PROGRAM MATERIALS
Program #2904
January 16, 2018

The New Normal: 8 Steps to Seeing if Your Company Defends Customer Data

Copyright ©2018 by Elizabeth G. Litten | Partner and HIPAA Privacy & Security Officer. All Rights Reserved. Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Fox Rothschild LLP
ATTORNEYS AT LAW

THE NEW NORMAL: 8 STEPS TOWARD DEFENDING COMPANY DATA

Elizabeth G. Litten

Partner and HIPAA Privacy & Security Officer

© 2017 Fox Rothschild

What is "Company Data"?

- Consumer information
- Employee information
- Product/service information
- Internal communications

= COMPANY ASSETS

Why Protect it?

- Consumers expect it…
- IBM survey (https://newsroom.ibm.com/2018-04-16-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security)
- 75% of consumers will not buy a product from a company they don't trust to protect their data (and 60% are more concerned about cybersecurity than "going to war")
- Laws require it (GDPR, HIPAA, state laws (including CCPA), potential federal (U.S.) law (Data Care Act – https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf, GLBA, the FTC Act, FCRA, etc.)
- Competitors (or thieves) may it use it to company's detriment

Step #1
Identify Person(s) in Charge of Data Privacy and Security and Define Role

- IT expertise + senior leadership ("C-suite") position and/or direct access (i.e., CISO)
- Role linked to priorities (risk mitigation versus commercialization or monetization of data)
- Org chart delineating delegation of data duties ("right to be forgotten;" internal audits; system access control; security incident response; etc.)

Step # 2
Have an Incident Response Plan

- Plan as though most valuable company data is lost or stolen
- Where and how is data is created, received, maintained and transmitted? (Asset inventory as part of security risk assessment)
- Mitigation, reporting, remediation

Step # 3
Train Employees on Cybersecurity Risks

- Identify common typical human errors and common mistakes
- Create compliance culture, including culture for reporting (consider maintenance of attorney-client privilege)

Employee Error: Working Too Fast!

- Things happen! 24/7
- Slow down!
- CALL!!! Do NOT email!

Employee Error: Bad Emails

- Never go away
- Reply All – Autofill
- Avoid making factual/legal conclusions
  - "We are going to have a recall!"
  - "The client's a [jerk][liar][cheat]."
  - "We are out of compliance."

Employee Error:
Falling for Phishing & Whaling Emails

- Will infect your computer
- Ransomware
- Click on the email address & verify domain
- Identify IT person/vendor to assist (before you click)

Common Threats the Company Faces

Phishing – Spoofed Emails

Reply-To: address is different than sender's address

nondescript or incorrect **From:** address

Subject: contains exclamation point

Poor grammar, overuse of capitalization

From: Webmail Help Desk <liuzf@dlut.edu.>
Reply-To: <xyxyz1@earthlink.net>
Date: Sun, 19 Jul 2009 11:48:41 -0700
Subject: [SPAM] Webmail Quota Alert!

This message was sent automatically by a program on the webmail. Your mailbox Quota Has Exceeded The Set Quota/Limit Which Is 20GB. You Are Currently Running On 23GB Due To Hidden Files And Folder On Your Mailbox. In Order To Increase Your Webmail Quota, You Must Validate Your Account Below:

asked to provide account information

Name;.....
Email Username;.....
Email Password;.....
Confirm Password.....

commands and threats

Failure To Validate Your Webmail Quota May Result In Loss Of Important Information In Your Mailbox Or Cause Limited Access To It. You will continue to receive this warning message periodically if your email account size on our data base continues Approaching Disk Limitations, you will be unable to receive new email
Thank you for your cooperation.

Webmail Help Desk.

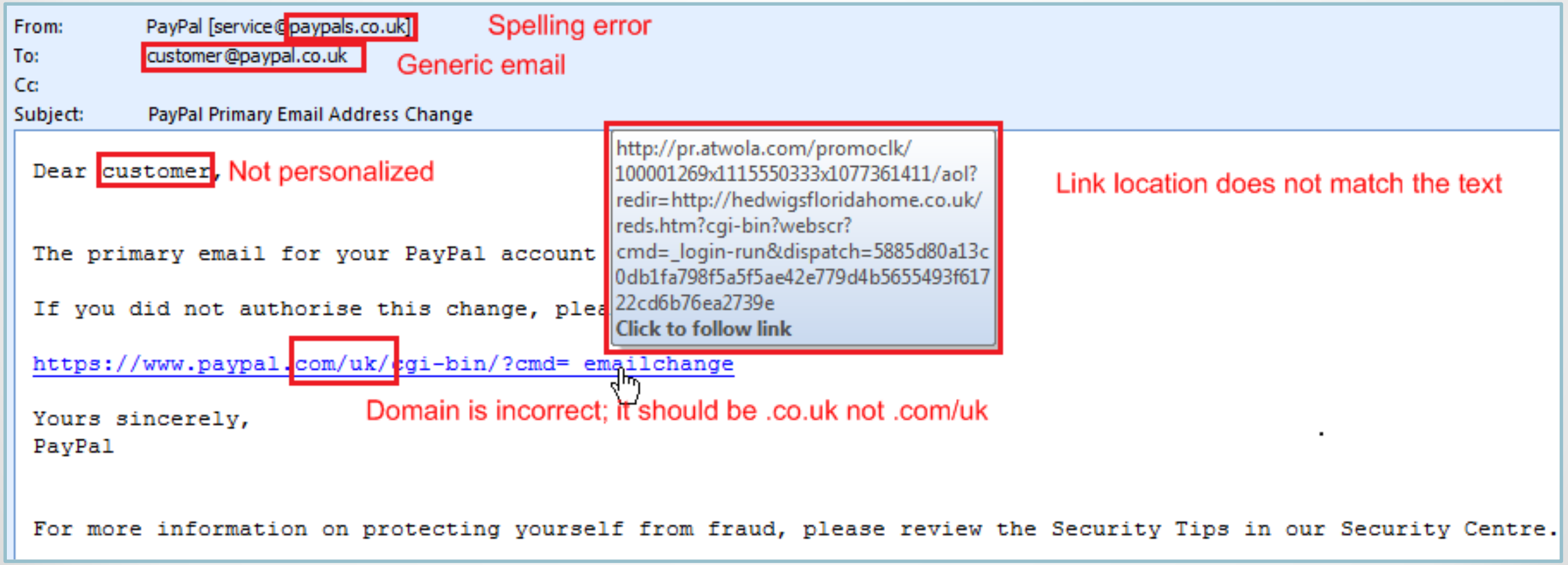
no contact information

Never click on links in email

Never use telephone number in email

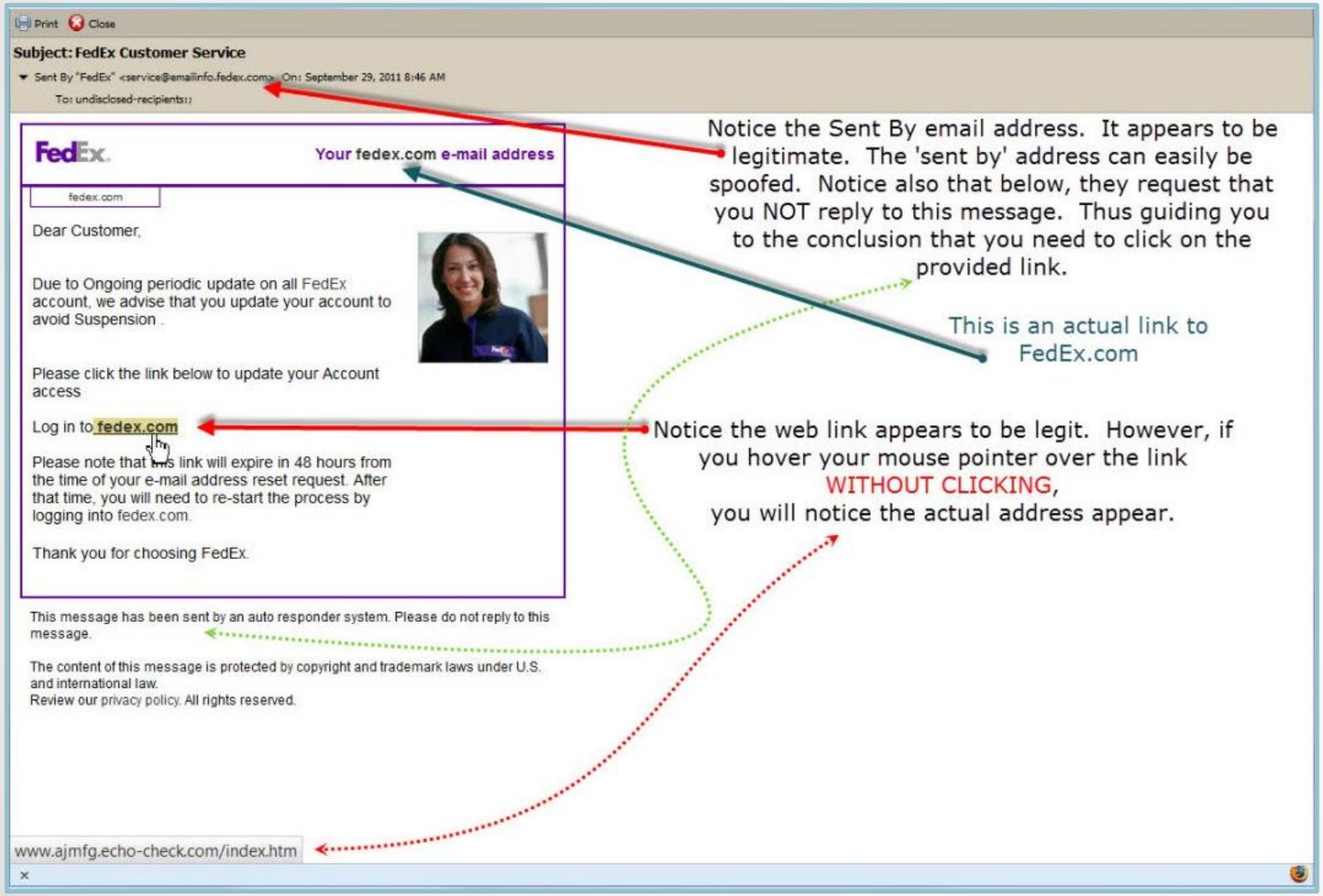
Common Threats the Company Faces

Phishing – Spoofed Emails



Common Threats the Company Faces

Phishing – Spoofed Emails



Never click on links in email

Never use telephone number in email

Create Compliance Culture

- Reward, don't blame
- Have user-friendly policies and procedures (read them – if counsel/C-suite doesn't understand them or find them helpful, will employees?
- Discourage creation of "dirty data" (bad email content, inadvertent/unnecessary collection of employee or customer sensitive information)

Create Compliance Culture, cont.

- Communications between attorney and client about legal matter
  - Usually protected
  - Can't be discovered by third parties
- Protect the privilege
  - Just client?
  - 3rd parties?
- Make sure recipient understands the privilege
  - Communications with unnecessary parties

Step # 4
Perform Security Risk Assessment

- Asset inventory: Where is your data?
- Stored internally
- Stored with 3rd Party:
  - DropBox, Google Drive, OneDrive, Evernote, Media Fire?
- Beware of applicable laws
- BYOD Policy

Step # 5
Create Policies for Portable Devices and Use of Social Media

- Portable devices:
  - Company owned or employee owned (BYOD)?
  - Laptops, tablets, iPads, smartphones, other
  - Procedure for remote use/access under security safeguards (access to company network/cloud only via secure access, such as VPN)
  - Employees sign policy
  - No texting of company data

Step # 5, cont.

- Social media: evaluate ethical and legal boundaries
  - National Labor Relations Act protections (no protections for maliciously false, offensive, inappropriate comments about employer or clients)
  - NLRA protections for communications among employees about improving conditions of jobs
  - Company may be held responsible for employee posts
- Reputational harm; customer harm
- State-specific employer requirements
  - NJ: prohibits employers from requesting or requiring employees or applicants to turn over personal account log-in/access info; prohibits waiver of privacy rights

Step # 6
Know Which Laws Apply

- U.S.
  - General applicability (FTC Act; Children's Online Privacy Protection Act (COPPA)
  - Industry-specific laws (HIPAA, FINRA, FERPA)
  - Potential federal law (tech industry-supported): Sen. Brian Schatz from Hawaii
- State laws
  - Extra-territorial, like the California Consumer Privacy Act
- Laws of other countries
  - Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)
  - EU: General Data Protection Regulations (GDPR)

Step # 7
Don't Overlook Hard Copies

- Hospitals: paper/film are most frequent sources of breached data (https://www.healthcare-informatics.com/news-item/cybersecurity/paper-records-films-most-common-type-healthcare-data-breach-study-finds)
- Create physical and administrative data privacy and security policies and procedures
  - Mailings (see https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/triple-s-management/index.html)
  - Dumpster diving (see https://www.hhs.gov/hipaa/for-professionals/faq/576/may-a-covered-entity-dispose-of-information-in-dumpsters/index.html and https://www.deseretnews.com/article/865601583/Client-files-with-personal-information-found-in-Dumpster.html)
  - Documents to be shredded (see https://www.ledger-enquirer.com/news/business/health-care/article205181029.html)

Step # 8
Follow the Data

- Identify which vendors/third parties access company data
- Verify vendor's need for access
- Include data privacy and security obligations in vendor contract
- Consider right to audit/perform due diligence
- Beware vendors that "de-identify" and use company data (and often sell to data aggregators)
- Consumer data, employee data, and company data/analytics are *company assets* that should be returned/destroyed following necessary access/use by vendor

Be Careful Out There!

