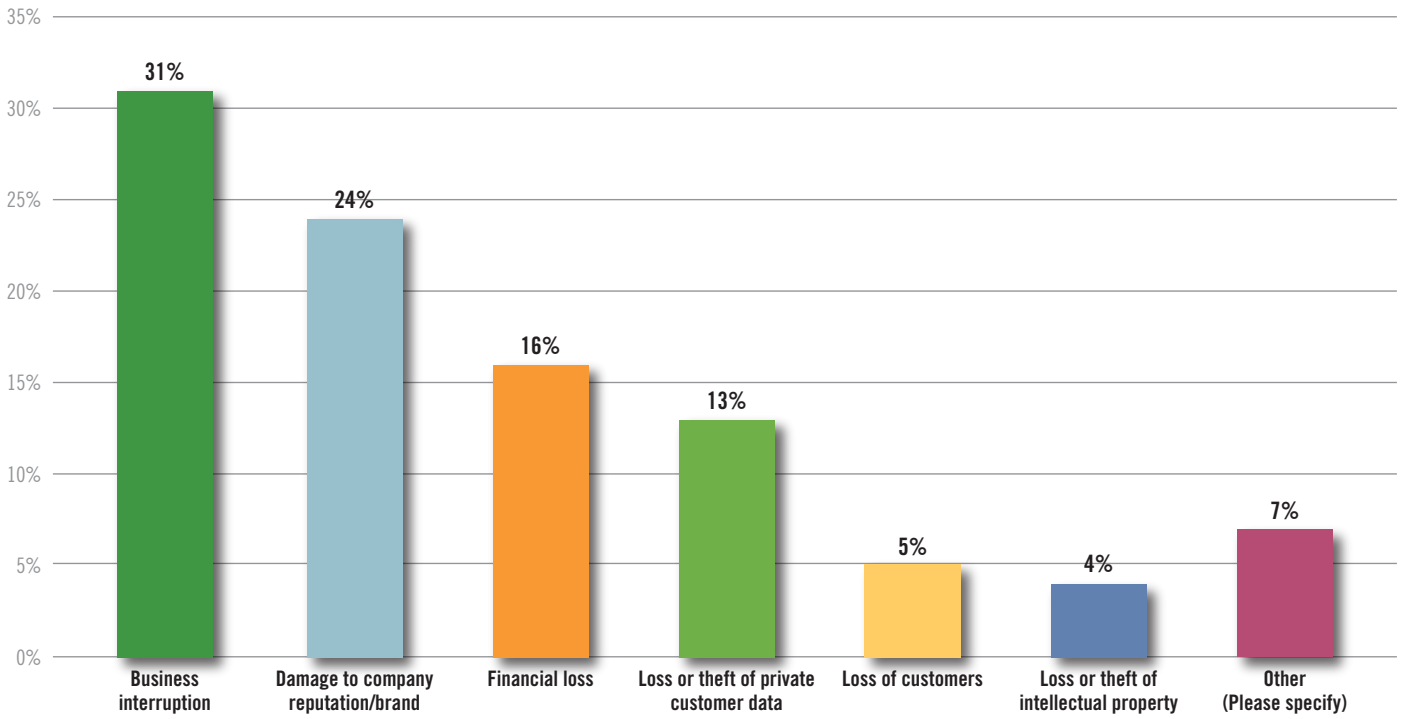
"I think we're toward the lower end in terms of risk, just because of the nature and profile of our business," explained the head of the legal department for a global manufacturing company. "We're not a sexy target to hack if someone is looking to do damage. We're not a big name; we're not a household name at all."

These are perilous assumptions.

"The size of the business and the type of data it keeps – or doesn't keep – can offer a false sense of comfort," says Litten. "We cannot stress enough that everyone is at risk."

Among the combined 54 percent who regard their risk as high or very high, sentiments focused on the ubiquity of attacks and breaches: "That's the reality today," one

With what impact of the foregoing risks are you most concerned?



respondent said. Another noted, "It's becoming too easy for individual bad guys to make a run at a company's network."

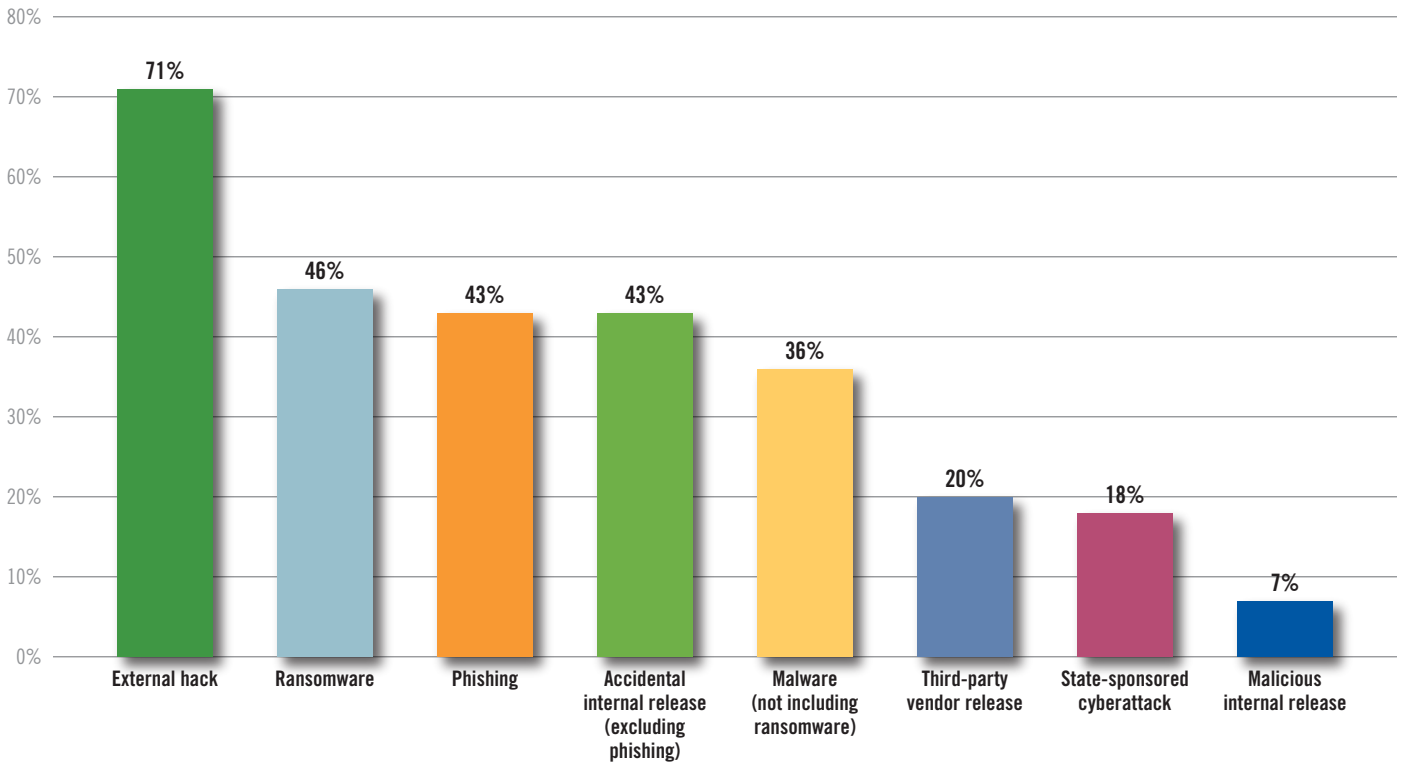
Regarding the impact on a company following a breach, respondents noted their top two concerns were business interruption and reputational damage, at 31 percent and 24 percent, respectively.

Among respondents, CEOs were the most concerned with business interruption, while CIOs were more likely to consider loss or theft of data most worrisome and legal officers were preponderantly concerned with reputational damage.

The focus on business interruption is well-placed. A significant breach, such as a ransomware attack, has the potential to bring all business activity to an immediate and potentially devastating halt. And even a small cyberattack can interrupt the normal flow of operations and business.

Financial loss was a principal concern for 16 percent of those surveyed. And while 13 percent expressed worry over the loss of customer data, only 5 percent viewed loss of customers as having a significant impact. Four percent feared the loss or theft of their intellectual property in an attack.

What do you believe are your company's biggest cybersecurity and data privacy risks?



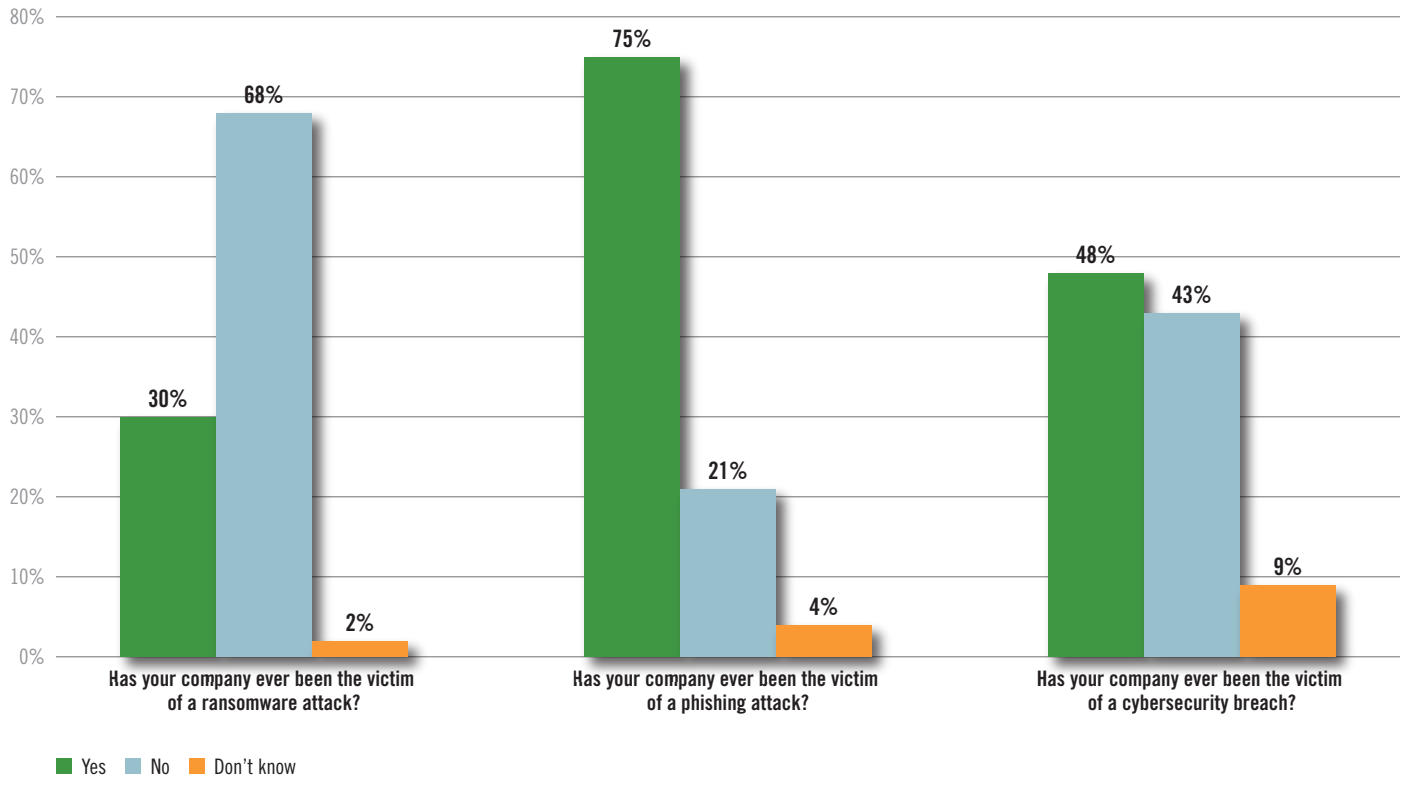
Executives are predominantly concerned with the threat posed by an external hack. However, the risk of a foreign state-sponsored cyberattack is underappreciated, as only 18 percent of survey participants identified it as a major concern. Executives must be mindful that politically active employees and high-profile customers are attractive and lucrative targets for foreign governments.

