PROGRAM MATERIALS
Program #30112
April 14, 2020

# COVID-19 and Privacy Law – A Balancing Act



Celesq® AttorneysEd Center
www.celesq.com

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

# COVID-19 and Privacy Law
# A Balancing Act

Michelle Schaap, Nicole DiMaria
Chiesa Shahinian & Giantomasi PC
April 14, 2020

# BEFORE WE BEGIN…

This outline has been prepared for a presentation regarding COVID-19 and Privacy Laws – A Balancing Act. Ms. Schaap and Ms. DiMaria are each admitted to practice law in the State of New Jersey. This outline is for informational purposes only and is not intended to constitute legal advice. Every matter has specific facts and special circumstances requiring its own analysis by legal counsel. References to websites, resources or publications in this outline are not intended, and should not be interpreted, as an endorsement by the authors of any product or opinion set forth therein. Website and resource addresses are provided for reference only and the presenters make no guarantee as to their accuracy or reliability.

CSG
Chiesa Shahinian & Giantomasi PC

# AGENDA

- Introduction
- HIPAA Applicability and Permitted Disclosures
- Other Privacy Law Applicability
- Practical Considerations
- Q&A

# INTRODUCTION


- Health Information Privacy vs. Public Health:
  - Privacy law includes exceptions for certain uses/disclosures impacting public health and safety
- Another key exception: written authorization of individual
- Common themes: reasonableness and "minimum necessary"
- Even if specific privacy regulatory scheme does not apply, voluntary compliance may be desirable



CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA – What is It?

- Health Insurance Portability and Accountability Act of 1996
- Privacy Rule - 45 C.F.R., Part 160, and Part 164, Subpart E.
- Security Rule - 45 C.F.R., Part 160, and Part 164, Subpart C
- Breach Notification Rule
- HITECH - amends parts of both Privacy Rule and Security Rule and implements Breach Notification Rule

CSG
Chiesa Shahinian & Giantomasi PC

# WHO IS RESPONSIBLE FOR COMPLIANCE?

- "Covered Entities":
  - Health care providers who transmit health care info in electronic form in connection with certain "transactions"
  - Health plans
  - Health care clearinghouses

CSG
Chiesa Shahinian & Giantomasi PC

# Who is Responsible for Compliance? Business Associates

- "Business Associate" - generally, outside companies and consultants that perform services "on behalf of" the Covered Entity involving the use or disclosure of health information
- "Business Associate Agreement"

# WHAT IS COVERED?

- "Protected Health Information" (PHI)
- Essentially, individually identifiable information that relates to health care and is received by Covered Entity (or a Business Associate on behalf of a Covered Entity)
- Bottom Line: HIPAA does not apply to most businesses



CSG
Chiesa Shahinian & Giantomasi PC

# INDIRECT HIPAA APPLICABILITY – EMPLOYER GROUP HEALTH PLAN

- HIPAA does not apply to "employers" as a class, but generally applies to employer "group health plans"
- HIPAA obligations apply to *information disclosed from the group health plan to the employer*
- COVID-19 diagnosis disclosed directly *by employee to employer* would not implicate HIPAA

CSG
Chiesa Shahinian & Giantomasi PC

# Even When HIPAA Applies, It Does Not Apply to All Health Information

- HIPAA does not apply to all health information held by Covered Entity or Business Associate
- Only applies to information held in the context of health care or other functions that make the entity a Covered Entity or Business Associate
- E.g., Does not apply to health information held by Covered Entity in the context of employment and held in personnel file (e.g., employment disability leave information)



CSG
Chiesa Shahinian & Giantomasi PC

# WHEN HIPAA WOULD CLEARLY APPLY…

- COVID-19 diagnosis of Covered Entity patient
- HIPAA prohibits use or disclosure of a patient's health information without the patient's written authorization UNLESS AN EXCEPTION APPLIES



CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA Exceptions

- Treatment
- Public Health
- Disclosures to Family, Friends, and Others
- Disclosures to Prevent a Serious and Imminent Threat




CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA Exceptions - Treatment

- Treatment – PHI may be used/disclosed as necessary to treat the patient or to treat a different patient; includes:
  - Coordination or management of health care and related services between healthcare providers
  - Consultation between providers
  - Referral of patients

CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA Exceptions - Public Health

- PHI may be disclosed:
  - To a public health authority (e.g., CDC or a state or local health department) for purposes of disease reporting
  - To persons at risk of contracting disease if authorized by other law (e.g., state law) to prevent or control spread of disease

CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA Exceptions - Disclosures to Family, Friends, and Other Involved Individuals

- May disclose PHI:
  - to patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care; or
  - as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death

  **IF:**
- Get verbal permission from patient or otherwise able to reasonably infer patient does not object; or
- If patient incapacitated or not available, may disclose if, in provider's professional judgment, disclosure is in patient's best interest



CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA Exceptions - Disaster Relief Notification

- May share PHI with disaster relief organizations (e.g., Red Cross) to coordinate notification of family members or others involved in patient's care of patient's location, general condition or death
- Do not need patient's authorization if doing so would interfere with disaster relief organization's ability to respond to emergency

CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA Exceptions - Facility Directories

- If patient does not object, may maintain following information in facility directory and disclose for directory purposes to (i) members of clergy or (ii) *others who identify patient by name*:
  - Patient's name
  - Patient's location in the covered health care provider's facility
  - Patient's condition described in general terms that does not communicate specific medical information about the individual (e.g., critical or stable, deceased, or treated and released); and
  - Patient's religious affiliation (only applies to clergy request)

# HIPAA Exceptions - Disclosures to Prevent a Serious and Imminent Threat

- May share PHI to anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public
- Must be consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct
- Deference to professional judgment of health professionals in making determinations about nature and severity of the threat to health and safety



CSG
Chiesa Shahinian & Giantomasi PC

# NOTE ABOUT DISCLOSURES TO MEDIA/PUBLIC

- Not specifically permitted without patient (or personal representative) authorization
- Could be reported as part of facility directory exception




CSG
Chiesa Shahinian & Giantomasi PC

# HIPAA - Minimum Necessary Standard

- Must make reasonable efforts to limit the information disclosed to the "minimum necessary" to accomplish the purpose of disclosure
- Applies to most disclosures (treatment is notable exception)
- May rely on certain requestor's representations that the information requested is the minimum necessary
  - E.g., public health authority like CDC

# HIPAA - Reasonableness

- "Reasonableness" = an element in many HIPAA requirements/exceptions
  - Must use "reasonable safeguards" to protect privacy and security of information
- Always document any subjective element of PHI disclosure decisions

# COVID-19 Related HIPAA Enforcement Waivers

- Office of Civil Rights (OCR) has waived certain sanctions/penalties for duration of COVID-19 public health emergency; for instance enforcement waivers for the following:
  - Hospitals for:
    - the requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care
    - the requirement to honor a request to opt out of the facility directory
    - the requirement to distribute a notice of privacy practices
    - the patient's right to request privacy restrictions
    - the patient's right to request confidential communications
  - Good faith use of telehealth technology in rendering telemedicine services



CSG
Chiesa Shahinian & Giantomasi PC

# If you are not a healthcare provider or business Associate…

- In the US, there is a patchwork of state-proactive legislation, as well as sector targeted legislation
- Even in time of crisis, these laws cannot be ignored
  - And with a remotely working staff, the risk of violations increases dramatically
- And 50 states have 50 different breach notification requirements
- Plus data retention/destruction laws



CSG
Chiesa Shahinian & Giantomasi PC

# NY Laws

- NY SHIELD Act applies to any business or entity that holds information regarding residents of NY
  - This legislation specifically speaks to employee related information
    - If you are taking your personnel's temperature before they are permitted onsite, are you storing this data?

# NYS-DFS Regulations

- The NY State Division of Financial Services Cyber Security Regulations (as does the NY SHIELD Act) requires businesses to vet their vendors
  - If your vendors are working remotely, how are those vendors securing their personnel and their environments as they “process” your data?

CSG
Chiesa Shahinian & Giantomasi PC

# CCPA

- The California Consumer Privacy Act, effective as of January 1, 2020, will be enforced as of July 1, 2020 – notwithstanding the COVID outbreak
  - If you have not already mapped your data to understand where all your data regarding CA residents are within your systems, doing so now in response to a consumer request will be challenging

CSG
Chiesa Shahinian & Giantomasi PC

# CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT

- Prohibits employers from using, disclosing or knowingly permitting the disclosure of "medical information which the employer possesses pertaining to its employees without the patient having first signed an authorization . . . ,"
- However, this Act does not speak to information that employers gather directly (only from healthcare provider)

CSG
Chiesa Shahinian & Giantomasi PC

# AMERICANS WITH DISABILITY ACT

- According to the EEOC,
  - ADA-covered employers are permitted to ask employees who call in sick whether they have symptoms of the pandemic virus. An employer may also take an employee's temperature before allowing them to enter the workplace

# EDUCATION TECHNOLOGY PROVIDERS: … A (SLIGHT) RELAXATION OF COPPA

- COPPA generally requires companies that collect personal information online from children under age 13 to provide notice of data collection and use practices, and obtain verifiable parental consent
- On April 9, 2020, the Federal Trade Commission ("FTC") issued guidance under the Children's Online Privacy Protection Act ("COPPA") for operators of educational technology:
  - In the educational context, schools can consent on behalf of parents to the collection of student personal information.
    - information must be used for a school-authorized educational purpose ONLY
    - service provider must still provide COPPA-required notice of its data collection and use practices.
      - And schools should make this information available to parents
    - Service providers should be able to delete personal information collected on request



CSG
Chiesa Shahinian & Giantomasi PC

# EVEN WITH PROACTIVE LEGISLATION IN MORE THAN 30 STATES, PRIVACY LAWS ARE SEEING EXCEPTIONS, AND IF WASHINGTON HAS ITS WAY….

- There are reports that the White House, under Jared Kushner, is planning to create a national coronavirus surveillance system to more precisely track where patients are seeking treatment
- The plan would gather information about hospital visits and treatments from multiple private-sector databases.
- While the White House has denied that this plan even exists, the details that have come out suggest otherwise…
  - And once the ability and data is out there, what else will it be used for in the name of national security?

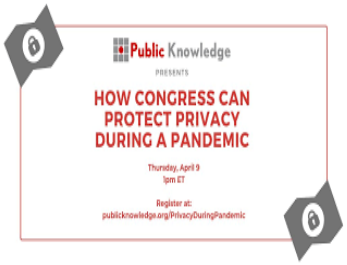
https://www.law360.com/health/articles/1261801/senate-dem-says-surveillance-not-way-to-fight-coronavirus?copied=1

CSG
Chiesa Shahinian & Giantomasi PC

# PUBLIC KNOWLEDGE, THE NOT FOR PROFIT ADVOCATE IS URGING

- "All response measures should be temporary in nature, limited in scope, restricted to using anonymized aggregate data wherever possible, and adopted only if they are a necessary response and the safety of the public."




- https://www.publicknowledge.org/documents/public-knowledge-letter-on-enlisting-big-data-in-fight-against-coronavirus/

CSG
Chiesa Shahinian & Giantomasi PC

# GDPR – RECITAL 46 ADDRESSES EPIDEMICS:

- "The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest ... for instance when processing is necessary for ... for monitoring epidemics and their spread."

# New Zealand's Privacy Commissioner Declared….

- "It will not be a breach of the Privacy Act for any accommodation provider or tourism operator to notify a medical officer or police officer of someone noncompliant with self-isolation obligations."

CSG
Chiesa Shahinian & Giantomasi PC

# ITALY, TOO….

- On February 3, 2020, Italy suspended certain data protection rights with the adoption of its Decree Non. 630 to combat the spread of COVID 19



CSG
Chiesa Shahinian & Giantomasi PC

# PERU, HOWEVER…

- Peruvian National Authority for the Protection of Personal Data warned that the disclosure of personal data of patients with COVID-19, ***without their consent***, is a violation of the Personal Data Protection Law, which can be sanctioned with fines up to $53,800.

CSG
Chiesa Shahinian & Giantomasi PC

# ASIDE FROM THE LAW, LET'S THINK SAFETY… FOR FIRST RESPONDERS

- In Maine and Florida, first responders are being provided information as to whether the residence to which they are being dispatched has a known case of COVID, so that first responders can be properly prepared responding to an emergency call.

CSG
Chiesa Shahinian & Giantomasi PC

# BEFORE WE WERE SHELTERING IN PLACE

- Businesses, landlords and tenants were grappling with what to disclose and to whom if there was a person on site diagnosed with COVID 19

CSG
Chiesa Shahinian & Giantomasi PC

# SO WHAT SHOULD YOUR BUSINESS BE DOING?

- Businesses, even if not subject to proactive privacy laws, are subject to breach notification laws if they disclose or have compromised personally identifiable information about individuals (whether employees or otherwise)



CSG
Chiesa Shahinian & Giantomasi PC

# COMPANIES SHOULD BE MINDFUL ABOUT

- What information they collect during this (or any other) crisis about its personnel and other office visitors
- How long that information is retained
- Where is the information stored
- Who can access this information
- Third party processor considerations
- Retention and destruction policies




CSG
Chiesa Shahinian & Giantomasi PC

# REMOTE WORKFORCE LEFT UNCHECKED…

"The risk of negligent employees and contractors causing a data breach or ransomware is getting worse. **Sixty percent** of respondents in companies that had a data breach say the **root cause of the data breach was a negligent employee or contractor,** …. **Sixty-one** percent of respondents say **negligent employees put their company at risk for a ransomware attack…**

https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf



CSG
Chiesa Shahinian & Giantomasi PC

# SAFEGUARD YOUR VIDEOCONFERENCES:

- Do not make meetings or classrooms public. Instead, either set a password or set up a waiting room and admit only intended participants
- Do not share the link to the conference through an unrestricted public post
- Restrict screen sharing to the host unless otherwise necessary
- Use meeting passwords


- Make sure that participants are using the most recent version of the platform
- Lock the meeting after all invited participants “arrive”

CSG
Chiesa Shahinian & Giantomasi PC

# Mitigate Third Party Risks

- Remember that your customers and vendors are now also largely working remotely
- Vet new AND existing vendors
  - Ask how they are securing and managing their remote work forces
  - Ask what they have done to secure their videoconferencing
  - Assess their practices… and ask for confirmation




CSG
Chiesa Shahinian & Giantomasi PC

# WHERE IS YOUR INCIDENT RESPONSE PLAN AND DO YOU NEED TO (TEMPORARILY) UPDATE POINTS OF CONTACT FOR THE INCIDENT RESPONSE TEAM?


- Data breaches will not happen conveniently….
  - And IF you are not in your office… or you were hit by ransomware, the incident response plan that is stored on your computer or at your office is NOT going to help!
- Review your points of contact…
  - Do you have home numbers? Cell numbers?
  - Home email addresses?



CSG
Chiesa Shahinian & Giantomasi PC

# RESOURCES:

- EEOC:
  - https://www.eeoc.gov/eeoc/newsroom/wysk/wysk_ada_rehabilitaion_act_coronavirus.cfm
- State Data Breach Laws:
  - https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
- State Internet Privacy Laws:
  - https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx
- State Data Disposal Laws:
  - https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx



CSG
Chiesa Shahinian & Giantomasi PC

# THANK YOU


**Michelle Schaap**

Member, Privacy & Data Security
Chiesa Shahinian & Giantomasi PC
973.530.2026
mschaap@csglaw.com



**Nicole DiMaria**

Member & Practice Group Leader, Healthcare & Hospital
Chiesa Shahinian & Giantomasi PC
973.530.2111
ndimaria@csglaw.com


CSG
Chiesa Shahinian & Giantomasi PC

*U.S. Equal Employment Opportunity Commission*

# What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws

*Technical Assistance Questions and Answers - Updated on April 9, 2020*

- *All EEOC materials related to COVID-19 are collected at www.eeoc.gov/coronavirus.*
- The EEOC enforces workplace anti-discrimination laws, including the Americans with Disabilities Act (ADA) and the Rehabilitation Act (which include the requirement for reasonable accommodation and non-discrimination based on disability, and rules about employer medical examinations and inquiries), Title VII of the Civil Rights Act (which prohibits discrimination based on race, color, national origin, religion, and sex, including pregnancy), the Age Discrimination in Employment Act (which prohibits discrimination based on age, 40 or older), and the Genetic Information Nondiscrimination Act.
- The EEO laws, including the ADA and Rehabilitation Act, continue to apply during the time of the COVID-19 pandemic, but they do not interfere with or prevent employers from following the guidelines and suggestions made by the CDC or state/local public health authorities about steps employers should take regarding COVID-19. **Employers should remember that guidance from public health authorities is likely to change as the COVID-19 pandemic evolves. Therefore, employers should continue to follow the most current information on maintaining workplace safety.**
- The EEOC has provided guidance (a publication entitled Pandemic Preparedness in the Workplace and the Americans With Disabilities Act [PDF version]), consistent with these workplace protections and rules, that can help employers implement strategies to navigate the impact of COVID-19 in the workplace. This pandemic publication, which was written during the prior H1N1 outbreak, is still relevant today and identifies established ADA and Rehabilitation Act principles to answer questions frequently asked about the workplace during a pandemic. It has been updated as of March 19, 2020 to address examples and information regarding COVID-19; **the new 2020 information appears in bold**.
- The World Health Organization (WHO) has declared COVID-19 to be an international pandemic. The EEOC pandemic publication includes a separate section that answers common employer questions about what to do after a pandemic has been declared. Applying these principles to the COVID-19 pandemic, the following may be useful:

## A. Disability-Related Inquiries and Medical Exams

**A.1. How much information may an employer request from an employee who calls in sick, in order to protect the rest of its workforce during the COVID-19 pandemic?** *(3/17/20)*

During a pandemic, ADA-covered employers may ask such employees if they are experiencing symptoms of the pandemic virus. For COVID-19, these include symptoms such as fever, chills, cough, shortness of breath, or sore throat. Employers must maintain all information about employee illness as a confidential medical record in compliance with the ADA.

**A.2. When screening employees entering the workplace during this time, may an employer only ask employees about the COVID-19 symptoms EEOC has identified as examples, or may it ask about any symptoms identified by public health authorities as associated with COVID-19?** *(4/9/20)*

As public health authorities and doctors learn more about COVID-19, they may expand the list of associated symptoms. Employers should rely on the CDC, other public health authorities, and reputable medical sources for guidance on emerging symptoms associated with the disease. These sources may guide employers when choosing questions to ask employees to determine whether they would pose a direct threat to health in the workplace. For example, additional symptoms beyond fever or cough may include new loss of smell or taste as well as gastrointestinal problems, such as nausea, diarrhea, and vomiting.

**A.3. When may an ADA-covered employer take the body temperature of employees during the COVID-19 pandemic?** *(3/17/20)*

Generally, measuring an employee's body temperature is a medical examination. Because the CDC and state/local health authorities have acknowledged community spread of COVID-19 and issued attendant precautions, employers may measure employees' body temperature. However, employers should be aware that some people with COVID-19 do not have a fever.

**A.4. Does the ADA allow employers to require employees to stay home if they have symptoms of the COVID-19?** *(3/17/20)*

Yes. The CDC states that employees who become ill with symptoms of COVID-19 should leave the workplace. The ADA does not interfere with employers following this advice.

**A.5. When employees return to work, does the ADA allow employers to require a doctor's note certifying fitness for duty?** *(3/17/20)*

Yes. Such inquiries are permitted under the ADA either because they would not be disability-related or, if the pandemic influenza were truly severe, they would be justified under the ADA standards for disability-related inquiries of employees. As a practical matter, however, doctors and other health care professionals may be too busy during and immediately after a pandemic outbreak to provide fitness-for-duty documentation. Therefore, new approaches may be necessary, such as reliance on local clinics to provide a form, a stamp, or an e-mail to certify that an individual does not have the pandemic virus.