Elizabeth G. Litten
Partner and HIPAA Privacy & Security Officer
elitten@foxrothschild.com
(609) 895-3320

Fox Rothschild LLP
ATTORNEYS AT LAW

HIPAA & Health Information Technology

Monitoring Legal Developments Relating to the Privacy and Security of Health Information

The Heavy Hit of HIPAA: Violations May Send You to Jail

By Elizabeth Litten on August 7, 2018

The recent **criminal conviction** of a Massachusetts physician provides a stark reminder that violating HIPAA can result in more than civil monetary penalties and the financial and reputational fall-out that results from a breach. In this case, perhaps the cover-up was worse than the crime, or maybe prosecutors decided that a conviction on other charges would have been harder to get. Either way, the case should alert covered entities and business associates to the fact that HIPAA violations can result in jail time and criminal fines.

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) investigates complaints and may impose civil monetary penalties (CMPs) for violations of HIPAA. The U.S. Department of Justice (DOJ) handles criminal investigations and penalties. This may not provide much comfort, but a CMP will not be imposed if the HIPAA violation is determined to constitute a criminal offense.

OCR will refer matters to DOJ for criminal enforcement in some cases or will work cooperatively with DOJ where a DOJ investigation on other grounds reveals a

potential HIPAA violation. **HHS reported** that OCR had referred 688 cases to the DOJ for criminal investigation as of June 30, 2018.

The criminal enforcement of HIPAA was described in a **Memorandum Opinion** issued in 2005 jointly to HHS and the Senior Counsel to the Deputy Attorney General by Steven Bradbury, then-acting Assistant Attorney General of the Office of Legal Counsel within DOJ (the DOJ Memo). The DOJ Memo explains that HIPAA allows for criminal penalties only for violations that involve the disclosure of "unique health identifiers" or "individually identifiable health information" (IIHI) that are made "knowingly" and in violation of HIPAA. Specifically, a person may be subject to criminal penalties if he or she knowingly (and in violation of HIPAA): (i) uses or causes to be used a unique health identifier; (ii) obtains IIHI; or (iii) discloses IIHI to another person. Criminal penalties range from misdemeanors to felonies. The maximum criminal penalty (a fine of up to $250,000 and imprisonment of up to 10 years) can be imposed if one of these offenses is committed "with intent to sell, transfer, or use [IIHI] for commercial advantage, personal gain, or malicious harm." The DOJ Memo explains that "knowingly" refers to knowledge of the facts that constitute the offense, not knowledge of the law being violated (HIPAA).

The DOJ Memo emphasizes the fact that criminal penalties are reserved for limited and specific violations of HIPAA: "Such punishment is reserved for violations involving `unique health identifiers' and [IIHI]… Thus, the statute reflects a heightened concern for violations that intrude upon the medical privacy of individuals." The DOJ Memo focuses on violations by covered entities. It notes that when a covered entity is not an individual, but is a corporate entity, the conduct of agents may be imputed to the entity when the agents act within the scope of employment, and the criminal liability of a corporate entity may be attributed to individuals in managerial roles.

DOJ might decide to seek a conviction for a violation of HIPAA when it believes such a conviction would be easier to get than a conviction for a violation of other federal laws governing health care providers (such as the anti-kickback statute). After all,

the DOJ Memo makes it clear that "knowing" refers to the conduct, not the state of the law. However, it should be noted, as per the DOJ Memo, that the DOJ's interpretation of "`knowingly' does not dispense with the *mens rea* requirement of section 1320d-6 [HIPAA] and create a strict liability offense; satisfaction of the 'knowing' element will still require proof that the defendant knew the facts that constitute the offense."

When a health care entity (like a large hospital system or health plan) has deep pockets, the OCR may decide to pursue very high civil monetary penalties and rely on the financial and reputational implications of the civil monetary penalties to act as a deterrence. On the other hand, the DOJ may seek to deter behavior associated with a wider range of criminal activities by pursuing jail time for a HIPAA violation.

In the case of the Massachusetts physician, it is also likely that the DOJ pursued the criminal charge because she lied about her relationship with the third party to which she disclosed patient information. My law partner **Charles DeMonaco**, a white collar defense attorney and former DOJ prosecutor, agrees:

> **"It is understandable why this doctor was indicted and convicted for these offenses. She was accused of lying to the agents, which is always a major hurdle in a criminal case. Even if an underlying crime cannot be established, a lie of a material fact to a government agent is a stand-alone false-statement felony. It also establishes consciousness of guilt. The doctor could have asserted her Fifth Amendment privilege against self-incrimination to avoid talking to the government agents. It is never a good thing for a doctor to speak with agents who are investigating the doctor's conduct without counsel and without proper protection of limited use immunity being sought prior to the interview. The government also proved that she accepted fees from the pharma company after providing the [IIHI] in violation of HIPAA. Under these facts, it is not surprising that this case was brought as a criminal prosecution and that a guilty verdict was returned.**

Everyone subject to HIPAA should be aware that a HIPAA violation involving disclosure or breach of IIHI may be the low-hanging fruit for criminal prosecutors originally focused on other violations of law. In particular, covered entities should carefully evaluate arrangements with third parties that involve the sharing of IIHI with those parties for commercial/personal gain or commercial harm. If the sharing of IIHI is not permitted under HIPAA and commercial gain or harm is involved, these violations could result in the most severe level of criminal penalties, including significant jail time.

HIPAA & Health Information Technology

Copyright © 2019, Fox Rothschild LLP All Rights Reserved. Attorney Advertising.

Fox Rothschild LLP
ATTORNEYS AT LAW

HIPAA & Health Information Technology

Monitoring Legal Developments Relating to the Privacy and Security of Health Information

To BAA or Not to BAA? The Question a Florida Provider Should Have Asked in 2011 Results in a Half Million Dollar Payment in 2018

By Elizabeth Litten on December 5, 2018

Yesterday's **listserv** announcement from the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) brought to mind this question. The post announces the agreement by a Florida company, Advanced Care Hospitalists PL (ACH), to pay $500,000 and adopt a "substantial corrective action plan". The first alleged HIPAA violation? Patient information, including name, date of birth, and social security number was viewable on the website of ACH's medical billing vendor, and reported to ACH by a local hospital in 2014.

To add insult (and another alleged HIPAA violation) to injury, according to the **HHS Press Release**, ACH did not have a business associate agreement (BAA) in place with the vendor, Doctor's First Choice Billings, Inc. (First Choice), during the period when medical billing services were rendered (an 8-month period running from November of 2011 to June of 2012). Based on the HHS Press Release, it appears that ACH only scrambled to sign a BAA with First Choice in 2014, likely after learning of the website issue. In addition, according to the HHS Press Release, the person hired by

ACH to provide the medical billing services used "First Choice's name and website, but allegedly without any knowledge or permission of First Choice's owner."

These allegations are head-spinning, starting with those implicating the "should've-been" business associate. First, how does a medical billing company allow an employee or any other individual access to its website without its knowledge or permission? Next, shouldn't someone at First Choice have noticed that an unauthorized person was posting information on its website back in 2011-2012, or at some point prior to its discovery by an unrelated third party in 2014? Finally, how does a medical billing company (a company that should know, certainly by late 2011, that it's most likely acting a business associate when it performs medical billing services), not realize that individually identifiable health information and social security numbers are viewable on its website by outsiders?

ACH's apparent lackadaisical attitude about its HIPAA obligations is equally stunning. What health care provider engaged in electronic billing was not aware of the need to have a BAA in place with a medical billing vendor in 2011? While the **Omnibus Rule** wasn't published until January of 2013 (at which point ACH had another chance to recognize its need for a BAA with First Choice), HHS has been publishing **FAQs** addressing all kinds of business associate-related issues and requirements since 2002.

It seems pretty obvious that ACH should have had a BAA with First Choice, but, in many instances, having a BAA is neither required by HIPAA nor prudent from the perspective of the covered entity. A BAA generally is not necessary if protected health information is not created, received, maintained or transmitted by or to the vendor in connection with the provision of services on behalf of a covered entity, business associate, or subcontractor, and having one in place may backfire. Consider the following scenario:

* Health Plan (HP), thinking it is acting out of an abundance of HIPAA caution, requires all of its vendors to sign BAAs.

* Small Law Firm (SLF) provides legal advice to HP, but does not create, receive, maintain or transmit protected health information in connection with the services it provides on behalf of HP.

* However, SLF signs HP's BAA at HP's request and because SLF thinks it might, at some point, expand the scope of legal services it provides to HP to include matters that require it to receive protected health information from HP.

* SLF suffers a ransomware attack that results in some of its data being encrypted, including data received from HP. It reviews HHS's fact sheet on Ransomware and HIPAA, and realizes that a HIPAA breach may have occurred, since it cannot rule out the possibility that it received protected health information from HP at some point after it signed the BAA and prior to the attack.

* SLF reports the attack to HP as per the BAA. Neither SLF nor HP can rule out the possibility that protected health information of individuals covered by HP was received by SLF at some point and affected by the attack.

HP is now in the position of having to provide breach notifications to individuals and HHS. Had it been more circumspect at the outset, deciding it would only ask SLF to sign a BAA if/when SLF needed protected health information in order to provide legal services on behalf of HP, it may have avoided these HIPAA implications completely.

So while it seems stunning that a health care provider entity such as ACH would have neglected to sign a BAA with First Choice before 2014, having a BAA in place when it is not necessary can create its own problems. Better to constantly ask (and carefully consider): to BAA or not to BAA?

HIPAA & Health Information Technology

Copyright © 2019, Fox Rothschild LLP All Rights Reserved. Attorney Advertising.

Fox Rothschild LLP
ATTORNEYS AT LAW

Elizabeth G. Litten, Partner and HIPAA Privacy & Security Officer

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

Princeton, NJ
Tel: 609.895.3320
Fax: 609.896.1469

Publications

The California Consumer Privacy Act: What You Need To Know

October 15, 2018 – Alerts
By Mark McCreary and Elizabeth Litten

Companies that are getting acclimated to the European Union's General Data Protection Regulation (GDPR) have a new and just as significant compliance challenge to confront: The California Consumer Privacy Act.

Signed into law in June, the California Consumer Privacy Act will change the way companies both inside and outside the state manage consumers' personal data by conferring a new set of rights on consumers, and a new set of responsibilities on the companies that handle their data.

Doubt California's influence? When is the last time you bought a car that wasn't compliant with California emissions standards? The new rules will affect a wide range of companies both inside and outside the U.S. The good news is, there is time to prepare. The act won't take effect until Jan. 1, 2020 and enforcement won't begin until at least six months after the Attorney General publishes rules implementing the law, or July 2020, the deadline for such rules to be completed, whichever comes first.

What follows is a short summary of the law, and how it will affect businesses with exposure to California residents.

Who Is Subject to the Law?

In short, the act applies to *for-profit* entities that collect and process California residents' personal information and do business in the state. A physical presence in California is not a requirement. In addition, the entity must meet at least one of the following criteria:

- Generate annual gross revenue > $25 million
- Receive or share data of > 50,000 California residents annually
- Derive at least 50 percent of annual revenue by selling residents' personal information

Non-profits and companies that don't meet any of the three above thresholds are exempt.

What Is Personal Information?

The act includes a broad definition of personal information. It is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably linked , directly or indirectly, with a particular consumer *or household*." Note the use of the term "household," meaning the data does not have to be associated with a name or specific individuals. The act lists a wide range of standard examples that includes Social Security numbers, drivers' license numbers and purchase histories, but also "unique personal identifiers" such as device identifiers and other online tracking technologies. Information that is publicly available and aggregated or de-identified data is excluded, as is medical or health information collected by a person or entity governed by California's Confidentiality of Medical Information Act or HIPAA.

What New Rights Are Given Consumers?

The law provides consumers with more control over their personal information in four ways:

- **Knowledge**: Consumers must be able to learn – generally through a publicly posted privacy policy and specifically by request – what personal information companies are collecting, how it is being collected and used, and whether and to whom it is being disclosed or sold.
- **Sale of Data:** Companies must make it easy for consumers to opt-out of having their personal information sold to a third party, and require consumers who are under 16 to opt-in in order to allow their information to be sold. Companies must post a "Do Not Sell My Personal Information" link on their homepages.
- **Data removal**: Consumers may request that companies delete their personal information and businesses must inform customers that they have this right. Businesses must comply with these requests and ensure the consumer's data is also deleted by third party contractors. There are some exceptions, for example if the data is needed to complete a transaction.
- **Service equality**: For the most part, companies cannot discriminate against consumers who exercise their privacy rights. However, the act sows confusion by allowing companies to charge a different price or provide a different level of service to customers if "that difference is reasonably related to the value provided to the consumer by the consumer's data." Businesses can offer consumers financial incentives to allow data collection.

Disclosure Responsibilities

Increased disclosure will be a large part of compliance. Companies will need to proactively explain privacy policies to consumers when data is collected. That includes informing consumers of their rights under the Act, the sort of personal information collected, the ways that data is used and the types of personal data the company has sold to third parties in the last year. These disclosures must be updated every 12 months.

Private Right of Action

Opening the door to a potential flood of litigation, the Act provides consumers a private right of action if their data "is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices." Consumers can file individual or class action lawsuits, and can recover between $100 to $750 in statutory damages per incident, or actual damages. It also allows consumers to seek injunctive and other forms of relief, and sets out different procedures for actions seeking actual versus statutory damages.

Penalties for Noncompliance

Companies that fail to comply with the act are subject to civil penalties of up to $2,500 per violation and $7,500 per intentional violation. Once notified of a violation by the Attorney General, companies have 30 days to come into compliance in order to avoid penalties.

How To Prepare

The Act has already been amended once, and may go through additional updates before it takes effect, but businesses should start to prepare now. Privacy policies, procedures and websites will need to be updated before it takes effect. Companies will want to catalog the types of data they collect and how that data is used.

Fox Rothschild's experienced Privacy & Data Security team can help. Our attorneys keep at the forefront of ever-changing data privacy law, providing practical, business-oriented compliance solutions to clients of all sizes in wide range of industries.

