KnowBe4

2021 State of Privacy and Security Awareness Report

EXECUTIVE SUMMARY

Knowledge may be power, but knowledge without action is useless. Today's digital world is constantly pushing information to people; organizations are no different, subjecting employees to multiple policies, regulations, laws, and standards.

It begs the question as to how effective this knowledge transfer is; in particular when it comes to cybersecurity and privacy.

We wanted to understand how much training about cybersecurity and privacy best practices employees receive. More importantly, how much of that is understood, and how much of that translates into a change in behavior?

To get some insight into this question, Osterman Research conducted an in-depth survey of U.S.-based employees during late 2020 and early 2021 to understand how much employees know and how they put what they know into action.

The research report includes responses from more than 1,000 U.S. employees and takes a deep dive into the security training they've received and how the changes in their work environments during 2020 have altered their approach to cybersecurity best practices.

Key Takeaways

Lack of Confidence Leads to Security Fails

While employees are generally quite confident with regard to password best practices, they lack confidence in a number of other areas related to cybersecurity – and lack of confidence leads to security fails. These include their inability to properly identify a social engineering attack, their inability to explain security expectations for privileged vs. "standard" users, and their inability to explain how cybersecurity risks could negatively impact their employer. Only a minority of the employees surveyed believe they are well-versed in and understand threats like phishing, business email compromise, or spear phishing, despite the fact that they are common and critical threats. Password safety can be jeopardized by credential phishing.

Is Ignorance Really Bliss?

Many employees are not aware of various security risks. For example, only 48% of employees believe it is likely or very likely that their mobile device could become infected with malware if they click on a suspicious link or attachment in an email. In fact, 24% believe that clicking on a suspicious link or attachment in an email represents little or no risk. We discovered that employees in government, healthcare, and education have the least understanding about various social engineering threats.

Frequency Matters

There is a relationship between the frequency of training and perception of risk. For example, employees who are trained once per month are 34% more likely to believe that clicking on a suspicious link or attachment in an email is risky compared to employees who receive training no more than twice per year. Employees who receive training once per month are 26% more likely to believe that reusing passwords is a risky behavior than employees who receive training no more than twice per year.

Finance Industry Shows More Interest in Training

The finance industry is the most likely to receive security awareness training: we discovered that 91% have received some form of training, while this figure is 88% in the technology space and 76% in healthcare. Another interesting finding: industries with the lowest risk also provide the most training, suggesting that the more aware employees are of various threats the better able they are to protect against them.

EXECUTIVE SUMMARY

Key Takeaways

COVID Stopped Lots of Us in Our Tracks

Employee cybersecurity and data privacy training was stopped for many employees during the lockdowns. Among employees who receive this training, 23% had their training stop at the beginning of the lockdowns, while another 22% saw their training cease temporarily at the commencement of the lockdowns, but then start up again. Only 55% of employees had continuous cybersecurity and data privacy training continue throughout the lockdowns. Interestingly, we discovered that the less employees' security training was interrupted during the lockdowns, the better they were at understanding good security practices. Specifically, those whose training never stopped were more likely to know that behaviors such as clicking on suspicious email links could lead to malware infection.

Some Employees Still Need to Learn the Basics

A significant proportion of employees still need training about the problems associated with basic, risky behaviors. For example, nearly one-third of employees still believe it is safe to plug into their computer a USB drive they received at a trade show. Forty-five percent believe that they have no need to take additional safeguards regarding cybersecurity because they don't work in an IT department

Can You Spell GDPR?

Many employees don't know whether their employer is subject to a variety of privacy regulations, such as the Payment Card Industry Data Security Standard or the California Consumer Privacy Act (soon to be supplanted by the recently passed California Privacy Rights Act), even though these are key regulations that impact a large percentage of U.S.-based businesses. An average of 44% of respondents were not sure whether their employer was subject to six different privacy regulations.

TABLE OF CONTENTS

Lack of Confidence Leads to Mediocre Results

IF YOU CAN'T EXPLAIN IT TO OTHERS...

One of the key signs of truly understanding something is the ability to explain it to others. Unfortunately, a significant proportion of employees lack the confidence needed to identify key attack vectors, detect a malware infection, or understand the important concepts about cybersecurity that employees should know to be a solid line of defense against security exploits like phishing. For example, as shown in Figure 1:

- Nearly one-half (45%) lack the confidence necessary to identify a social engineering attack, including, but not limited to, phishing. This continues to be important since phishing saw a significant increase during 2020 and 2021 as a result of the pandemic.
- More than one-third (34%) lack confidence that they could name at least two warning signs that their computer or devices had been infected with malware.
- More than one-third (35%) are not confident that they can describe to their senior management the security risks that are created when employees work from home. This, even though the survey was conducted approximately 10 months into a pandemic when many employees were forced to work from home and a large percentage are still doing so.
- Many employees are not aware of proper email practices. For example, 50% agree or strongly agree that when confronted with a suspected social engineering attempt through email that they should respond to the sender for confirmation – not a good idea!
- Forty-three percent believe that bypassing their corporate cloud server in favor of local copies of documents is safe. And more than one-third (39%) mistakenly believe that using a personal cloud server account to share files between the office and home is a best practice.

FIGURE 1:

Employee Confidence About Key Cybersecurity Best Practices

Issue	Very Confident	Confident	Not Sure	Somewhat Confident	Not at all Confident
You can identify a phishing email	42%	34%	10%	10%	4%
Your current set of passwords is both strong and has not been previously compromised	42%	35%	11%	8%	3%
You can confidently describe the steps needed to actively secure work information and resources while working remotely	31%	38%	16%	9%	6%
You have to describe to your senior management the negative impacts to your organization posed by cybersecurity risks	29%	34%	17%	13%	7%
You can name at least two warning signs that malware has infected your desktop/laptop computer or mobile device	29%	38%	16%	12%	6%
You have to describe to your senior management the security risks created by storing work information in personal cloud applications	29%	32%	20%	10%	8%
You have to describe to your senior management the security risks created by employees working from home	28%	37%	17%	11%	7%
You have to describe to your senior management how security expectations for privileged users differ from those for standard users	27%	32%	22%	10%	9%
You can identify a social engineering attack	25%	30%	26%	9%	10%

Source: Osterman Research, Inc.