## B. Confidentiality of Medical Information

**B.1. May an employer store in existing medical files information it obtains related to COVID-19, including the results of taking an employee's temperature or the employee's self-identification as having this disease, or must the employer create a new medical file system solely for this information?** *(4/9/20)*

The ADA requires that all medical information about a particular employee be stored separately from the employee's personnel file, thus limiting access to this confidential information. An employer may store all medical information related to COVID-19 in existing medical files. This includes an employee's statement that he has the disease or suspects he has the disease, or the employer's notes or other documentation from questioning an employee about symptoms.

**B.2. If an employer requires all employees to have a daily temperature check before entering the workplace, may the employer maintain a log of the results?** *(4/9/20)*

Yes. The employer needs to maintain the confidentiality of this information.

**B.3. May an employer disclose the name of an employee to a public health agency when it learns that the employee has COVID-19?** *(4/9/20)*

Yes.

**B.4. May a temporary staffing agency or a contractor that places an employee in an employer's workplace notify the employer if it learns the employee has COVID-19?** *(4/9/20)*

Yes. The staffing agency or contractor may notify the employer and disclose the name of the employee, because the employer may need to determine if this employee had contact with anyone in the workplace.

## C. Hiring and Onboarding

**C.1. If an employer is hiring, may it screen applicants for symptoms of COVID-19?** *(3/18/20)*

Yes. An employer may screen job applicants for symptoms of COVID-19 after making a conditional job offer, as long as it does so for all entering employees in the same type of job. This ADA rule applies whether or not the applicant has a disability.

**C.2. May an employer take an applicant's temperature as part of a post-offer, pre-employment medical exam?** *(3/18/20)*

Yes. Any medical exams are permitted after an employer has made a conditional offer of employment. However, employers should be aware that some people with COVID-19 do not have a fever.

**C.3. May an employer delay the start date of an applicant who has COVID-19 or symptoms associated with it?** *(3/18/20)*

Yes. According to current CDC guidance, an individual who has COVID-19 or symptoms associated with it should not be in the workplace.

**C.4. May an employer withdraw a job offer when it needs the applicant to start immediately but the individual has COVID-19 or symptoms of it?** *(3/18/20)*

Based on current CDC guidance, this individual cannot safely enter the workplace, and therefore the employer may withdraw the job offer.

**C.5. May an employer postpone the start date or withdraw a job offer because the individual is 65 years old or pregnant, both of which place them at higher risk from COVID-19?** *(4/9/20)*

No. The fact that the CDC has identified those who are 65 or older, or pregnant women, as being at greater risk does not justify unilaterally postponing the start date or withdrawing a job offer. However, an employer may choose to allow telework or to discuss with these individuals if they would like to postpone the start date.

## D. Reasonable Accommodation

*In discussing accommodation requests, employers and employees may find it helpful to consult the Job Accommodation Network (JAN) website for types of accommodations, www.askjan.org. JAN's materials specific to COVID-19 are at https://askjan.org/topics/COVID-19.cfm.*

**D.1. If a job may only be performed at the workplace, are there reasonable accommodations for individuals with disabilities absent undue hardship that could offer protection to an employee who, due to a preexisting disability, is at higher risk from COVID-19?** *(4/9/20)*

There may be reasonable accommodations that could offer protection to an individual whose disability puts him at greater risk from COVID-19 and who therefore requests such actions to eliminate possible exposure. Even with the constraints imposed by a pandemic, some accommodations may meet an employee's needs on a temporary basis without causing undue hardship on the employer.

Low-cost solutions achieved with materials already on hand or easily obtained may be effective. If not already implemented for all employees, accommodations for those who request reduced contact with others due to a disability may include changes to the work environment such as designating one-way aisles; using plexiglass, tables, or other barriers to ensure minimum distances between customers and coworkers whenever feasible per CDC guidance or other accommodations that reduce chances of exposure.

Flexibility by employers and employees is important in determining if some accommodation is possible in the circumstances. Temporary job restructuring of marginal job duties, temporary transfers to a different position, or modifying a work schedule or shift assignment may also permit an individual with a disability to perform safely the essential functions of the job while reducing exposure to others in the workplace or while commuting.

**D.2. If an employee has a preexisting mental illness or disorder that has been exacerbated by the COVID-19 pandemic, may he now be entitled to a reasonable accommodation (absent undue hardship)?** *(4/9/20)*

Although many people feel significant stress due to the COVID-19 pandemic, employees with certain preexisting mental health conditions, for example, anxiety disorder, obsessive-compulsive disorder, or post-traumatic stress disorder, may have more difficulty handling the disruption to daily life that has accompanied the COVID-19 pandemic.

As with any accommodation request, employers may: ask questions to determine whether the condition is a disability; discuss with the employee how the requested accommodation would assist him and enable him to keep working; explore alternative accommodations that may effectively meet his needs; and request medical documentation if needed.

**D.3. In a workplace where all employees are required to telework during this time, should an employer postpone discussing a request from an employee with a disability for an accommodation that will not be needed until he returns to the workplace when mandatory telework ends?** *(4/9/20)*

Not necessarily. An employer may give higher priority to discussing requests for reasonable accommodations that are needed while teleworking, but the employer may begin discussing this request now. The employer may be able to acquire all the information it needs to make a decision. If a reasonable accommodation is granted, the employer also may be able to make some arrangements for the accommodation in advance.

**D.4. What if an employee was already receiving a reasonable accommodation prior to the COVID-19 pandemic and now requests an additional or altered accommodation?** *(4/9/20)*

An employee who was already receiving a reasonable accommodation prior to the COVID-19 pandemic may be entitled to an additional or altered accommodation, absent undue hardship. For example, an employee who is teleworking because of the pandemic may need a different type of accommodation than what he uses in the workplace. The employer may discuss with the employee whether the same or a different disability is the basis for this new request and why an additional or altered accommodation is needed.

## E. Pandemic-Related Harassment Due to National Origin, Race, or Other Protected Characteristics

**E.1. What practical tools are available to employers to reduce and address workplace harassment that may arise as a result of the COVID-19 pandemic?** *(4/9/20)*

Employers can help reduce the chance of harassment by explicitly communicating to the workforce that fear of the COVID-19 pandemic should not be misdirected against individuals because of a protected characteristic, including their national origin, race, or other prohibited bases.

Practical anti-harassment tools provided by the EEOC for small businesses can be found here:

- Anti-harassment policy tips for small businesses
- Select Task Force on the Study of Harassment in the Workplace (includes detailed recommendations and tools to aid in designing effective anti-harassment policies; developing training curricula; implementing complaint, reporting, and investigation procedures; creating an organizational culture in which harassment is not tolerated):
  - report;
  - checklists for employers who want to reduce and address harassment in the workplace; and,
  - chart of risk factors that lead to harassment and appropriate responses.

## F. Furloughs and Layoffs

**F.1. Under the EEOC's laws, what waiver responsibilities apply when an employer is conducting layoffs?** *(4/9/20)*

Special rules apply when an employer is offering employees severance packages in exchange for a general release of all discrimination claims against the employer. More information is available in EEOC's technical assistance document on severance agreements.

Ponemon INSTITUTE

November 2018

# 2018 State of Cybersecurity in Small & Medium Size Businesses

Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC

KEEPER Cybersecurity Starts Here®

# 2018 State of Cybersecurity in Small & Medium Size Businesses (SMBs)

Ponemon Institute, November 2018

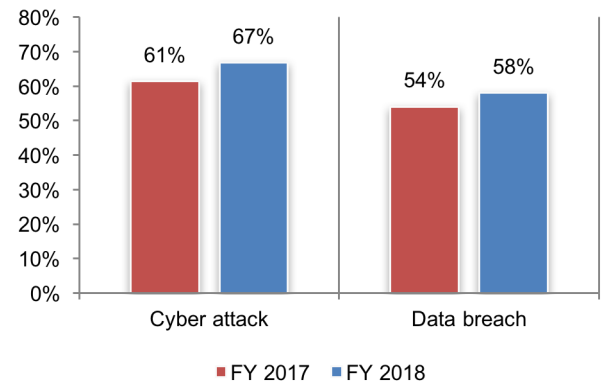
## Part 1. Executive summary

Small businesses increasingly face the same cybersecurity risks as larger companies, but only 28 percent of the companies represented in this study rate their ability to mitigate threats, vulnerabilities and attacks as highly effective. Most participants in this research say attacks against their companies are targeted and sophisticated with severe financial consequences. According to this study's findings, the weakest link in these companies' security posture is the negligent insider or contractor as they are considered the number one reason a company can have a data breach, phishing attack or a ransomware attack.

Ponemon Institute is pleased to present the results of *The 2018 State of Cybersecurity in Small and Medium Size Businesses* sponsored by Keeper Security. The goal of this study is to track how small and medium size companies address the same threats faced by larger companies. This report features the findings from 2018 and 2017.

**Figure 1. Our company experienced a cyber attack and data breach in the past 12 months**

Yes responses




This research's sample included approximately 1,045 individuals from companies in the United States and the United Kingdom; these companies had head counts ranging from less than 100 to 1,000. In this report, we present the consolidated findings for 2017 and 2018.

As Figure 1 illustrates, cyber attacks on SMBs have increased from 61 percent of respondents in 2017 to 67 percent of respondents in 2018. The occurrence of data breaches involving customer and employee information over 12 months also increased from 54 percent of respondents to 58 percent of respondents.

In the aftermath of these incidents, the respondents' companies spent an average of $1.43 million, a 33 percent increase from $1.03 million in 2017, because of the damage or theft of IT assets. In addition, disruption to normal operations cost an average of $1.56 million, a 25 percent increase from $1.21 million in 2017.

**Following are the most salient findings of this research.**

- Phishing attacks and advanced malware/zero day attacks are increasing. Respondents reported phishing/social engineering attacks increased from 48 percent in 2017 to 52 percent in 2018 and advanced malware/zero day attacks increased from 16 percent to 24 percent.

- The risk of negligent employees and contractors causing a data breach or ransomware is getting worse. Sixty percent of respondents in companies that had a data breach say the root cause of the data breach was a negligent employee or contractor, an increase from 54 percent in 2017. Sixty-one percent of respondents say negligent employees put their company at risk for a ransomware attack, an increase from 58 percent of respondents in 2017.

- More companies are affected by exploits and malware that evaded their intrusion detection system (72 percent of respondents) or anti-virus solution (82 percent of respondents).

- Mobile devices are the most vulnerable endpoints or entry points to networks and enterprise systems, according to 55 percent of respondents. Almost half (49 percent) of respondents say the use of mobile devices to access business-critical applications and IT infrastructure affects their companies' security posture.

- More companies have experienced ransomware attacks (61 percent of respondents vs. 52 percent of respondents in 2017) and 70 percent of respondents in these companies report that the ransom was paid. The average payment in these cases was $1,466.

- To strengthen their cybersecurity postures, companies need more in-house expertise and budget. However, almost half (47 percent) of respondents say they have no understanding of how to protect their companies against cyber attacks.

- Responsibility for determining IT security priorities is dispersed throughout the company. As a result, the ability to have effective leadership in the IT security function is missing in most companies. In fact, 35 percent of respondents say no one function determines IT security priorities.

- Passwords are often compromised or stolen because employees use weak passwords. Forty percent of respondents say their companies experienced an attack involving the compromise of employees' passwords; the average cost of each attack was $383,365.

- A lack of visibility into employees' password practices is exacerbating the likelihood of attacks involving passwords. Protection of passwords mostly involves human memory (53 percent of respondents) and spreadsheets (51 percent of respondents). Only 18 percent of respondents say their organizations rely upon browser extensions.

- More companies are using single sign-on (SSO) to simplify and increase the security of user access to their companies' applications and data.

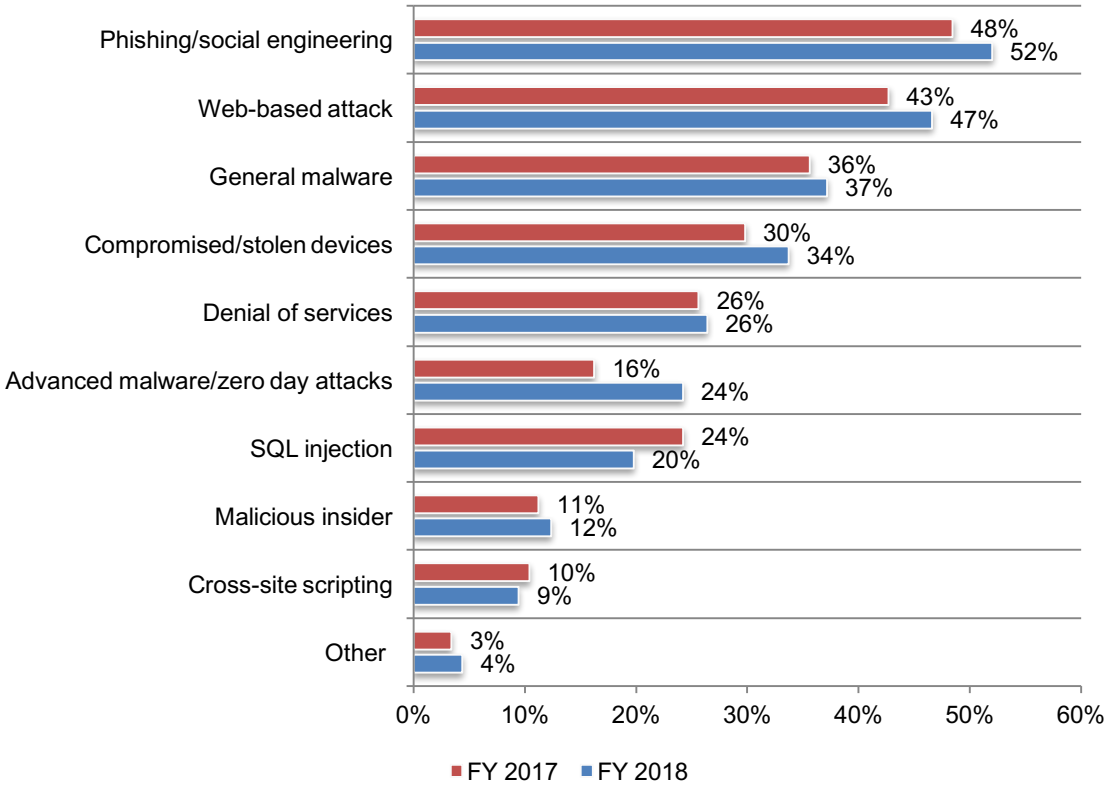
## Part 2. Key findings

- Trends in SMB cyber attacks and data breaches
- Ransomware attacks continue to increase
- Password practices and policies
- Cybersecurity posture and governance
- Technologies in place to address the threat

### Trends in SMB cyber attacks and data breaches

**Cyber attacks and data breaches target SMBs.** As discussed, most businesses represented in this study experienced a cyber attack or a data breach with severe financial consequences (67 percent and 58 percent, respectively). As shown in Figure 2, phishing/social engineering continues to be the number one attack SMBs experience (52 percent of respondents). Other frequent attacks are web-based attacks and general malware (47 percent and 37 percent of respondents, respectively). The type of attack that increased the most is advanced malware/zero day attacks (from 16 percent of respondents in 2017 to 24 percent of respondents in 2018).

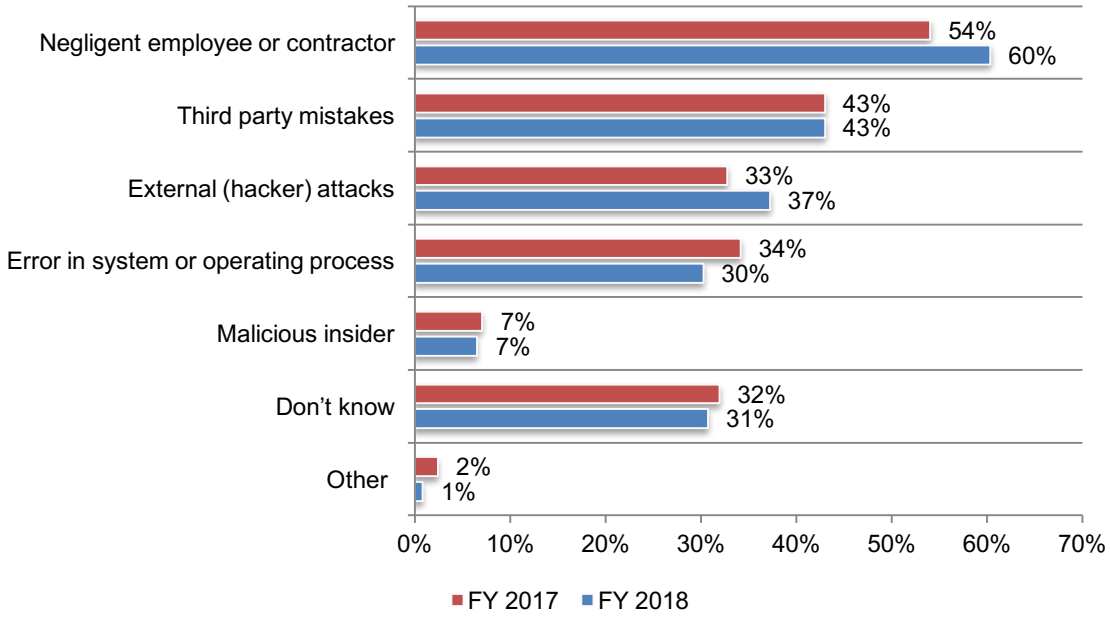
**Figure 2. What types of attacks did your business experience?**
More than one choice allowed



**Businesses are losing more records in a data breach.** Companies represented in this research lost an average of 10,848 individual records over the past 12 months as a result of the data breach, an increase from an average of 9,350 in last year's study.

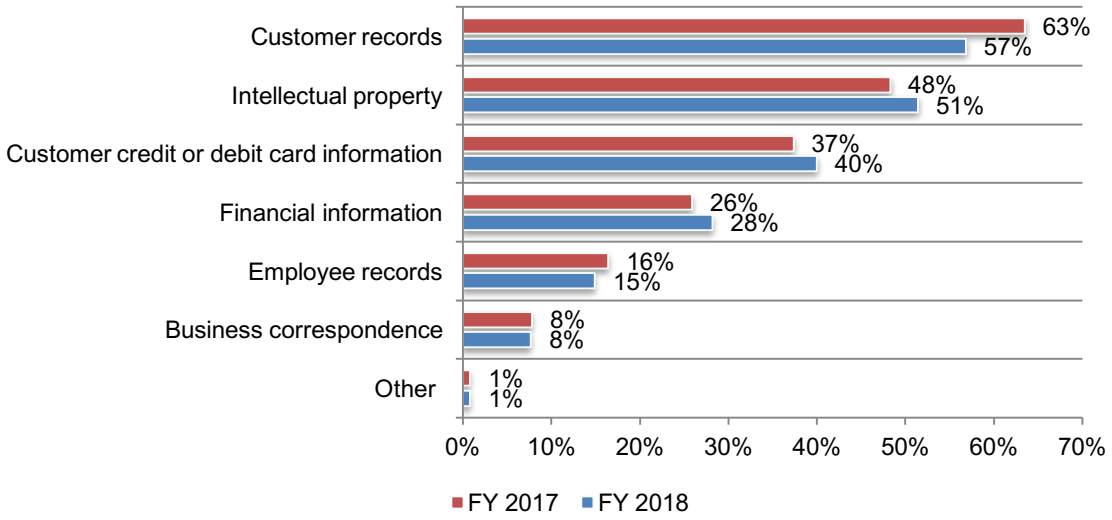
As shown in Figure 3, of the 58 percent of respondents who say their company had a data breach, they cite the root cause as negligent employees or contractors (60 percent of respondents), which increased from 54 percent in 2017. This is followed by third party mistakes (43 percent of respondents) and external (hacker) attacks (37 percent of respondents). However, almost a third of respondents (31 percent) say their companies could not determine the cause of the incident.