"The nation-state threat is so much greater a risk than people think," says McCreary. "This goes far beyond discussions of political elections that may or may not have been influenced. Certain foreign governments are engaging in cyber conduct that poses significant risks for many businesses. The vulnerability of companies to these threats should not be underestimated."

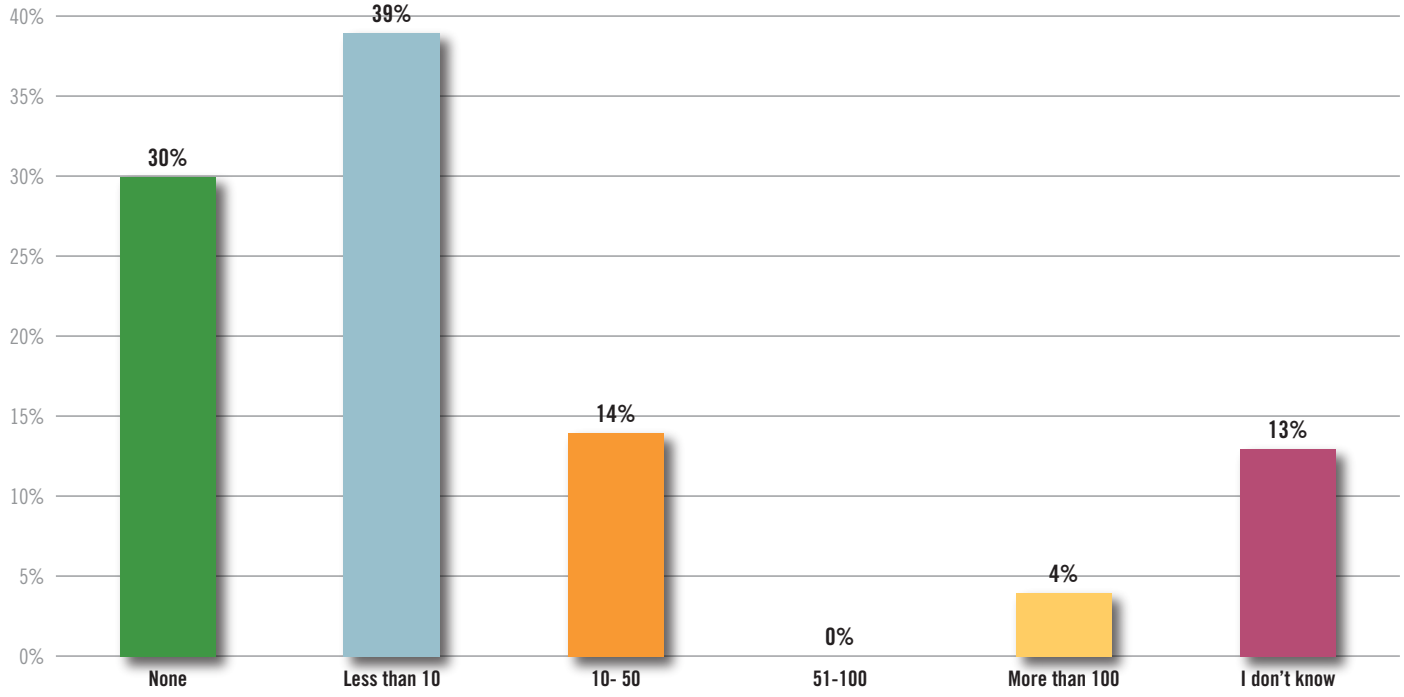
Ransomware was viewed by 46 percent of respondents as the biggest risk. Third-party vendor release and malicious internal release alarmed only 20 percent and 7 percent, respectively.

"Ransomware is the one we're concerned about," noted the CEO of a tech transfer company. "I'm not sure if it's real for us or not, but because it's so unknown, it's the one I fear."

Within the past five years, please indicate “Yes,” “No” or “Don’t know” for the following:

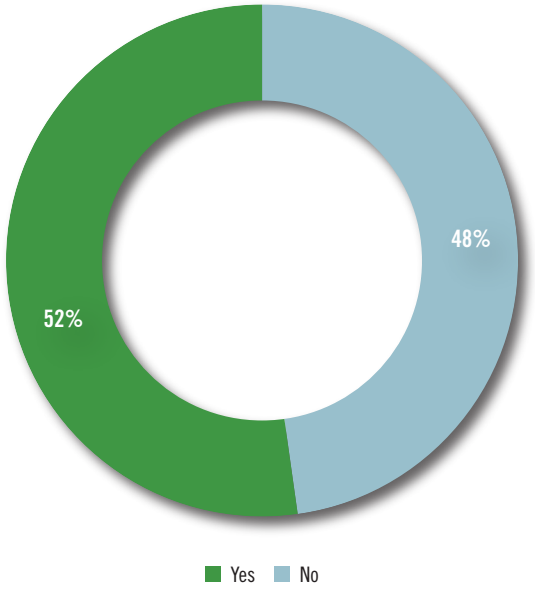


How many security breaches, about which you are aware, has your company been the victim of in the past twelve months?

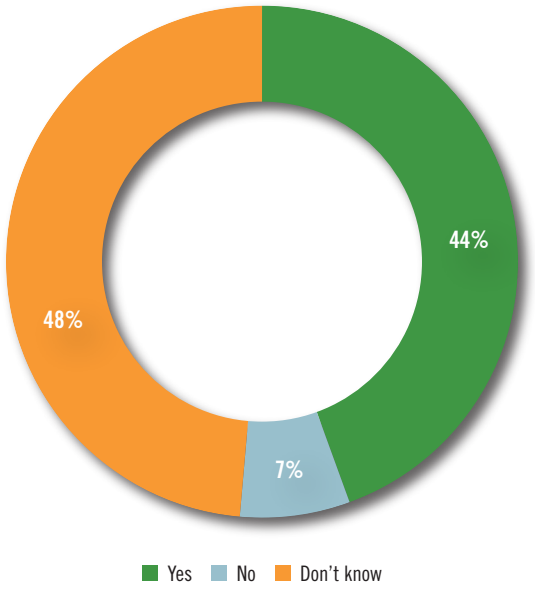


DATA ACROSS BORDERS

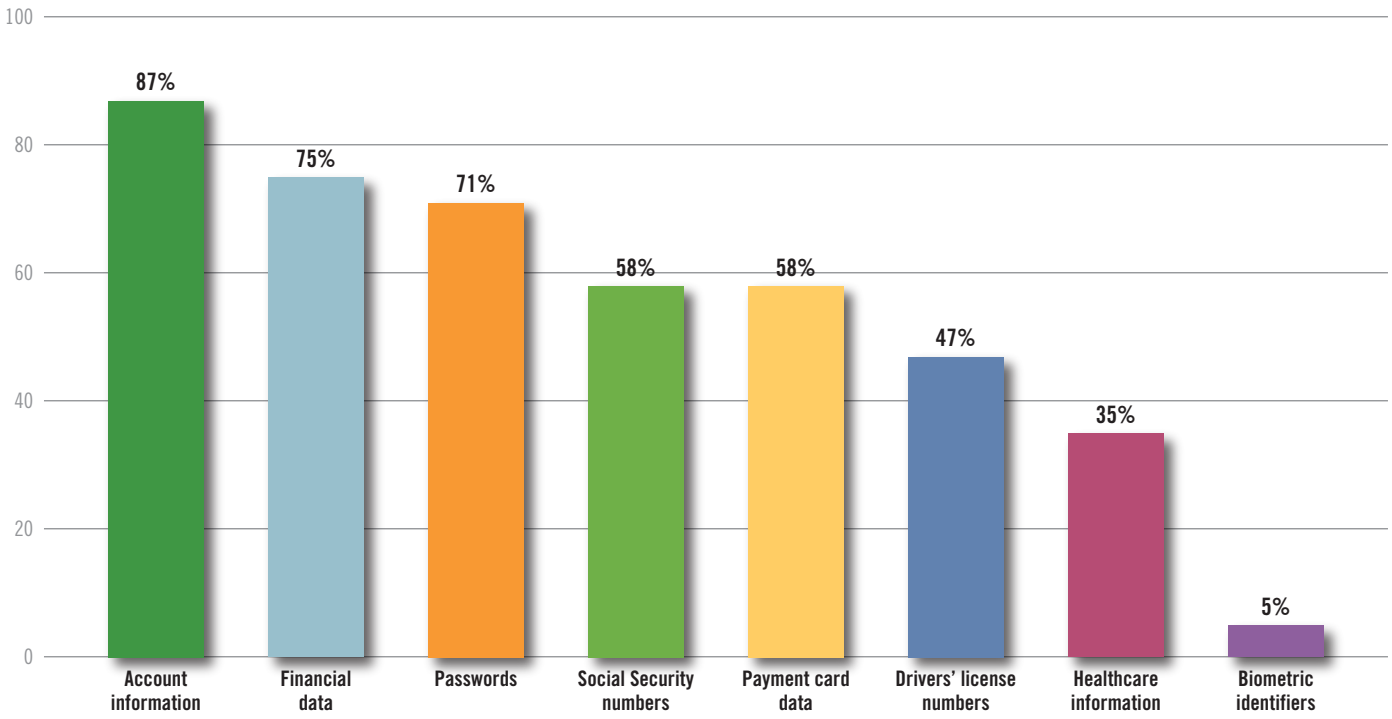
Do you share data across country borders within your company or with distributors, third-party suppliers or other partners?



Will your company be in compliance with the European Union's General Data Protection Regulation (GDPR) by May 25, 2018?



Please indicate all of the types of data that your company collects and stores.



More than half of respondents collect and store at least five types of customer data, including account information (87 percent), Social Security numbers (58 percent) and payment card data (58 percent). Less than half retain drivers' license numbers and health care information, and just 5 percent gather biometric identifiers.

While half of survey participants confirmed they share data across borders, only 44 percent expressed confidence that they would be in compliance with GDPR – the European Union's General Data Protection Regulation – by the May 25 deadline. These new regulations carry penalties for violations as high as 20 percent of a company's global revenue.

"Many businesses don't realize the scope of GDPR and how they will be impacted by it," says Litten. "They simply haven't wrapped their minds around it yet, and with the May 25, 2018, compliance deadline looming, they are inadvertently putting their companies at considerable risk. The financial penalties for noncompliance are truly steep."