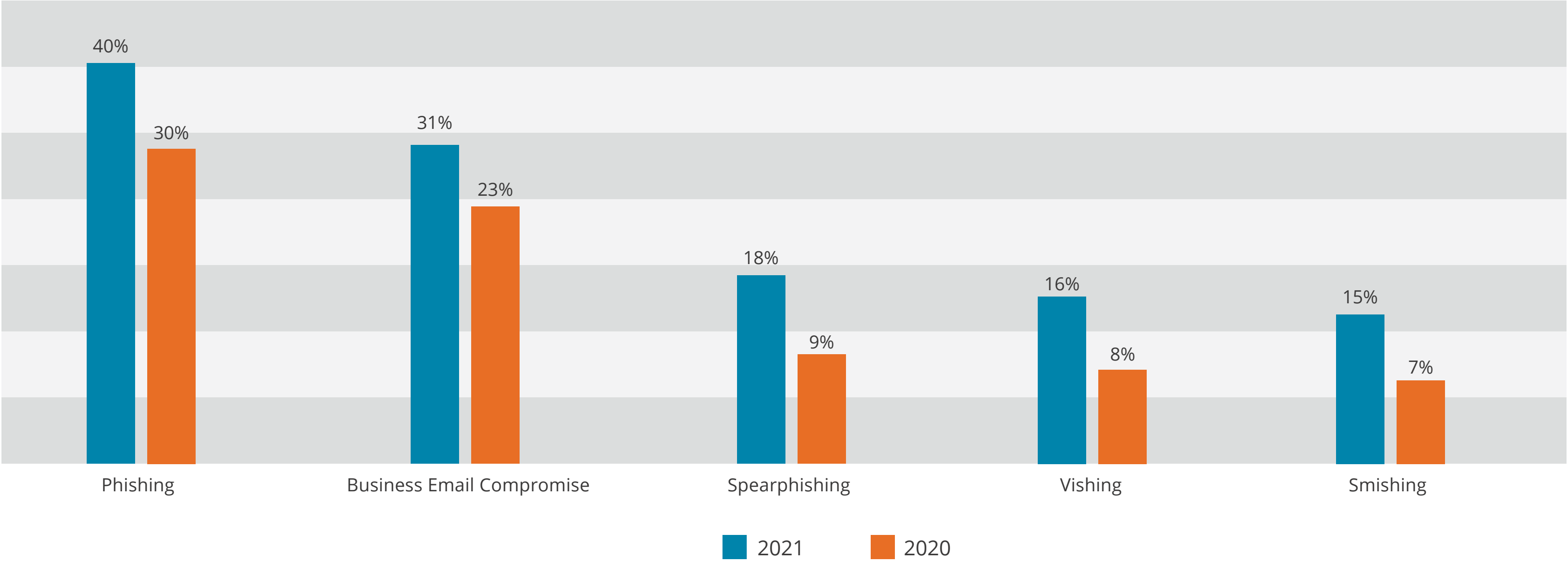
SOCIALLY AWKWARD ABOUT SOCIAL ENGINEERING

Although 40% of employees believe that they understand and could explain phishing threats to others "very well," understanding of various other social engineering threats drops off substantially from there. As shown in Figure 2, only 31% feel they understand and could explain business email compromise, even though business email compromise is an enormous and growing problem costing businesses millions of dollars each year. Understanding of other social engineering threats is even lower.

FIGURE 2:

Percentage of Employees Who Understand Social Engineering Threats "Very Well"

2021 compared to 2020



Why Is This Important?

The starting point in being able to address any cybersecurity issue – and most other issues – is the ability to understand it and explain it to others. Conversely, an inability to understand or explain important issues, especially in the context of cybersecurity, means that those who cannot are more vulnerable to exploitation and creating security risk through their behavior.

The More You Train, the More They Know

PEOPLE ARE CONSISTENTLY INCONSISTENT

Many employees know well the risks that are inherent in using email, leaving their computer unattended, and similar everyday work behaviors. For example:

- Forty-eight percent of employees believe it is likely or very likely that their mobile device could become infected with malware if they click on a suspicious link or attachment in an email, and the same proportion believe a malware infection is likely if they use the same password for multiple applications or connect to a public Wi-Fi network.
- But some knowledge of workplace-based risks does not seem to carry over to home and personal use. Case in point: only 31% of employees believe that allowing family members or friends to use work devices for personal activities outside of work hours is risky or a serious risk, and only 31% believe that using the default password on their home router represents this level of risk. Similarly, 24% of employees believe that clicking on a suspicious link or attachment in an email represents little or no risk.

TRAINING FREQUENCY MATTERS

We discovered that the more employees are trained, the more they understand the danger of risky behaviors. For example, as shown in Figure 3, employees who are trained once per month on cybersecurity issues are significantly more likely to believe that clicking on a suspicious link or attachment in an email is risky compared to employees who are trained less frequently. Similarly, except for awareness about connecting to a public Wi-Fi network, generally the more training employees receive the more they're aware of the risks associated with the variety of ways technology is used.

FIGURE 3:

Percentage Who Believe It Is Likely or Very Likely That Various Behaviors Will Result in a Malware Infection Based on the Amount of Cybersecurity Awareness Training They Receive

	FREQUENCY OF TRAINING			
Behavior	**Once per Month**	**A Few Times per Quarter**	**Once per Quarter**	**No More than Twice per Year**
Clicking a suspicious link or attachment in an email	60%	46%	49%	44%
Using weak/simple passwords	51%	46%	47%	42%
Using the same password for multiple applications	55%	50%	50%	44%
Leaving your computer unlocked while away	51%	51%	42%	37%
Connecting to a public Wi-Fi network, e.g., in an airport or coffee shop	51%	49%	46%	47%

Source: Osterman Research, Inc.

Why Is This Important?

Employees must understand that there is a relationship – sometimes a very strong one – between what they do when using a computer and other devices and the risks their employer can face when these devices are not used securely. At the same time, employers must understand that there is a relationship between the amount and quality of training that they provide to employees and the depth of understanding of security risks. This training should include not only how to deal with corporate technology and networks, but the inherent risks associated with using personal devices, home networks, and the like – an issue that became more prominent during 2020 and 2021 with remote work.

Missing the Cyber Forest for the Trees

JUST BECAUSE THEY ARE AWARE DOESN'T MEAN THEY CARE

While many employees are aware of what cybersecurity risks look like, as well as the various best practices they should pursue when computing or working online, many employees just don't practice safe computing. For example:

- When survey respondents were given five options for what constitutes the most likely sign that a desktop or laptop computer has become infected with malware, 52% correctly identified popups rapidly interrupting other programs as the most likely indicator. However, 48% considered other indicators as most likely, such as slower than normal internet speeds and the availability of an operating system update.
- When respondents were given six options about the best way to create a strong password that would be difficult for a cybercriminal to determine, 46% correctly chose "using a unique password for every device and application." However, 34% thought that simply using a special character (e.g., a "&" or "$") was the best way to create a strong password. In fact, slightly more than 3% of respondents thought that using a sequence of consecutive numbers was the best way to create a strong password, and almost 5% thought that reusing a previously used password was the best approach.
- The research discovered that 46% of employees are using a password manager to organize and secure their passwords, and another 16% of respondents plan to use one in the future. Only 53% of respondents agree or strongly agree that password managers are a good way to maintain strong password security practices.
- We found that while 52% of employees would be very likely to report a security incident, 27% will only probably do this, and the remaining 21% are either not sure of what they would do or would refuse to do so.
- Many employees (most, in some cases) understand that some behaviors are inherently risky, such as failing to use a password to access a laptop or mobile device or sharing a computer with others. On the other hand, nearly one-half (49%) of respondents consider that not encrypting data on a mobile device or laptop represents no more than a moderate risk, and many consider it to have little risk, as shown in Figure 4.

FIGURE 4:

Perceived Security Risk of Various Behaviors

Issue	Low Risk	Moderate Risk	High Risk
Keeping your laptop close by when traveling	43%	36%	22%
Disposing of documents at your home office using a shredder	40%	38%	23%
Storing data backups in a technology vendor's offsite location	13%	47%	40%
Not using biometric authentication (e.g., your fingerprint) to access your laptop or mobile device	12%	47%	41%
Allowing others to use or handle your computer	11%	31%	59%
Not encrypting the data on your laptop or mobile device	10%	39%	51%
Not using a password to access your laptop or mobile device	9%	29%	62%

Source: Osterman Research, Inc.

Why Is This Important?

The key to ensuring the security of corporate data and finances is employees understanding and following best practices. Put simply, employees who don't follow best practices cannot keep these assets safe. Understanding warning signs of risk, as well as the best practices needed to compute and work safely online, are critical skills that every employee should have in order to cut the chances of security incidents and consequences for their employer.