For information on how Fox Rothschild can help your company get ready for the California Consumer Privacy Act, Contact Privacy & Data Security Practice Co-Chair Mark McCreary at mmccreary@foxrothschild.com or Co-Chair Elizabeth Litten at elitten@foxrothschild.com

© 2019 All content of this web site is the property and copyright of Fox Rothschild LLP and may not be reproduced in any format without prior express permission.
Contact marketing@foxrothschild.com for more information or to seek permission to reproduce content.
Attorney Advertising. Website by Great Jakes

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."

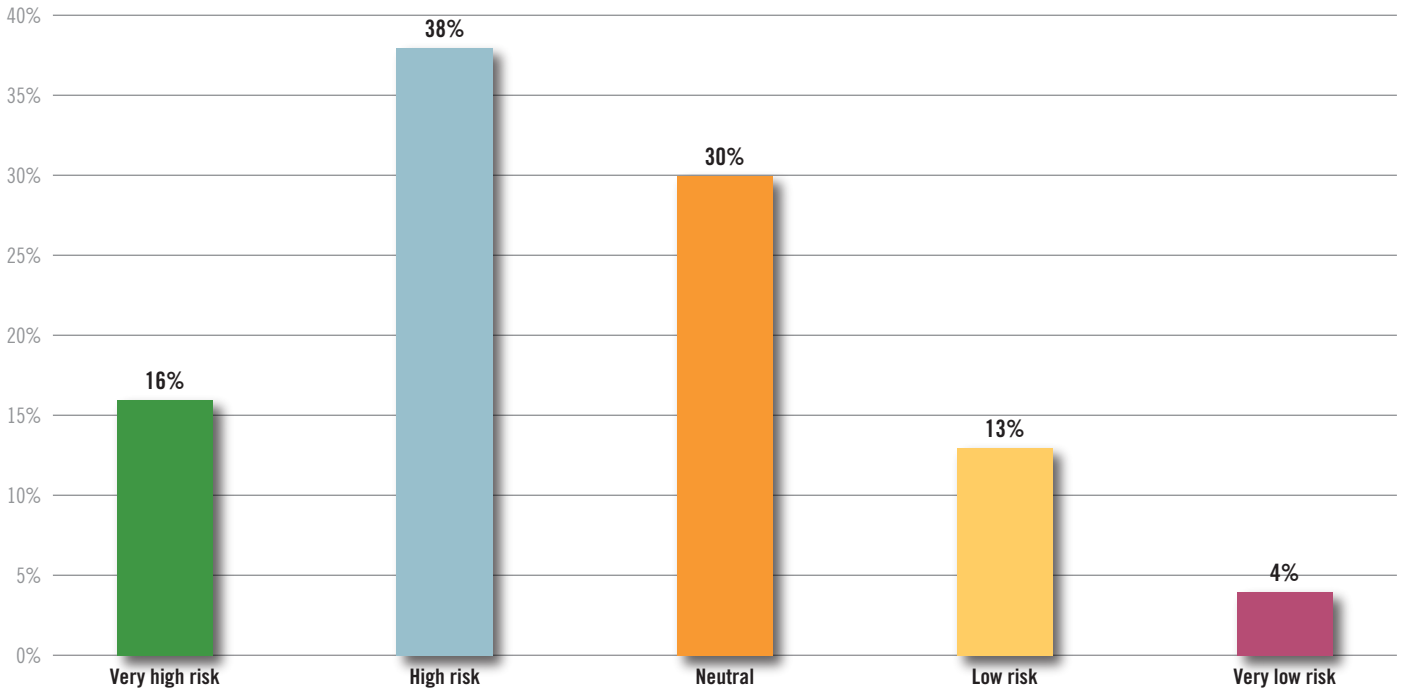
- "With the exception of a year with a major hardware or software upgrade, 10 percent of an IT budget dedicated to system security strikes me as a bare minimum," says McCreary.

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.

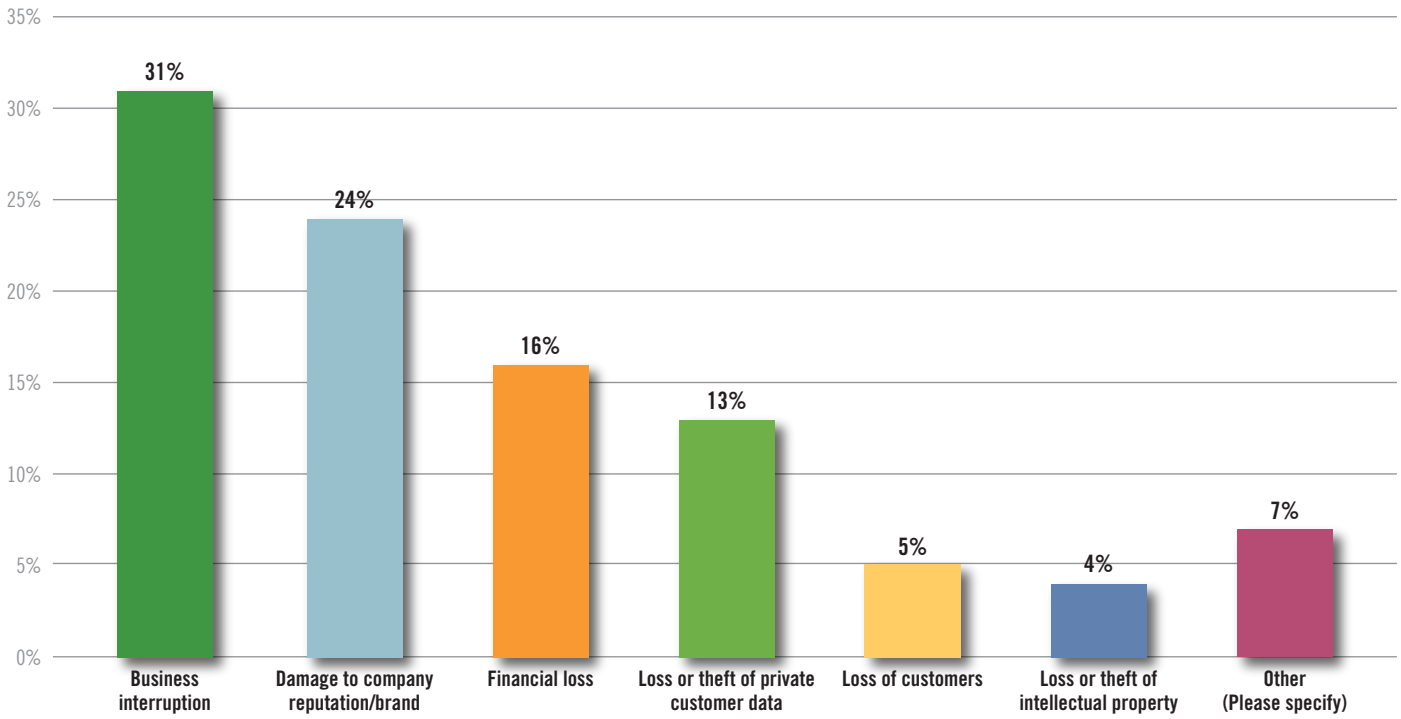
"I think we're toward the lower end in terms of risk, just because of the nature and profile of our business," explained the head of the legal department for a global manufacturing company. "We're not a sexy target to hack if someone is looking to do damage. We're not a big name; we're not a household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

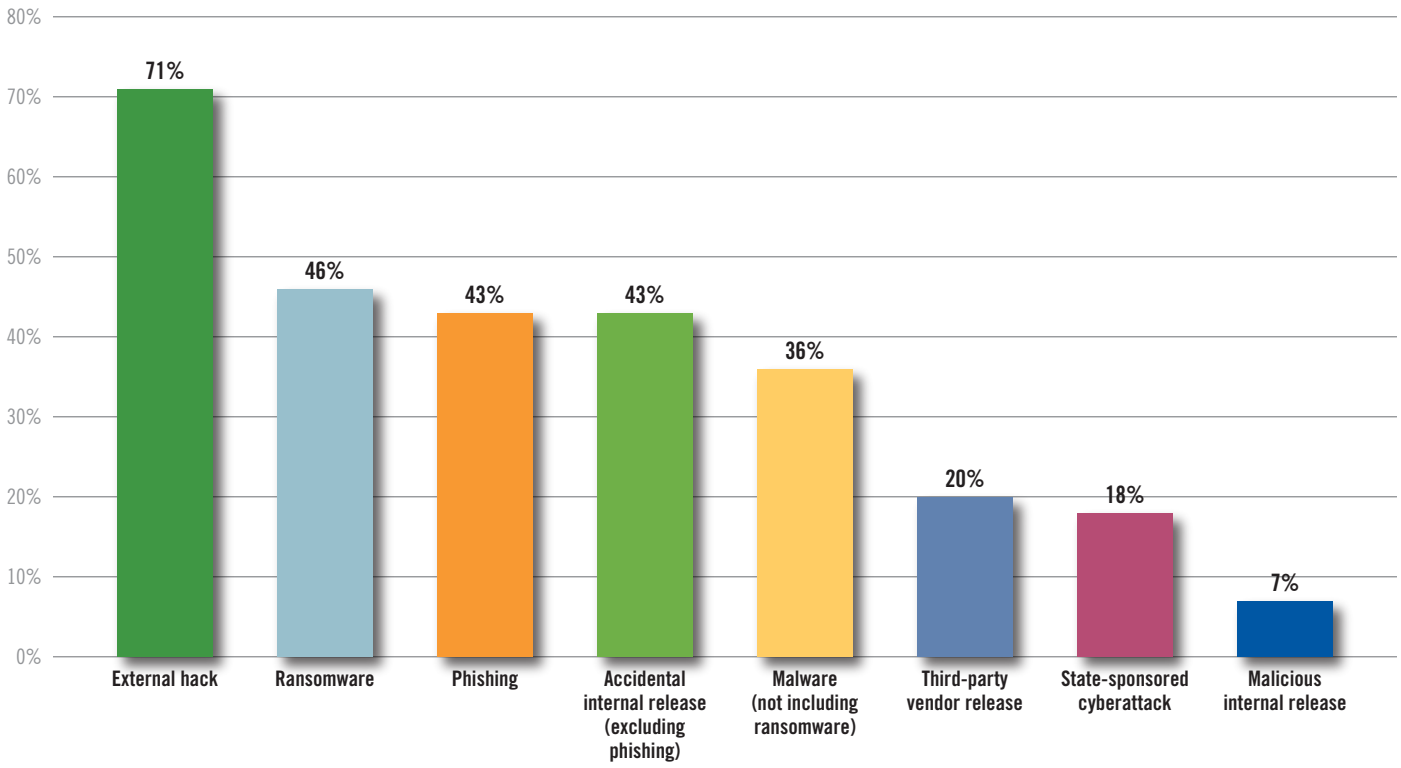
Regarding the impact on a company following a breach, respondents noted their top two concerns were business interruption and reputational damage, at 31 percent and 24 percent, respectively.

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?



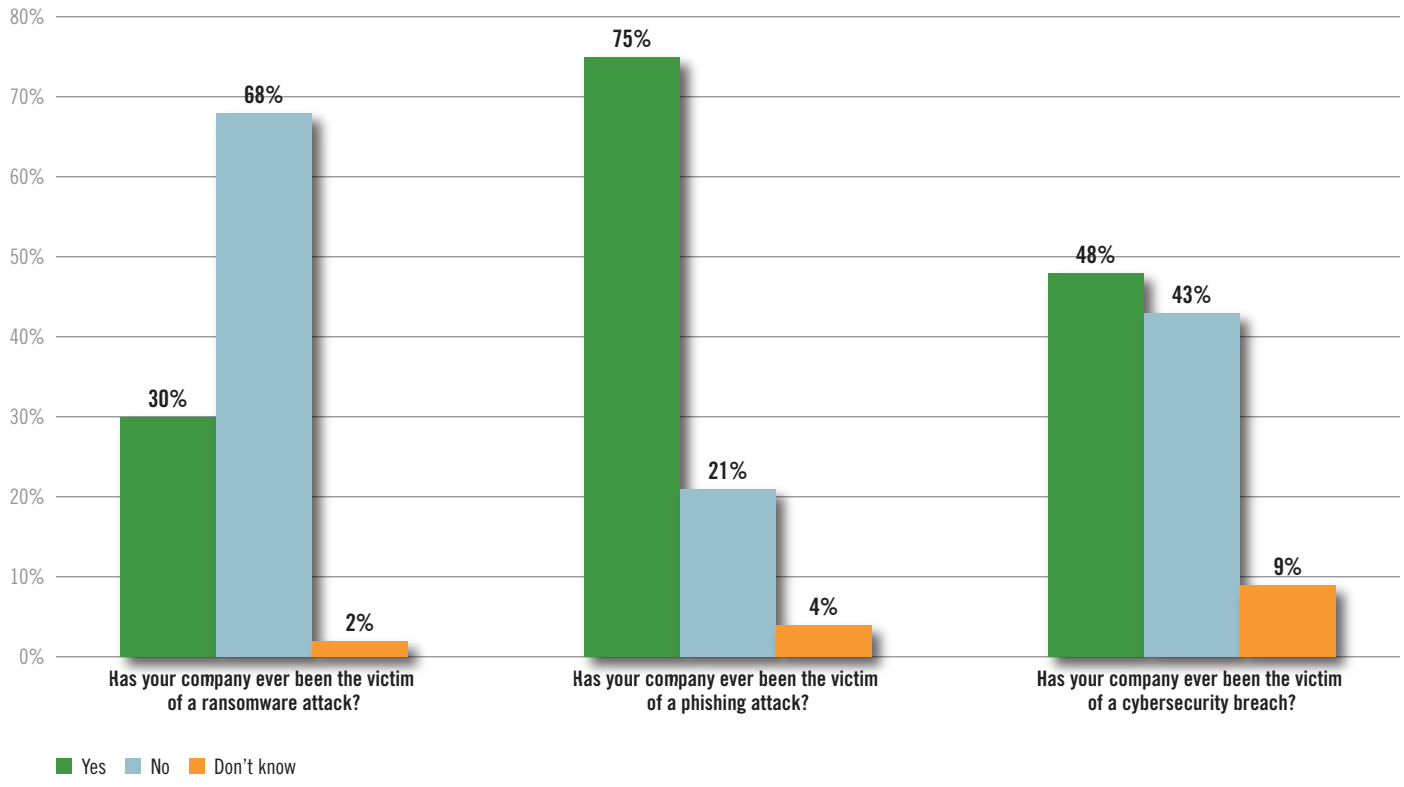
Executives are predominantly concerned with the threat posed by an external hack. However, the risk of a foreign state-sponsored cyberattack is underappreciated, as only 18 percent of survey participants identified it as a major concern. Executives must be mindful that politically active employees and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