Anecdotally, professionals on the front lines of GDPR compliance are discovering that companies do not understand the regime's reach.

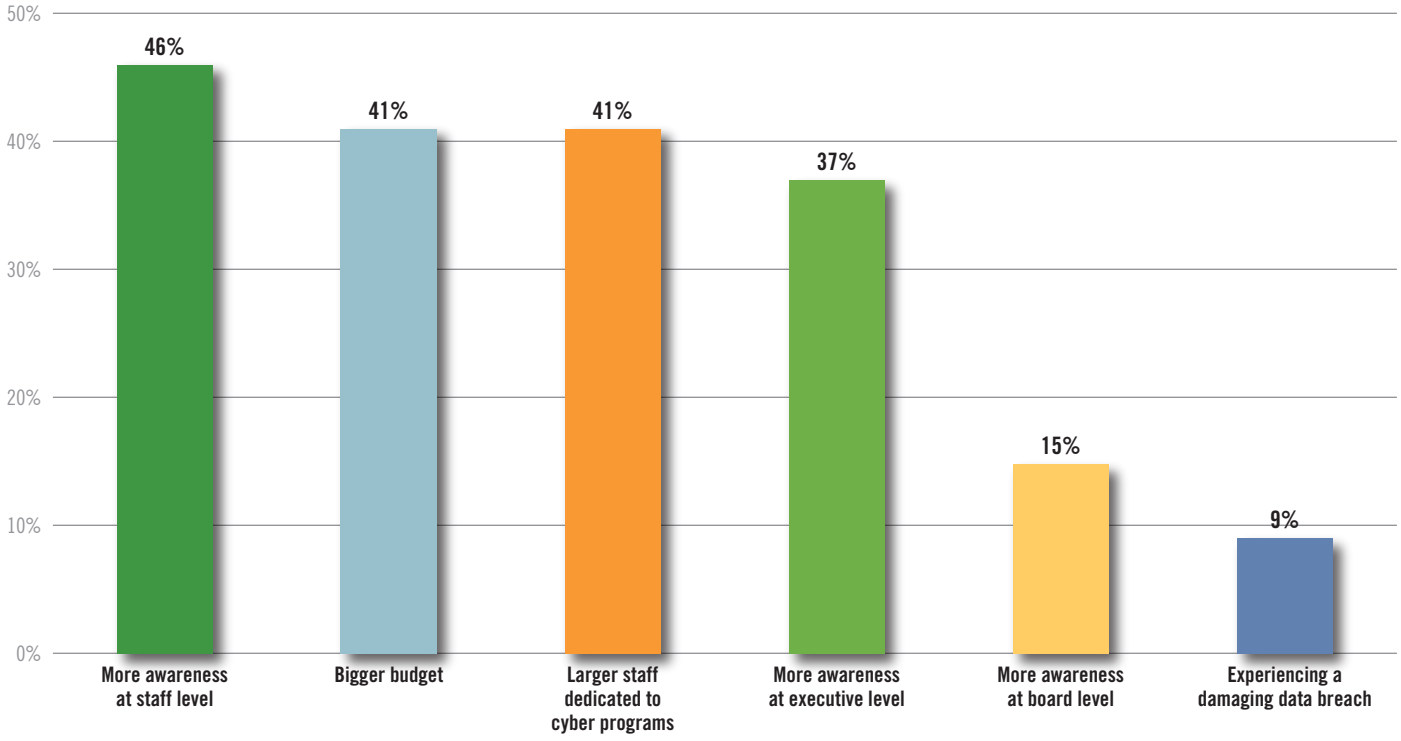
"When we explain to clients that you must comply with GDPR whenever you provide services to a third party that is subject to GDPR, we see a lot of wide eyes," says McCreary. "That is often the first moment they truly grasp that they have a GDPR problem they need to remedy."

The problem may also stem from not understanding what types of data are covered.

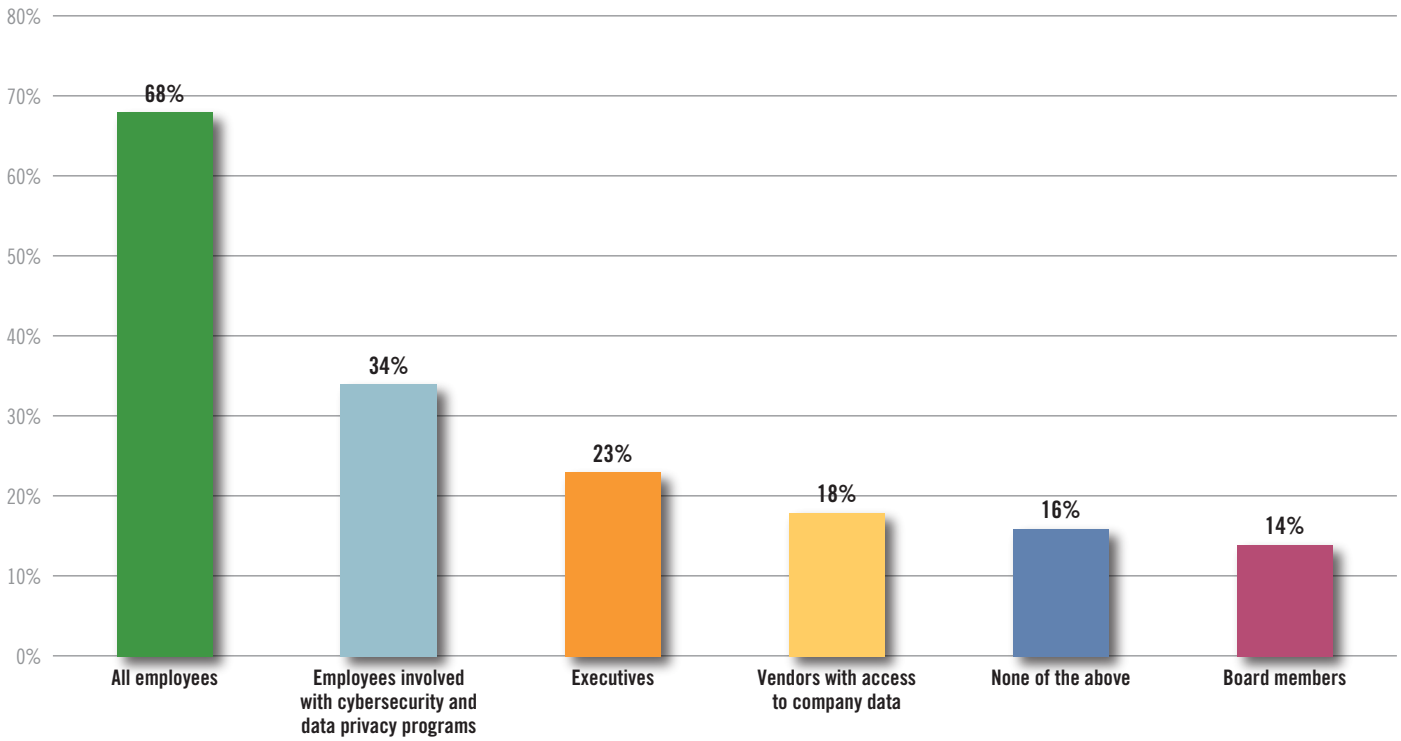
"GDPR is astonishingly broad. It applies to basic personal information, not just sensitive data," McCreary says. "A key provision allows customers to compel companies to delete their personal data, which is an extremely complicated task because you cannot simply delete information anymore. Data is tenacious. It's sitting in backups, in emails, in a host of other places."

STILL STRUGGLING WITH TRAINING

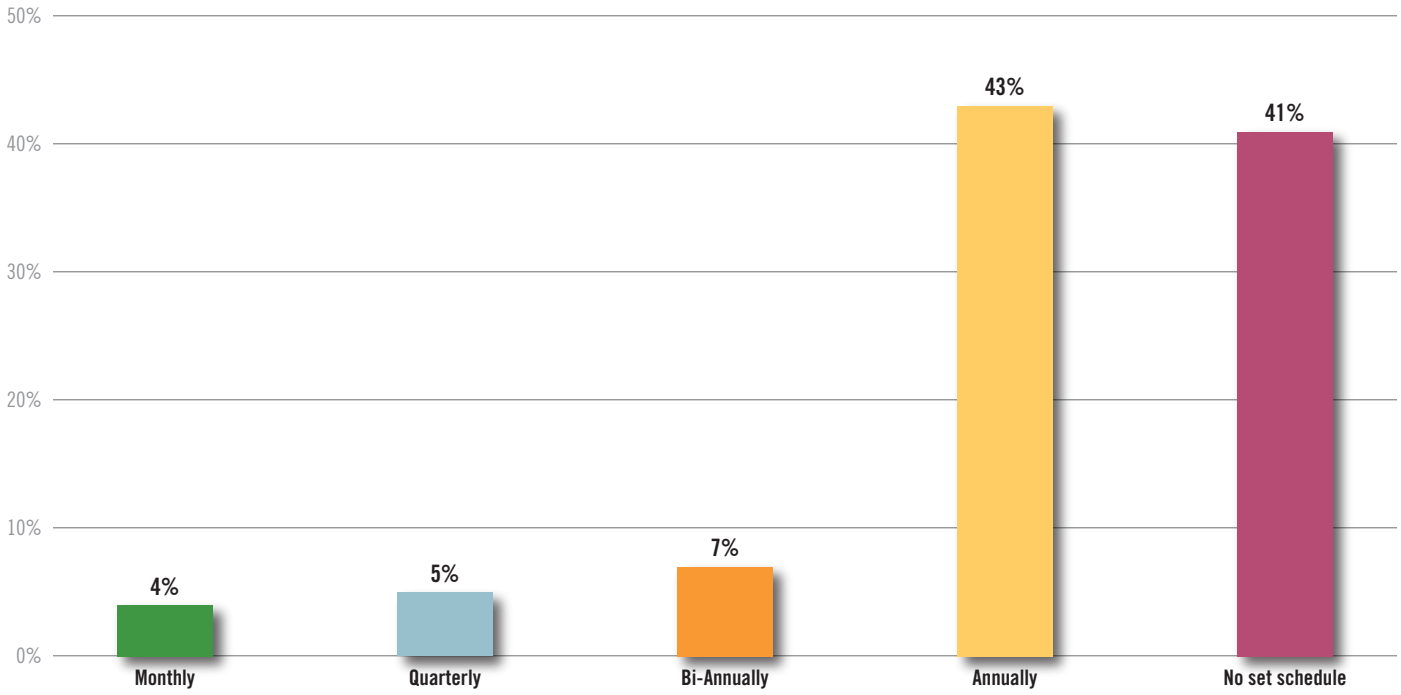
What do you believe would help make your company's cybersecurity and data privacy program stronger/more secure?



To what group(s) does your company provide cybersecurity and data privacy training?



How often do you provide formal training to staff on cybersecurity and data privacy programs?



When asked what factors would strengthen their company's data privacy program, 46 percent of respondents pointed to an increased level of staff awareness on cybersecurity risks – in a word, training.

"Too many people take computers for granted; they don't think about, or understand, the significance of the different ways they use these devices," revealed a survey respondent.