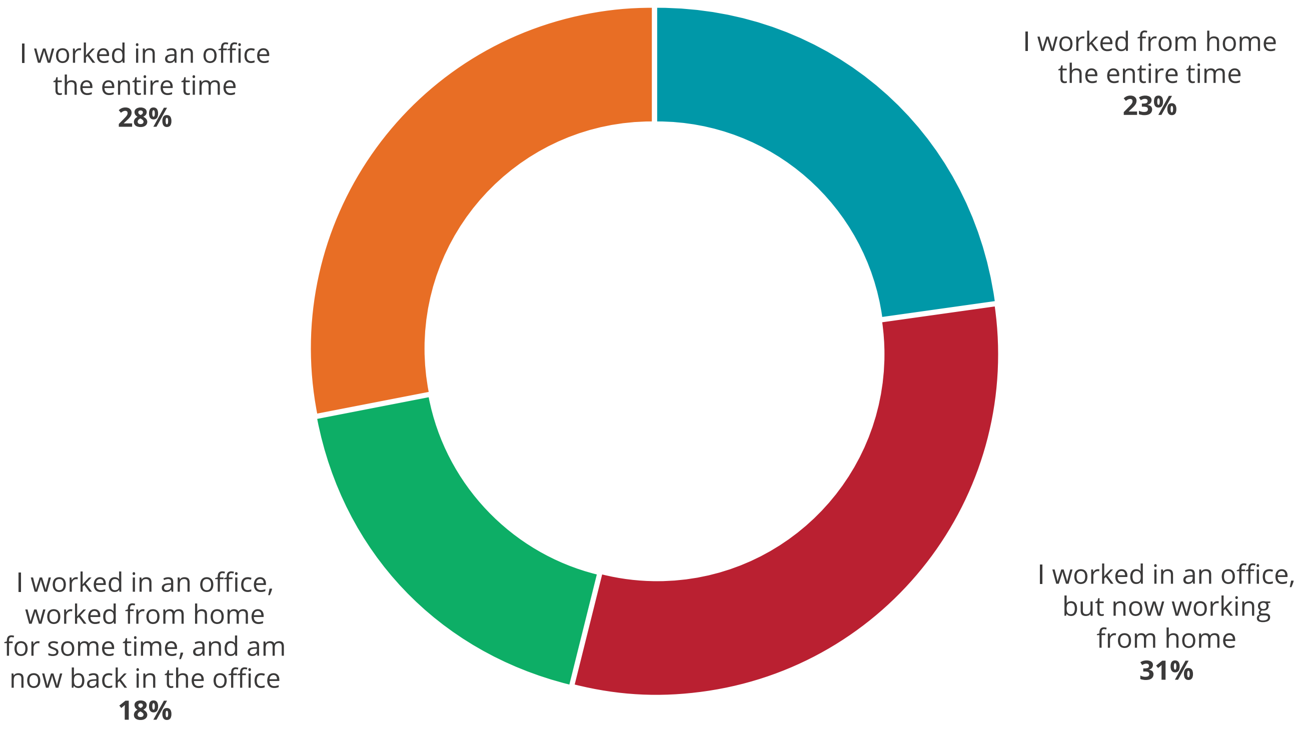
Work-From-Home Has Magnified Security Risks

2020 WAS THE YEAR OF WORKING FROM HOME

The COVID-19 pandemic dominated our way of life in 2020. For many fortunate enough to stay employed through this crisis, this meant setting up home offices, often for the first time. As shown in Figure 6, nearly one-half (49%) of those surveyed transitioned from an in-office or other workplace environment to an at-home work environment during the pandemic. This had several significant ramifications on organizations: employees had to find new ways of working and collaborating with others, employers had to find new ways to support and secure employees' online and offline activities, while both had to reimagine many interactions with customers and prospects.

FIGURE 6:

Employees' Work Situation From January 1, 2020 Through Late 2020



Source: Osterman Research, Inc.

SECURITY AWARENESS TRAINING WAS INTERRUPTED

Another ramification of the enforced work-from-home environment for many employees? A hiatus or outright end to cybersecurity and data privacy training. We discovered that among employees who receive this type of training, 23% had their training cease indefinitely as soon as the lockdowns began. Another 22% had their training stop temporarily as the lockdowns began, but then resumed. Only 55% of employees had continuous cybersecurity and data privacy training throughout the lockdowns.

THE IMPACT OF WORKING FROM HOME

The work-from-home phenomenon, carried with it several serious, negative consequences, such as curtailed security training for many employees as well as significant increases in phishing, ransomware, and other malicious activities by bad actors. These had major impacts on employers and employees alike, but our research discovered that there have also been some positives as well. For example:

- Fifty-seven percent of those surveyed agree or strongly agree that working from home has made them think more often about cybersecurity risks and how they might address them. Twenty-nine percent were not sure what impact working from home had on them in this regard, while only 14% disagreed.
- Videoconferencing, typically through Zoom or Microsoft Teams, was the go-to solution for replacing previous in-person interactions between employees and coworkers, contractors, customers and prospects. Many employees reported keeping some important best practices regarding these online meetings, including 53% who likely or very likely keep their microphone muted when not speaking, 51% who at least attempt to prevent unauthorized people from eavesdropping or seeing sensitive data during meetings, and 47% who ensure their meeting is secured with a password.
- Moreover, while not a stellar proportion, 38% of employees feel that the best way to secure a live meeting is by creating a password for entry into the meeting. Another 30% believe that the best way to secure a live meeting is by sending room links directly to attendees.

ONGOING TRAINING MAKES A DIFFERENCE

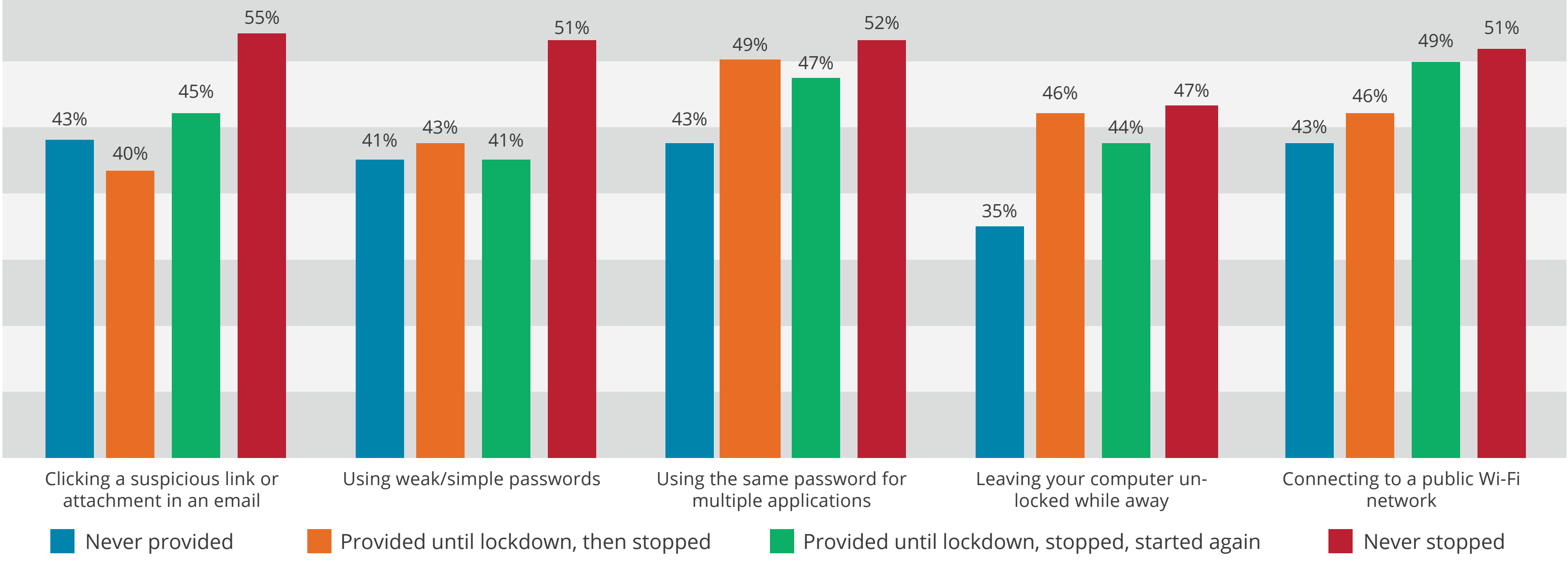
As noted in the Executive Summary, we asked survey respondents what happened to their security and privacy training after the lockdowns had begun. While we found that some respondents had never received this training, others had their training cease shortly after the lockdowns began, some had it stop then start up again, while for others their training continued without any breaks.