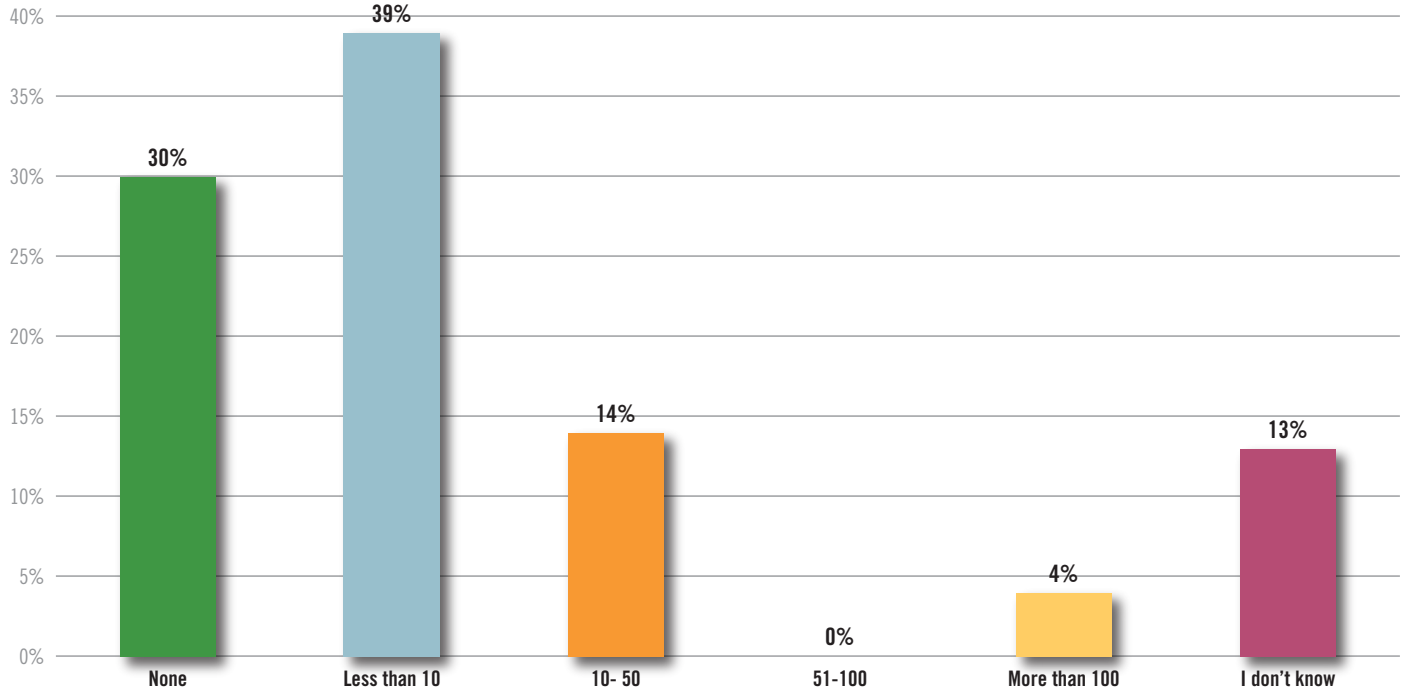
Ransomware was viewed by 46 percent of respondents as the biggest risk. Third-party vendor release and malicious internal release alarmed only 20 percent and 7 percent, respectively.

"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:

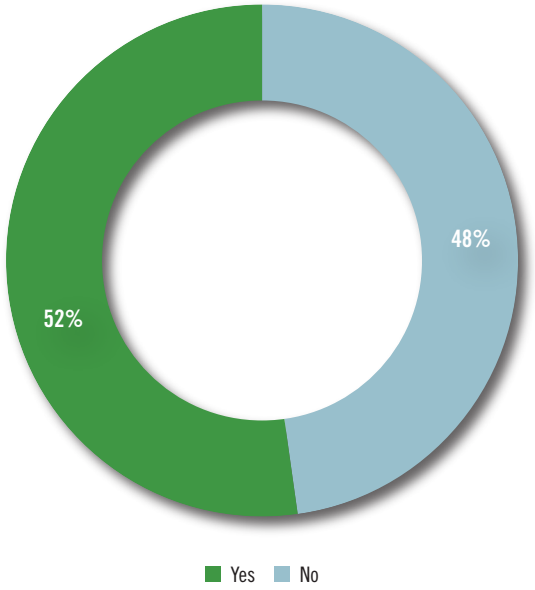


How many security breaches, about which you are aware, has your company been the victim of in the past twelve months?

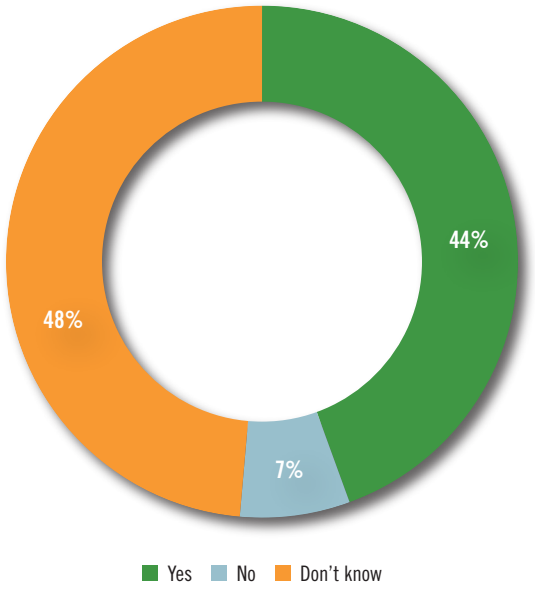


DATA ACROSS BORDERS

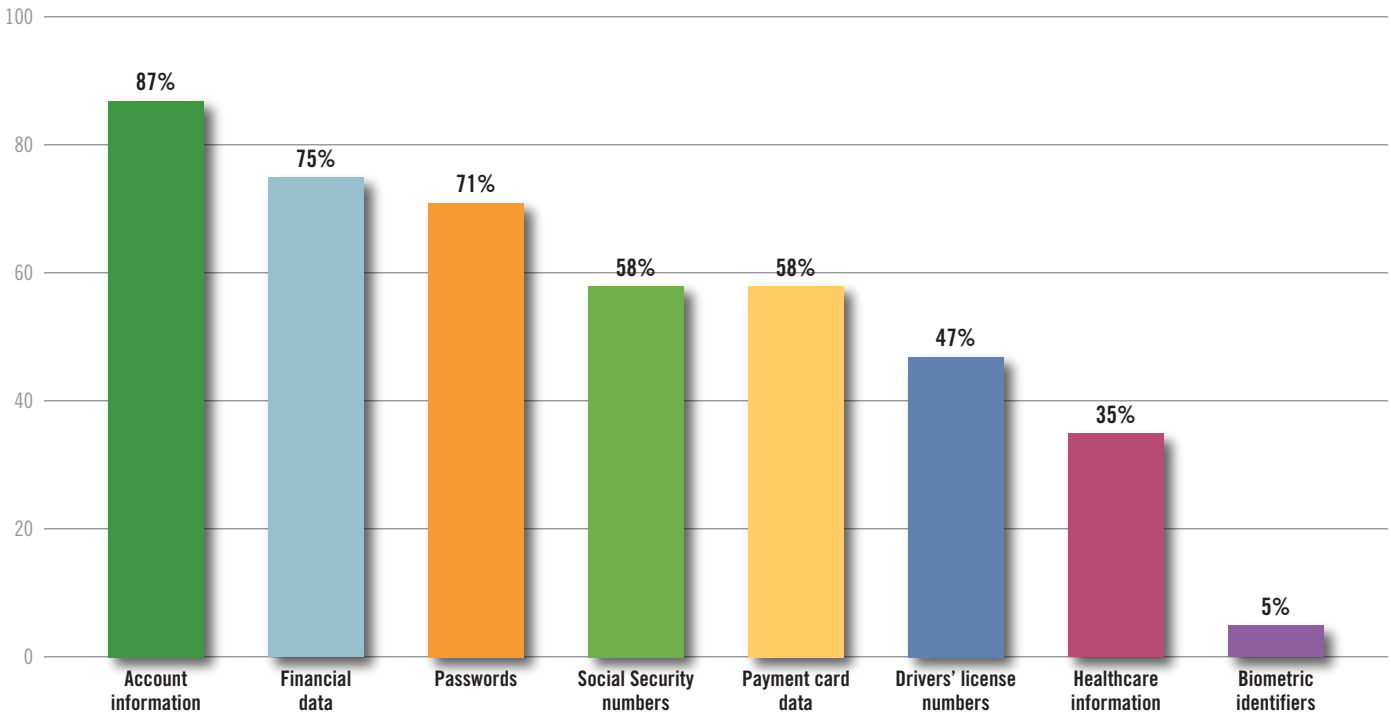
Do you share data across country borders within your company or with distributors, third-party suppliers or other partners?



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.

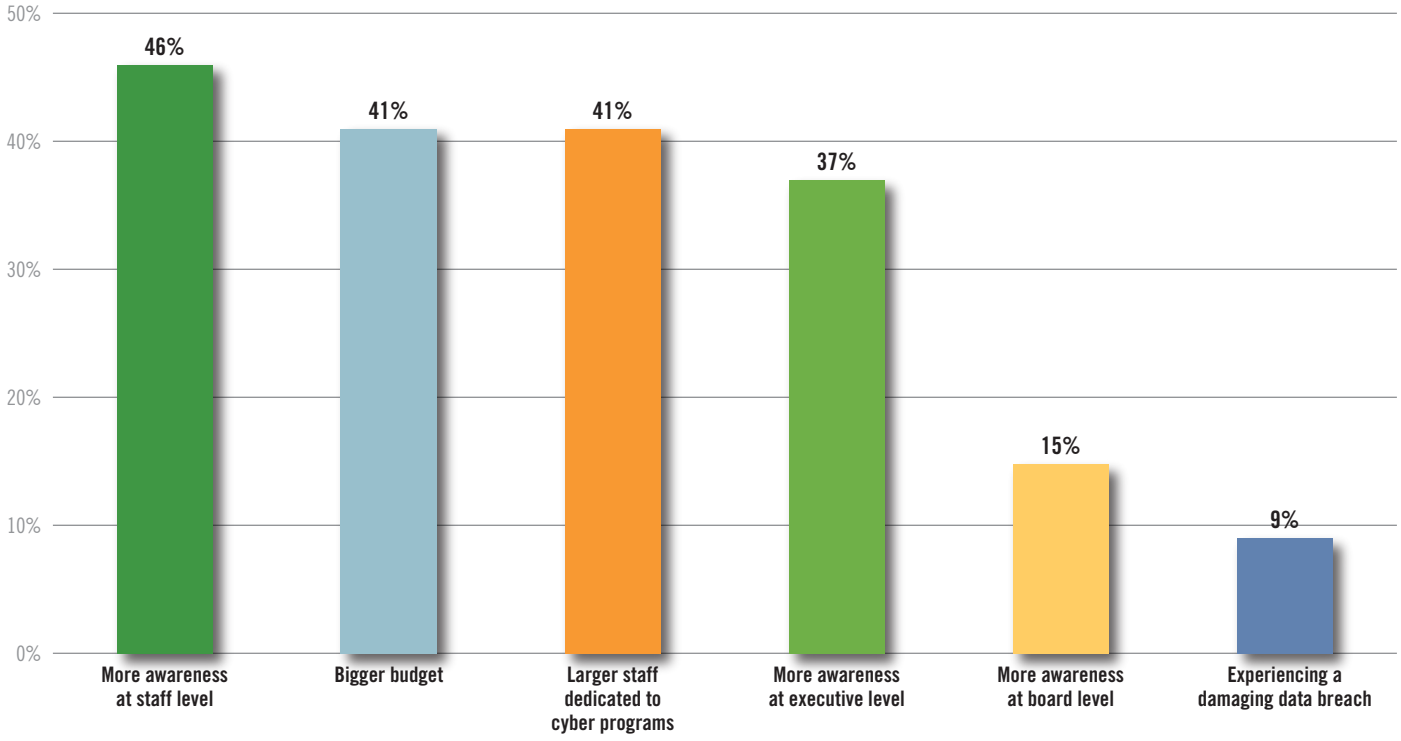
"When we explain to clients that you must comply with GDPR whenever you provide services to a third party that is subject to GDPR, we see a lot of wide eyes," says McCreary. "That is often the first moment they truly grasp that they have a GDPR problem they need to remedy."