**Figure 3. What was the root cause of the data breaches your business experienced?**
More than one choice allowed



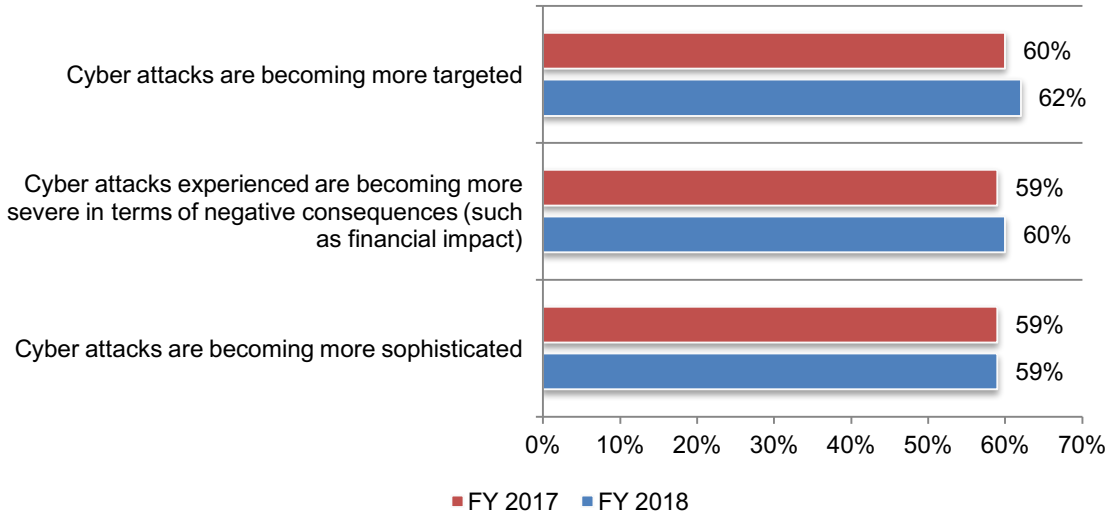
B**usinesses are most concerned about protecting customer records and intellectual property.** When asked what information cyber attackers are most likely to target, 57 percent of respondents say customer records are their biggest concern. More than half of respondents (51 percent) say they worry about the protection of their intellectual property.

**Figure 4. What types of information are you most concerned about protecting from cyber attackers?**
Two choices allowed




**Cyber attacks against SMBs are not diminishing**. Most respondents say cyber attacks against their companies are targeted, severe and sophisticated (62 percent, 60 percent and 59 percent, respectively); these values have not changed significantly since 2017, as shown in Figure 5.

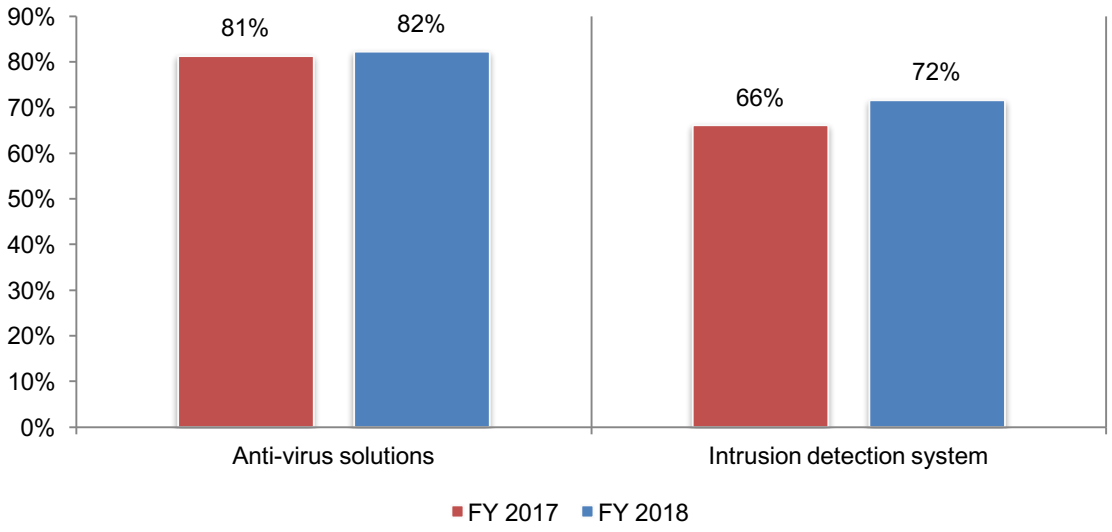
**Figure 5. Perceptions about cyber attacks against their companies**
Strongly Agree and Agree responses combined



**Businesses are vulnerable to exploits and malware**. Only 40 percent of respondents say the technologies currently used by their organization can detect and block most cyber attacks. As discussed previously, SMBs have experienced more advanced malware and zero day attacks in 2018.

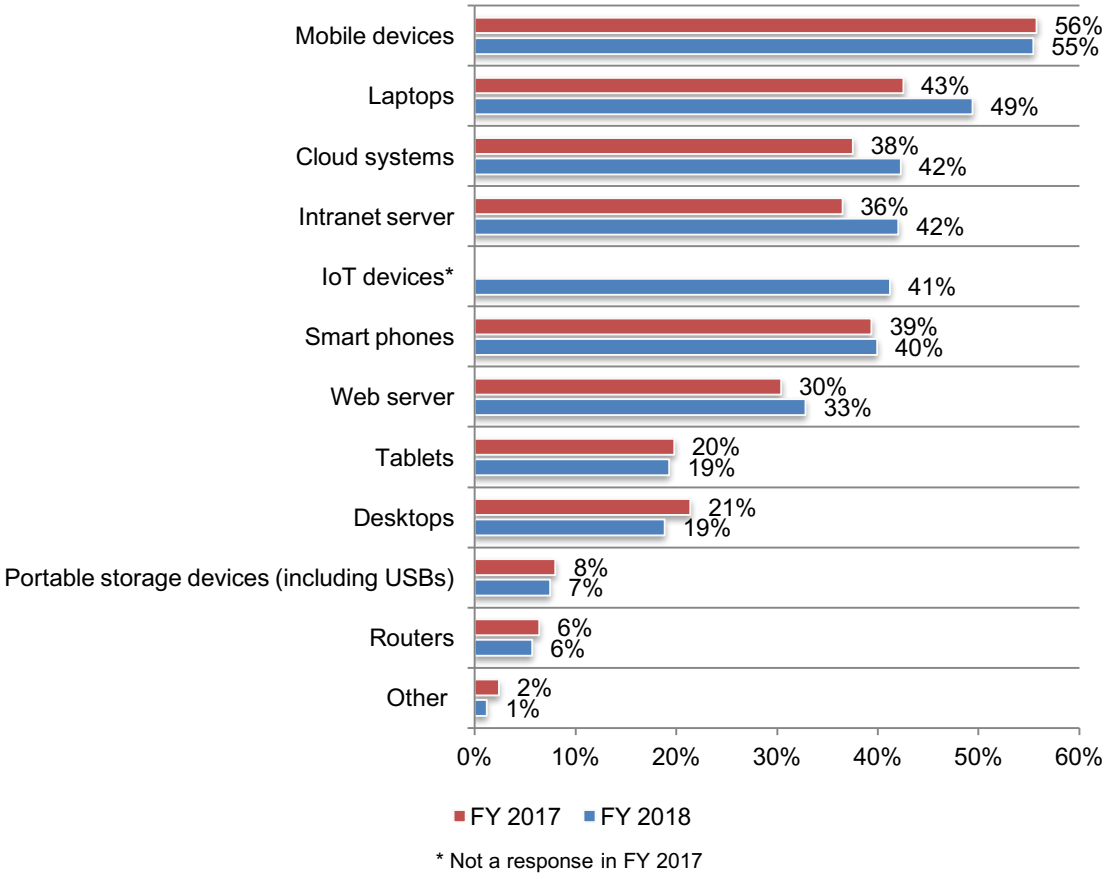
Figure 6 reveals that 72 percent of respondents (an increase from 66 percent in the previous study) say exploits and malware evaded intrusion detection systems moreover, 82 percent of respondents (an increase from 81 percent last year) say they have evaded their anti-virus solutions.

**Figure 6. Has your business experienced situations when exploits and malware have evaded their intrusion detection system or anti-virus solutions?**
Yes responses presented



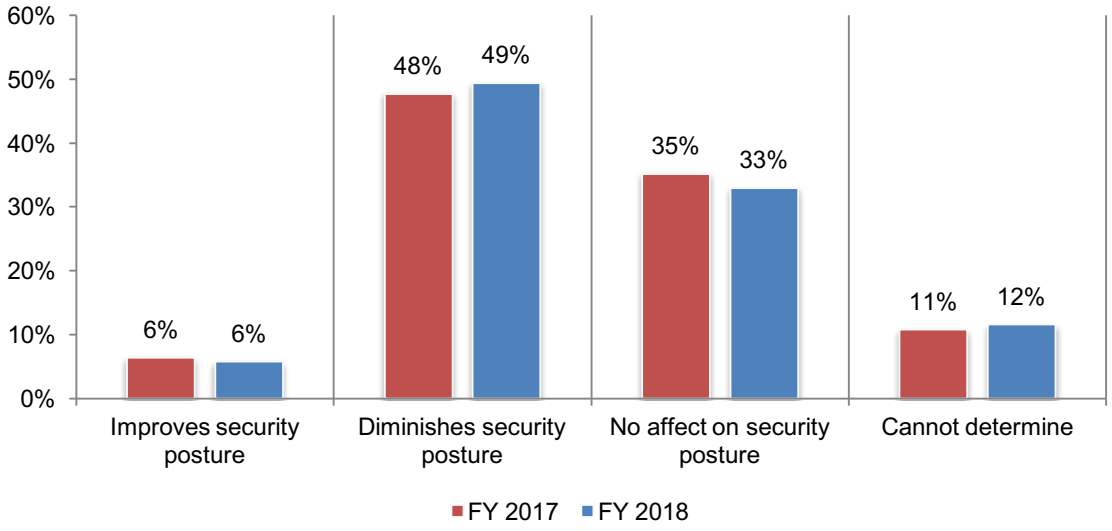
**Mobile devices are the most vulnerable endpoints or entry points to networks and enterprise systems**. As shown in Figure 7, mobile devices are considered, by far, the most vulnerable endpoint or entry point to respondents' companies' networks and enterprise systems. However, laptops and intranet servers have increased in their vulnerability. For the first time, IoT devices were included and 41 percent say they are a very vulnerable entry point.

**Figure 7. What are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems?**
Three choices allowed



**More mobile devices will be used to access business-critical applications and IT infrastructure.** Currently, an average of 45 percent of business-critical applications are accessed from mobile devices such as smartphones and tablets. As shown in Figure 8, nearly half (49 percent) of respondents say these devices diminish their companies' security posture.

**Figure 8. How does the use of mobile devices to access business-critical applications and IT infrastructure affect your organization's security posture?**

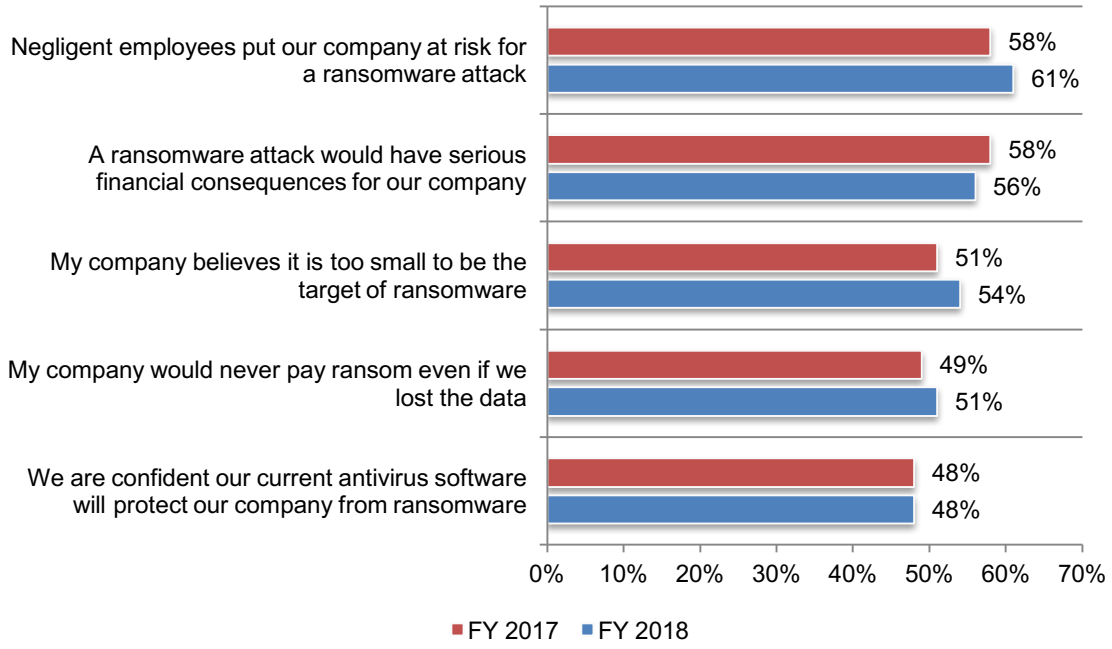


**Ransomware attacks continue to increase**

**The weakest link in a company's ability to stop a ransomware attack is the negligent employee.** In the context of this research, ransomware is defined as a sophisticated piece of malware that blocks victims' access to their files.

Sixty-one percent of respondents say negligent employees put their company at risk for a ransomware attack and 56 percent of respondents say these attacks can have serious financial consequences, as shown in Figure 9. Less than half (48 percent) of respondents are confident that their current anti-virus software will protect their company from ransomware.

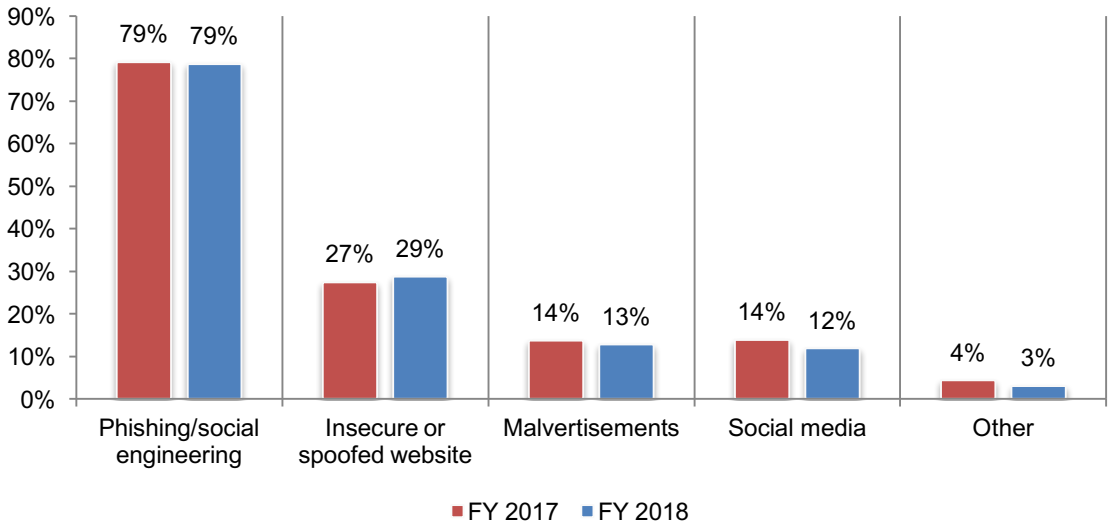
**Figure 9. Perceptions regarding ransomware**
Strongly agree and Agree responses combined



**Ransomware attacks increase significantly since last year**. Sixty-one percent of respondents say their company experienced either unsuccessful or successful ransomware attacks within the past three months (11 percent), within the past 6 months (17 percent), within the past 12 months (19 percent) or more than 12 months ago (14 percent). In 2017, 52 percent of respondents said they experienced a ransomware attack.

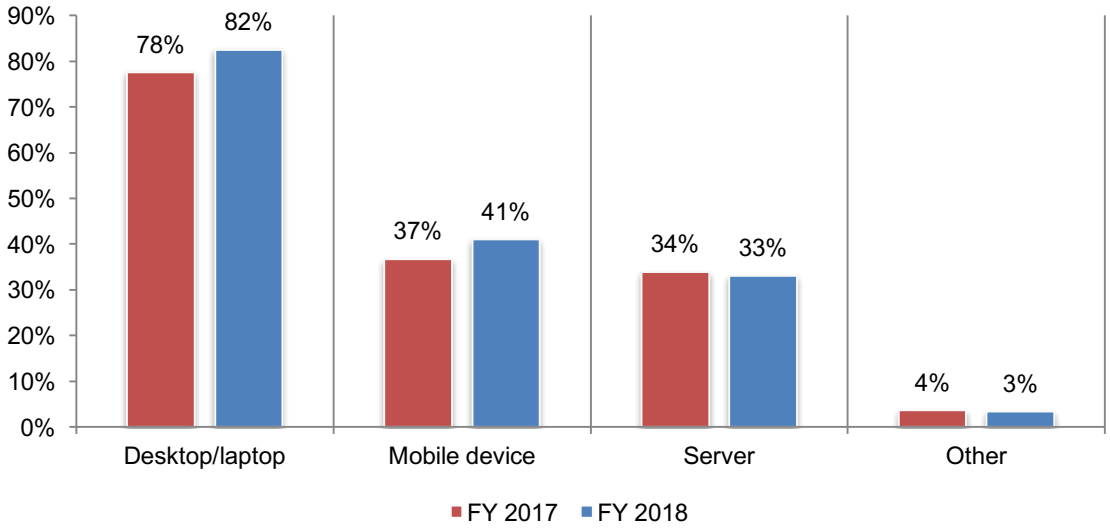
As shown in Figure 10, the ransomware experienced by companies in this study was mainly unleashed via phishing/social engineering attacks (79 percent of respondents) followed by an insecure or spoofed website (29 percent of respondents). This finding coincides with both the increase in phishing/social engineering and the increase in negligent employees as the root cause of a data breach.

**Figure 10. How was the ransomware unleashed?**
More than one choice allowed



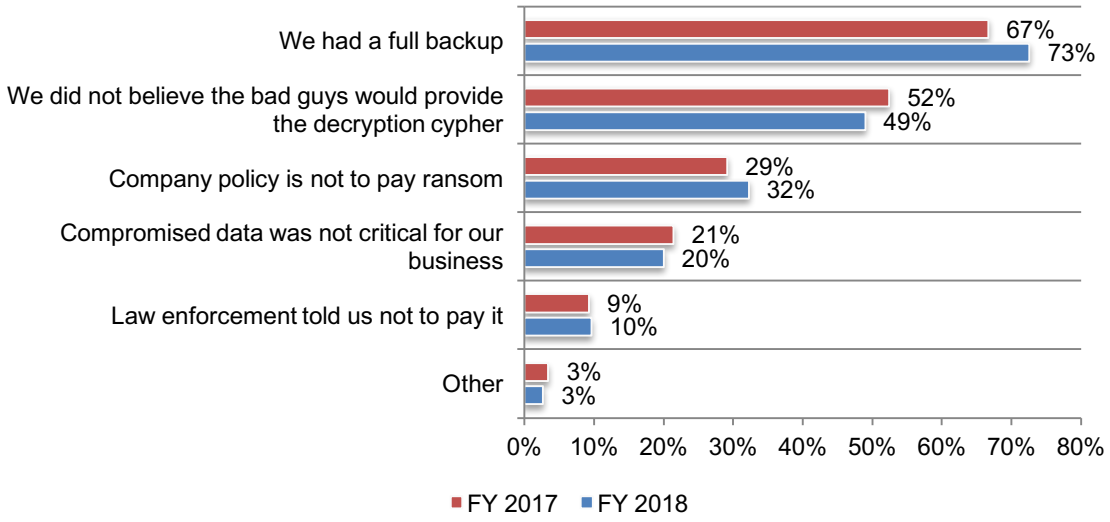
**The devices considered the most vulnerable as a point of entry are the ones most often attacked.** As shown in Figure 11, the devices most often compromised by ransomware were desktop/laptop (82 percent) and mobile device (41 percent), as shown in Figure 11.