We found continuity of training really does make a difference. For example, as shown in Figure 7, a much higher proportion of employees whose training never stopped during the lockdowns correctly indicated that a variety of behaviors, such as clicking a suspicious link in an email or attachment, could lead to a malware infection on their computer or mobile device. We found relative consistency across the various questions we posed in this regard, demonstrating that the more consistent the training, the more likely that employees will understand the importance of good security practices.

FIGURE 7:

Likelihood That a Computer or Mobile Device Will Become Infected With Malware From

Percentage responding “likely” or “very



Source: Osterman Research, Inc.

Why Is This Important?

The work environment for tens of millions of U.S.-based employees, as well as hundreds of millions more worldwide has changed. Many companies are allowing employees to continue working from home through late 2021, and many are enabling hybrid work indefinitely.

This remote work scenario has significant implications for companies in the context of enabling security capabilities for their workforce. They must enable robust security and security awareness training for remote employees, something that many are finding is not as easily achieved as when employees are centralized in a corporate workplace. Maintaining proper training is especially important given that cybercriminals ramped up their efforts at phishing attempts and distributing ransomware during the pandemic and show no signs of slowing down.

The Importance of Privacy

FIRST THE GOOD NEWS

A bright spot across the results we collected was that employees largely understand some, if not all, best practices related to data privacy, as shown in Figure 9. For example:

- More than three-fourths (76%) of employees understand that they should show customers the corporate privacy statement before collecting their data.
- More than seven in 10 (73%) of employees understand the need to report privacy violations, even inadvertent ones, to their employer's privacy office.
- Seven out of ten (70%) understand that they should still run privacy audits even if they use third-party data processing vendors with robust track records.

That said, there are some areas that clearly need improvement:

- Forty-five percent believe that they can legally collect information on volunteers' political views as long as they justify the collection in their data protection impact assessment, even though they are not permitted to do so.
- Forty-four percent of employees believe it's acceptable to use a single privacy regulation as a template in satisfying all other privacy regulations. Because of important differences between privacy regulations, that's not a good idea.

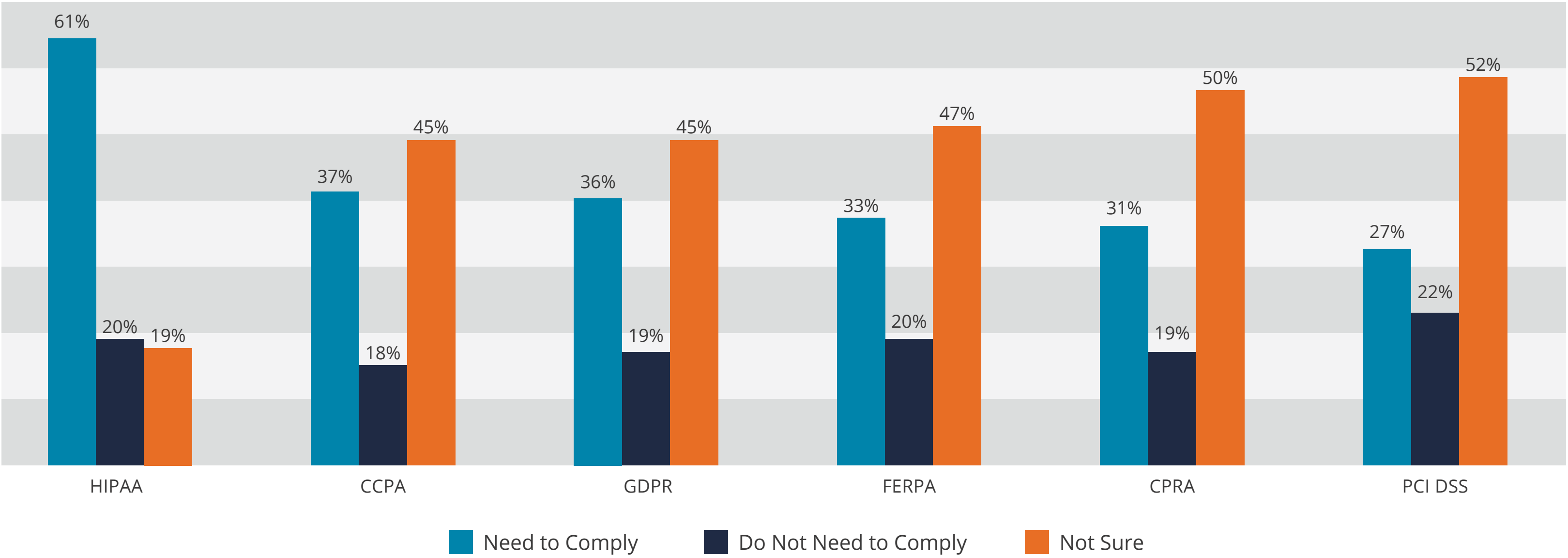
IS IT ALL DOWNHILL FROM HERE?

But the results don't support an entirely rosy picture when it comes to privacy knowledge. The last few years have seen a surge in privacy regulations, both at the state and federal levels. Driven in part by public outcry, these regulations have placed many new requirements on companies already grappling with the ever-present threat of data breach and other forms of compromise.

With these new requirements comes a continual need to keep employees informed of these requirements. This basic knowledge is one of the aspects we sought to analyze in our report.

FIGURE 8:

Employee Awareness of Their Organization’s Need to Comply With Various Privacy Regulations



Source: Osterman Research, Inc.

As shown in Figure 8, most employees understand that their employer must comply with the Health Insurance Portability and Accountability Act (HIPAA) – 61% know that compliance is required, 20% know (or at least believe) that compliance is not needed, and only 19% are unsure. However, things go downhill from there: roughly one-half of employees are not sure whether their employer must satisfy the privacy requirements of the various regulations shown in the table.

That’s a problem. As with cybersecurity, employees are the last line in addressing privacy issues, and so they must know that privacy protections must be applied to the customer data they handle. For example, if a salesperson at a U.S.-based company is dealing with an inquiry from a French prospect, she should know that the prospect’s personal information is subject to the European Union’s GDPR and manage the data accordingly. The fact that such a large proportion of employees is simply not sure whether their employer is subject to various privacy regulations does not bode well for organizations’ ability to adequately process information that is subject to privacy regulations.