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

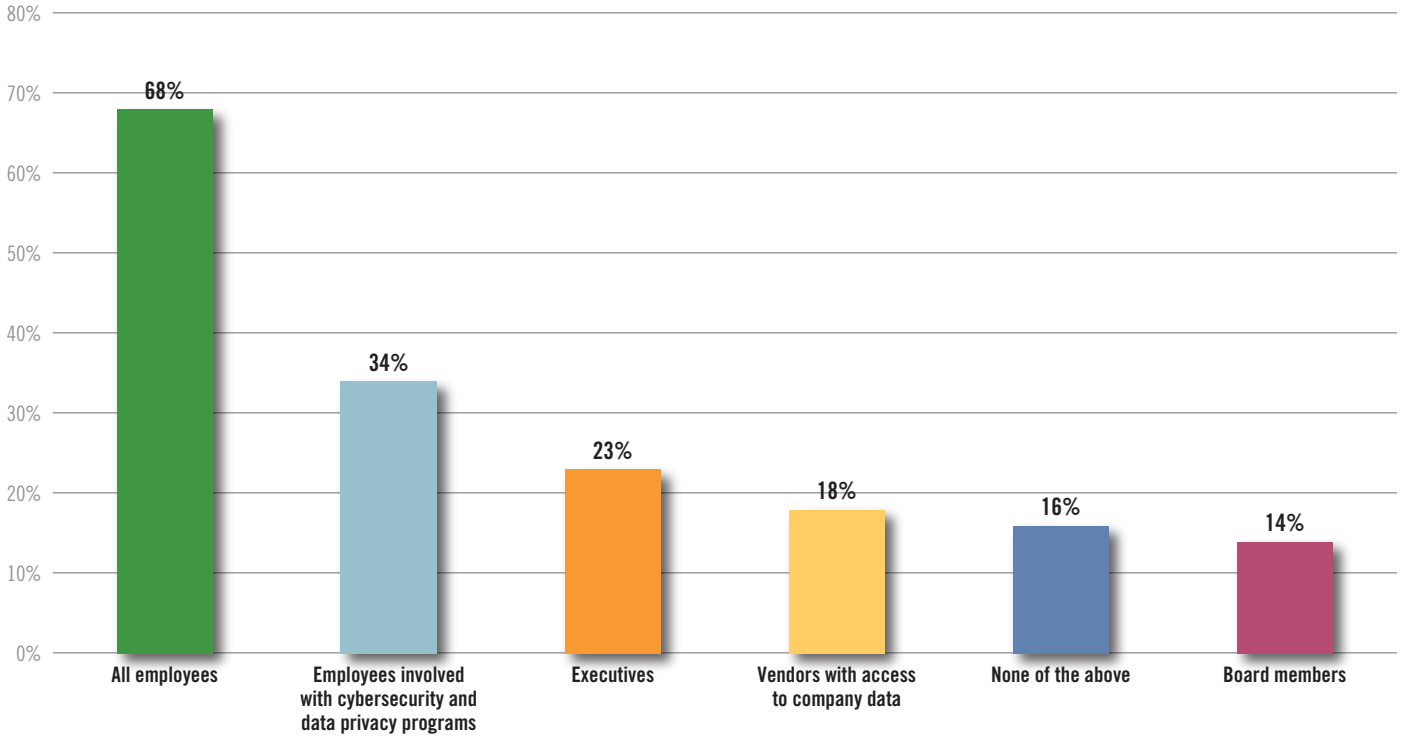
"GDPR is astonishingly broad. It applies to basic personal information, not just sensitive data," McCreary says. "A key provision allows customers to compel companies to delete their personal data, which is an extremely complicated task because you cannot simply delete information anymore. Data is tenacious.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

STILL STRUGGLING WITH TRAINING

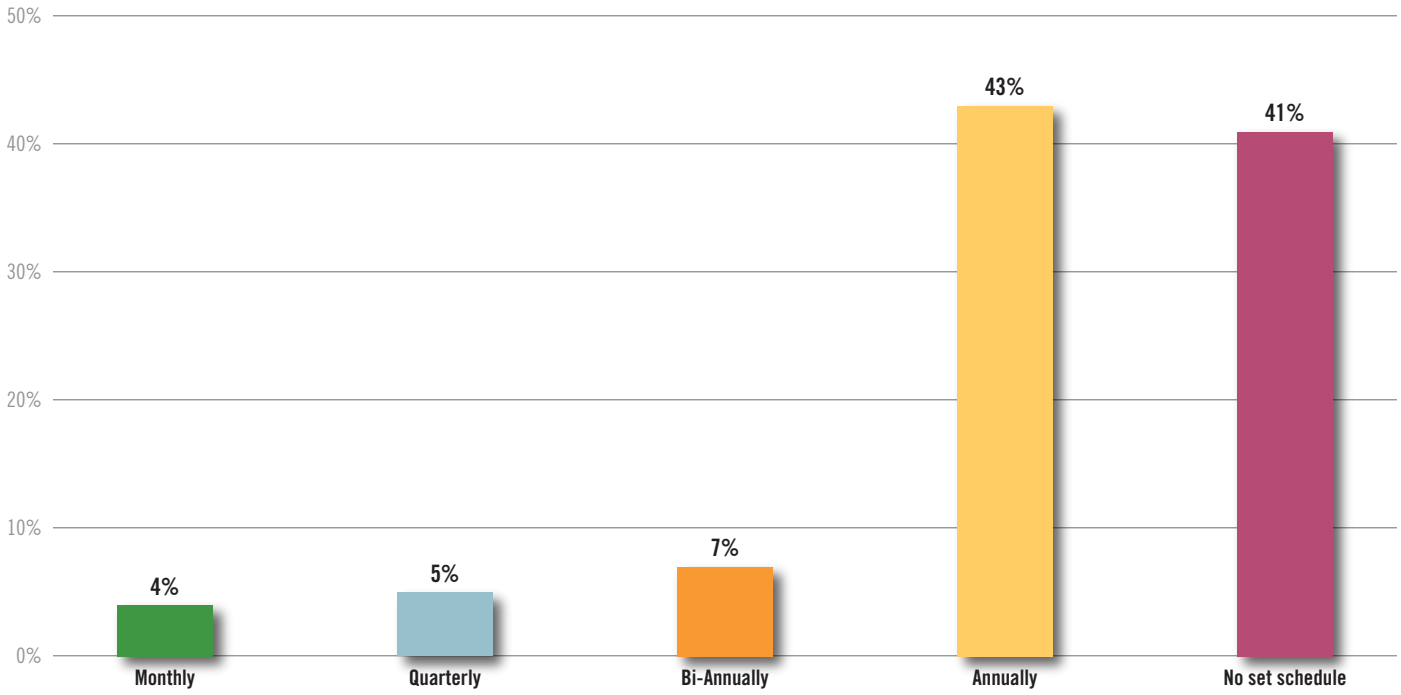
What do you believe would help make your company's cybersecurity and data privacy program stronger/more secure?



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.

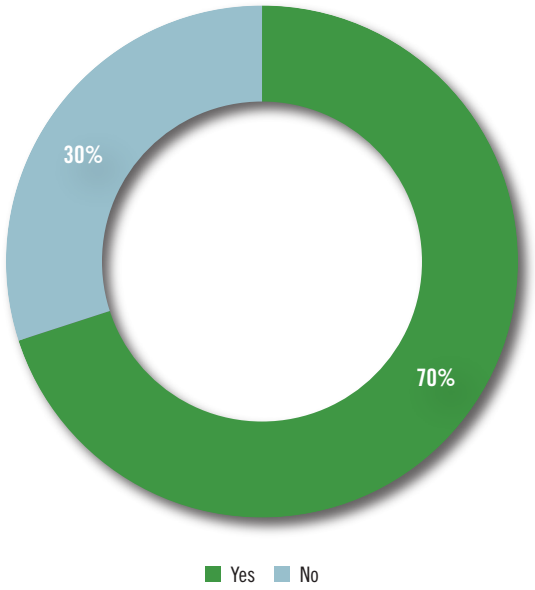
Interestingly, almost a quarter of participants noted they train only their executives on privacy. Cybersecurity professionals noted that while executives may appear to be at a higher risk for targeting, any employee can compromise the entire company's security.

"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."

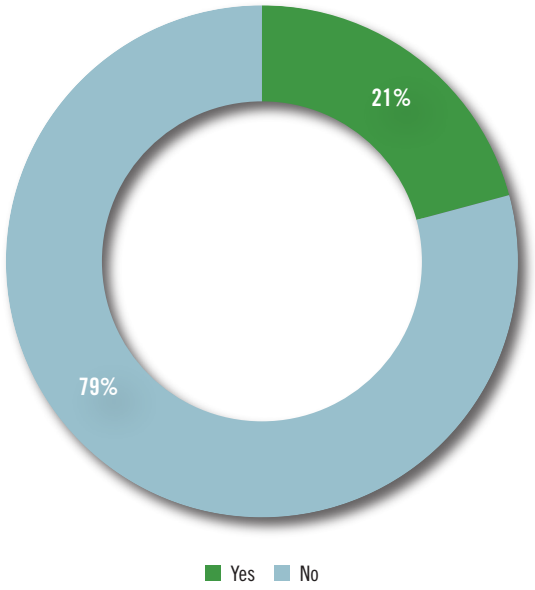
Annual training is marginally adequate, but only if it is accompanied by periodic and random testing to determine the efficacy of the training. Notably, companies that engage in the most regular training – two to four times per year – are the ones that truly understand that the risk of a breach offsets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

INSURANCE IN PLACE – BUT DETAILS FOGGY

Do you have cyber liability insurance?

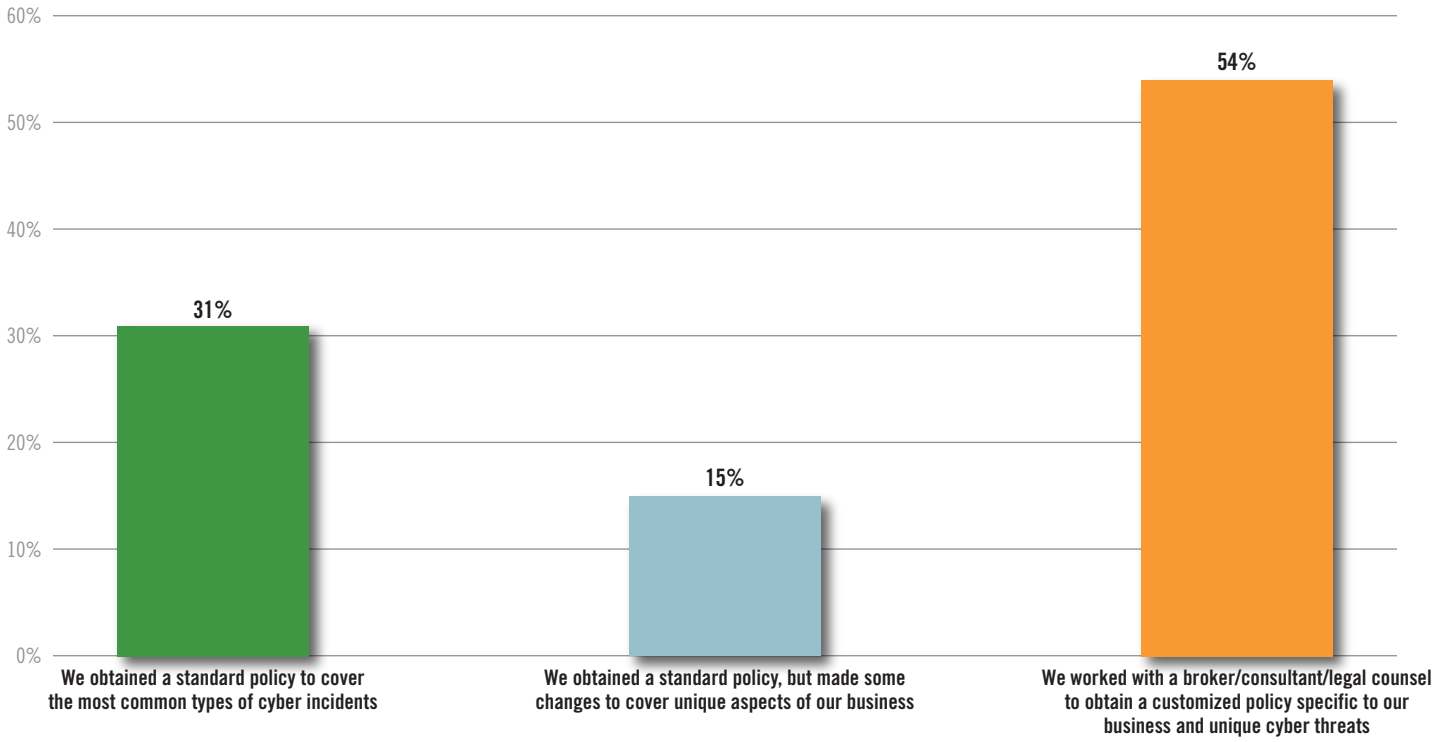


Within the past five years, have you filed a claim?



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.