A slightly lower number of participants – 41 percent – indicated that a larger budget and more staff dedicated to cybersecurity would strengthen their initiatives.

Other responses were widely varied, with respondents looking for better products from information technology vendors, increased cooperation among corporate officers tasked with information and security or more and diversified training.

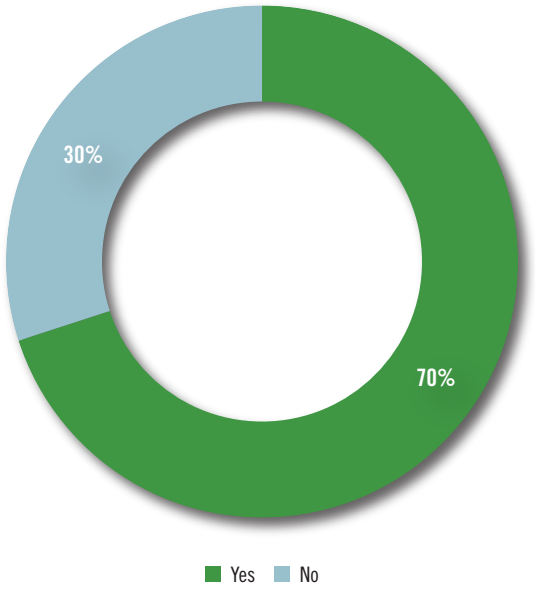
Interestingly, almost a quarter of participants noted they train only their executives on privacy. Cybersecurity professionals noted that while executives may appear to be at a higher risk for targeting, any employee can compromise the entire company's security.

"All it takes is one person to click on one email link, and the hackers have made their way into your system," McCreary says. "Nearly every data breach that winds up as front-page news involved the compromise of a privileged account, and more often than not, it can be traced back to a single phishing email."

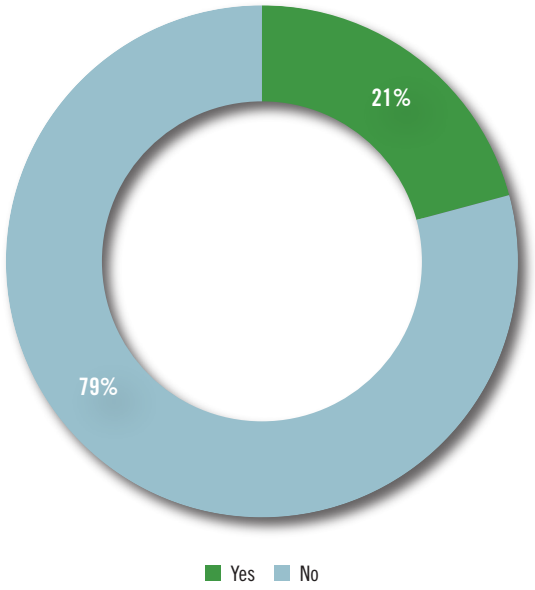
Annual training is marginally adequate, but only if it is accompanied by periodic and random testing to determine the efficacy of the training. Notably, companies that engage in the most regular training – two to four times per year – are the ones that truly understand that the risk of a breach offsets the lost productivity due to staff time spent in training.

INSURANCE IN PLACE – BUT DETAILS FOGGY

Do you have cyber liability insurance?

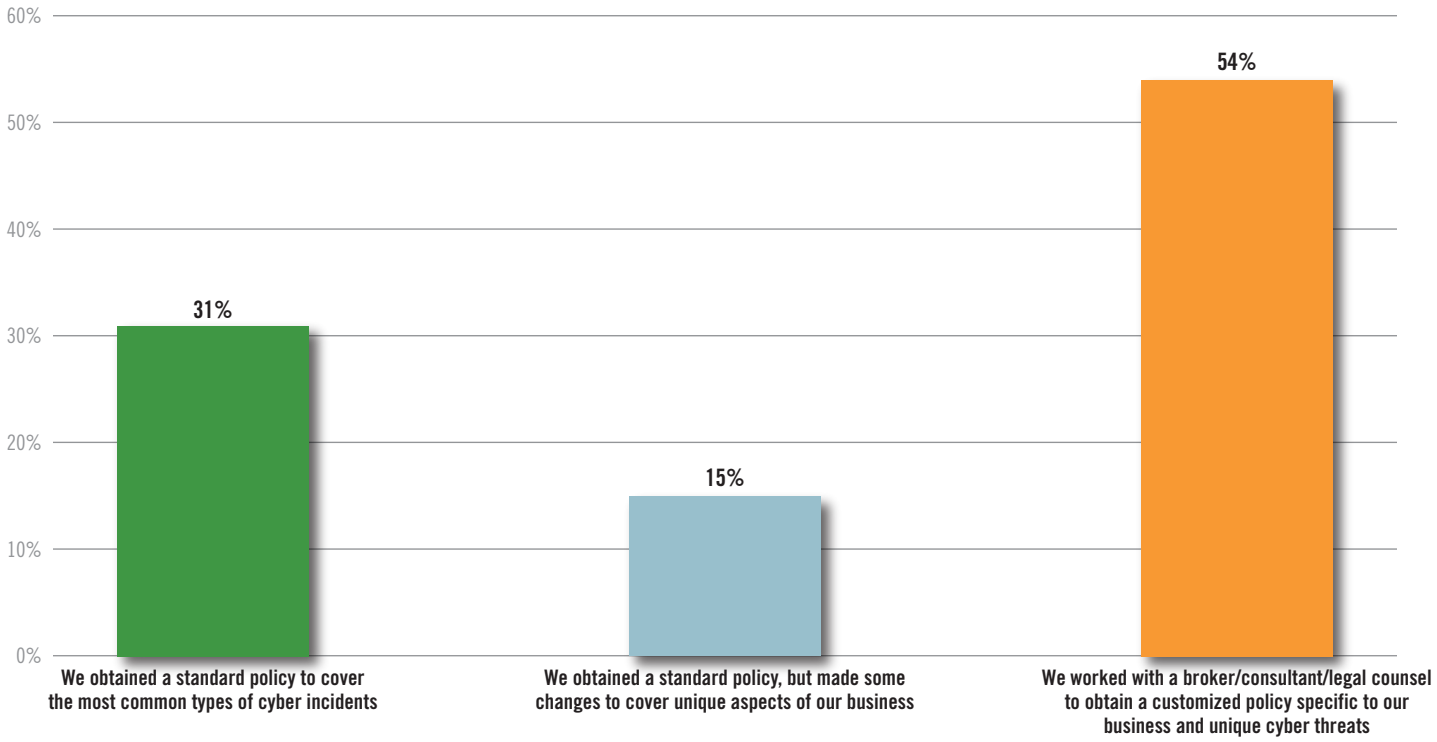


Within the past five years, have you filed a claim?



A majority of survey participants (70 percent) stated they have cyber liability insurance coverage. However, only 21 percent reported filing a claim within the last five years.

Which of the following best describes how you acquired your cyber liability insurance policy?



One survey participant learned the limitations of his company's policy the hard way when his first-ever cyber insurance claim was denied after an outage.

"When we got the policy, we talked to underwriters, we went through a broker," the tech executive explained. "Our claim was rejected and we're fighting them over that. We're using this as a test case of our broker."

Companies must be certain they have adequate coverage and that insurance policies match their specific needs. A typical directors' and officers' liability policy, for example, doesn't cover data or security breaches connected with cyberattacks. And even policies that do explicitly cover cyberattacks may have unanticipated limitations.

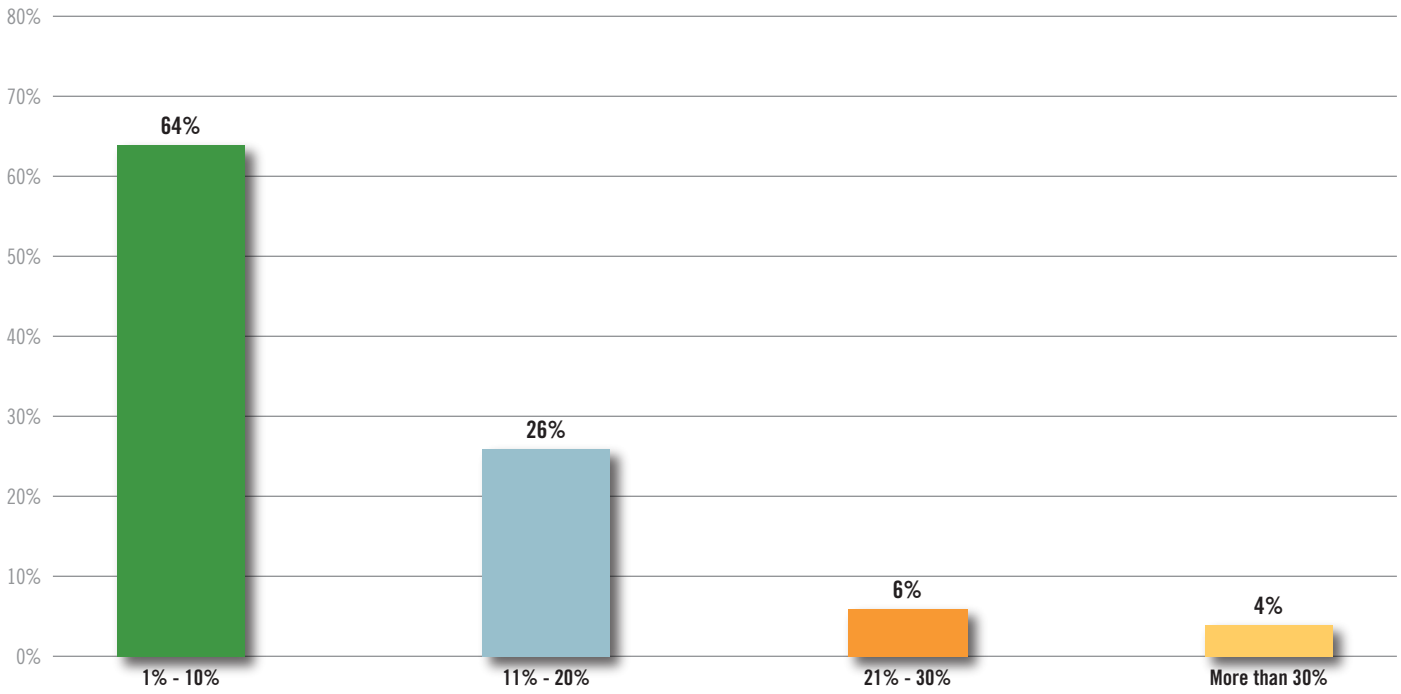
"Unfortunately, cyber insurance remains non-standardized," says Litten. "In the health care industry, for example, there are wildly different expectations of the levels of coverage needed under a cyber liability insurance policy, and there are significant variations in policy terms."

Working with a broker or other specialist can minimize a policy's potential shortcomings, such as excluding employee error, inadequate sublimits for fines or underestimating the full cost of a business interruption.

"An executive may think, 'We're secure; we have a cyber insurance policy.' But if they don't have the right coverage, they may find themselves in a world of trouble when a breach or other incident occurs," McCreary says. "By working with a broker or with legal counsel who can advise on insurance coverage, companies will have a true sense of security because they will have a more effective policy in place that is suited to their needs."