Further corroborating the need to improve privacy awareness among employees is that only 24% of those surveyed are very confident that they would be able to describe to their senior management the details of their company’s privacy statement, although another 40% consider themselves to be confident.

FIGURE 9:

Agreement With Various Statements About Privacy Issues

Threat	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
We should show customers our privacy statement before we collect their data.	43%	33%	18%	4%	2%
If we use a third-party vendor with a great track record to help process the personal information of our employees, we should still run audits to ensure that they are meeting the processing and security demands of regional privacy regulations.	33%	36%	23%	5%	2%
If someone mistakenly emails me employee tax information that I don't look at, then realized their mistake and asks me to delete it, I should still report the mistake to my company's privacy office.	18%	40%	20%	5%	2%
Our corporate website tracks customer interactions with online advertisements. We don't collect personal details, but we do capture IP addresses and browsing history. This information needs to be protected just like other types of personal information.	4%	33%	22%	7%	6%
If we suffered a data breach, the notification to the parties affected should include a description of the incident, the potential consequences and risks posed to customers, some suggested actions, descriptions of assistance we're offering to help, our mitigation strategy, and finally our contact information. That's all we need to tell them.	2%	36%	24%	8%	3%
Our department collects lots of information about our customers, not all of which is necessary to collect. Although we have strong security policies that keep all information safe, I should still make a report about this to my senior management.	34%	38%	24%	7%	5%
Our company implements privacy controls and practices "by design" instead of as an afterthought.	36%	34%	30%	8%	2%
If personal data of our customers and prospects was breached, we should notify them only if required to do so by statute.	23%	28%	18%	16%	12%
Determining the origin of data is a good way to determine when privacy regulations apply.	5%	41%	26%	7%	2%

Source: Osterman Research, Inc.

FIGURE 9:

Agreement With Various Statements About Privacy Issues (Cont'd)

Threat	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
We have a privacy policy that goes into detail letting customers know exactly what personal data we will collect from them and when we will collect it, but we don't have to tell them how we intend to use it.	23%	28%	24%	15%	10%
Our company uses purchasing history to infer product recommendations for our customers, but the data does not contain personal details like a person's name, race, or age, so this is not really personal data.	22%	30%	29%	12%	7%
Once a person has seen our privacy statement, any information we collect - whether by tracking their clicks on our website or by retaining information they provide to us voluntarily - goes into our records. Once there, we aren't obligated to give individuals access because it has become an official business document.	21%	33%	29%	10%	6%
Our company collects names, addresses, and dates of birth of consenting data subjects. Next month we'll be expanding to include biometric information. Because data subjects have already consented, and because of our strong security practices, we can proceed and stay in compliance with the GDPR.	20%	30%	30%	12%	8%
Although there are a number of regional privacy regulations, it's OK to use one privacy regulation as the standard to remain in compliance with all of them.	17%	27%	30%	17%	9%
We will be collecting information on volunteers' political views. If we justify this collection in our data protection impact assessment, we'll be in compliance with privacy regulations.	17%	28%	33%	14%	8%

Source: Osterman Research, Inc.

Why Is This Important?

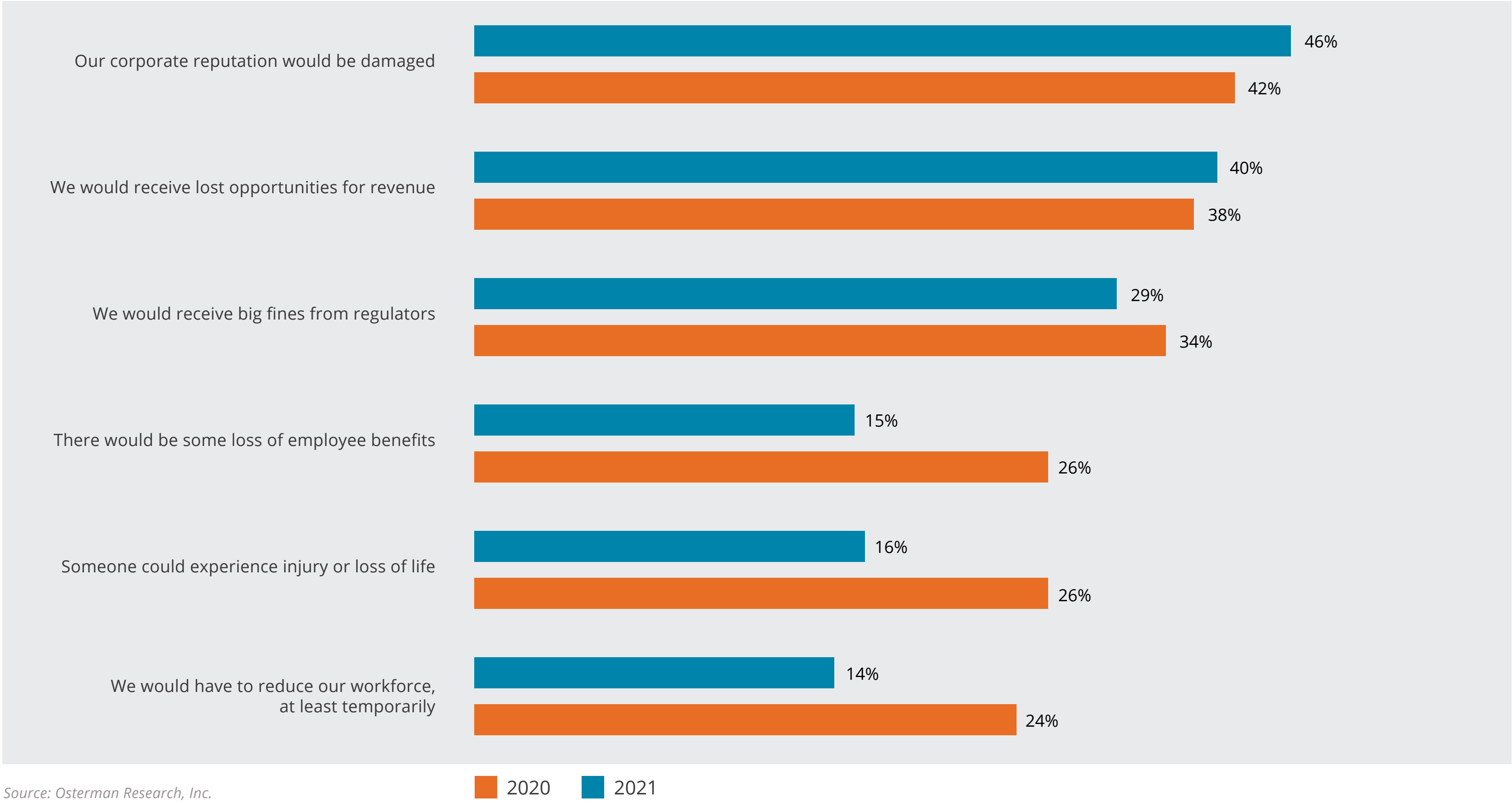
The ability to understand corporate privacy statements and act upon them is essential for every employee who deals with sensitive data that might be subject to privacy regulations. Privacy regulations are quickly becoming the norm in several countries and U.S. states, and so it's management's responsibility to ensure that employees understand their obligations to protect sensitive data. While the ideal is for corporate policy systems to process data subject to privacy regulations automatically, policies and technology alone cannot solve the problem.