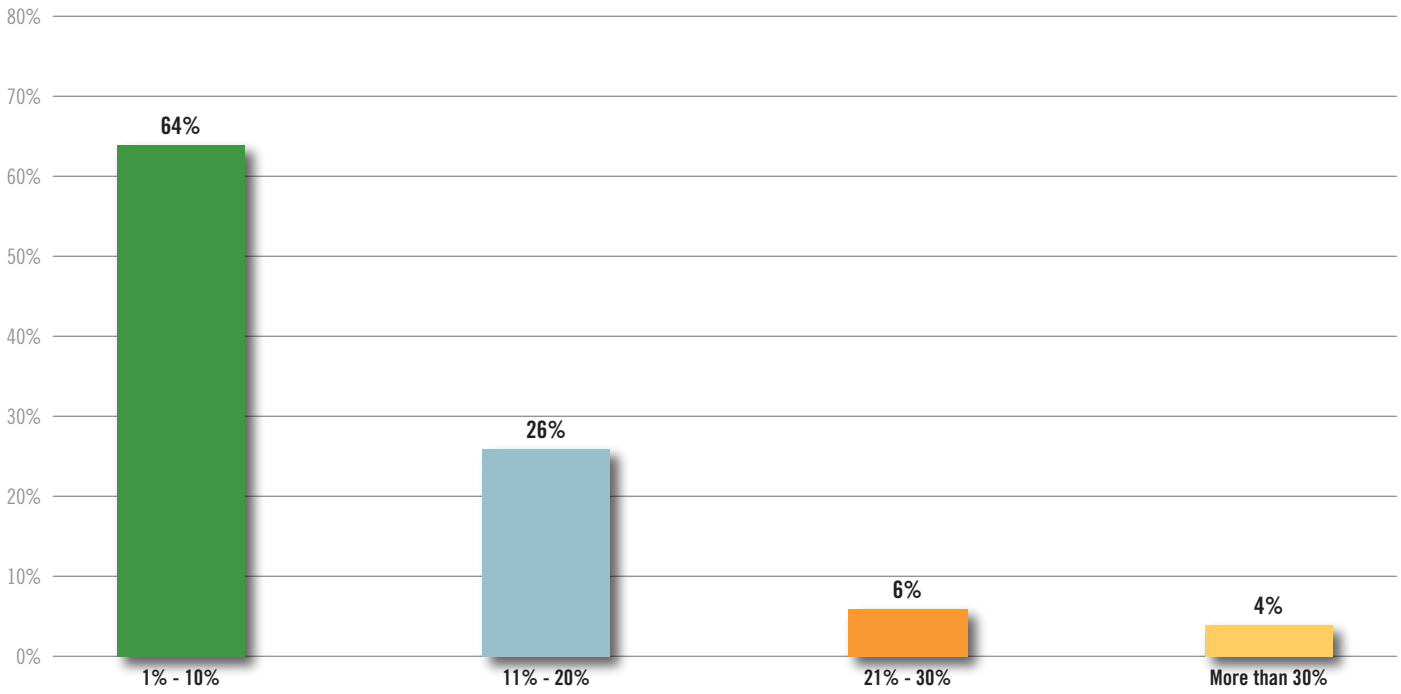
"Unfortunately, cyber insurance remains non-standardized," says Litten. "In the health care industry, for example, there are wildly different expectations of the levels of coverage needed under a cyber liability insurance policy, and there are significant variations in policy terms."

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."

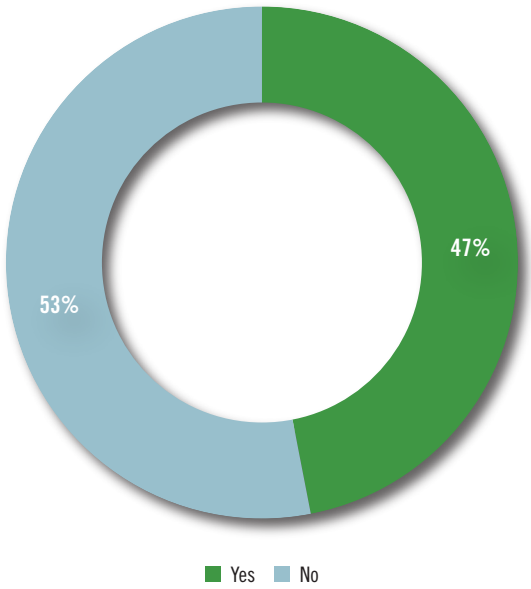
SECURITY QUESTIONS ON BUDGET AND STAFFING

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

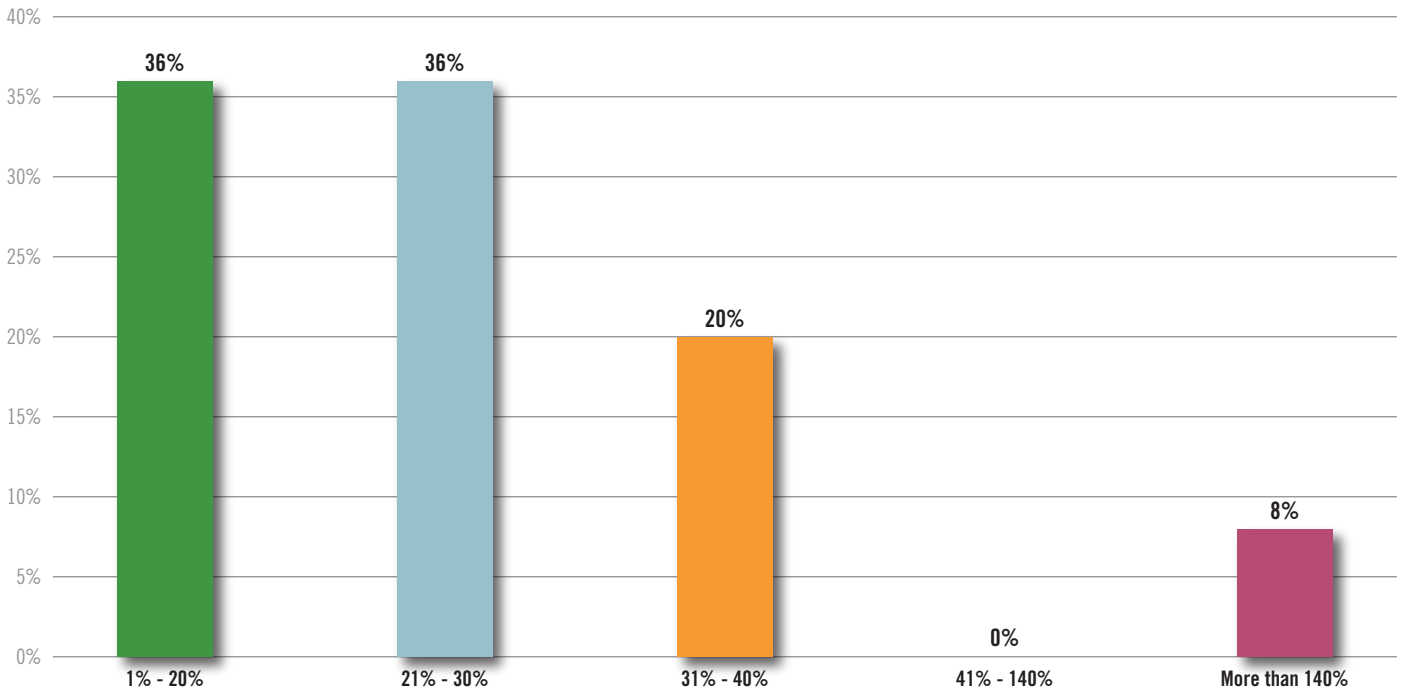


Only 36 percent of survey participants reported spending more than a tenth of their IT budgets on cybersecurity and data privacy, which is barely adequate, according to experts. A mere 4 percent of respondents dedicate more than 30 percent of their IT budgets to these efforts.

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?

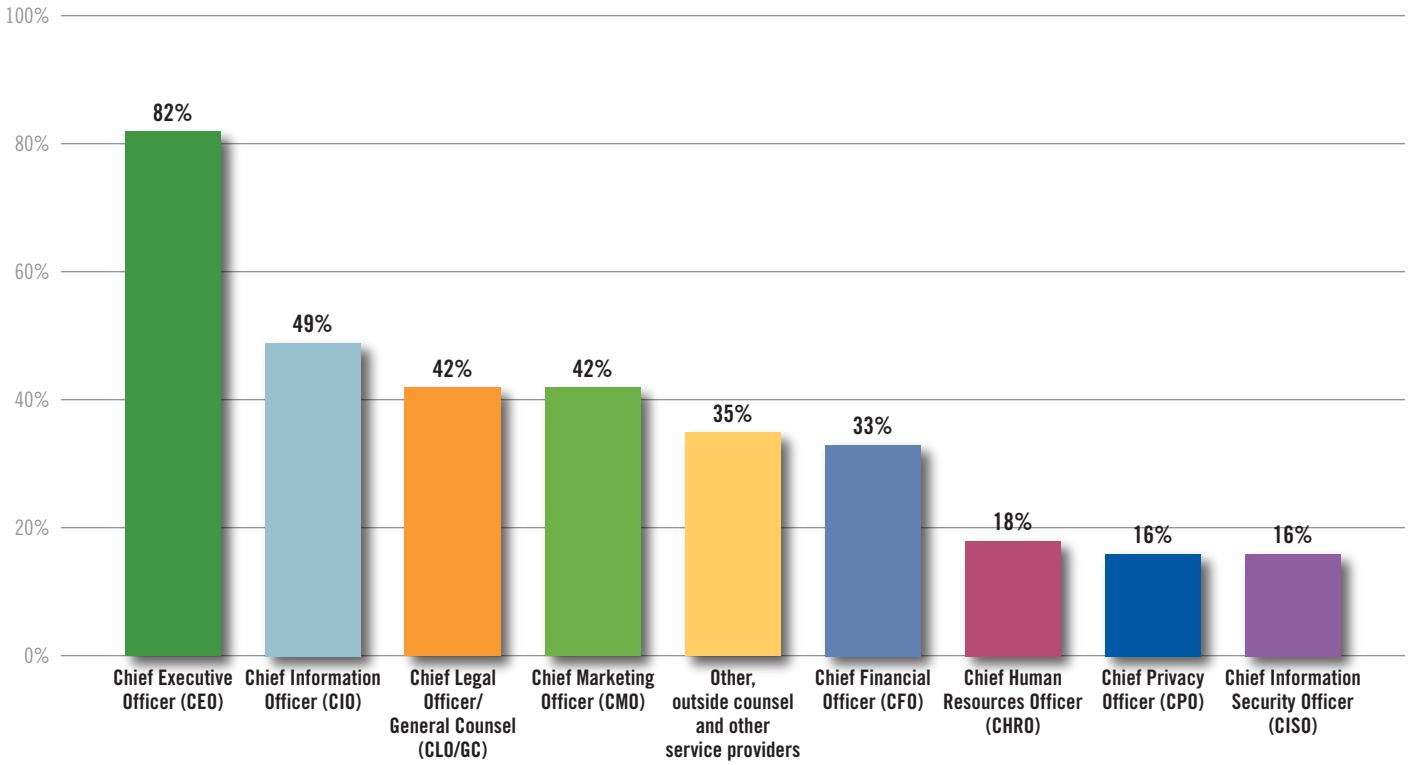


And yet a majority of respondents conceded that their budget – regardless of the level – is insufficient to respond to a breach. Eight percent reported they need a 140 percent or more boost. As for the 47 percent who believe their current spending to be at an appropriate level, a review of their allocations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

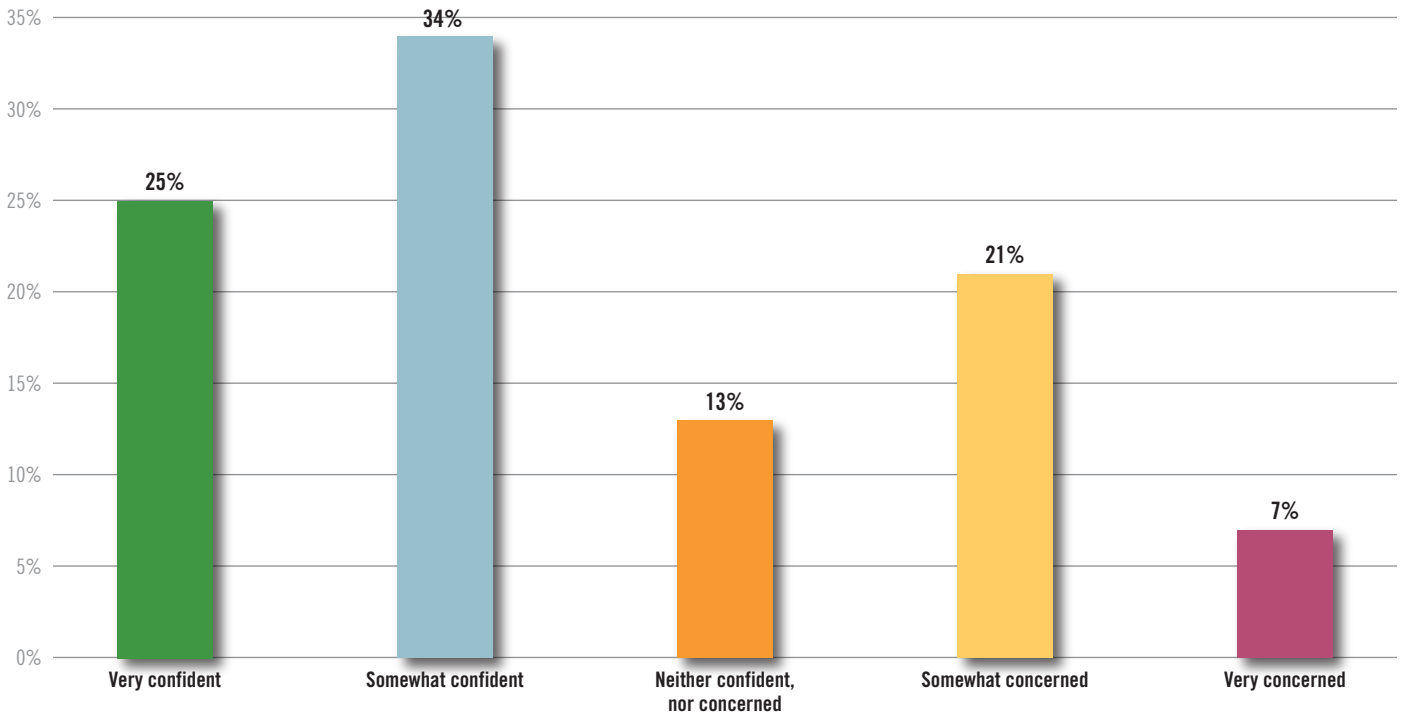
Some businesses have not even taken the step of making a plan for a cybersecurity incident response, despite the fact that most companies today have long since accepted the need to plan for other types of disasters.

"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?