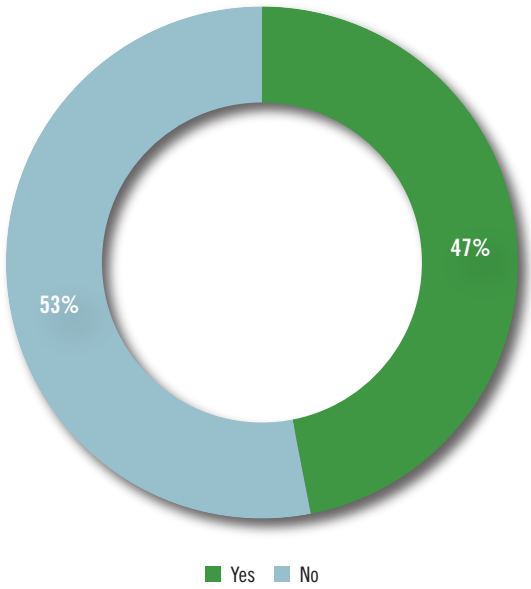
SECURITY QUESTIONS ON BUDGET AND STAFFING

What percentage of your company's IT budget is dedicated to cybersecurity and data privacy programs?

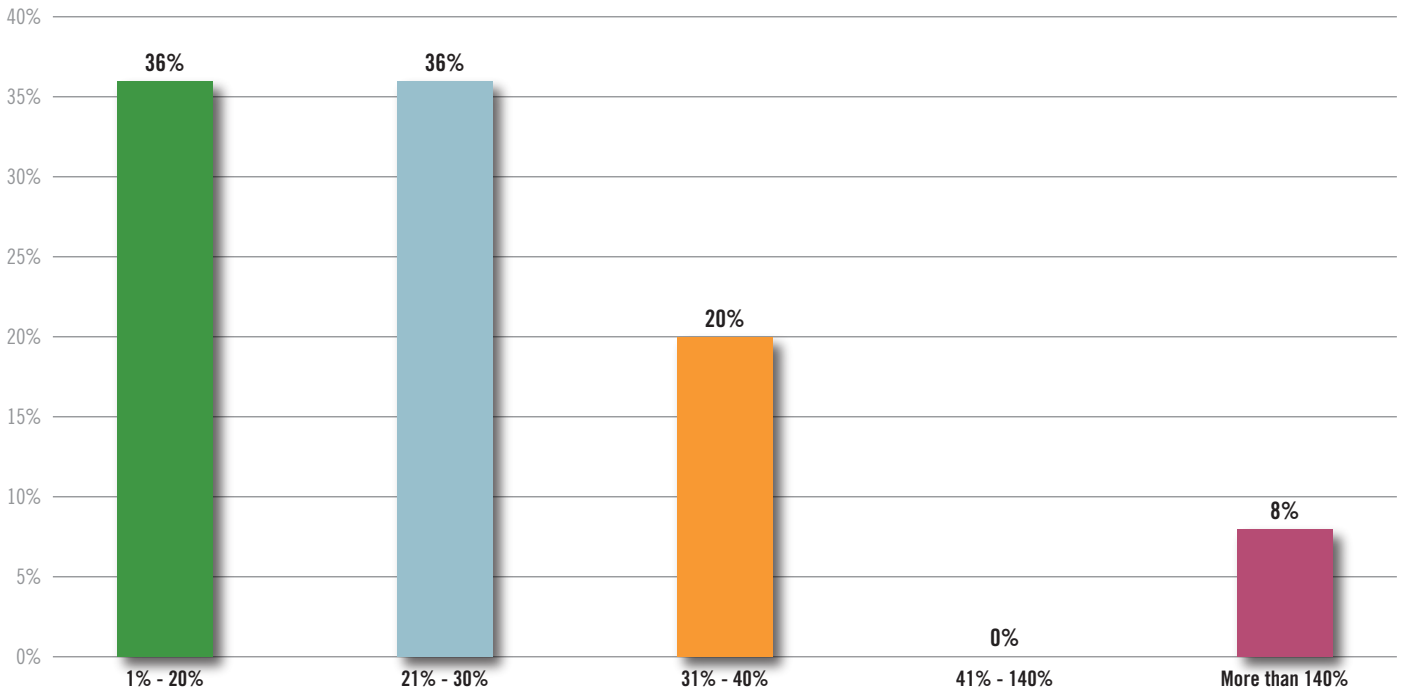


Only 36 percent of survey participants reported spending more than a tenth of their IT budgets on cybersecurity and data privacy, which is barely adequate, according to experts. A mere 4 percent of respondents dedicate more than 30 percent of their IT budgets to these efforts.

Do you believe that budget is sufficient to adequately manage a breach response?



How much more budget would be required to adequately protect your company?

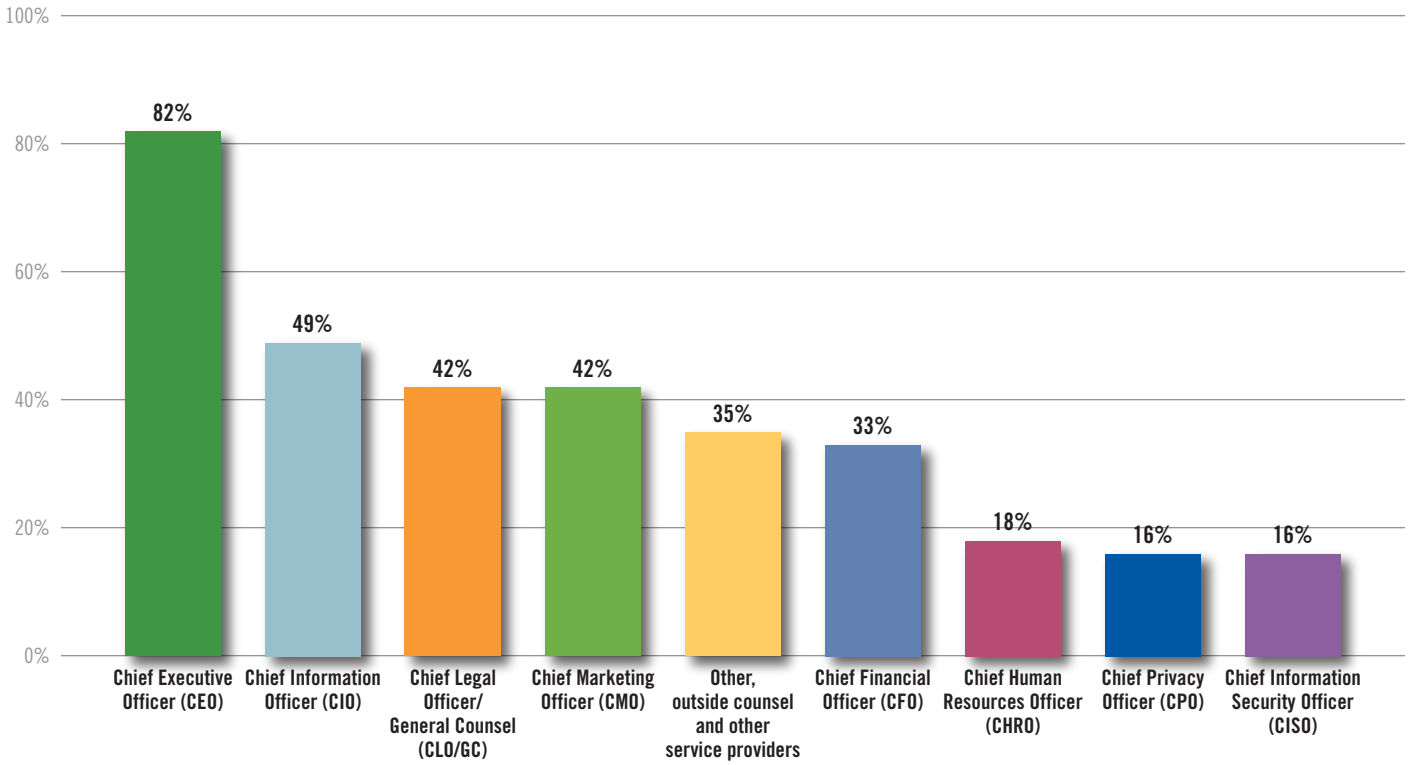


And yet a majority of respondents conceded that their budget – regardless of the level – is insufficient to respond to a breach. Eight percent reported they need a 140 percent or more boost. As for the 47 percent who believe their current spending to be at an appropriate level, a review of their allocations is critical to ensuring the funds are truly sufficient in the event of a breach.

Accounting factors complicate any analysis of the budget issue. Companies use a variety of methods to record IT spending on personnel, software and hardware, training and maintenance. So there cannot be a one-size-fits-all budget recommendation. It is imperative, however, that at least one staff member is dedicated to information security.

"If a company decides to house cybersecurity responsibilities solely with its CIO – who has countless other tasks to attend to – security is going to take a back seat to other matters," says McCreary. "Hire or appoint someone whose sole job focus is data privacy and cybersecurity. In this environment, it's critical for a business' IT team to have that individual."

In the event of a cybersecurity incident, please identify those involved in organizing the company's response.



In the event of a cybersecurity incident, 82 percent of respondents said the company would involve the CEO. A wide range of additional individuals would also be involved in the response process, including staff from the legal, marketing, finance, human resources, risk, compliance and information technology departments. More than a third (35 percent) of survey respondents indicated they would involve their outside legal counsel and other service providers in helping to organize the company's response. Companies must candidly assess whether their internal resources are adequate to respond to an incident and, when necessary, consider involving outside resources.

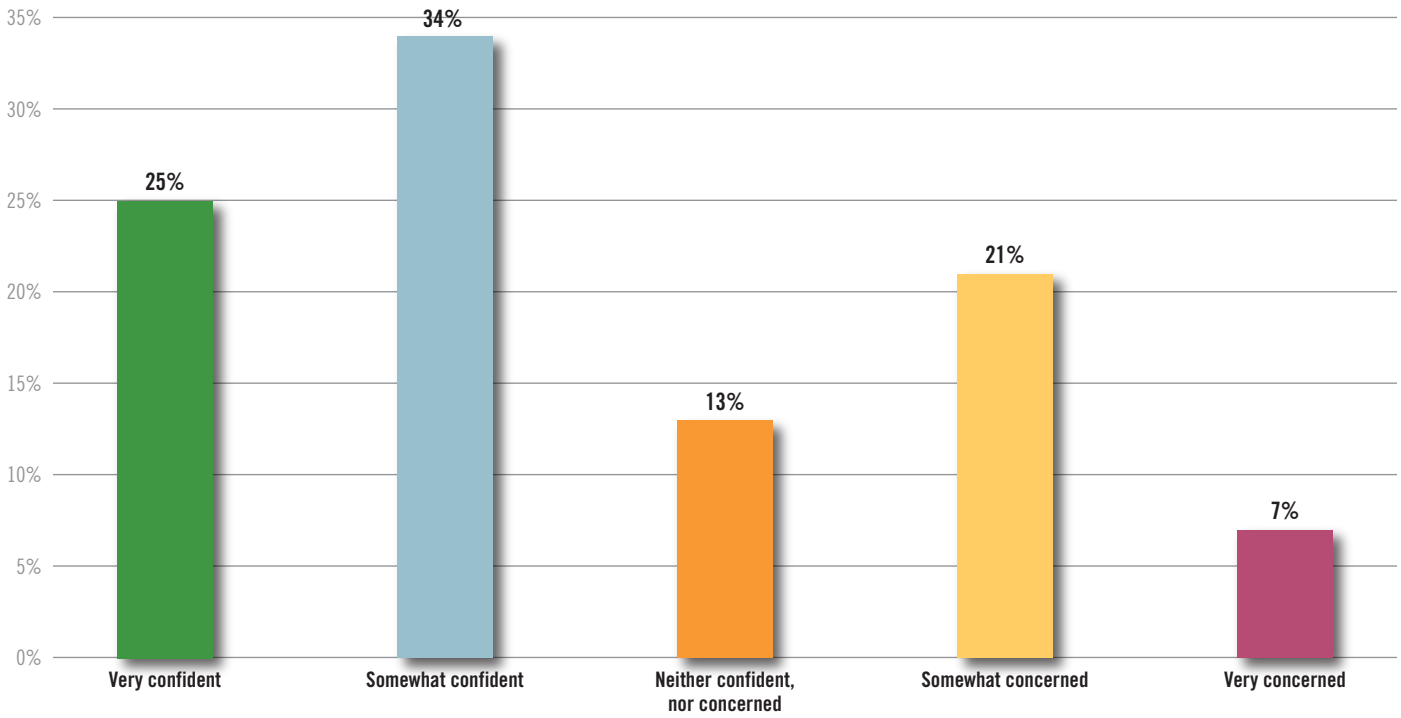
Some businesses have not even taken the step of making a plan for a cybersecurity incident response, despite the fact that most companies today have long since accepted the need to plan for other types of disasters.