What Do Breaches Mean to Employees?

LIFE CAN BE A BREACH SOMETIMES...

Survey respondents were asked about the likelihood that their organization would suffer consequences in the event of a major privacy breach. As shown in Figure 10, 42% of employees believe it is likely or very likely that a major privacy breach would result in damage to their employer's reputation. Another 38% believe it is likely that there would be lost revenue for their employer, and 34% believe their organization would receive significant fines from regulators.

FIGURE 10:
Likelihood of Various Issues Resulting From a Major Privacy Breach
Percentage responding "likely" or "very likely"



Source: Osterman Research, Inc.

WHY AREN'T EMPLOYEES MORE PROACTIVE?

So, if this many employees understand the serious consequences that can arise from a major privacy breach, why don't they do more to try and prevent them? One explanation might be that employees outside of IT just don't see it as their responsibility to consider the security ramifications of what they do in their specific roles. For example, the survey asked employees about their agreement with the following statement:

> *"I'm a privileged user, but I don't work in IT. That means that I have a responsibility to perform my job duties carefully, but that's it. It's not appropriate for me to take additional safeguards within our systems."*

The survey found that 45% of employees either agree or strongly agree with that statement. In other words, most employees simply don't consider it their responsibility to worry very much about security issues or their consequences – and they don't even consider that it's appropriate for them to do so! Their view seems to be that it is IT's job to deal with security, not theirs. Therefore, it's incumbent upon corporate management to create a more mature security culture and help employees understand the importance of their becoming more proactive about security issues, and that it really is appropriate for them to focus on security even as a non-IT employee.

THE CONSEQUENCES ARE REAL AND GETTING WORSE

The consequences of data breaches and privacy violations are by no means theoretical: for example, since enforcement of the GDPR began on May 25, 2018, the European Union has handed down 474 separate enforcement actions for violation of the GDPR with fines totaling €257.1 million (U.S. $312.4 million) through December 2020. Moreover, just four weeks into 2021, the European Union issued another 19 fines totaling €17.2 million (U.S. $20.9 million), or nearly U.S. $750,000 in fines per day. While the European Union began slowly, issuing only a handful of fines in the beginning months of the GDPR's enforcement, the pace has quickened, and fines are being issued more frequently as time goes on. We anticipate a similar pattern with other privacy regulations.

THERE ARE MANY OPPORTUNITIES FOR PRIVACY VIOLATIONS

Survey respondents believe that there are multiple opportunities for privacy violations to occur within their organizations. For example, 32% to 41% of survey respondents believe that each of the following actions is either likely or very likely to result in a privacy violation:

- Employee records are stored in a publicly accessible online server.
- Customer information is collected from an onsite event and stored in an unsecured location.
- Employees are permitted to store personal data on their desktop/laptop computers and mobile devices.

Why Is This Important?

Privacy violations can hurt, as shown by the growing number of GDPR enforcement actions in the less than three years since implementation of the regulation. The growing number of privacy regulations around the world, including an increasing number within the United States, means that the likelihood of punishment for privacy violations is increasing, making organizations more vulnerable to mistakes from their employees. Proper training of employees on their data privacy obligations is essential to mitigate risk.

Differences Among Industries

As noted elsewhere in this report, Osterman Research conducted surveys across seven industries: finance, technology, healthcare, professional services, retail, education and government. In this section, we compare these industries and examine important differences among them.

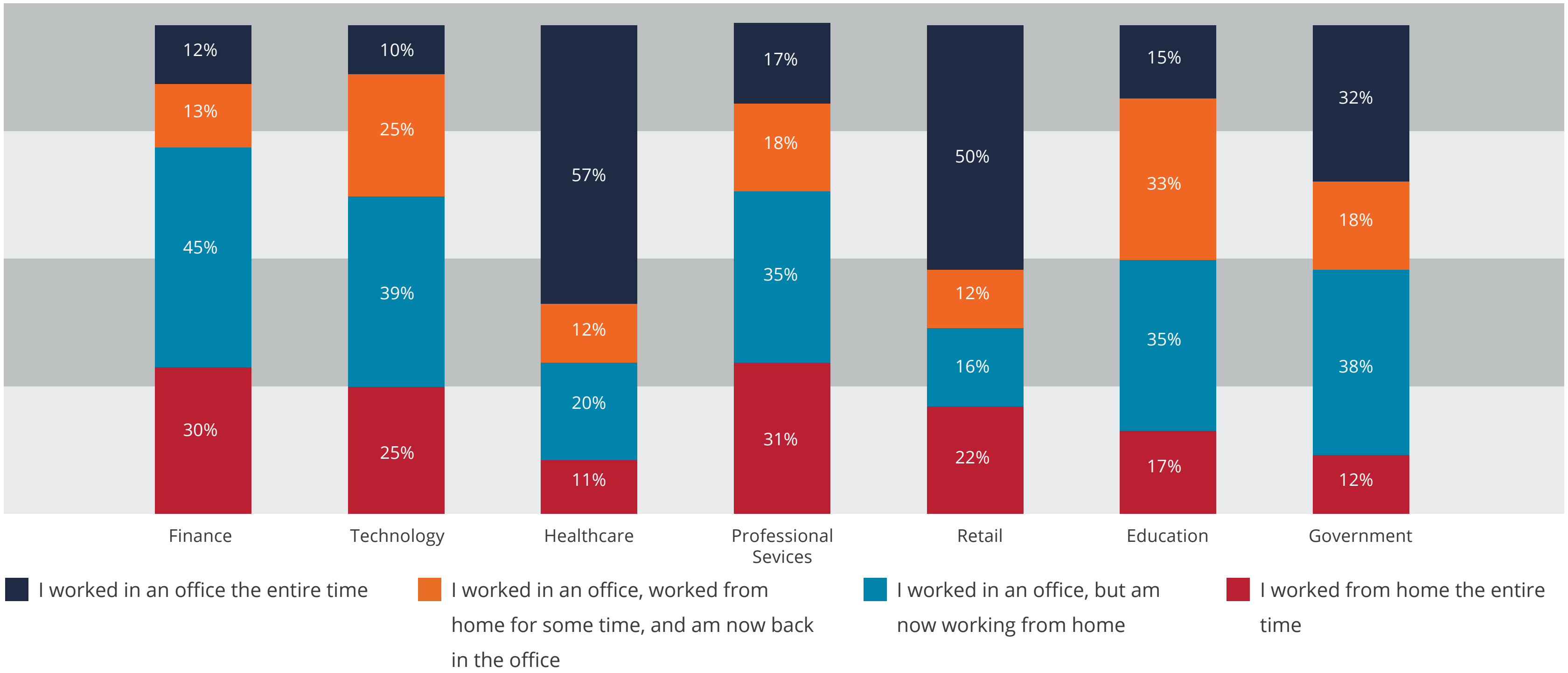
KEY DIFFERENCES BETWEEN INDUSTRIES

The study noted important differences among employees in these various industries, as discussed below:

- **Significant Differences in Working From Home:** Employees in the professional services and finance industries were the most likely to have worked from home prior to the pandemic-induced lockdowns; while those in healthcare, government, and education were among the least likely to have done so. However, the industries in which employees were most likely to have transitioned from in-office to at-home work were finance, technology and government, as shown in Figure 11.