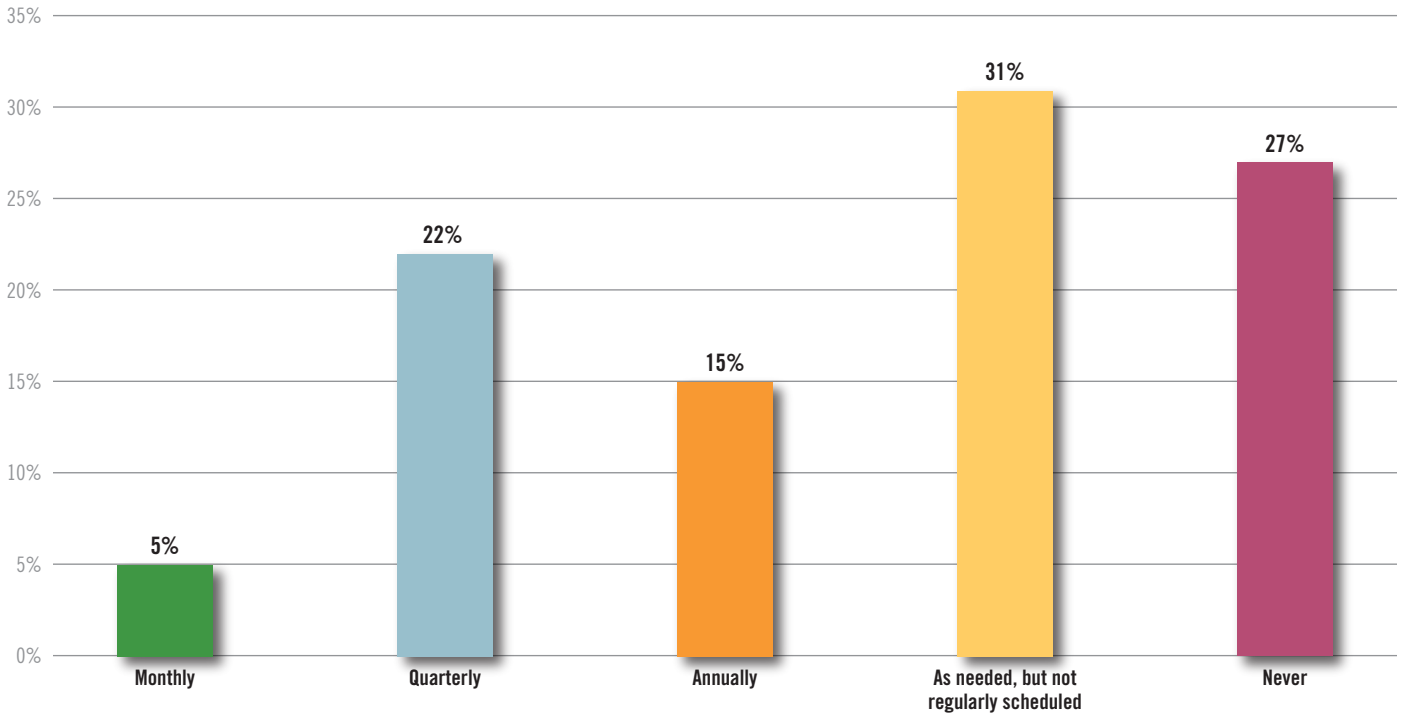


Most respondents indicated some level of confidence in their companies' cybersecurity and data privacy programs, including a quarter who are very confident and 34 percent who are somewhat confident.

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

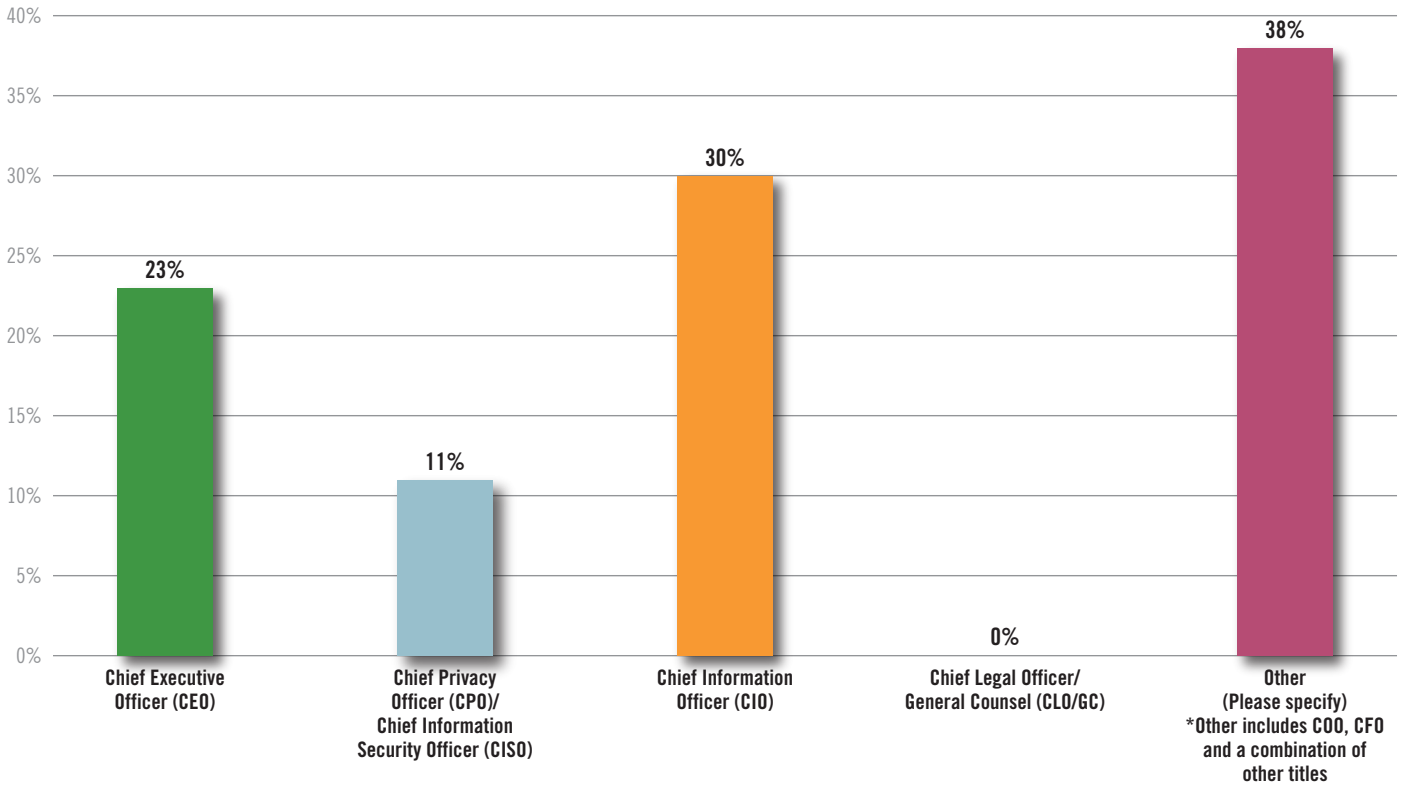
"In the health care industry, there is rampant and widespread fear over hacking," Litten says. "So many of them painfully recall May 2017, when the WannaCry attack hit, which was especially hard on hospitals and others in the health care industry. For U.S. health care entities subject to HIPAA, ransomware 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?

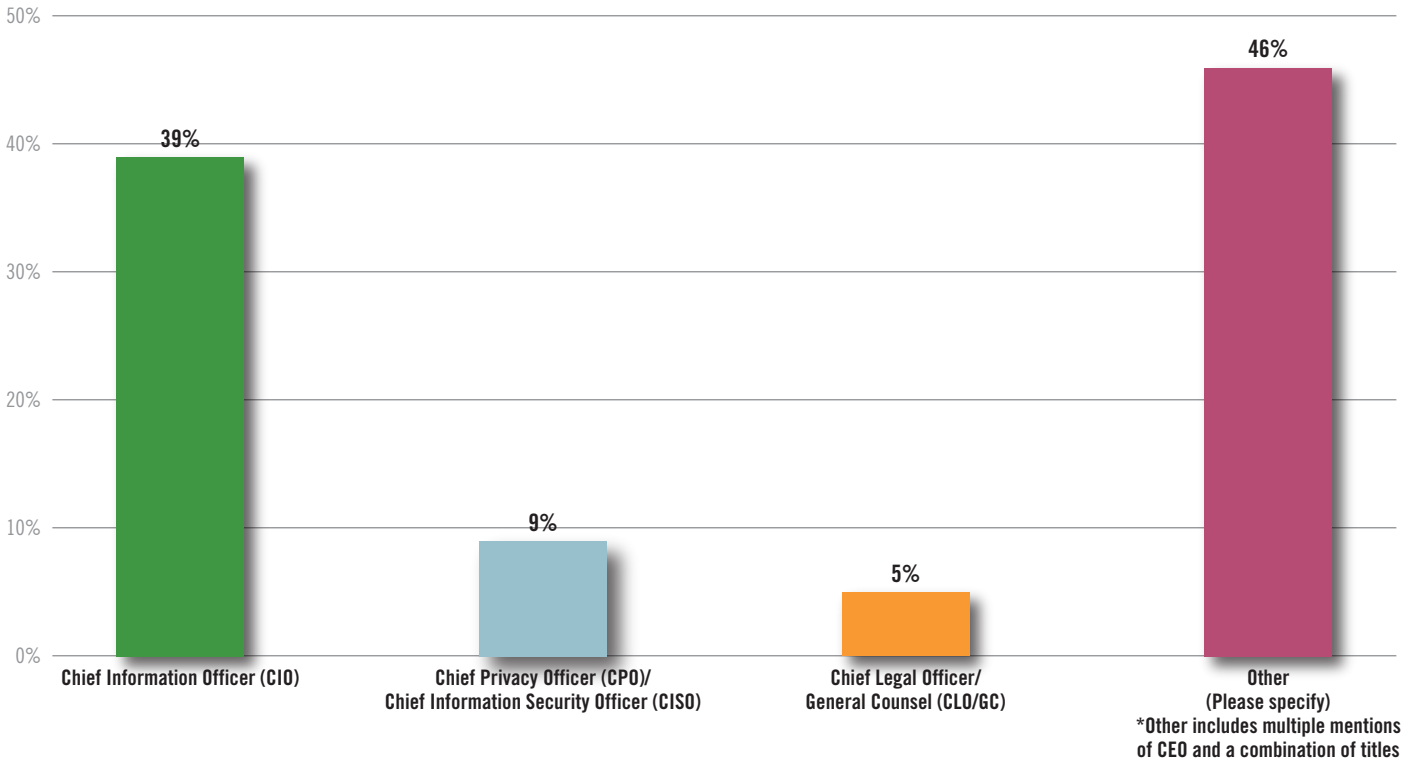


The responsibility to inform directors varies among company officers. Survey results indicated that no one officer role is predominantly tasked with this, although 30 percent reported assigning this duty to the chief information officer.

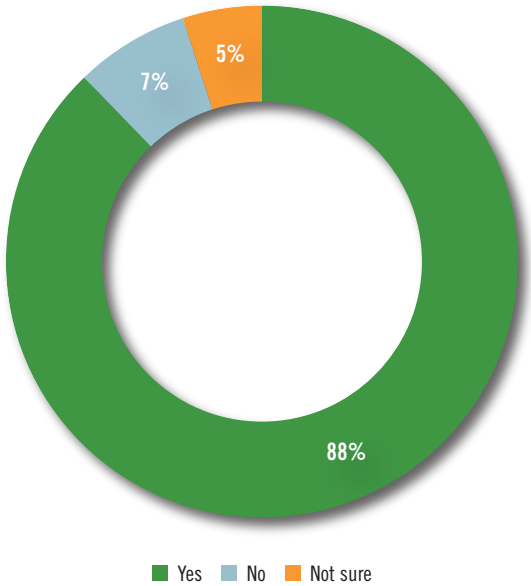
Cybersecurity professionals recommend that a chief technology, privacy or information security officer update the board. Whoever takes on the responsibility must be unquestioningly adept at explaining the threats to the business, providing options to address those threats and delivering all relevant 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?

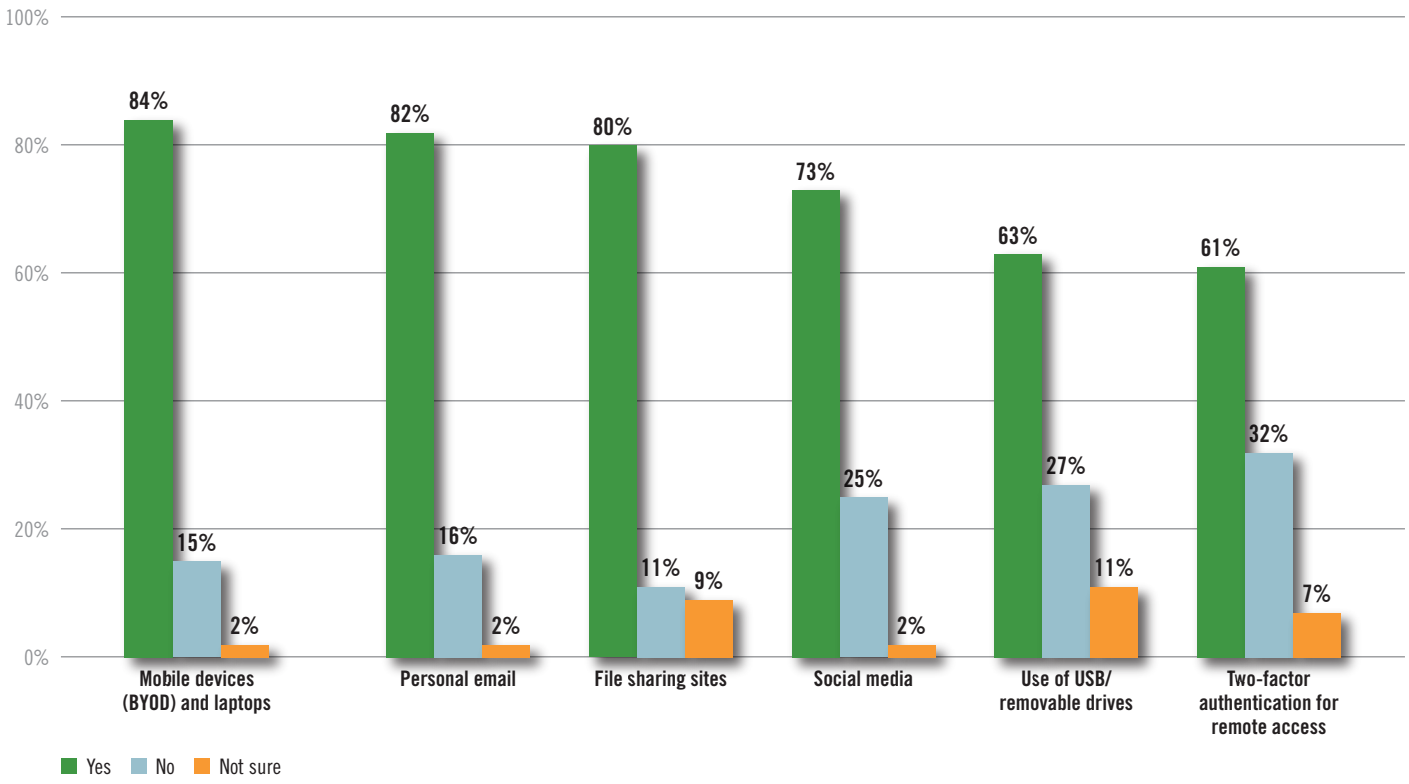


Do you have policies and procedures in place governing employees' handling of electronic data?