**Figure 11. What type of device(s) was compromised by ransomware?**
More than one choice allowed




**For successful ransomware attacks, more companies are paying the ransom.** The average ransom was $1,466, and 70 percent of respondents say their companies paid the ransom. Last year, 60 percent of respondents said they paid the ransom. As shown in Figure 12, companies that **did not** pay the ransom attributed the decision to having a full backup (73 percent of respondents) or not trusting the criminals to provide the decryption cypher (49 percent of respondents).

**Figure 12. Why did your company not pay the ransom?**
More than one choice allowed

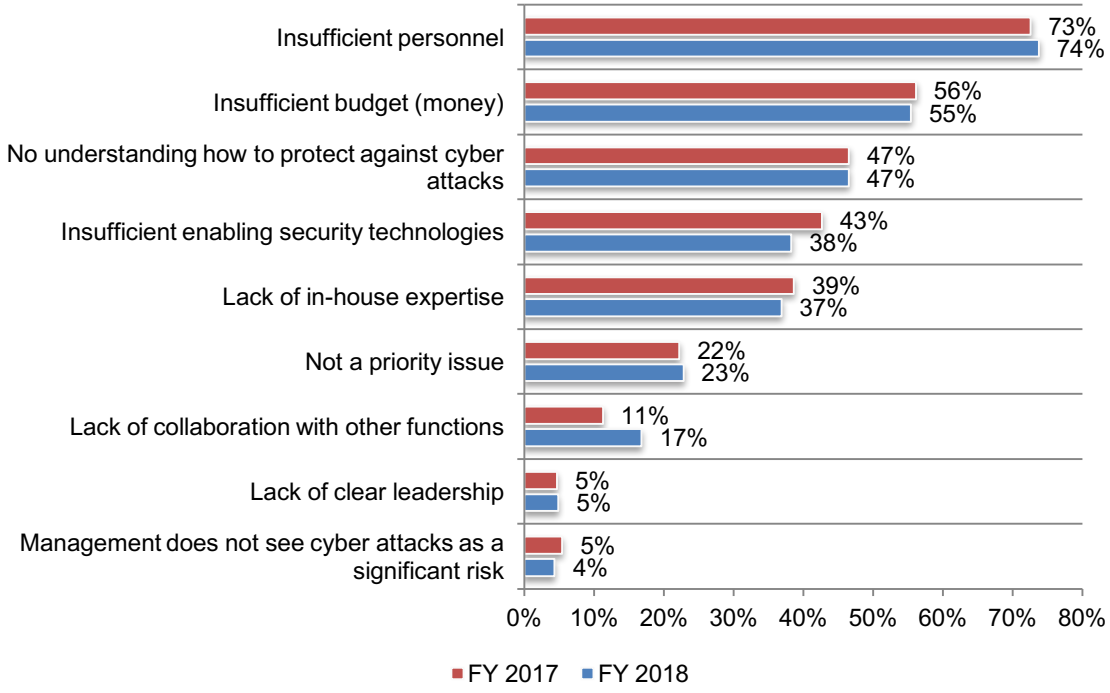


**Cybersecurity posture and governance**

**SMBs continue to struggle with insufficient personnel and money.** Figure 13 lists the challenges companies face when trying to create a stronger security posture.

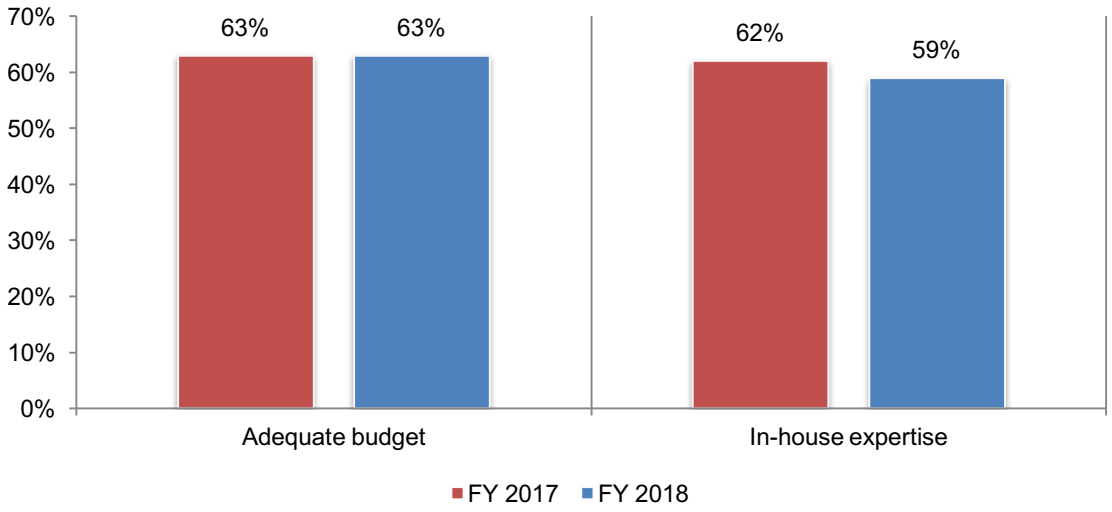
The biggest problem is not having the personnel to mitigate cyber risks, vulnerabilities and attacks (74 percent of respondents). The next biggest challenges are insufficient budget (55 percent of respondents) and no understanding of how to protect against cyber attacks (47 percent of respondents).

**Figure 13. What challenges keep your IT security posture from being fully effective?**
Three choices allowed



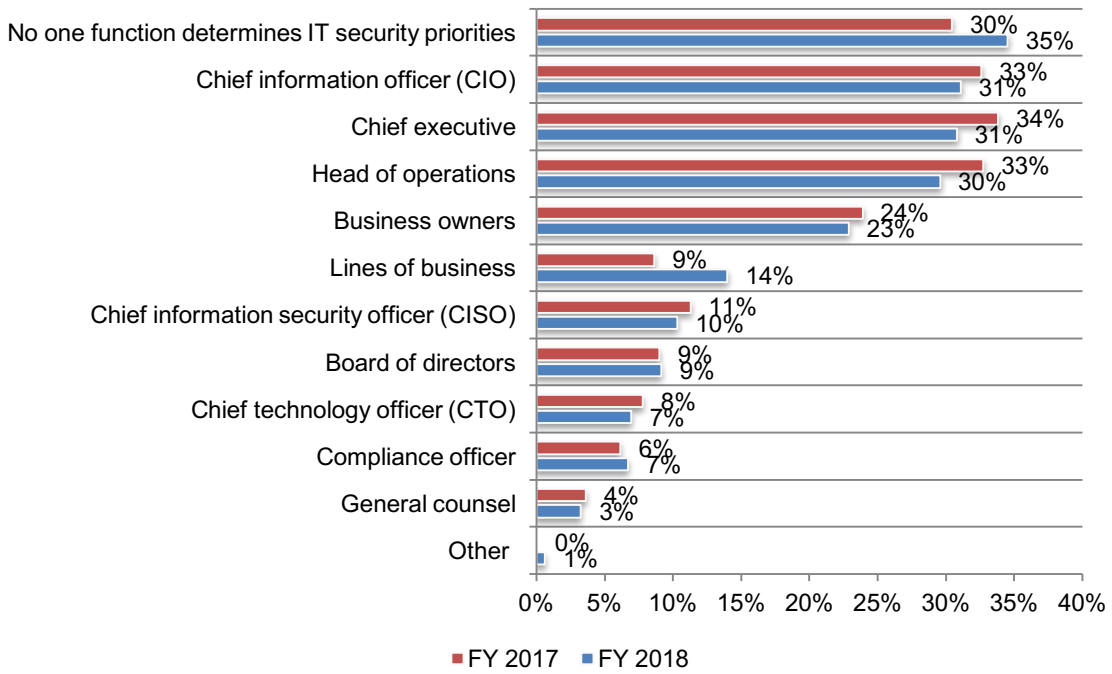
As Figure 14 shows, 63 percent of respondents say their companies do not have an adequate budget to achieve a strong cybersecurity posture. Fifty-nine percent of respondents say their companies do not have adequate in-house expertise to achieve a strong cybersecurity posture.

**Figure 14. Does your organization have an adequate budget and in-house expertise to achieve a strong cybersecurity posture?**
No and Unsure responses combined




**Leadership is lacking when determining IT security priorities.** As shown in Figure 15, 35 percent of respondents say no one person is responsible for determining IT security priorities, an increase from 30 percent of respondents in last year's research. According to the findings, responsibility for companies' IT security strategy is dispersed throughout the company.

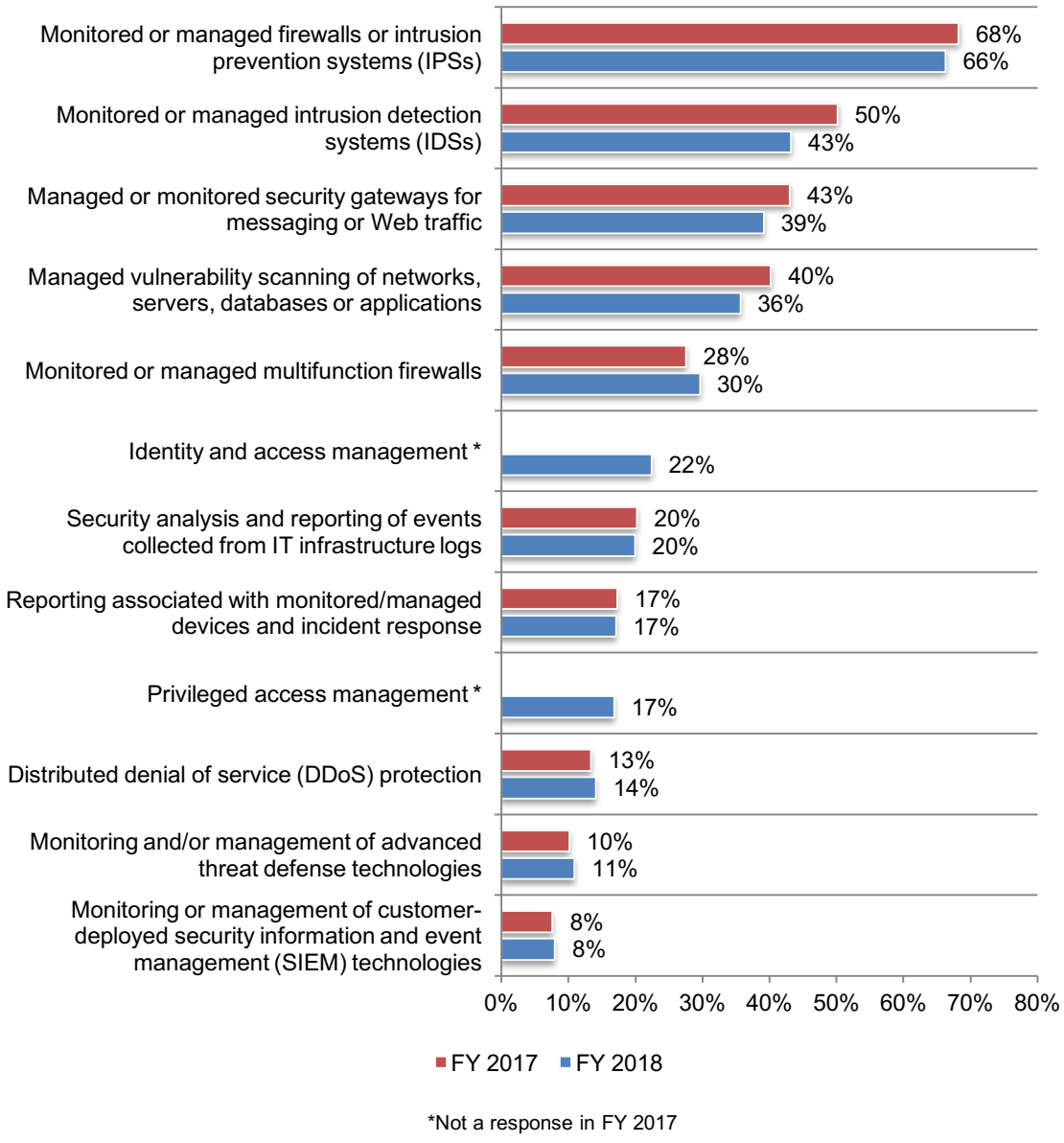
**Figure 15. Who determines IT security priorities?**
Two choices allowed



**More SMBs are engaging managed security services providers (MSSPs) to support the IT security function.** On average, 29 percent of a company's IT security operations are supported by MSSPs, this is an increase from 21 percent in last year's study.

According to Figure 16, 66 percent of respondents say their MSSP monitors or manages firewalls or intrusion prevention systems (IPS). Forty-three percent say they use MSSPs to monitor or manage intrusion detection systems (IDSs).

**Figure 16. What services are provided by MSSPs to support your IT security posture?**
More than one choice permitted

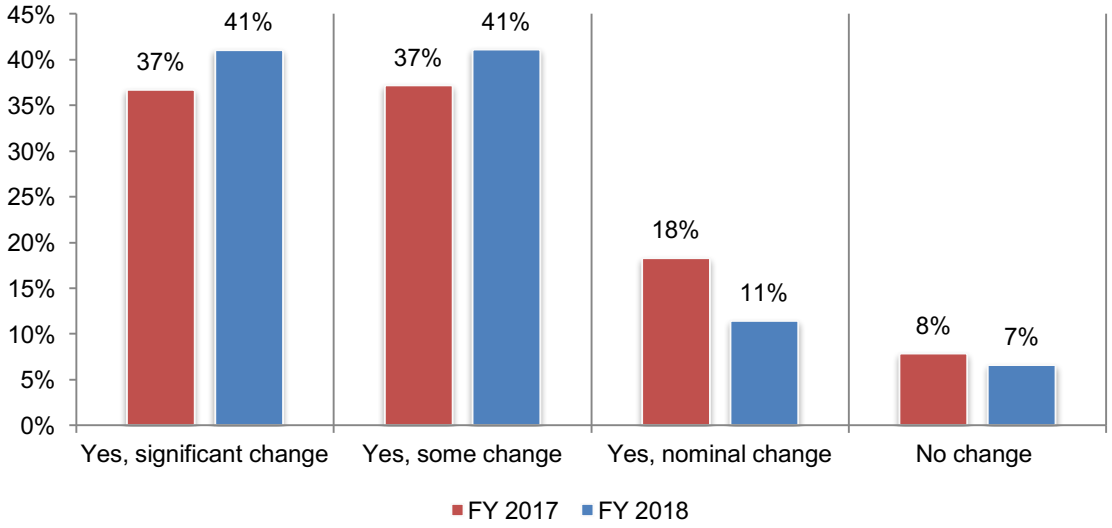



*Not a response in FY 2017

**Compliance with the new General Data Protection Regulation (GDPR) is a burden for SMBs already challenged with not having an adequate IT security budget**. The GDPR took effect on May 25, 2018. It establishes new requirements related to the export of personal data outside the European Union. In last year's research, respondents were asked to predict if the GDPR would require significant changes to their companies' privacy and security strategies.

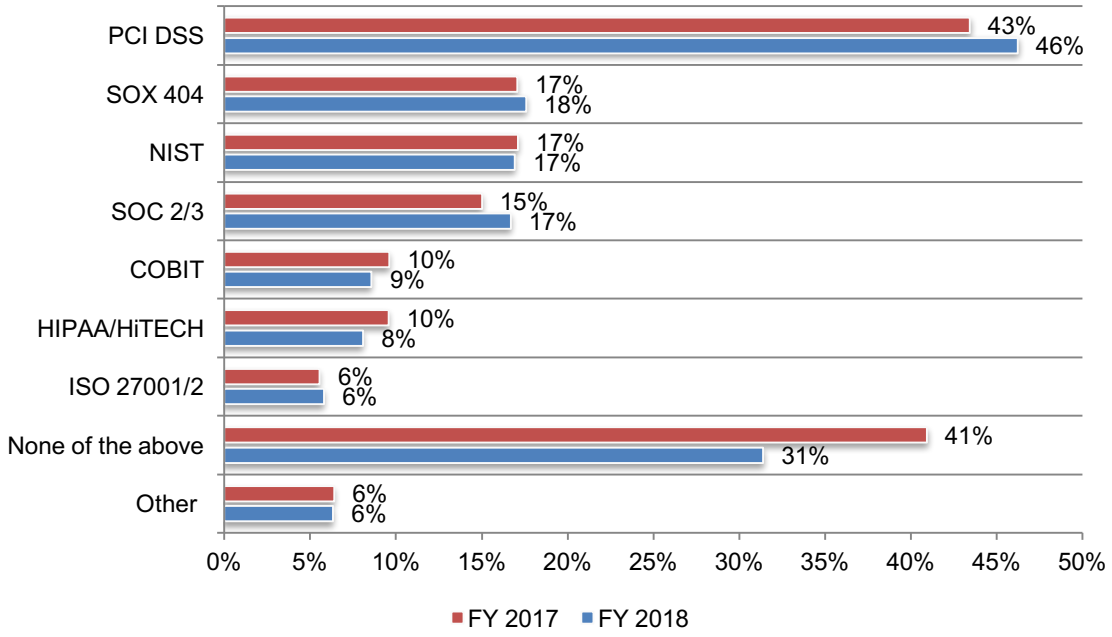
As Figure 17 shows, last year 92 percent of respondents said the new regulations would require changes to their privacy and security strategy. Similarly, in 2018, 93 percent of respondents say the new regulation did require significant changes. Only 19 percent of respondents say they have achieved a high level of compliance with GDPR.

**Figure 17. Will the GDPR require significant changes in your privacy and security strategy?**



**More SMBs are adopting IT security guidelines or standards.** Figure 18 presents the leading IT security guidelines and standards. Forty-six percent of respondents say they comply with PCI DSS. Thirty-one percent of respondents say they do not comply with any of the standards, a significant decline from 41 percent of respondents in the 2017 study.