"We don't have a formalized plan," acknowledged the CEO of a U.S.-based medical device research company. "We've got tornado, severe weather and electrical outage as well as all of these other plans, but not a cybersecurity one. We probably should have one."

They certainly should. Even an average-sized breach will be at least as costly as weather- or electricity-related disasters. And in addition to the financial harm a business suffers in the wake of a breach, it is also exposed to potentially devastating reputational damage. Customers and other stakeholders know that companies can't prevent natural disasters, but the fallout from cyberattacks is considered preventable.

POLICY AND GOVERNANCE LAGS

How confident are you in your company's cybersecurity and data privacy program?

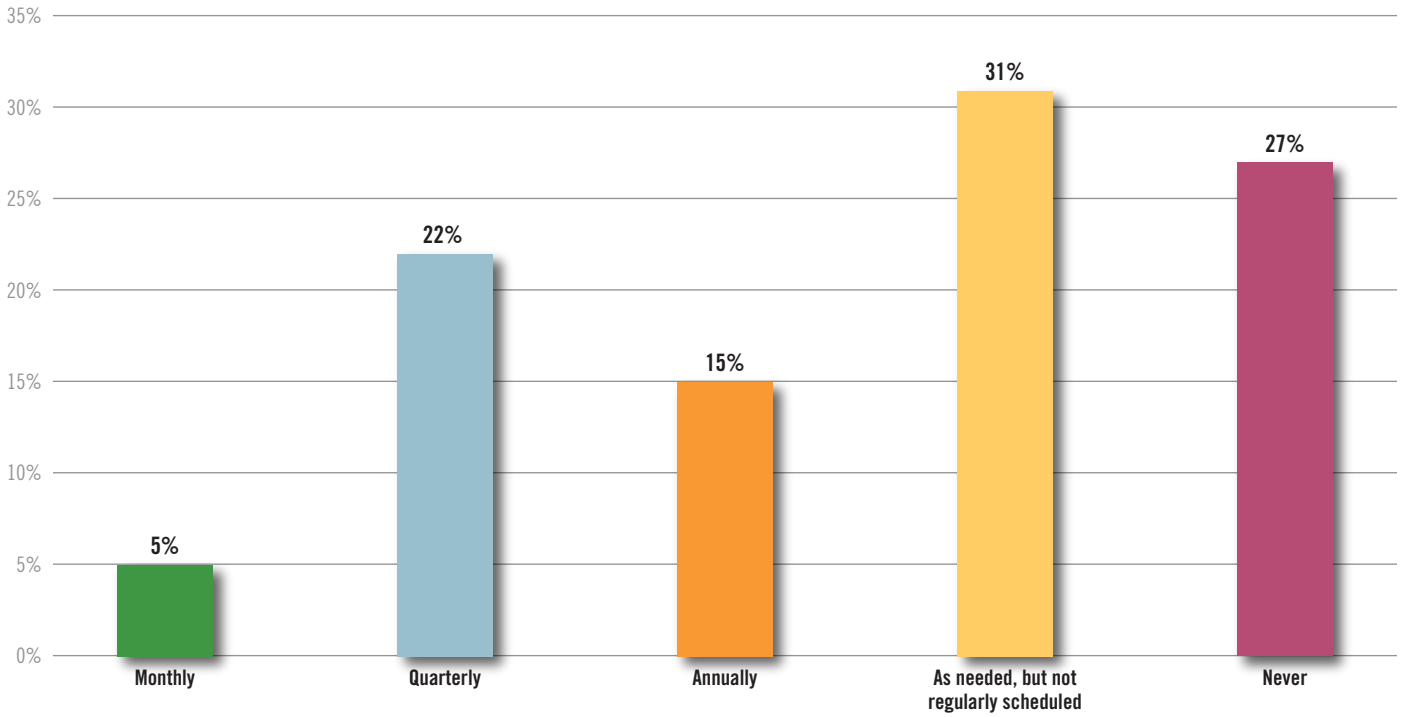


Most respondents indicated some level of confidence in their companies' cybersecurity and data privacy programs, including a quarter who are very confident and 34 percent who are somewhat confident.

Tellingly, when broken down by sector, those in health care expressed the highest level of concern and the lowest level of confidence.

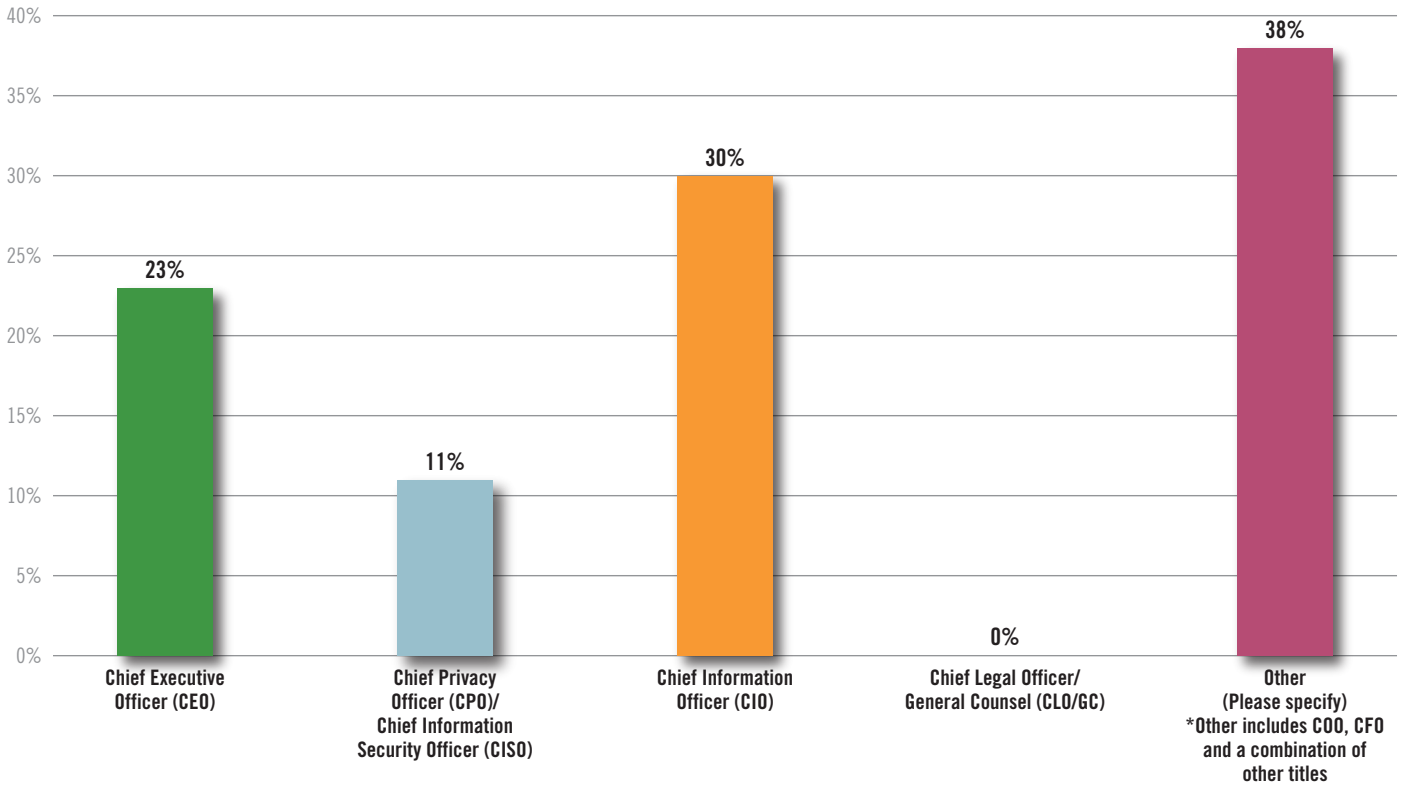
"In the health care industry, there is rampant and widespread fear over hacking," Litten says. "So many of them painfully recall May 2017, when the WannaCry attack hit, which was especially hard on hospitals and others in the health care industry. For U.S. health care entities subject to HIPAA, ransomware attacks that may involve protected health information, even those that merely encrypt data and do not appear to view, copy or take it, are presumed to be HIPAA breaches and will require expensive reporting and notice obligations unless the incident response demonstrates a low probability of compromise."

How often does your company's Board of Directors receive cybersecurity and data privacy program updates?



The survey revealed that a disturbing 27 percent of respondents never report to their directors on cybersecurity and data privacy. While company officers are mandated to notify directors in the event of a breach, the board members should also receive regular quarterly updates on data security.

Who is responsible for reporting cybersecurity and data privacy program updates to the Board of Directors?