FIGURE 11:

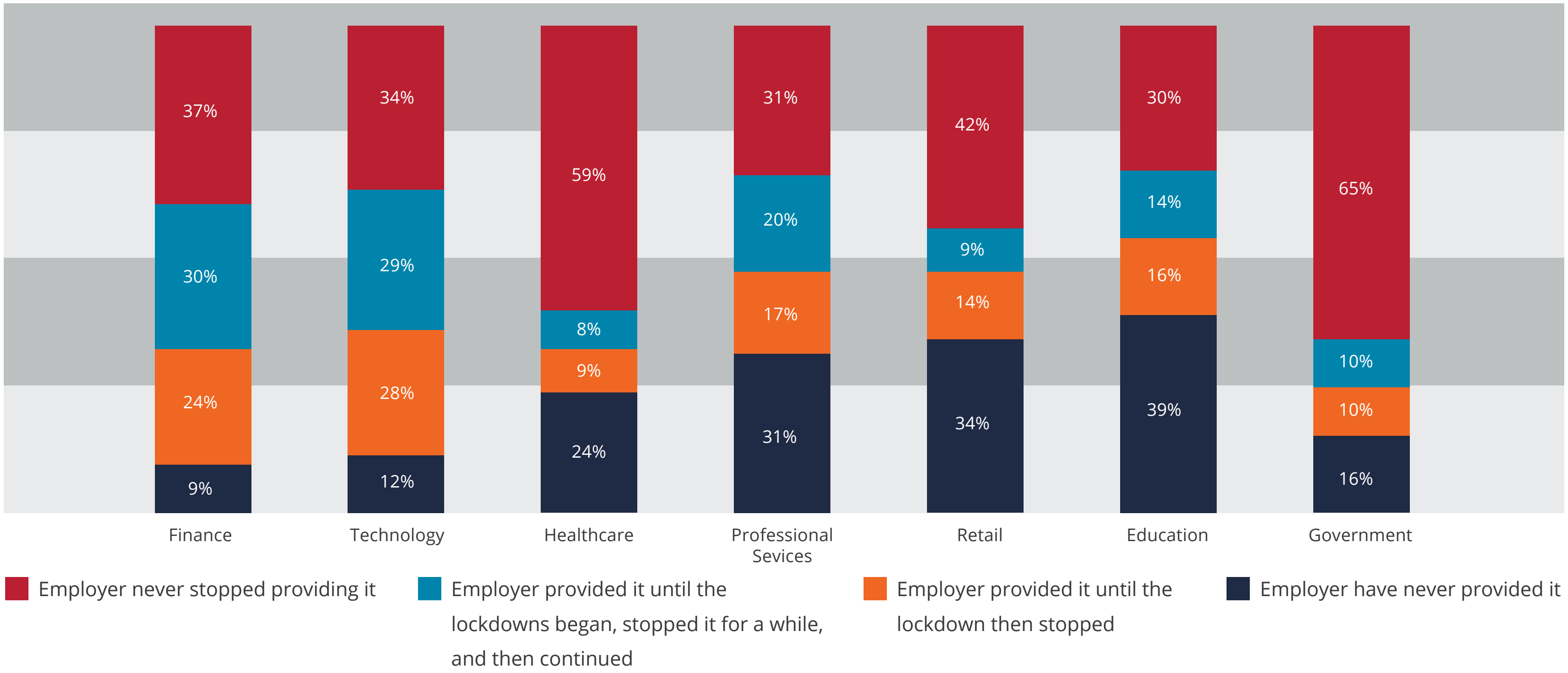
Employees' Work Venues Across Various Industries During 2020



Source: Osterman Research, Inc.

- **Employees in the Finance Industry Receive the Most Training:** Financial services employees are the most likely to receive security and privacy awareness training: 91% have received some form of training, followed by employees in the technology space (88%), and government (84%). At the other end of the spectrum are employees in education, where only 61% have received any sort of security or privacy training, as shown in Figure 12.

FIGURE 12:
Status of Employee Security and Privacy Training During 2020 by Industry



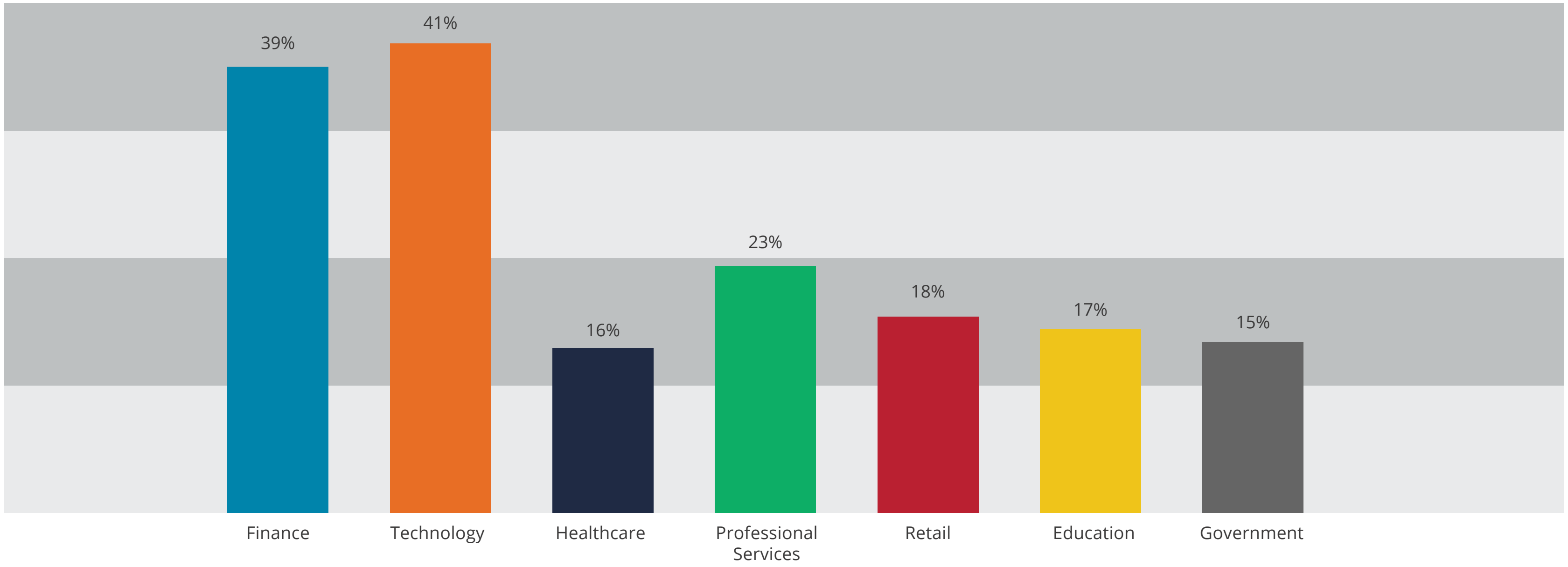
Source: Osterman Research, Inc.

- **Government and Healthcare Employees Lack Confidence in Addressing Key Security Issues:** Employees in the government and healthcare space are significantly less confident about how to address several important issues relative to security best practices. For example, only 14% and 22% of government and healthcare employees, respectively, are very confident that they can describe to their senior management the negative impacts posed by cybersecurity risks; by contrast, 47% and 50% of technology and finance employees, respectively, are this confident. Similarly, only 16% of government employees are very confident in explaining to senior management the security risks created by storing work information in personal cloud applications, whereas 38% of finance employees and 49% of technology employees are very confident they can do so.
- **Healthcare and Education Employees Lack Understanding of Social Engineering Threats:** Employees in government, healthcare and education have the least understanding about a variety of social engineering threats. When asked about the extent to which employees understand five types of social engineering threats (phishing, spear phishing, business email compromise, vishing, and smishing), only 15% of employees in the government space responded with an average of "very well," while employees in the healthcare and education industries fared little better: 16% and 17%, respectively. In contrast, employees in the finance space averaged 39% when asked if they understand these threats "very well," and the figure was 41% in the technology space. The average of those responding "very well" in terms of their understanding of key social engineering threats is shown in Figure 13.