**Figure 18. Which IT security guidelines or standards does your company comply with?**
More than one choice permitted



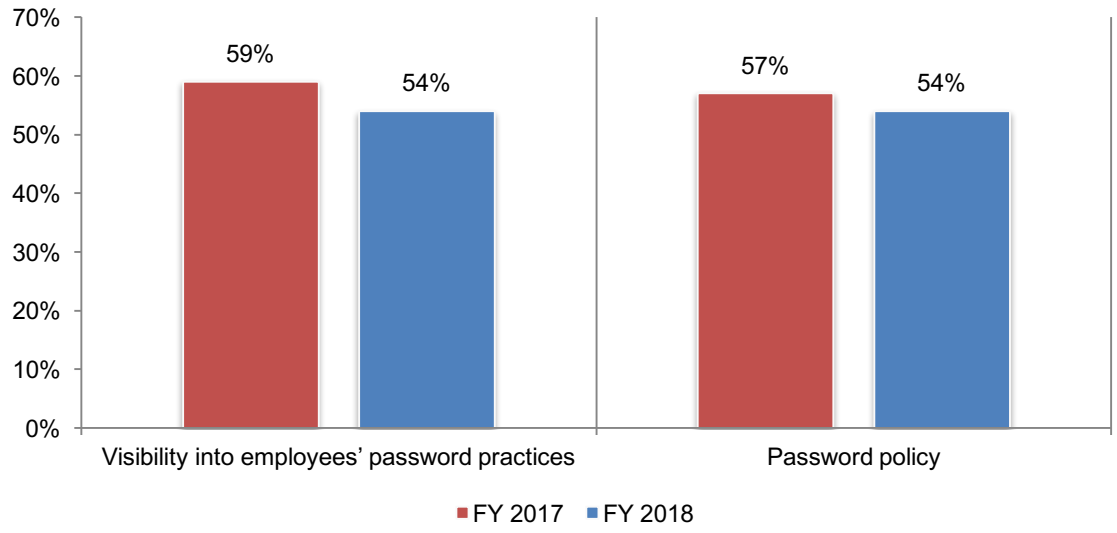
**Password practices and policies**

**Strong passwords and biometrics are an essential part of a company's security defense.** Forty percent of respondents say their companies had an attack involving the compromise of employees' passwords in the past year, and the average cost of each attack was $383,365.

Similar to last year's findings, 62 percent of respondents say they rely upon strong passwords and/or biometrics to reduce the risk of attack. In 2017, 60 percent of respondents agreed with this risk mitigation strategy.

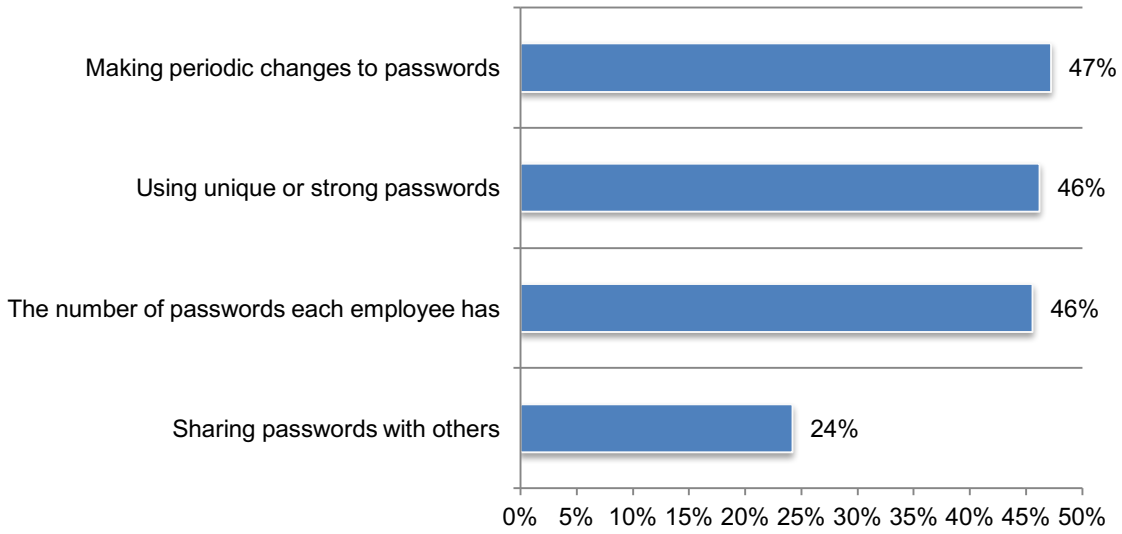
However, as Figure 19 demonstrates, 54 percent of respondents say they do not have, or are unsure if they have, visibility into employees' password practices such as the use of unique or strong passwords and sharing passwords with others. Fifty-four percent of respondents do not have, or are unsure their company has, a policy pertaining to employees' use of passwords and/or biometrics, such as a fingerprint.

**Figure 19. Does your organization have visibility into employees' password practices and a password policy?**
No and Unsure responses combined



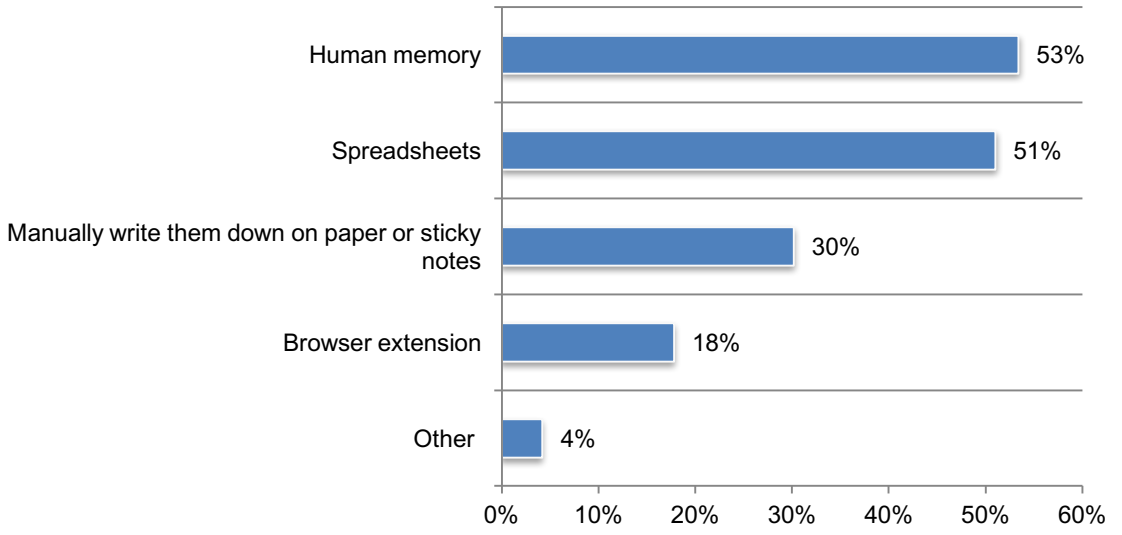
**The ability to determine employees' password practices is not effective.** Of the 45 percent of respondents who say they have visibility into employees' password practices, less than half of respondents say they are able to determine if employees are making periodic changes to passwords (47 percent), using unique or strong passwords (46 percent) and determining the number of passwords each employee has (46 percent). Only 24 percent of respondents say they are able to determine if employees are sharing passwords.

**Figure 20. Is your company able to determine employees' password practices?**
More than one choice allowed



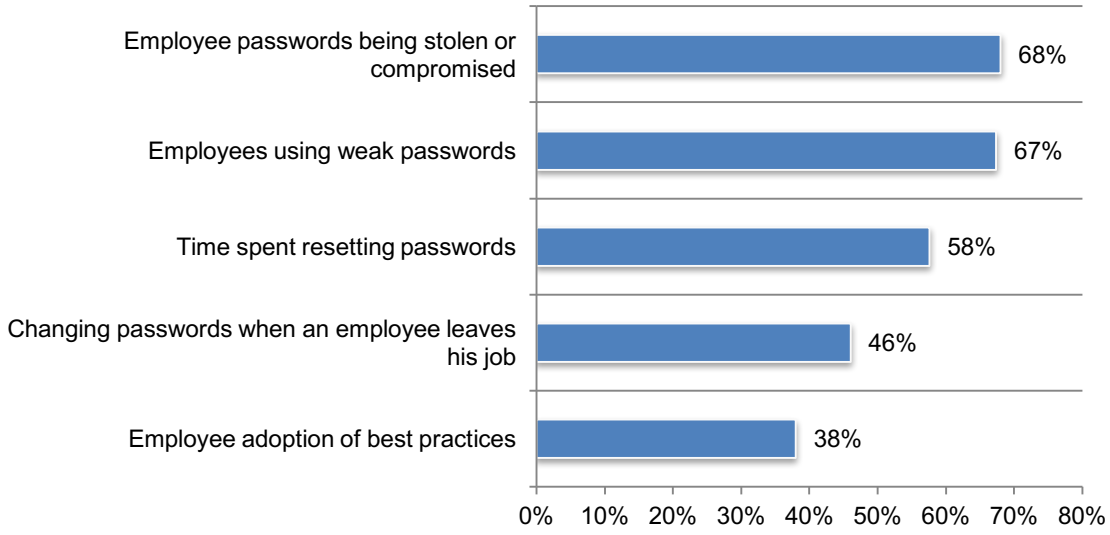

**Human memory and spreadsheets are used to protect passwords**. Only 22 percent of respondents say their companies require employees to use a password manager. Of the 74 percent of respondents who say password managers are not required, 53 percent of respondents say their companies rely upon human memory and 51 percent of respondents say they use spreadsheets.

**Figure 21. What does your organization use to manage and protect its passwords?**
More than one choice allowed



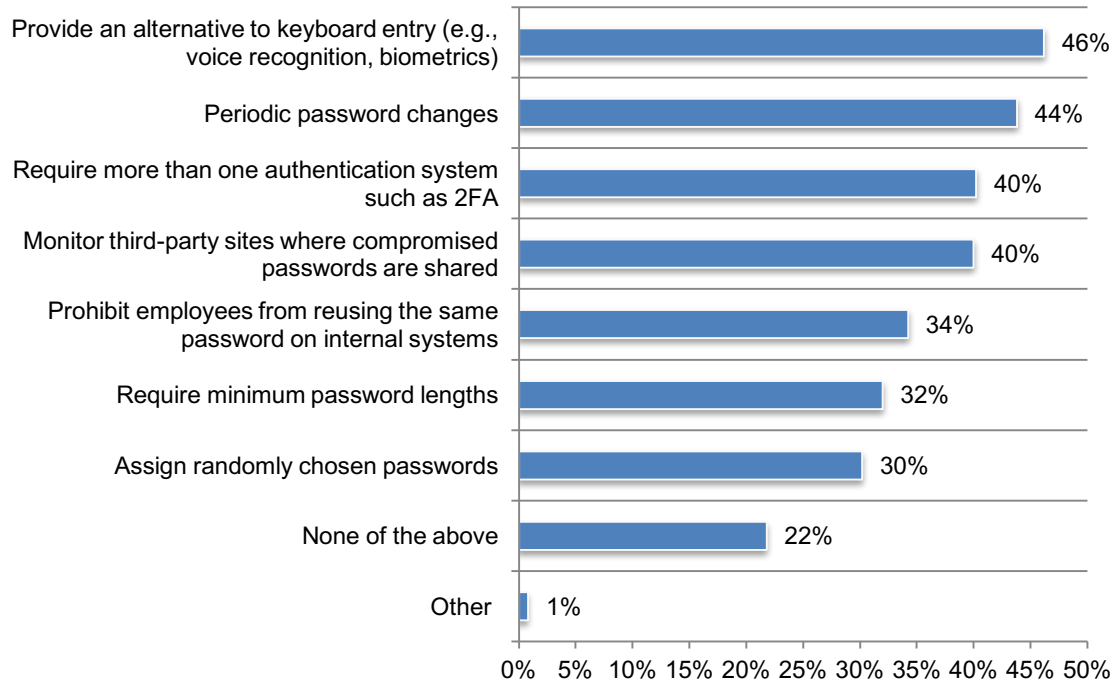
**Employees' use of weak passwords leads to stolen or otherwise compromised passwords.** Figure 22 lists what respondents think are the biggest pain points in managing employees' passwords. As shown, 68 percent of respondents say having to deal with passwords being stolen or compromised followed by employees using weak passwords (67 percent of respondents).

**Figure 22. What is your biggest pain point about employees and their passwords?**
Two choices allowed



**Biometrics or voice recognition are most often used to protect passwords.** Figure 23 lists possible measures companies can take to safeguard employees' passwords. The top choices are to have an alternative to keyboard entry (46 percent of respondents), mandate periodic password changes (44 percent of respondents), require more than one authentication system such as 2FA (40 percent of respondents) and monitor third-party sites where compromised passwords are shared (40 percent of respondents).

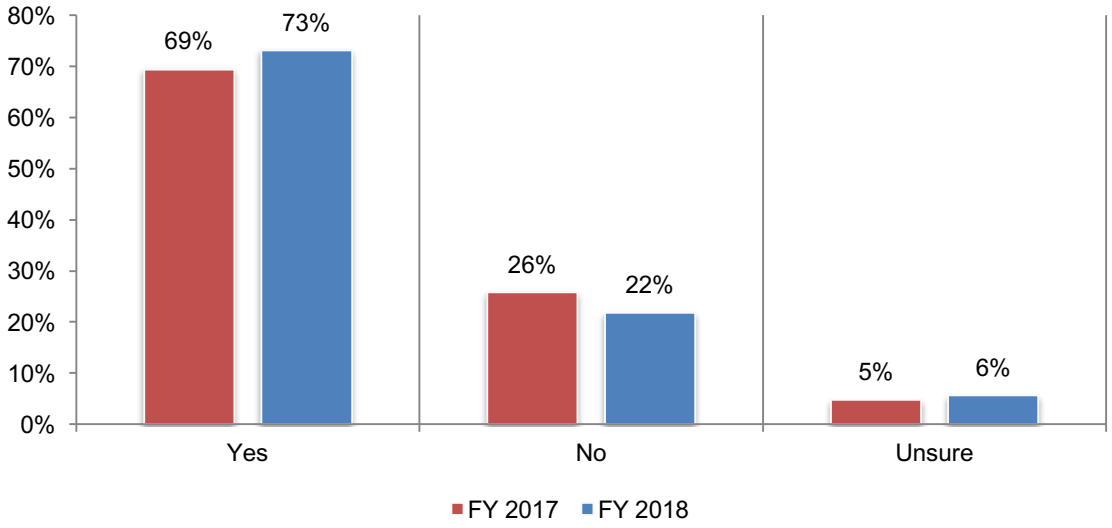
**Figure 23. Does your organization take any of the following steps to safeguard passwords?**
More than one choice allowed



**More respondents in this year's research say their companies have implemented SSO either fully (31 percent) or partially implemented (27 percent).** SSO is defined as a property of access control of multiple related, yet independent, software systems. A user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords; or, in some configurations, seamlessly sign on at each system.

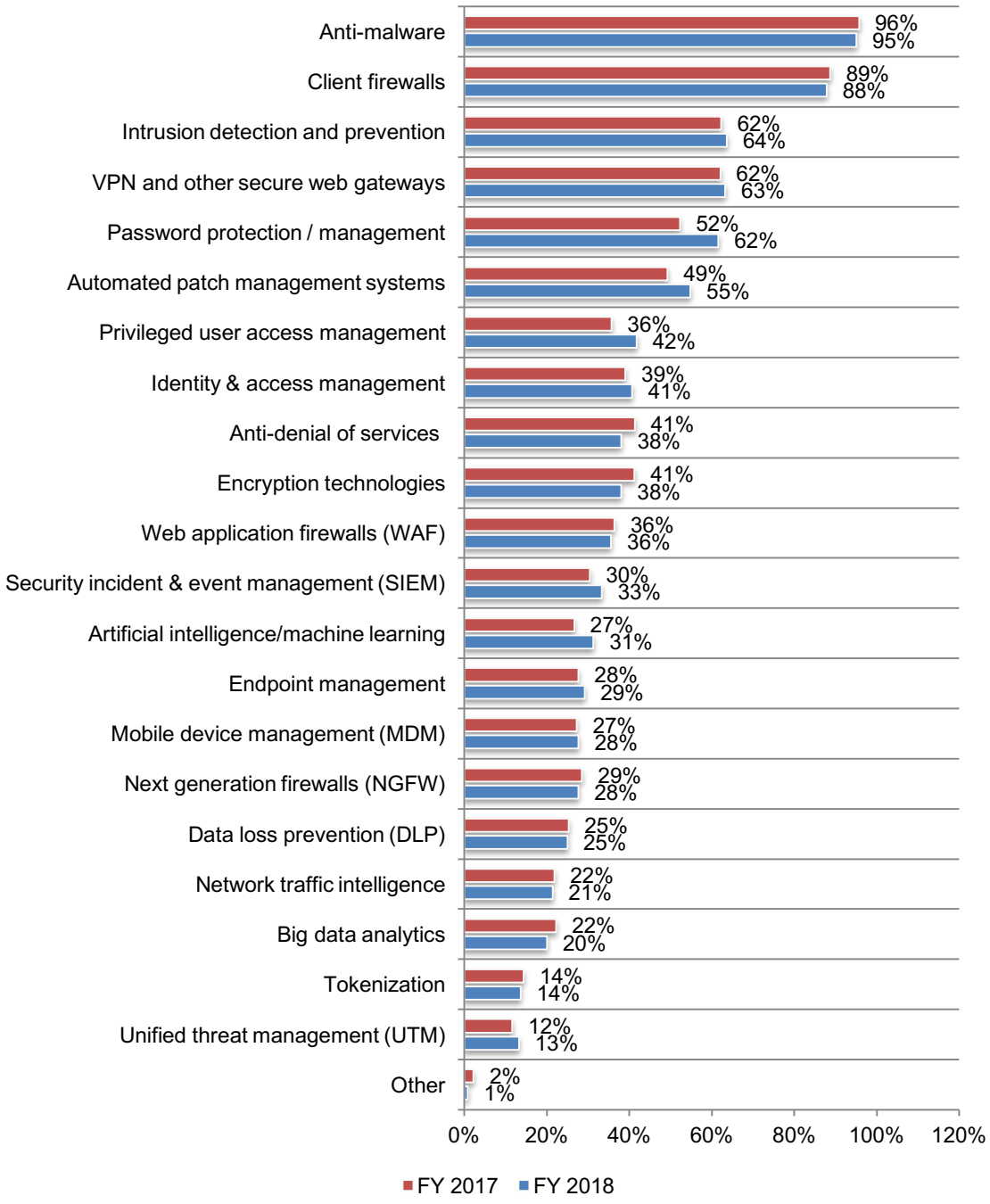
As can be seen in Figure 24, these respondents largely believe SSO increases the security of user access to their companies' applications and data (73 percent).

**Figure 24. Does SSO simplify and increase the security of user access to your organization's applications and data?**



**Password protection and management has increased in importance.** According to Figure 25, almost all (95 percent) respondents believe anti-malware is critical. Nearly as many say client firewalls (88 percent of respondents) are important. Password protection and management has increased significantly in importance since 2017 (from 52 percent of respondents to 62 percent of respondents). Also increasing are automated patch management systems (49 percent of respondents to 55 percent of respondents) and privileged user access management (from 36 percent of respondents to 42 percent of respondents).