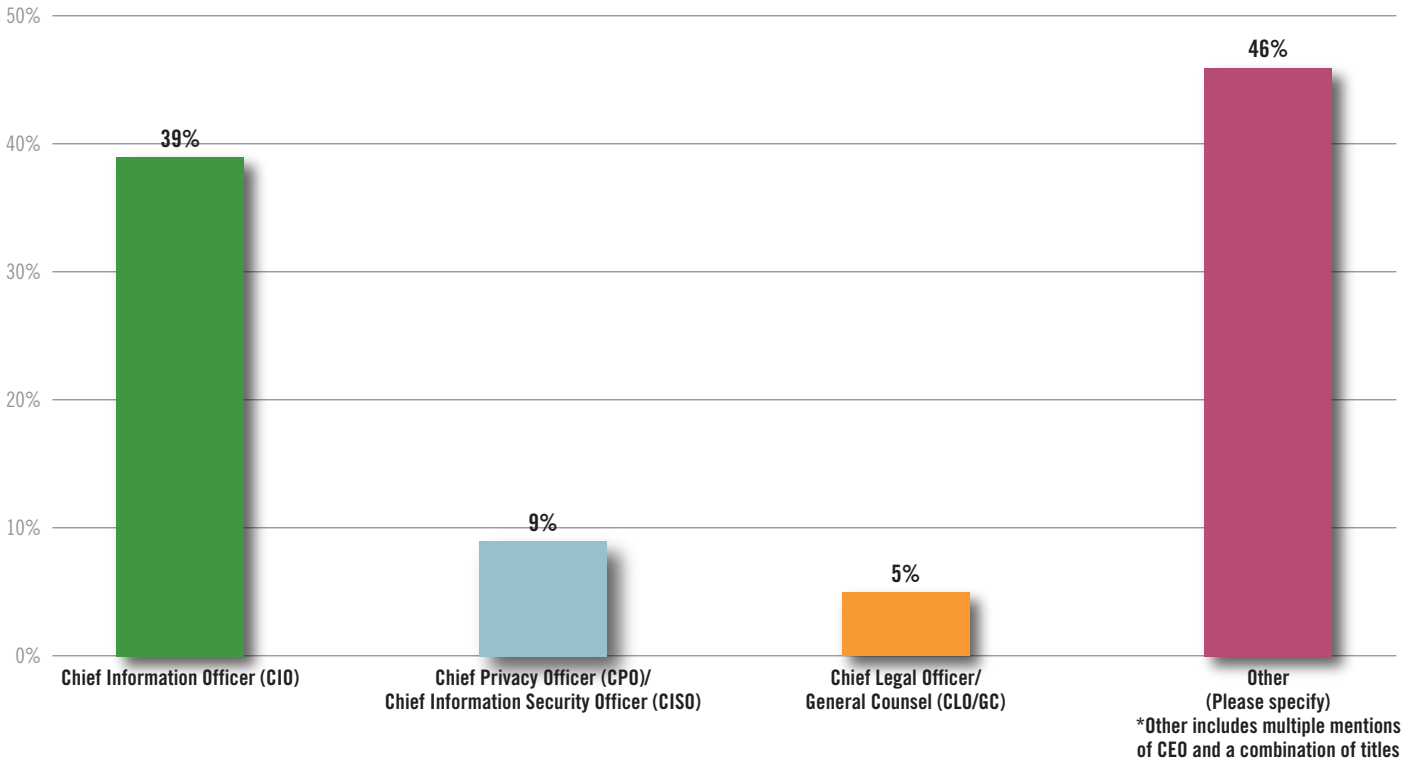


The responsibility to inform directors varies among company officers. Survey results indicated that no one officer role is predominantly tasked with this, although 30 percent reported assigning this duty to the chief information officer.

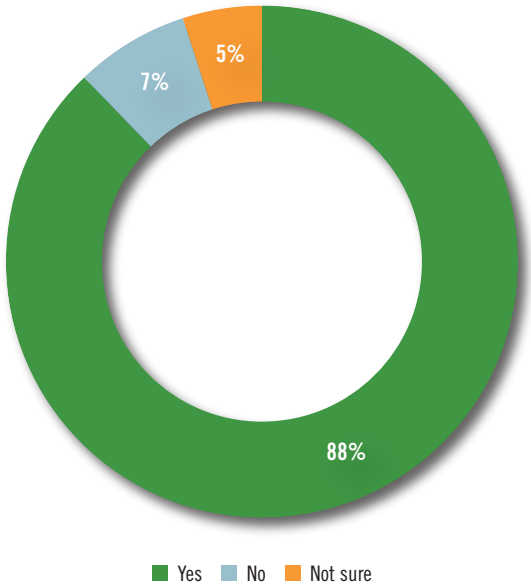
Cybersecurity professionals recommend that a chief technology, privacy or information security officer update the board. Whoever takes on the responsibility must be unquestioningly adept at explaining the threats to the business, providing options to address those threats and delivering all relevant messages to an audience who is likely to be neither well-versed in cybersecurity nor aware of the resources required to prevent or respond to an incident.

"For the board to function properly, it's essential to be confident that the right answers to the right questions are being delivered by the right person," McCreary says.

Who is responsible for developing your company's cybersecurity and data privacy program?

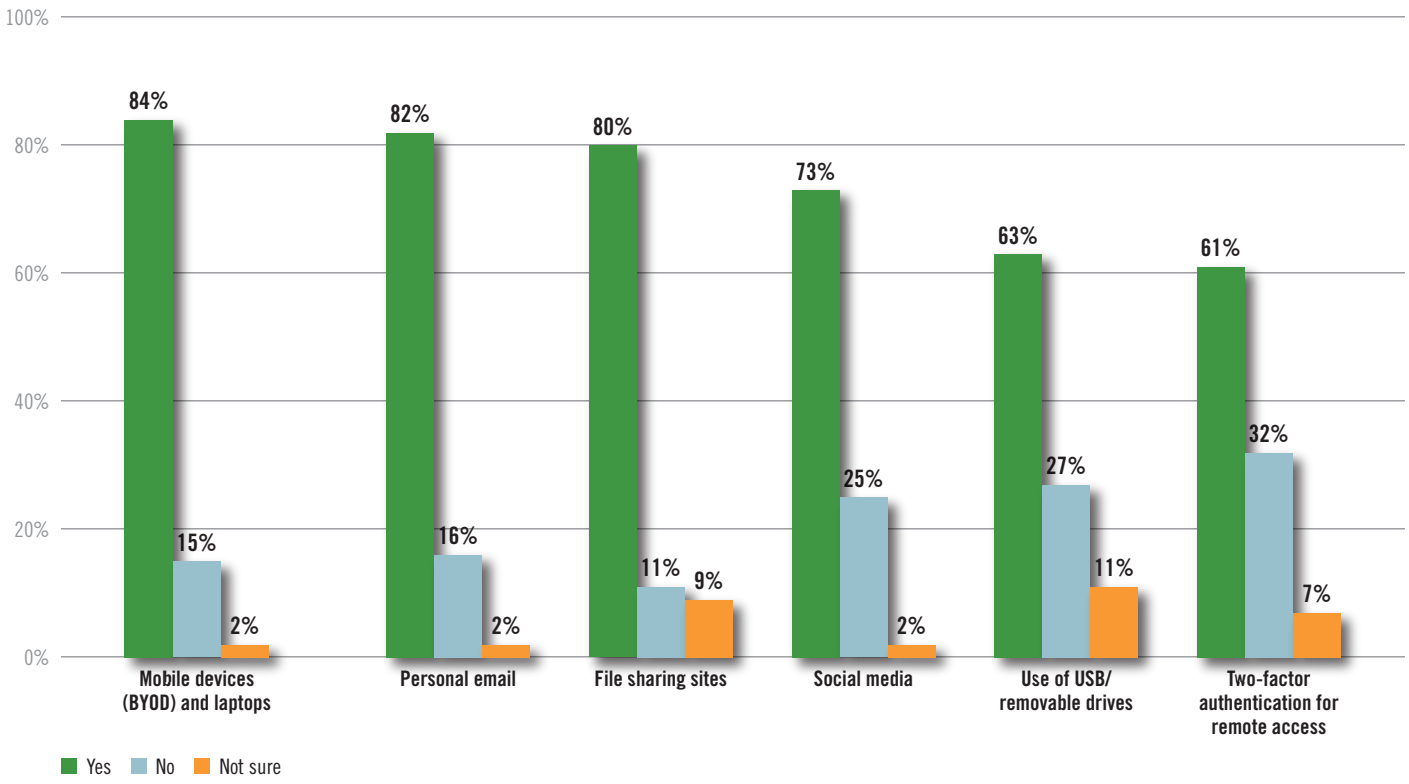


Do you have policies and procedures in place governing employees' handling of electronic data?



Thankfully, the message that policies pertaining to electronic data are critical for companies has been received: 88 percent of respondents have codified employees' handling of electronic data, including bring-your-own mobile phone and laptops, personal email, file sharing, social media, removable drives and two-factor authenticated remote access. Only 7 percent have no such policies in place, and 5 percent are unsure about whether anything exists for their business.

Do you have policies governing or restricting the following?



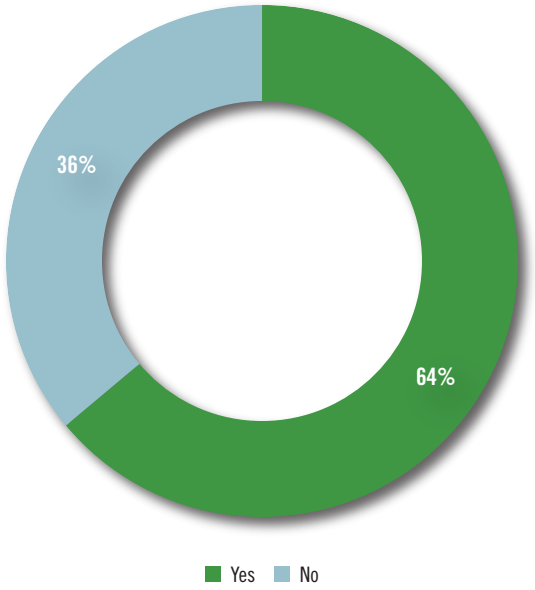
"We don't effectively address bring-your-own-device policies," said the general counsel of a San Francisco-based tech service company. "To do it well, you have to have the right to completely delete all the device's data. People would revolt."

Companies should assess and review their policies to determine if they adequately cover employee behavior, such as defining acceptable social media and personal email use. They should also ensure the policies explicitly address privacy and data use.