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?



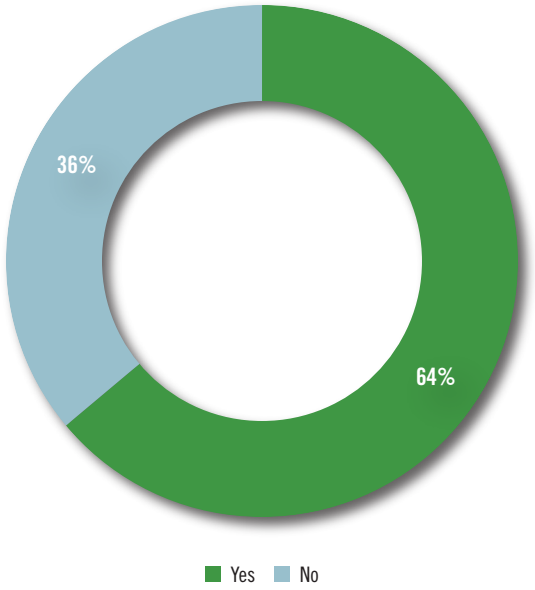
"We don't effectively address bring-your-own-device policies," said the general counsel of a San Francisco-based tech service company. "To do it well, you have to have the right to completely delete all the device's data. People would revolt."

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.

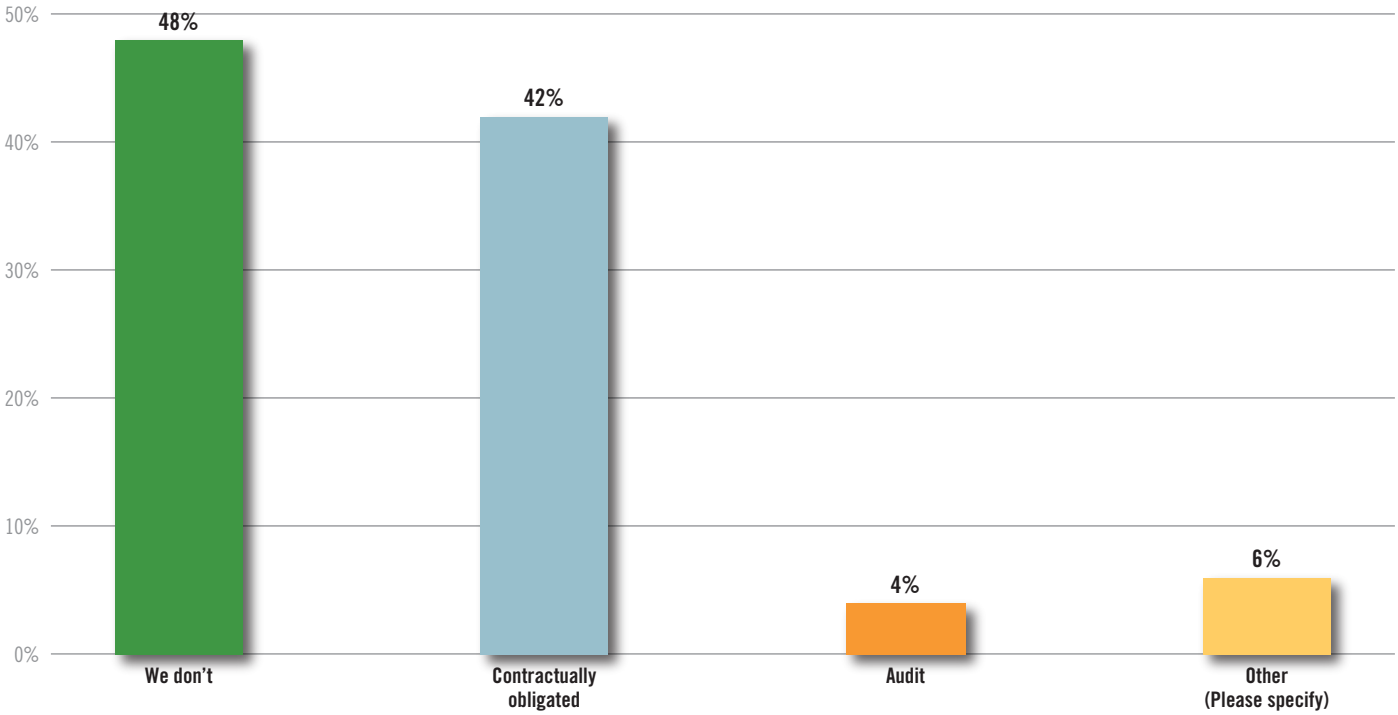
"By regularly auditing its data and security policies, practices and protocols, a company can identify what's working and what needs improvement," McCreary says. "Should a company find itself in the unfortunate position of experiencing multiple data breaches, scrutiny is likely to ensue, and the Federal 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.

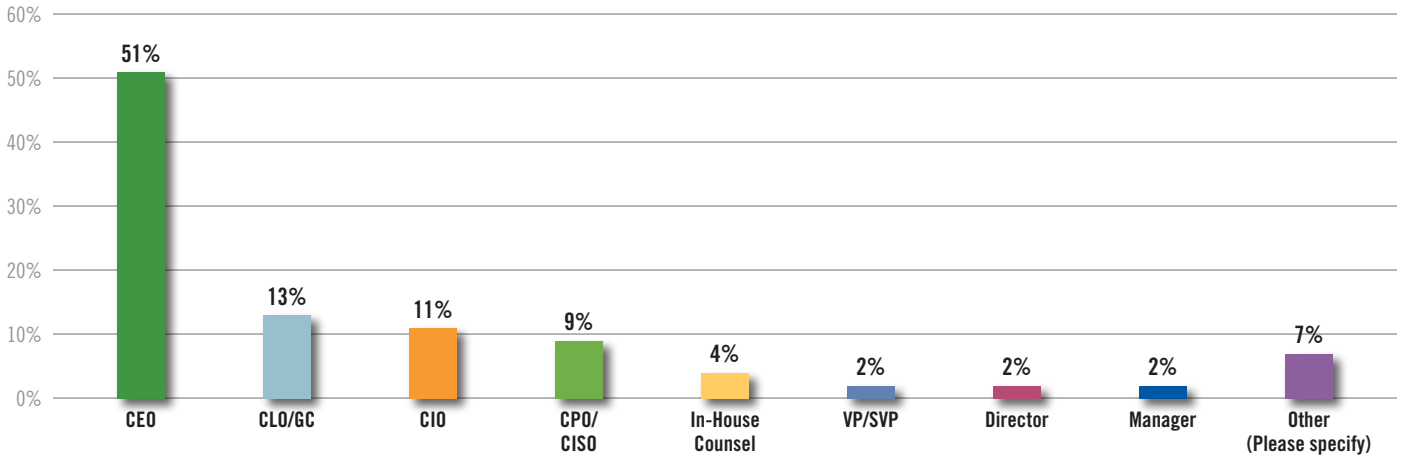
Nonetheless, every organization must take steps to ensure that vendors and partners are protecting data. New York law now requires organizations to incorporate third parties in mandatory cybersecurity risk assessments.

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.

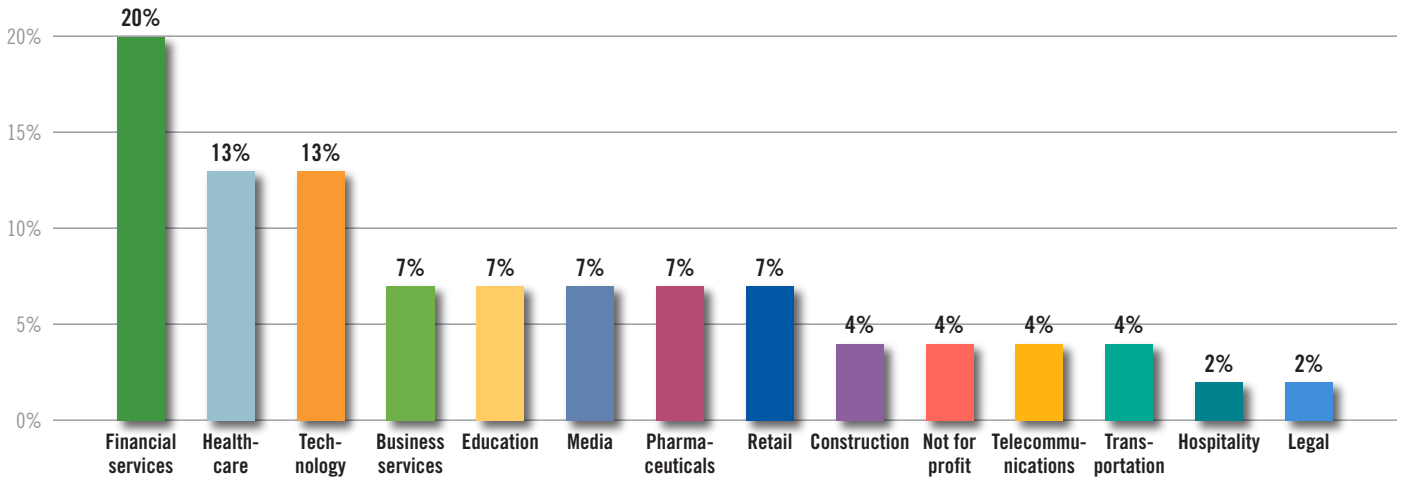
"We had all of our IT outsourced to a company that grew into the virtual world without telling us what was involved in terms of the risk," explained the CEO of a medical device research company. "Because of our size and the amount of data we stored, we decided to bring it all in-house."

RESPONDENT DEMOGRAPHICS

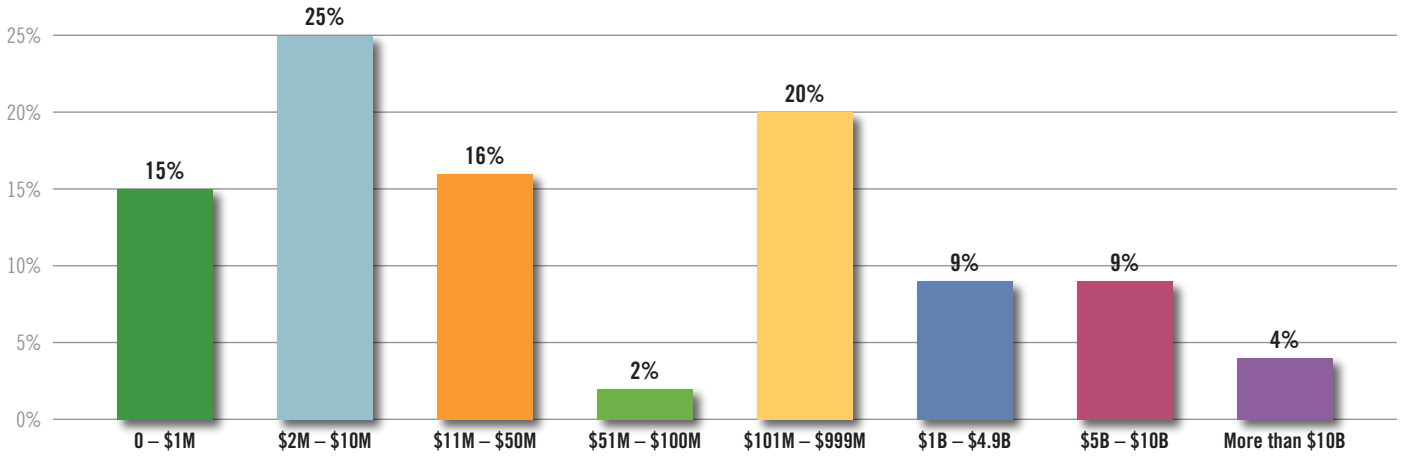
Which of the following most closely matches your job title?



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

Copyright © 2018 Fox Rothschild LLP. All rights reserved. Fox Rothschild LLP is a national law firm with offices throughout the United States. For more information, visit www.foxrothschild.com. This publication is intended for general information purposes only. It does not constitute legal advice. The reader should consult with knowledgeable legal counsel to determine how applicable laws apply to specific facts and situations. This publication is based on the most current information at the time it was written. Since it is possible that the laws or other circumstances may have changed since publication, please call us to discuss any action you may be considering as a result of reading this publication.