**Figure 25. Security technologies considered essential and very important**
More than one choice allowed



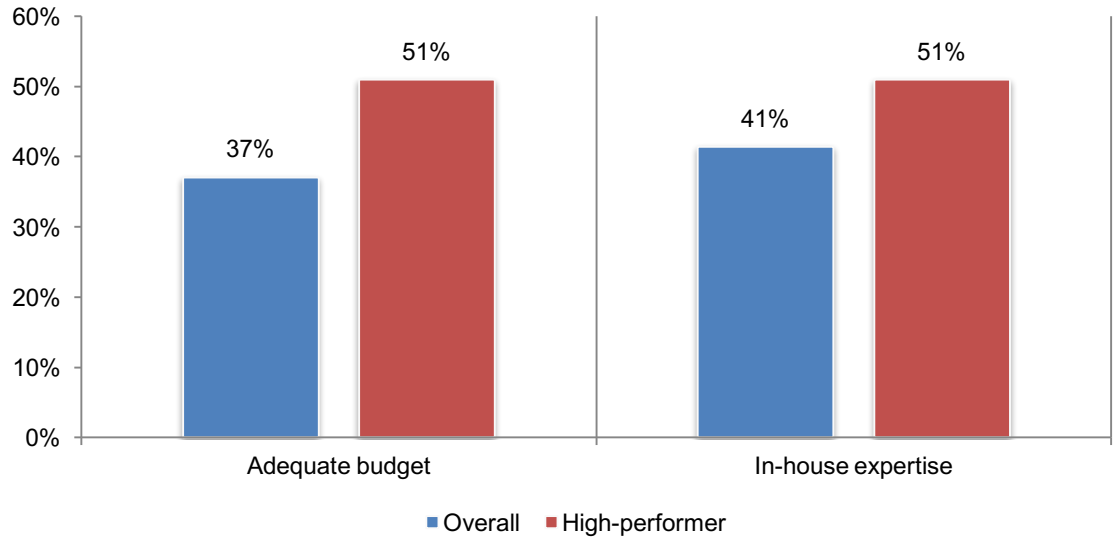
**The best practices of high-performing companies**

In this section, we present a special analysis of the 115 respondents from high-performing companies. These respondents say their companies are highly effective at mitigating risks, vulnerabilities and attacks across the enterprise. We compare their responses to the overall sample of respondents to learn the best practices of companies that are highly effective in mitigating the risk of data breaches and cyber attacks.

**High-performing companies have higher budgets and in-house expertise.** As shown in Figure 26, more than half of respondents (51 percent) in high-performing companies vs. 37 percent of respondents in the overall sample say their budget is adequate for achieving a strong IT security posture. High-performing companies are also allocating a higher percentage of the IT budget to IT security (15 percent vs. 12 percent).

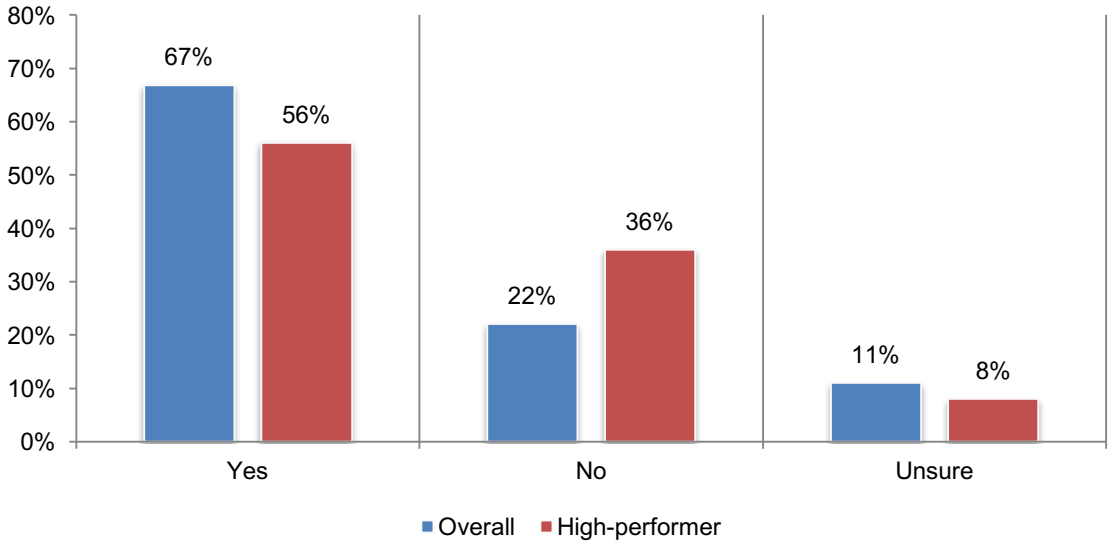
A larger budget is helpful in staffing the IT security function with experts. Fifty-one percent of respondents say their companies have the necessary in-house expertise for achieving a strong security posture. An average of 41 percent of the IT staff support IT security operations. In contrast, an average of only 36 percent of the IT staff supports IT security operations in the overall sample.

**Figure 26. Differences in perceptions about budget and in-house expertise**
Yes responses presented



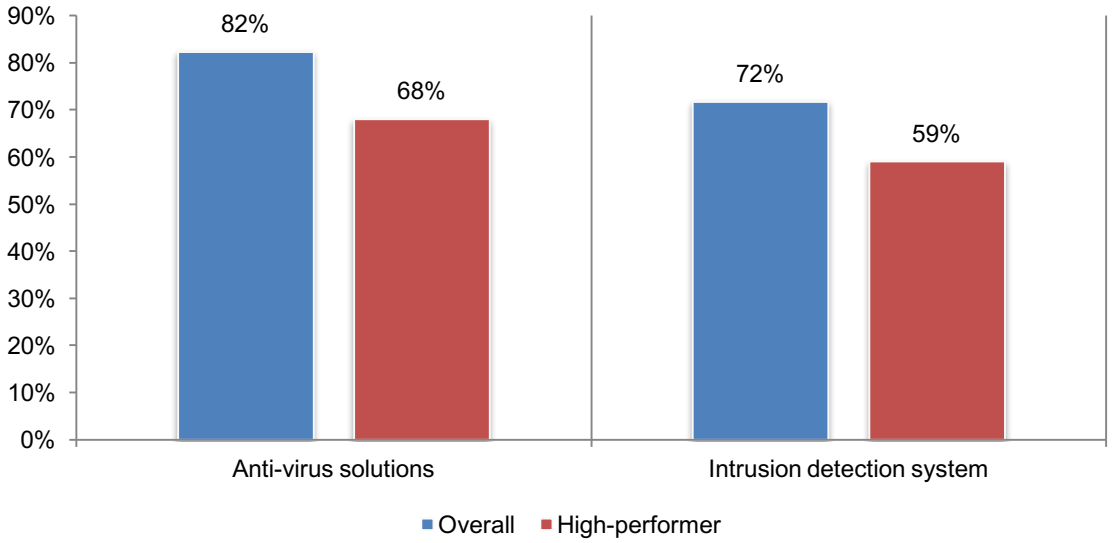
**High-performing companies are less likely to experience a cyber attack.** As shown in Figure 27, 67 percent of respondents in the overall sample had a cyber attack in the past 12 months as opposed to 56 percent of respondents in high-performing companies.

**Figure 27. Has your organization experienced a cyber attack in the past 12 months?**



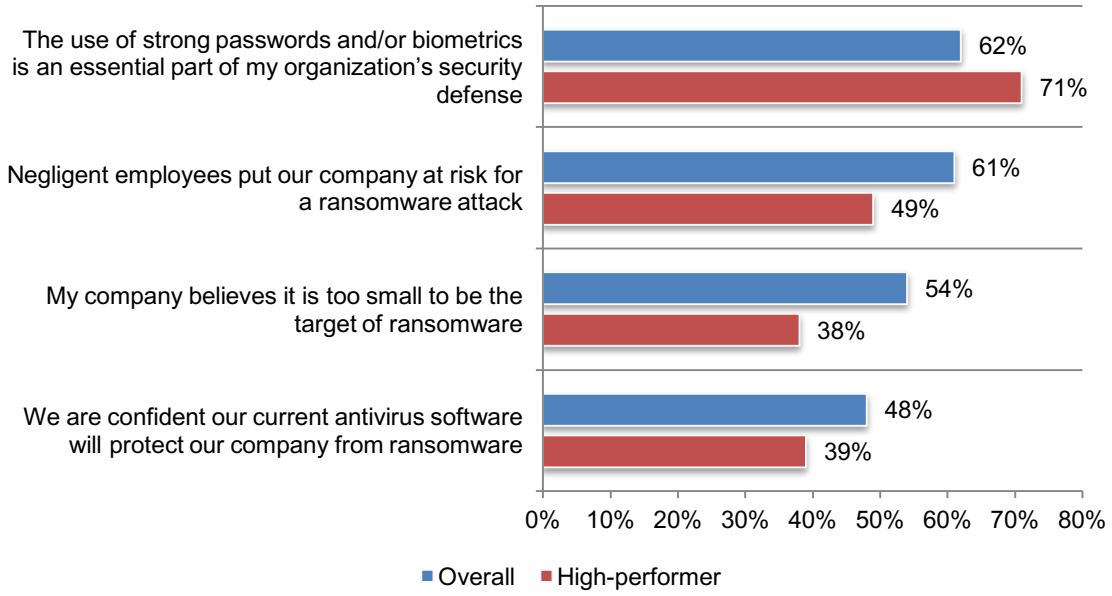

As shown in Figure 28, high-performing companies are less likely to experience exploits where malware evaded intrusion detection systems and anti-virus solutions.

**Figure 28. Has your organization experienced exploits where malware evaded intrusion detection systems and anti-virus solutions?**
Yes responses presented



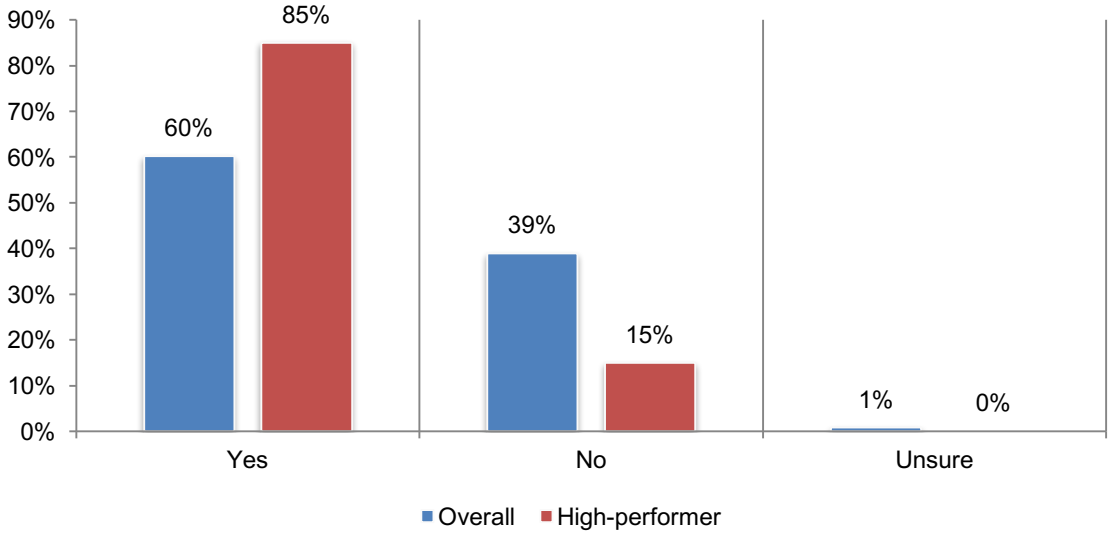
**High-performing companies are more likely to require the use of strong passwords and/or biometrics.** According to Figure 29, 71 percent of respondents from high-performing companies vs. 62 percent of respondents in the overall sample say the use of strong passwords and/or biometrics is an essential part of their organization's security defense. Respondents in high-performing companies are less likely to agree that negligent employees put their companies at risk for a ransomware attack, that their companies are too small to be a target of ransomware. They are also less confident that their current antivirus software will protect their companies from ransomware.

**Figure 29. Perceptions about password security and ransomware**
Strongly agree and Agree responses combined



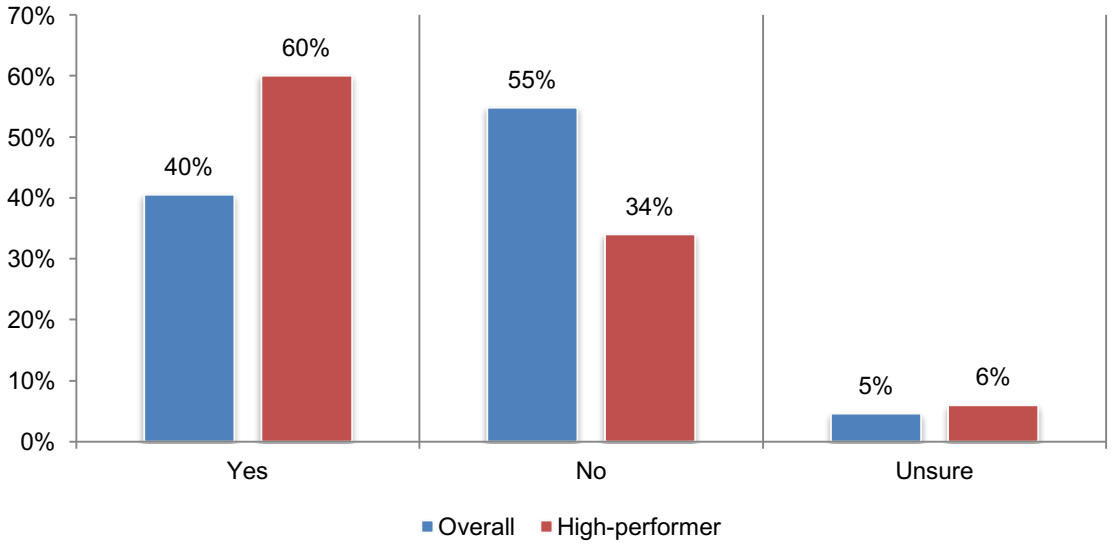

**High-performing companies are more likely to have an incident response plan.** According to Figure 30, 85 percent of respondents from high-performing companies have an incident response plan vs. 60 percent of the overall sample of respondents say they have such a plan.

**Figure 30. Does your company have an incident response plan?**



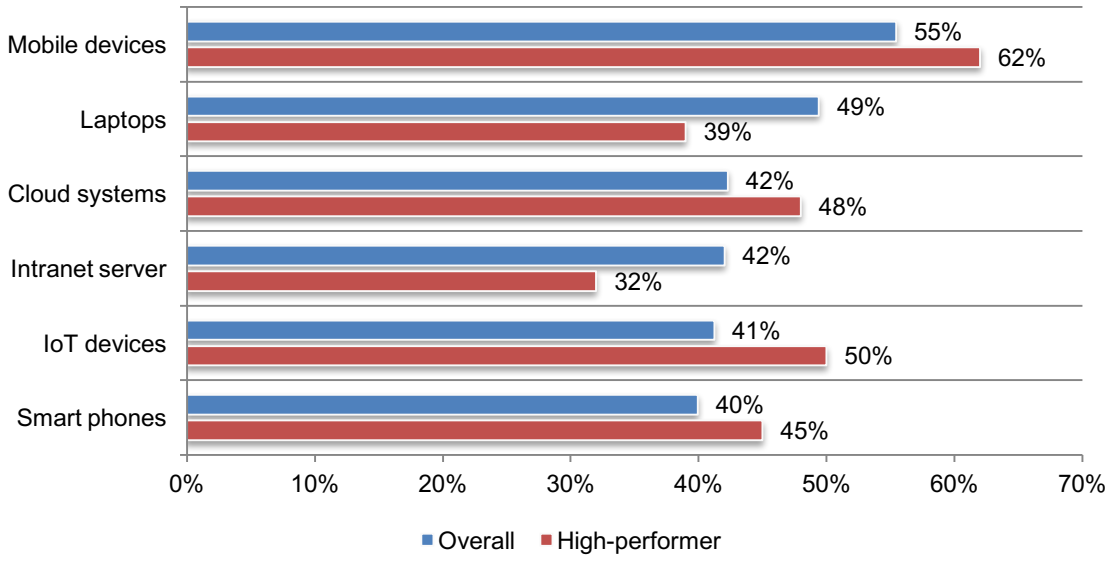
**More high-performing companies have password policies for employees.** As shown in Figure 31, 60 percent of respondents from high-performing companies say their companies have a password policy vs. 40 percent of respondents in the overall sample.

**Figure 31. Does your company have a password policy for employees?**



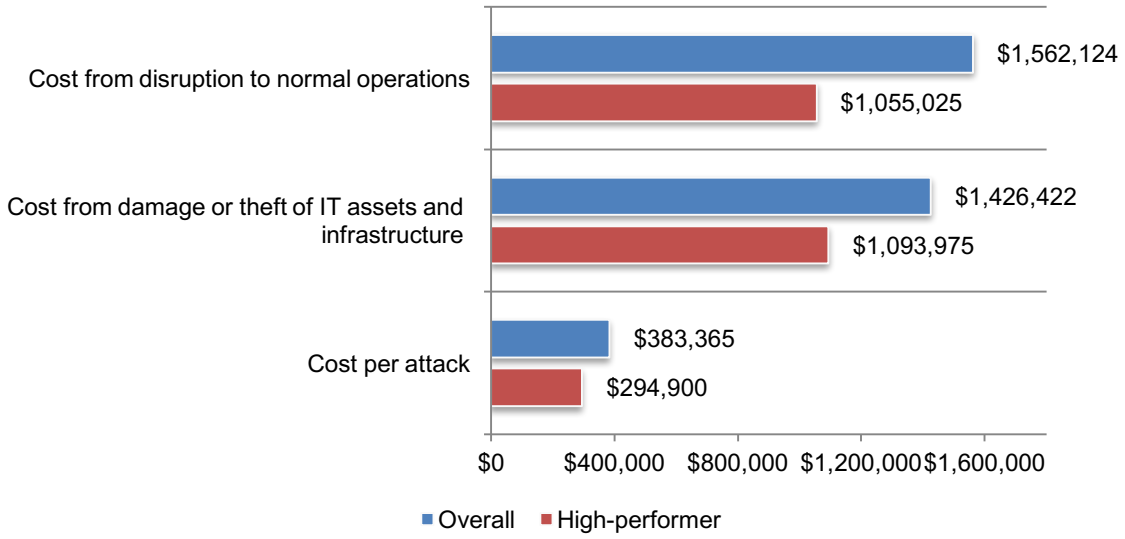

**High-performing companies are most likely to believe mobile devices are the most vulnerable endpoints.** These companies are also most likely to say IoT devices and cloud systems are vulnerable entry points and less likely to consider laptops and Intranet servers to be vulnerable entry points.

**Figure 32. What are the most vulnerable endpoints or entry points to your companies' networks and enterprise systems?**
More than one response permitted



**The financial consequences following a security incident are much less severe for high-performing companies.** According to Figure 33, the benefit of having a more effective security strategy is a lower cost of the compromises companies experienced. The biggest difference between the two groups of respondents is the cost from disruption to normal operations.