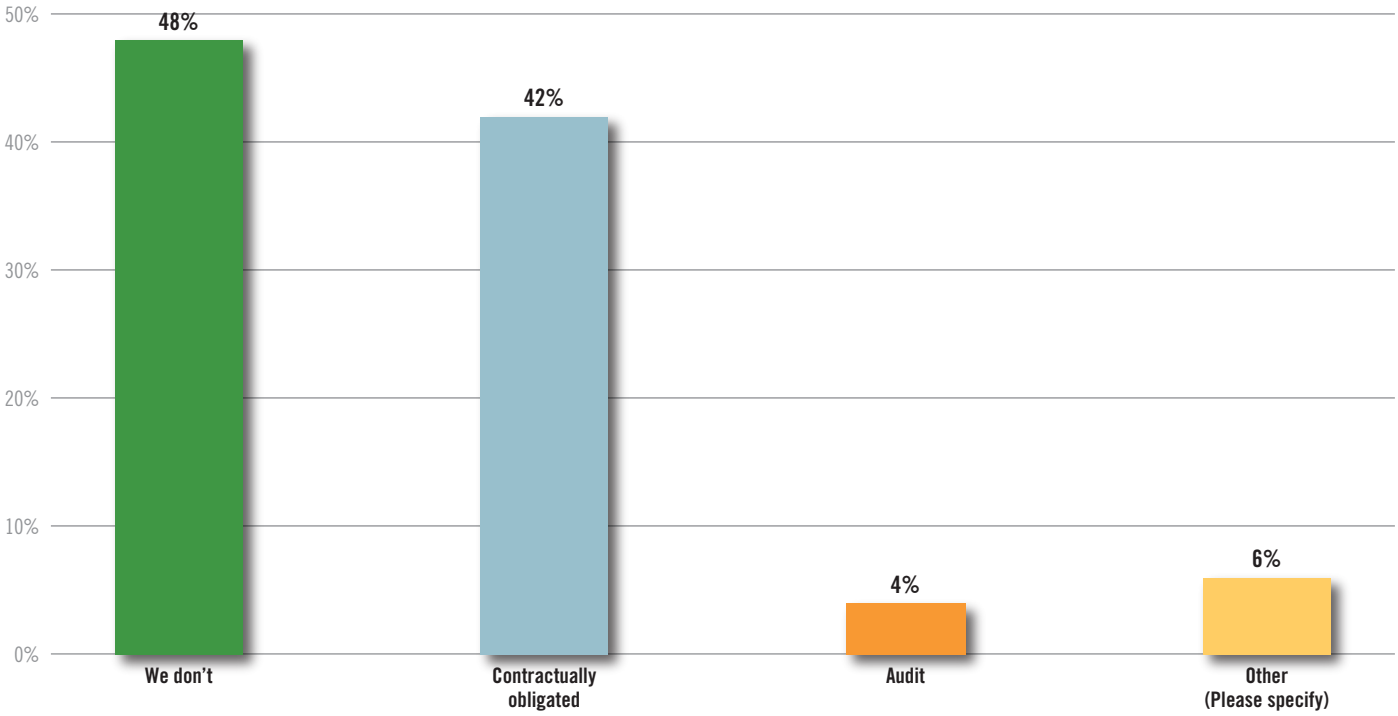
"By regularly auditing its data and security policies, practices and protocols, a company can identify what's working and what needs improvement," McCreary says. "Should a company find itself in the unfortunate position of experiencing multiple data breaches, scrutiny is likely to ensue, and the Federal Trade Commission and state attorneys general are certain to react negatively if it's determined that appropriate policies, practices and procedures were not in place."

Litten adds, "For companies subject to HIPAA, the Department of Health and Human Services can impose civil monetary penalties and require robust compliance plans. As of the end of January 2018, it settled or imposed penalties in 53 cases for a total of more than $75 million. Many of the highest amounts were paid in connection with entities that were found to have had lax privacy and security practices and failed to remediate known problems."

Do you require that your company's partners/suppliers/third-party service providers adhere to your company's cybersecurity and data privacy standards?



How do you verify the cybersecurity and data privacy programs of your company's partners/suppliers/third-party service providers?



While 64 percent of respondents require partner companies, suppliers or vendors to adhere to their security and privacy standards, only 18 percent said they train such third parties. That leaves 36 percent of survey participants utterly unaware of whether third parties are matching their company's standards. Forty-eight percent don't verify third-party compliance, but 42 percent rely on contractual obligations to shield them from a vendor's potential shortcomings.

"Many businesses view their contract with a third party as sufficient," McCreary says. "That may be the case, or it may not. If a company suffers a breach and has reputational damage as a result, your business' fate may hinge on whether that third party has the financial wherewithal to withstand that indemnification being enforced."

Fully auditing vendors, reported by only 4 percent of survey participants, is a best practice, but might be impractical for all but the largest of companies that have the resources to conduct them, McCreary says.

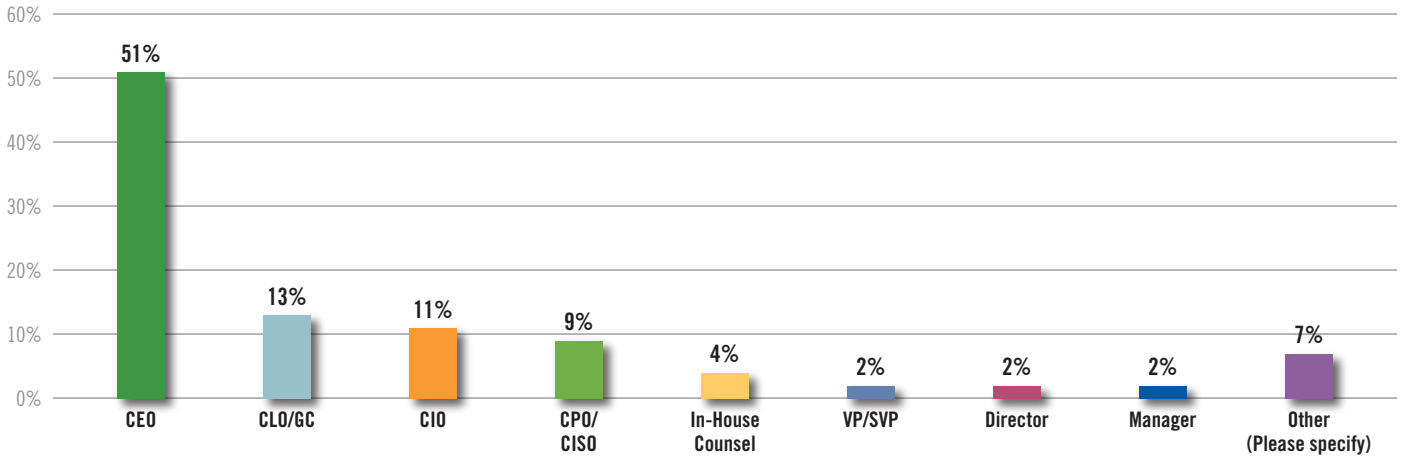
Nonetheless, every organization must take steps to ensure that vendors and partners are protecting data. New York law now requires organizations to incorporate third parties in mandatory cybersecurity risk assessments.

One survey participant recently stopped using an outside vendor for IT and data storage because the vendor was exposing the company to more risk than he was comfortable with.

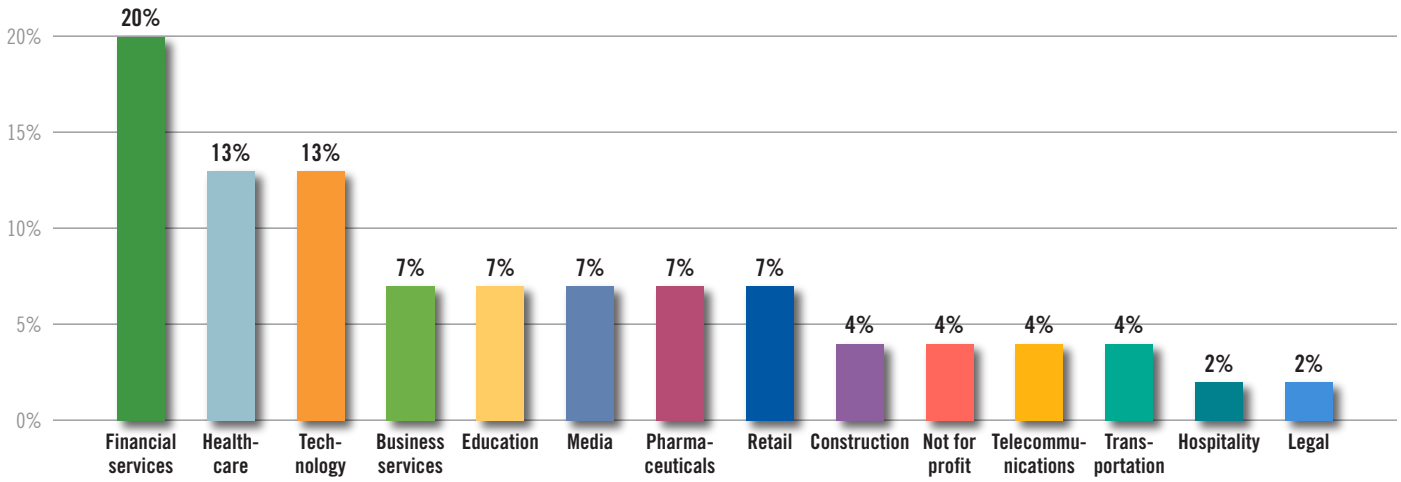
"We had all of our IT outsourced to a company that grew into the virtual world without telling us what was involved in terms of the risk," explained the CEO of a medical device research company. "Because of our size and the amount of data we stored, we decided to bring it all in-house."

RESPONDENT DEMOGRAPHICS

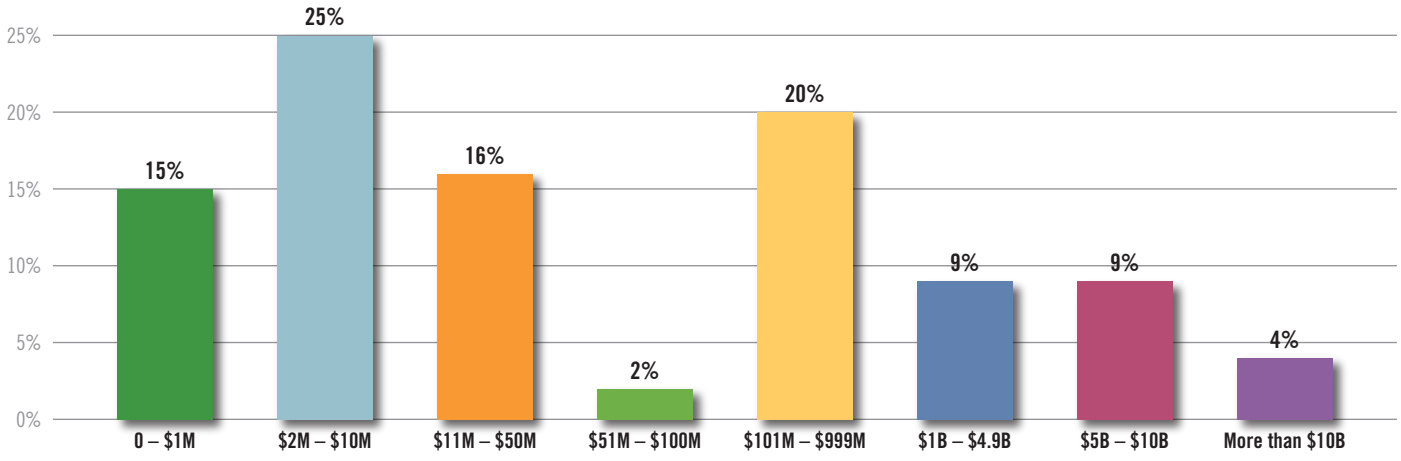
Which of the following most closely matches your job title?



Please select your company's primary industry.



What is your company's annual revenue?



ABOUT US

DATA FOCUSED. PRIVACY STRONG.

Data thieves never stop probing for weaknesses, so Fox Rothschild's Privacy & Data Security team never lets down its guard.

We're Dedicated to Protecting Your Sensitive Information

Customer Data
Employee Records
Intellectual Property & Trade Secrets
Personally Identifiable Information
Proprietary & Confidential Data
Protected Health Information

www.foxrothschild.com/cybersecurity

PRIVACY AND DATA SECURITY PRACTICE GROUP CO-CHAIRS:

Elizabeth G. Litten
HIPAA Privacy & Security Officer and Partner
elitten@foxrothschild.com
Tel: 609.895.3320

Mark G. McCreary, CIPP/US
Chief Privacy Officer and Partner
mmccreary@foxrothschild.com
Tel: 215.299.2010

www.foxrothschild.com