**Figure 33. The cost of compromises**
Extrapolated values (US$)



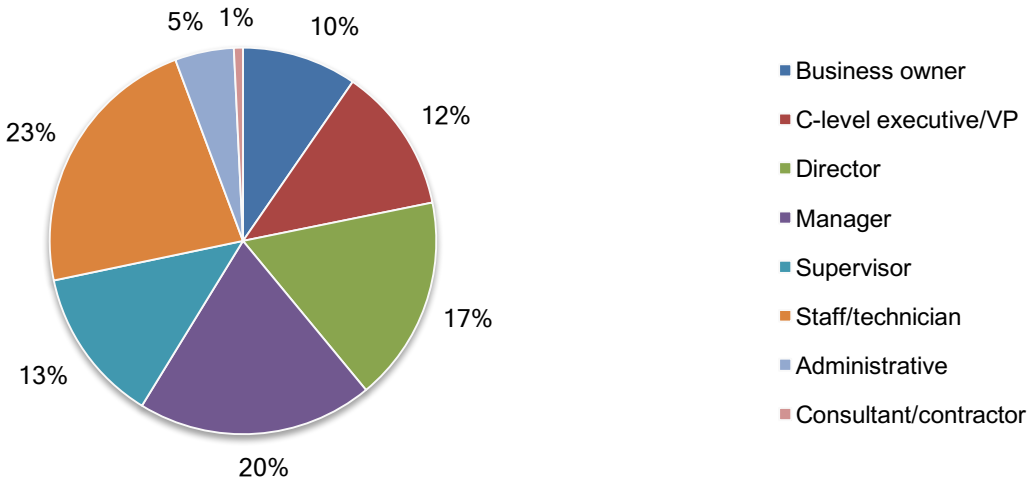
## Part 3. Methods

The survey's sampling frame comprised of 28,919 IT practitioners and IT security practitioners from companies in the United States and United Kingdom; these companies had headcounts ranging from less than 100 to 1,000. Table 1 shows that there were 1,149 returned surveys. After screening and reliability checks, we removed 104 surveys. Thus, the final sample consisted of 1,045 surveys (a 3.6 percent response rate).

| **Table 1. Sample response** | Freq | Pct% |
|---|---|---|
| Sampling frame | 28,919 | 100.0% |
| Total returns | 1,149 | 4.0% |
| Rejected or screened surveys | 104 | 0.4% |
| Final sample | 1,045 | 3.6% |

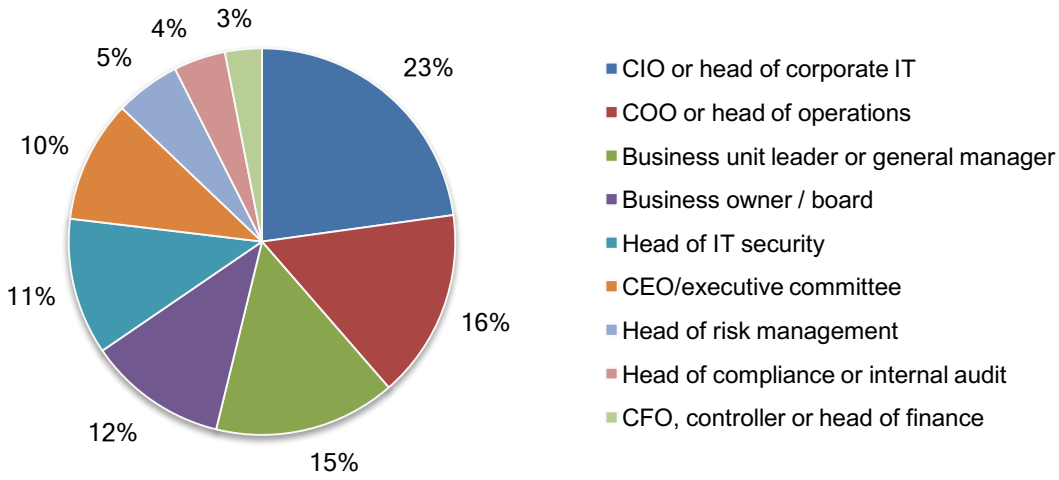
Pie Chart 1 reports the respondents' organizational level within their companies. By design, 72 percent of respondents are at or above the supervisory levels.

**Pie Chart 1. Position level within the organization**



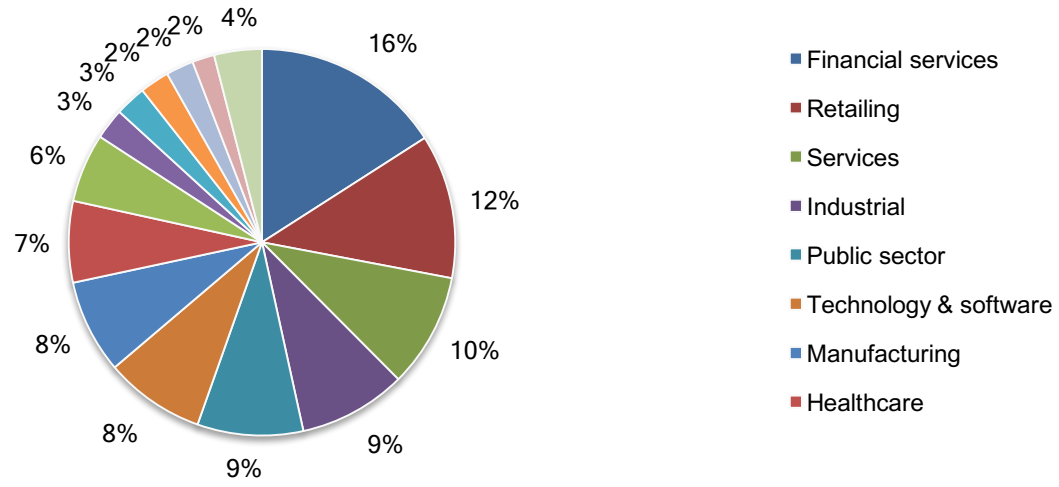
As shown in Pie Chart 2, 23 percent of respondents report directly to their company's CIO or head of corporate IT, 16 percent report to the company's COO or head of operations, 15 percent report to the company's business unit leader or general manager, 12 percent report to the business owner or board, and 11 percent of respondents report to the company's head of IT security.

**Pie Chart 2. The commands reported to in your current role**




Pie Chart 3 provides the industries of the respondents' companies. Financial services (16 percent of respondents) is the largest segment, followed by retail (12 percent of respondents), services (10 percent of respondents), and industry (9 percent of respondents) and the public sector (also 9 percent of respondents).

**Pie Chart 3. Primary industry focus**



**Part 4. Caveats to this study**

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

## Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from July 19 2018 to July 31, 2018.

| Survey response | FY 2018 | FY 2017 |
|---|---|---|
| Total sampling frame | 28,919 | 29,988 |
| Total returns | 1,149 | 1,152 |
| Rejected surveys | 104 | 112 |
| Final sample | 1,045 | 1,040 |
| Response rate | 3.6% | 3.5% |
| Sample weight | 1.00 | 1.00 |

**Part 1. Screening Questions**

| S1. What range best describes the full-time employee headcount of your organization? | FY 2018 | FY 2017 |
|---|---|---|
| Less than 100 | 157 | 168 |
| 100 to 250 | 160 | 172 |
| 251 to 500 | 229 | 209 |
| 501 to 750 | 245 | 252 |
| 751 to 1,000 | 254 | 239 |
| More than 1,000 [STOP] | - | - |
| Total | 1,045 | 1,040 |

| S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply. | FY 2018 | FY 2017 |
|---|---|---|
| Setting IT security priorities | 66% | 62% |
| Managing IT security budgets | 57% | 57% |
| Selecting vendors and contractors | 46% | 49% |
| Determining IT security strategy | 45% | 46% |
| Evaluating program performance | 44% | 44% |
| None of the above [STOP] | 0% | 0% |
| Total | 259% | 257% |

| S3. How do you rate your level of involvement in the evaluation, selection, and/or implementation of IT security products or services in your organization? | FY 2018 | FY 2017 |
|---|---|---|
| Very high level of involvement | 33% | 34% |
| High level of involvement | 43% | 43% |
| Moderate level of involvement | 19% | 19% |
| Low level of involvement | 5% | 5% |
| Not involved [STOP] | 0% | 0% |
| Total | 100% | 100% |

**Part 2: Security Posture**

| Q1. How would you describe your organization's IT security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)? 1 = not effective to 10 = very effective | FY 2018 | FY 2017 |
|---|---|---|
| 1 or 2 | 9% | 11% |
| 3 or 4 | 34% | 38% |
| 5 or 6 | 28% | 30% |
| 7 or 8 | 17% | 14% |
| 9 or 10 | 11% | 7% |
| Total | 100% | 100% |
| Extrapolated value | 5.24 | 4.87 |

| Q2. What challenges keep your organization's IT security posture from being fully effective? Please choose the top three challenges. | FY 2018 | FY 2017 |
|---|---|---|
| Insufficient budget (money) | 55% | 56% |
| Insufficient personnel | 74% | 73% |
| Lack of in-house expertise | 37% | 39% |
| Lack of clear leadership | 5% | 5% |
| Insufficient enabling security technologies | 38% | 43% |
| No understanding how to protect against cyber attacks | 47% | 47% |
| Management does not see cyber attacks as a significant risk | 4% | 5% |
| Lack of collaboration with other functions | 17% | 11% |
| Not a priority issue | 23% | 22% |
| Other | 0% | 0% |
| Total | 300% | 300% |

| Q3. What types of information are you most concerned about protecting from cyber attackers? Please choose two top choices. | FY 2018 | FY 2017 |
|---|---|---|
| Customer credit or debit card information | 40% | 37% |
| Financial information | 28% | 26% |
| Intellectual property | 51% | 48% |
| Customer records | 57% | 63% |
| Employee records | 15% | 16% |
| Business correspondence | 8% | 8% |
| Other (please specify) | 1% | 1% |
| Total | 200% | 200% |

| Q4. Who determines IT security priorities in your organization? Top two choices. | FY 2018 | FY 2017 |
|---|---|---|
| Business owners | 23% | 24% |
| Board of directors | 9% | 9% |
| Chief executive | 31% | 34% |
| Head of operations | 30% | 33% |
| Chief information officer (CIO) | 31% | 33% |
| Chief technology officer (CTO) | 7% | 8% |
| Chief information security officer (CISO) | 10% | 11% |
| Compliance officer | 7% | 6% |
| General counsel | 3% | 4% |
| Lines of business | 14% | 9% |
| No one function determines IT security priorities | 35% | 30% |
| Other (please specify) | 1% | 0% |
| Total | 200% | 200% |

| Q5. Is your organization's budget adequate for achieving a strong IT security posture? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 37% | 37% |
| No | 52% | 52% |
| Unsure | 11% | 11% |
| Total | 100% | 100% |

| Q6. What percentage of your organization's IT budget is dedicated to IT security activities? | FY 2018 | FY 2017 |
|---|---|---|
| Less than 5% | 16% | 19% |
| 5 to 10% | 31% | 27% |
| 11 to 15% | 23% | 25% |
| 16 to 20% | 18% | 19% |
| 21 to 25% | 6% | 6% |
| 26 to 30% | 3% | 3% |
| 31 to 40% | 3% | 1% |
| 41 to 50% | 0% | 0% |
| More than 50% | 0% | 0% |
| Total | 100% | 100% |
| Extrapolated value | 12.1% | 11.6% |

| Q7. Does your organization have the in-house expertise necessary for achieving a strong IT security posture? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 41% | 38% |
| No | 48% | 52% |
| Unsure | 11% | 10% |
| Total | 100% | 100% |

| Q8. What percentage of your organization's IT personnel support IT security operations? | FY 2018 | FY 2017 |
|---|---|---|
| Less than 5% | 0% | 0% |
| 5 to 10% | 4% | 5% |
| 11 to 15% | 7% | 8% |
| 16 to 20% | 10% | 12% |
| 21 to 25% | 14% | 15% |
| 26 to 30% | 10% | 11% |
| 31 to 40% | 8% | 8% |
| 41 to 50% | 11% | 8% |
| More than 50% | 35% | 33% |
| Total | 100% | 100% |
| Extrapolated value | 36% | 36% |

| Q9a. What percentage of your organization's IT security operations are supported by managed security service providers (MSSPs)? | FY 2018 | FY 2017 |
|---|---|---|
| None [Skip Q10] | 41% | 47% |
| Less than 10% | 9% | 10% |
| 10% to 25% | 8% | 12% |
| 26% to 50% | 11% | 11% |
| 51% to 75% | 18% | 9% |
| 76% to 100% | 14% | 10% |
| Total | 100% | 100% |
| Extrapolated value | 29% | 21% |

| Q9b. Following are core services typically provided by MSSPs. Please check all services provided by MSSPs to support your organization's IT security posture. *not a response in 2017 | FY 2018 | FY 2017 |
|---|---|---|
| Monitored or managed firewalls or intrusion prevention systems (IPSs) | 66% | 68% |
| Monitored or managed intrusion detection systems (IDSs) | 43% | 50% |
| Monitored or managed multifunction firewalls | 30% | 28% |
| Managed or monitored security gateways for messaging or Web traffic | 39% | 43% |
| Security analysis and reporting of events collected from IT infrastructure logs | 20% | 20% |
| Reporting associated with monitored/managed devices and incident response | 17% | 17% |
| Managed vulnerability scanning of networks, servers, databases or applications | 36% | 40% |
| Distributed denial of service (DDoS) protection | 14% | 13% |
| Monitoring or management of customer-deployed security information and event management (SIEM) technologies | 8% | 8% |
| Monitoring and/or management of advanced threat defense technologies | 11% | 10% |
| Identity and access management * | 22% | |
| Privileged access management * | 17% | |
| Total | 323% | 298% |

| Q10. Does your organization strive to comply with leading IT security guidelines or standards? Please check the standards that your organization attempts to comply with. | FY 2018 | FY 2017 |
|---|---|---|
| PCI DSS | 46% | 43% |
| ISO 27001/2 | 6% | 6% |
| SOC 2/3 | 17% | 15% |
| COBIT | 9% | 10% |
| SOX 404 | 18% | 17% |
| NIST | 17% | 17% |
| HIPAA/HiTECH | 8% | 10% |
| None of the above | 31% | 41% |
| Other (please specify) | 6% | 6% |
| Total | 158% | 165% |

| Q11. What percent of your organization's business-critical applications are accessed from mobile devices such as smart phones, tablets and others? Your best guess is welcome. | FY 2018 |
|---|---|
| Zero | 0% |
| Less than 10% | 5% |
| 11 to 25% | 17% |
| 36 to 50% | 37% |
| 51 to 75% | 30% |
| 76 to 100% | 11% |
| Total | 100% |
| Extrapolated value | 45% |

**Part 3: Cyber Attacks**

| Q12a. Has your organization experienced a cyber attack in the past 12 months? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 67% | 61% |
| No | 22% | 24% |
| Unsure | 11% | 14% |
| Total | 100% | 100% |

| Q12b. If yes, what best describes the type of attacks experienced by your organization? Please select all that apply. | FY 2018 | FY 2017 |
|---|---|---|
| Advanced malware / zero day attacks | 24% | 16% |
| Phishing / social engineering | 52% | 48% |
| SQL injection | 20% | 24% |
| Cross-site scripting | 9% | 10% |
| Denial of services | 26% | 26% |
| Compromised / stolen devices | 34% | 30% |
| Malicious insider | 12% | 11% |
| General malware | 37% | 36% |
| Web-based attack | 47% | 43% |
| Other (please specify) | 4% | 3% |
| Total | 266% | 248% |

| Q13a. Has your organization ever experienced situations when exploits and malware have evaded your intrusion detection system? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 72% | 66% |
| No | 20% | 22% |
| Unsure | 8% | 12% |
| Total | 100% | 100% |

| Q13b. Has your organization ever experienced situations when exploits and malware have evaded your anti-virus solutions? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 82% | 81% |
| No | 12% | 13% |
| Unsure | 6% | 5% |
| Total | 100% | 100% |

| Please rate the following statements using the five-point scale provided below each item. | | |
|---|---|---|
| Q14a. Cyber attacks experienced by my organization are becoming more **targeted**. | **FY 2018** | **FY 2017** |
| Strongly agree | 28% | 27% |
| Agree | 34% | 33% |
| Unsure | 16% | 19% |
| Disagree | 13% | 13% |
| Strongly disagree | 9% | 9% |
| Total | 100% | 100% |

| Q14b. Cyber attacks experienced by my organization are becoming more **sophisticated**. | **FY 2018** | **FY 2017** |
|---|---|---|
| Strongly agree | 23% | 26% |
| Agree | 36% | 33% |
| Unsure | 21% | 21% |
| Disagree | 13% | 12% |
| Strongly disagree | 8% | 8% |
| Total | 100% | 100% |

| Q14c. Cyber attacks experienced by my organization are becoming more **severe** in terms of negative consequences (such as financial impact). | **FY 2018** | **FY 2017** |
|---|---|---|
| Strongly agree | 26% | 27% |
| Agree | 34% | 32% |
| Unsure | 22% | 24% |
| Disagree | 12% | 12% |
| Strongly disagree | 5% | 5% |
| Total | 100% | 100% |

| Q14d. The use of strong passwords and/or biometrics is an essential part of my organization's security defense. | **FY 2018** | **FY 2017** |
|---|---|---|
| Strongly agree | 31% | 28% |
| Agree | 31% | 32% |
| Unsure | 20% | 19% |
| Disagree | 12% | 13% |
| Strongly disagree | 7% | 7% |
| Total | 100% | 100% |

| Q15a. My company believes it is too small to be the target of ransomware. | **FY 2018** | **FY 2017** |
|---|---|---|
| Strongly agree | 22% | 20% |
| Agree | 32% | 31% |
| Unsure | 15% | 15% |
| Disagree | 22% | 23% |
| Strongly disagree | 10% | 11% |
| Total | 100% | 100% |

| Q15b. My company would never pay ransom even if we lost the data. | FY 2018 | FY 2017 |
|---|---|---|
| Strongly agree | 25% | 22% |
| Agree | 26% | 27% |
| Unsure | 26% | 26% |
| Disagree | 16% | 17% |
| Strongly disagree | 7% | 8% |
| Total | 100% | 100% |

| Q15c. Negligent employees put our company at risk for a ransomware attack. | FY 2018 | FY 2017 |
|---|---|---|
| Strongly agree | 24% | 24% |
| Agree | 37% | 34% |
| Unsure | 14% | 15% |
| Disagree | 18% | 18% |
| Strongly disagree | 7% | 8% |
| Total | 100% | 100% |

| Q15d. A ransomware attack would have serious financial consequences for our company. | FY 2018 | FY 2017 |
|---|---|---|
| Strongly agree | 25% | 23% |
| Agree | 31% | 35% |
| Unsure | 21% | 21% |
| Disagree | 18% | 16% |
| Strongly disagree | 5% | 6% |
| Total | 100% | 100% |

| Q15e. We are confident our current antivirus software will protect our company from ransomware. | FY 2018 | FY 2017 |
|---|---|---|
| Strongly agree | 22% | 22% |
| Agree | 26% | 26% |
| Unsure | 20% | 19% |
| Disagree | 24% | 24% |
| Strongly disagree | 9% | 9% |
| Total | 100% | 100% |

| Q16. Have you or your company experienced ransomware? | FY 2018 | FY 2017 |
|---|---|---|
| Yes, within the past 3 months | 11% | 10% |
| Yes, within the past 6 months | 17% | 14% |
| Yes, within the past 12 months | 19% | 18% |
| Yes, more than 12 months ago | 14% | 9% |
| No (Skip to Part 4) | 39% | 48% |
| Total | 100% | 100% |

| Q17. How many ransomware incidents have you or your company experienced? | FY 2018 | FY 2017 |
|---|---|---|
| 1 | 44% | 47% |
| 2 to 5 | 36% | 31% |
| 6 to 10 | 15% | 17% |
| Greater than 10 | 5% | 5% |
| Total | 100% | 100% |

| Q18. How was the ransomware unleashed? Please select all that apply. | FY 2018 | FY 2017 |
|---|---|---|
| Phishing/social engineering | 79% | 79% |
| Insecure or spoofed website | 29% | 27% |
| Social media | 12% | 14% |
| Malvertisements | 13% | 14% |
| Other | 3% | 4% |
| Total | 135% | 139% |

| Q19. What type of device was compromised by ransomware? Please select all that apply. | FY 2018 | FY 2017 |
|---|---|---|
| Desktop/laptop | 82% | 78% |
| Mobile device | 41% | 37% |
| Server | 33% | 34% |
| Other | 3% | 4% |
| Total | 160% | 152% |

| Q20. How much was the ransom? | FY 2018 | FY 2017 |
|---|---|---|
| Less than $100 | 10% | 13% |
| $100 to $500 | 26% | 30% |
| $501 to $1,000 | 30% | 30% |
| $1,001 to $5,000 | 12% | 13% |
| $5,001 to $10,000 | 10% | 7% |
| More than $10,000 | 12% | 8% |
| Total | 100% | 100% |
| Extrapolated value (US$) | 1,466 | $941 |

**UK amount was converted from GBP to dollars*

| Q21a. Did your company pay the ransom? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 70% | 60% |
| No | 30% | 40% |
| Total | 100% | 100% |

| Q21b. If you did not pay a ransom, why not? | FY 2018 | FY 2017 |
|---|---|---|
| We had a full backup | 73% | 67% |
| Company policy is not to pay ransom | 32% | 29% |
| Law enforcement told us not to pay it | 10% | 9% |
| We did not believe the bad guys would provide the decryption cypher | 49% | 52% |
| Compromised data was not critical for our business | 20% | 21% |
| Other | 3% | 3% |
| Total | 186% | 182% |

**Part 4. Data breach experience**

| Q22a. Has your organization experienced an incident involving the loss or theft of sensitive information about customers, target customers or employees (a.k.a. data breach) in the past 12 months? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 58% | 54% |
| No [skip to Part 5] | 42% | 46% |
| Total | 100% | 100% |

| Q22b. If yes, with respect to your organization's largest breach over the past 12 months, how many individual records were lost or stolen? | FY 2018 | FY 2017 |
|---|---|---|
| Less than 100 | 33% | 33% |
| 100 to 500 | 23% | 26% |
| 501 to 1,000 | 15% | 15% |
| 1,001 to 10,000 | 14% | 14% |
| 10,001 to 50,000 | 8% | 7% |
| 50,001 to 100,000 | 6% | 4% |
| 100,001 to 1,000,000 | 1% | 1% |
| More than 1,000,000 | 0% | 0% |
| Total | 100% | 100% |
| Extrapolated value | 10,848 | 9,350 |

| Q22c. If yes, what were the root causes of the data breaches experienced by your organization? Please select that apply. | FY 2018 | FY 2017 |
|---|---|---|
| Malicious insider | 7% | 7% |
| External (hacker) attacks | 37% | 33% |
| Negligent employee or contractor | 60% | 54% |
| Error in system or operating process | 30% | 34% |
| Third party mistakes | 43% | 43% |
| Other (please specify) | 1% | 2% |
| Don't know | 31% | 32% |
| Total | 209% | 206% |

| Q23. Does your organization have an incident response plan for responding to cyber attacks and data breaches? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 60% | 55% |
| No | 39% | 44% |
| Unsure | 1% | 1% |
| Total | 100% | 100% |

**Part 5. Password practices and policies**

| Q24a. Does your organization have **visibility in**to employees' password practices? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 45% | 41% |
| No | 50% | 52% |
| Unsure | 4% | 7% |
| Total | 100% | 100% |

| Q24b. If yes, are you able to determine the following steps taken by employees? Please select all that apply. | FY 2018 |
|---|---|
| Using unique or strong passwords | 46% |
| Making periodic changes to passwords | 47% |
| Sharing passwords with others | 24% |
| The number of passwords each employee has | 46% |
| Total | 163% |

| Q25a. Does your organization have a policy pertaining to employees' use of passwords? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 47% | 43% |
| No | 49% | 52% |
| Unsure | 5% | 5% |
| Total | 100% | 100% |

| Q25b. If yes, does your organization strictly enforce this policy? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 32% | 32% |
| No | 64% | 63% |
| Unsure | 4% | 5% |
| Total | 100% | 100% |

| Q26a. Does your organization require employees to use a password manager? | FY 2018 |
|---|---|
| Yes | 22% |
| No | 74% |
| Unsure | 4% |
| Total | 100% |

| Q26b. If no, what does your organization use to manage and protect its passwords? | FY 2018 |
|---|---|
| Spreadsheets | 51% |
| Manually write them down on paper or sticky notes | 30% |
| Human memory | 53% |
| Browser extension | 18% |
| Other (please specify) | 4% |
| Total | 157% |

| Q27. What is your biggest pain point about employees and their passwords? Please select your top two choices. | FY 2018 |
|---|---|
| Time spent resetting passwords | 58% |
| Changing passwords when an employee leaves his job | 46% |
| Employees using weak passwords | 67% |
| Employee passwords being stolen or compromised | 68% |
| Employee adoption of best practices | 38% |
| Total | 277% |

| Q28. Does your organization take any of the following steps? Please select all that apply. | FY 2018 |
|---|---|
| Periodic password changes | 44% |
| Assign randomly chosen passwords | 30% |
| Require minimum password lengths | 32% |
| Prohibit employees from reusing the same password on internal systems | 34% |
| Provide an alternative to keyboard entry (i.e., voice recognition, biometrics) | 46% |
| Require more than one authentication system such as 2FA | 40% |
| Monitor third-party sites where compromised passwords are shared | 40% |
| None of the above | 22% |
| Other (please specify) | 1% |
| Total | 289% |

| Q29. What would prevent your organization from adopting biometrics? | FY 2018 |
|---|---|
| Too costly | 43% |
| Difficult to enforce | 48% |
| Too risky if biometric information was lost | 43% |
| Still need passwords as backup | 39% |
| Total | 172% |

**Single sign-on (SSO)** is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system.

| Q30. Does your organization use SSO? | FY 2018 | FY 2017 |
|---|---|---|
| Yes, fully implemented across the enterprise | 31% | 27% |
| Yes, partially implemented across the enterprise | 27% | 24% |
| No (skip to Q32) | 42% | 50% |
| Total | 100% | 100% |

| Q31. Do you believe that SSO increases the security of user access to your organization's applications and data? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 73% | 69% |
| No | 22% | 26% |
| Unsure | 6% | 5% |
| Total | 101% | 100% |

| Q32. In your opinion, how does the use of mobile devices such as tablets and smart phones to access business-critical applications and IT infrastructure affect your organization's security posture? | FY 2018 | FY 2017 |
|---|---|---|
| Improves security posture | 6% | 6% |
| Diminishes security posture | 49% | 48% |
| No affect on security posture | 33% | 35% |
| Cannot determine | 12% | 11% |
| Total | 100% | 100% |

**Part 6. Enabling Security Technologies**

| Q33. Do the security technologies currently used by your organization detect and block most cyber attacks? | FY 2018 | FY 2017 |
|---|---|---|
| Yes | 40% | 39% |
| No | 60% | 61% |
| Total | 100% | 100% |

| Q34. How important are each of the following security technologies used your organization **today**? Please use the following importance scale for each technology listed. Leave blank if a given technology is not deployed by your organization. % Essential and Very Important responses combined. | FY 2018 | FY 2017 |
|---|---|---|
| Anti-malware | 95% | 96% |
| Anti-denial of services | 38% | 41% |
| Artificial intelligence/machine learning | 31% | 27% |
| Privileged user access management | 42% | 36% |
| Automated patch management systems | 55% | 49% |
| Password protection / management | 62% | 52% |
| Big data analytics | 20% | 22% |
| Data loss prevention (DLP) | 25% | 25% |
| Encryption technologies | 38% | 41% |
| Tokenization | 14% | 14% |
| Endpoint management | 29% | 28% |
| Mobile device management (MDM) | 28% | 27% |
| Client firewalls | 88% | 89% |
| Identity & access management | 41% | 39% |
| Intrusion detection and prevention | 64% | 62% |
| Network traffic intelligence | 21% | 22% |
| Next generation firewalls (NGFW) | 28% | 29% |
| VPN and other secure web gateways | 63% | 62% |
| Security incident & event management (SIEM) | 33% | 30% |
| Unified threat management (UTM) | 13% | 12% |
| Web application firewalls (WAF) | 36% | 36% |
| Other | 1% | 2% |
| Total | 864% | 842% |

| Q35. In your opinion, what are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems? | FY 2018 | FY 2017 |
|---|---|---|
| Desktops | 19% | 21% |
| Laptops | 49% | 43% |
| Tablets | 19% | 20% |
| Smart phones | 40% | 39% |
| Web server | 33% | 30% |
| Intranet server | 42% | 36% |
| Routers | 6% | 6% |
| Portable storage devices (including USBs) | 7% | 8% |
| Cloud systems | 42% | 38% |
| Mobile devices | 55% | 56% |
| IoT devices* | 41% | |
| Other (please specify) | 1% | 2% |
| Total | 356% | 300% |

**Internet of things*

**Part 7. The cost of compromises**

| Q36a. Approximately, how much did damage or theft of IT assets and infrastructure cost your organization over the past 12 months? | FY 2018 | FY 2017 |
|---|---|---|
| We had no compromises | 32% | 34% |
| Less than $5,000 | 8% | 8% |
| $5,001 to $10,000 | 2% | 2% |
| $10,001 to $50,000 | 5% | 6% |
| $50,001 to $100,000 | 5% | 6% |
| $100,001 to $250,000 | 7% | 8% |
| $250,001 to $500,000 | 9% | 8% |
| $500,001 to $999,999 | 8% | 9% |
| $1 million to $5 million | 11% | 10% |
| $5 million to $10 million | 11% | 6% |
| More than $10 million | 2% | 1% |
| Total | 100% | 99% |
| Extrapolated value (US$) | $1,426,422 | $1,027,053 |

**UK amount was converted from GBP to dollars*

| Q36b. Approximately, how much did disruption to normal operations cost your organization over the past 12 months? | FY 2018 | FY 2017 |
|---|---|---|
| We had no compromises | 32% | 33% |
| Less than $5,000 | 8% | 8% |
| $5,001 to $10,000 | 2% | 2% |
| $10,001 to $50,000 | 6% | 6% |
| $50,001 to $100,000 | 4% | 4% |
| $100,001 to $250,000 | 7% | 10% |
| $250,001 to $500,000 | 9% | 9% |
| $500,001 to $999,999 | 8% | 9% |
| $1 million to $5 million | 10% | 9% |
| $5 million to $10 million | 7% | 6% |
| More than $10 million | 5% | 3% |
| Total | 100% | 100% |
| Extrapolated value (US$) | $1,562,124 | $1,207,965 |

| Q37a. Have you had an attack involving the compromise of employees' passwords in the past year? | FY 2018 |
|---|---|
| Yes | 40% |
| No | 52% |
| Unsure | 8% |
| Total | 100% |

| Q37b. If yes, how much did each attack cost your organization? | FY 2018 |
|---|---|
| Less than $10,000 | 3% |
| $10,001 to $50,000 | 7% |
| $50,001 to $100,000 | 14% |
| $100,001 to $250,000 | 29% |
| $250,001 to $500,000 | 22% |
| $500,001 to $1,000,000 | 13% |
| More than $1,000,000 | 12% |
| Total | 100% |
| Extrapolated value (US$) | $383,365 |

| Part 8. General Data Protection Regulation (GDPR) | |
|---|---|
| Q38. Is your organization required to comply with GDPR? | FY 2018 |
| Yes | 72% |
| No [Skip to Part 9] | 19% |
| Unsure [Skip to Part 9] | 9% |
| Total | 100% |

| Q39. If yes, did compliance require significant changes in your privacy and security strategies? | FY 2018 | FY 2017 |
|---|---|---|
| Yes, significant change | 41% | 37% |
| Yes, some change | 41% | 37% |
| Yes, nominal change | 11% | 18% |
| No change | 7% | 8% |
| Total | 100% | 100% |

| Q40. Using the following 10-point scale, please rate your organization's level of compliance with the GDPR. 1 = not ready and 10 = ready. | FY 2018 |
|---|---|
| 1 or 2 | 18% |
| 3 or 4 | 23% |
| 5 or 6 | 20% |
| 7 or 8 | 21% |
| 9 or 10 | 19% |
| Total | 100% |
| Extrapolated value | 5.48 |

**Part 9. Role & Organizational Characteristics**

| D1. What best describes your position level within the organization? | FY 2018 | FY 2017 |
|---|---|---|
| Business owner | 10% | 10% |
| C-level executive/VP | 12% | 11% |
| Director | 17% | 17% |
| Manager | 20% | 21% |
| Supervisor | 13% | 12% |
| Staff/technician | 23% | 24% |
| Administrative | 5% | 4% |
| Consultant/contractor | 1% | 1% |
| Total | 100% | 100% |

| D2. Which of the following commands do you report to in your current role? | FY 2018 | FY 2017 |
|---|---|---|
| Business owner / board | 12% | 12% |
| CEO/executive committee | 10% | 9% |
| COO or head of operations | 16% | 16% |
| CFO, controller or head of finance | 3% | 3% |
| CIO or head of corporate IT | 23% | 27% |
| Business unit leader or general manager | 15% | 13% |
| Head of compliance or internal audit | 4% | 4% |
| Head of risk management | 5% | 5% |
| Head of IT security | 11% | 11% |
| Total | 100% | 100% |

| D3. What best describes your organization's primary industry classification? | FY 2018 | FY 2017 |
|---|---|---|
| Aerospace & defense | 1% | 1% |
| Agriculture & food services | 1% | 2% |
| Communications | 2% | 2% |
| Construction and real estate | 3% | 3% |
| Consumer goods | 6% | 6% |
| Education & research | 2% | 2% |
| Entertainment, media and publishing | 1% | 3% |
| Financial services | 16% | 14% |
| Healthcare | 7% | 7% |
| Industrial | 9% | 9% |
| Logistics and distribution | 1% | 1% |
| Manufacturing | 8% | 8% |
| Pharmaceuticals | 2% | 3% |
| Public sector | 9% | 9% |
| Retailing | 12% | 12% |
| Services | 10% | 9% |
| Technology & software | 8% | 7% |
| Transportation | 3% | 2% |
| Total | 100% | 100% |

**Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.**

## Ponemon Institute

*Advancing Responsible Information Management*

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and companies.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

**About Keeper Security, Inc.**

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. Keeper is the leading provider of *zero-knowledge* security and encryption software covering password management, cybersecurity, dark web monitoring, digital file storage and messaging. Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 Certified and is also certified for use by the Federal government through the System for Award Management (SAM) and the General Services Administration (GSA). Keeper protects businesses of all sizes across every major industry sector.

Public Knowledge

April 9, 2020

The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce, Science, and Transportation
555 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
511 Hart Senate Office Building
Washington, DC 20510

**Re: Hearing on Enlisting Big Data in the Fight Against Coronavirus**

Dear Chairman Wicker and Ranking Member Cantwell,

The proper use of personal data has the potential to have important benefits for public health as we face the COVID-19 crisis. Technology can and should play an important role during this effort to save lives, such as to spread public health messages and increase access to health care. However, efforts to contain the virus must not be used as a cover to usher in a new era of greatly expanded systems of invasive digital surveillance. Allowing access to personal data without guardrails threatens fundamental rights and liberties and opens the door for communities to be exposed to civil rights harms through the exploitation of their data.

One such guardrail should be that the collection and processing of personal data must be necessary and proportionate to the pandemic response as well as the protection of public health. All response measures should be temporary in nature, limited in scope, restricted to using anonymized aggregate data whenever possible, and adopted only if they are a necessary response to the COVID-19 crisis. The data collected and processed should be limited to the minimum necessary amount for the purposes of implementing measures for pandemic response. There must also be limits on processing newly collected or acquired personal data for purposes unconnected to public health and services. The personally identifiable data should not be kept or repurposed except in the case of narrowly defined medical research purposes and pandemic preparedness. For those specific uses, informed and explicit consent of the individual should be required.

Another guardrail would be requiring adequate security measures to protect personal data. Attempts to respond to this pandemic cannot be used as justification for

compromising people's digital safety; this crisis does not minimize the need for security protections in the context of pandemic response. Data must be maintained in a secure environment and transmitted through secure methods. And any claims that publicly shared data has been anonymized must be based on evidence and supported with sufficient information explaining the anonymization process.

Any use of digital surveillance technologies in responding to COVID-19, including big data and artificial intelligence systems, must include risk assessments that address concerns around discrimination and other rights abuses against racial minorities, people living in poverty, and other marginalized populations, whose needs and lived realities may be obscured or misrepresented in large datasets. We should bear in mind the last time mass surveillance power expanded was when Congress passed the Patriot Act. It was argued, as it is being argued now, that increased surveillance was necessary in order to protect Americans. Instead, the tools designed to address terrorism ended up being used by law enforcement during the course of ordinary investigations, which only exacerbated the difference in policing between white communities and communities of color.[1] We need to learn from these previous lessons and do our best to ensure that this expansion of data collection practices is limited, and that those limitations apply to both public and private entities. Also, all data collection efforts undertaken as a response to the pandemic should include means for active and meaningful participation of all relevant stakeholders, and, in particular, marginalized population groups.

The final guardrail is requiring accountability provisions for any pandemic responses that collect or process data. This is a fundamental safeguard against abuse. First, there must be transparency about the measures taken so that they can be scrutinized and, if appropriate, later modified, retracted, or overturned. Furthermore, any decision-making related to data collection and processing in the context of pandemic response must be informed by guidance and directions of public health authorities; therefore, the guidance and decisions must be made publicly available. Additionally, individuals must be given the opportunity to know about and challenge any COVID-19 related measures to collect, aggregate, retain, and use personal data. Individuals must have access to their data and be allowed to correct or delete their data when practicable. Finally, there must be real, commensurate consequences for governments' and companies' failure to protect personal data.

We have identified a few key areas where legislation would provide immediate privacy benefits and significantly reduce the harms as outlined in this letter. These include:

[1] Benjamin Wallace-Wells, *Patriot Act*, New York Magazine (August 26, 2011) https://nymag.com/news/9-11/10th-anniversary/patriot-act/.

1. **Creating Rules for Public-Private Data Sharing.** If governments enter into data sharing arrangements with other entities, those arrangements must be based in law and memorialized in writing. The existence of these agreements and information necessary to assess their impact on privacy must be publicly disclosed, with sunset clauses, public oversight and other safeguards by default. Businesses involved in efforts by governments to tackle COVID-19 must undertake due diligence to ensure they respect human rights. Any new data or processing for this purpose must be firewalled from other business and commercial interests. Furthermore, the results of any data-sharing should be made public in a machine-readable format, if the publicization of the results would not result in re-identification of the individuals whose data was collected. It would also have the added benefit of allowing others to iterate and innovate. Preference for these data sharing arrangements should not be given to large players in the data ecosystem; we've already seen increasing consolidation in the technology space,[2] and these initiatives should not add fuel to the fire.
2. **Closing the HIPAA Privacy Loophole.** HIPAA does not currently cover technology like health apps, direct-to-consumer genetic tests, and other consumer-focused health technology, like wearable fitness monitors. As it has become more difficult than ever to personally interact with a doctor or hospital, consumers are relying on these technologies to assess their risk, as well as to make and even participate in medical appointments. This means consumers are giving up their health data without adequate protection. Congress should give HHS the authority to promulgate clear and public rules regulating this growing industry to ensure that all Americans' health data is kept private and secure, no matter who is collecting it.
3. **Protecting Geolocation Data.** While federal law prevents cell phone network operators from disclosing geolocation data to anyone other than emergency services, mobile phone operating system providers and mobile applications can disclose this data to anyone. Geolocation data can reveal a person's politics, sexual preferences, religion, and other sensitive characteristics. The government having access to geolocation data, and all that it reveals, is deeply concerning. Americans should not need to make their highly sensitive location data available for exploitation as the cost of staying in touch with emergency services at all times. Congress must prevent our geolocation data from being exploited by any actor who has access to that information; therefore, we are asking that current geolocation data protections that apply to cell phone network operators be applied to phone operating systems.

We look forward to working with the committee to ensure that privacy protections are built into public health initiatives during this time of crisis.

---

[2] Alex Petros, *Acquisitions in the Time of COVID: Big Tech Gets Bigger,* Public Knowledge (April 7,2020) https://www.publicknowledge.org/blog/acquisitions-in-the-time-of-covid-big-tech-gets-bigger/

Sincerely,

Sara Collins

Policy Counsel

Public Knowledge

Cc: Senate Commerce Committee Members