FIGURE 13:

Extent to Which Employees in Various Industries Understand Social Engineering Threats

Percentage who know threats "very well"



Source: Osterman Research, Inc.

- **But Healthcare and Education Employees Know Some Stuff, Too:** While healthcare and education employees are less capable in their understanding of social engineering threats, they are somewhat savvier than their counterparts in finance and technology companies in some ways. For example, healthcare and education (along with those in professional services) are more likely to know the best way to secure a live meeting: 43-45% in healthcare, education and professional services know this versus 31-33% in finance and technology. Similarly, 56-66% of employees in healthcare, education, professional services, retail, and government know the most likely indicator that their desktop or laptop computer has been infected with malware, while only 37-39% in finance and technology know this. Even more interesting is that 48-60% of employees in healthcare, education, professional services, retail and government can identify the best way to create a strong password that would be difficult for a cybercriminal to determine, while only 28-38% of those in finance and technology know this.
- **Won't Someone Please Think of the Password Managers?:** While 27-34% of employees in the finance and technology space strongly agree with the idea that password managers are a good way to maintain strong password security practices, only 11-16% of employees in healthcare, education, professional services, retail and government agree strongly. The lower regard for password managers among the latter industries may be the result (or the cause) of password managers being used less in these industries. We discovered that use of a password manager has reached 63-70% among employees in the finance and technology industries, but only 28-40% in the other industries.
- **Finance and Technology Companies Know Privacy the Best:** Interestingly, even though government, education and healthcare are heavily focused on privacy, and are the subject of various privacy regulations focused specifically on their industries, employees in these industries are much less confident in their ability to describe to their senior management the details of their corporate privacy statement – only 9-13% of employees in government, education and healthcare are "very confident" they can do so. By contrast, 41-52% of employees in finance and technology are very confident in their ability to explain to their senior management their company's privacy statement and 24% of employees in the professional services space are confident they can do this. In contrast, while 31-32% of employees in the finance and technology space "strongly agree" with the mistaken notion that using a single, regional privacy regulation as a template for all other privacy regulations is a good idea, only 9-16% of employees in other industries agree this strongly with the idea of a one-size-fits-all approach to privacy regulation.

Risk Analysis

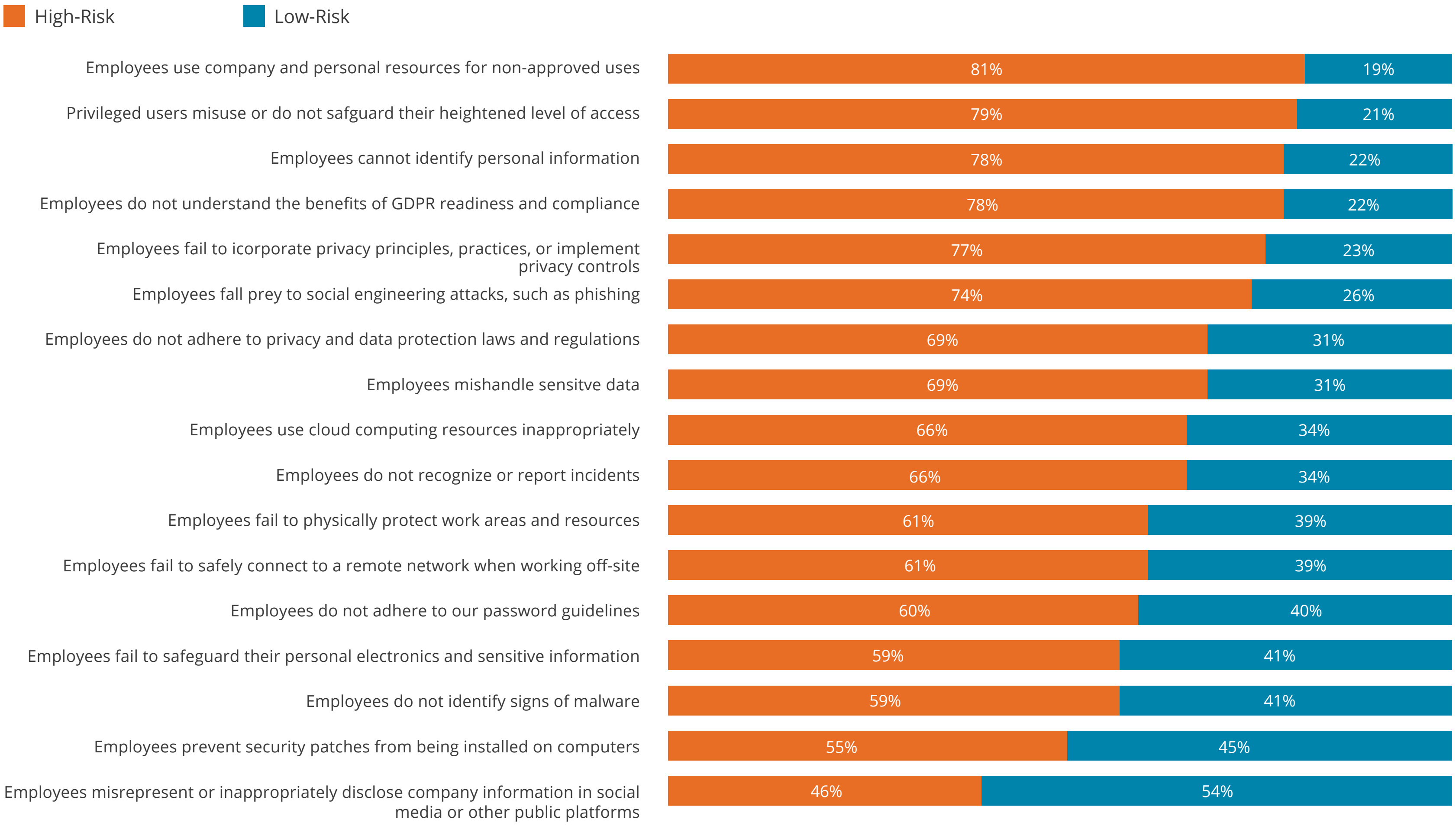
Osterman Research categorized the survey questions into 17 risk categories, as shown below (the number of questions/question components that were assigned to each risk category is shown in parentheses):

Category	Issue	Number of Questions
Incident Reporting	Employees do not recognize or report incidents	4
Physical Security	Employees fail to physically protect work areas and resources	3
Identifying Malware	Employees do not identify signs of malware	8
Cloud Computing	Employees use cloud computing resources inappropriately	7
Identifying Personal Information	Employees cannot identify personal information	4
Phishing and Social Engineering Awareness	Employees fall prey to social engineering attacks, such as phishing	10
Working Remotely	Employees fail to safely connect to a remote network when working off-site	5
Responsible Use of Social Media	Employees misrepresent or inappropriately disclose company information in social media or other public forums	2
Password Best Practices	Employees do not adhere to our password guidelines	5
Mobile Device Safety	Employees fail to safeguard their personal electronics and sensitive information	13
Secure Data Handling	Employees mishandle sensitive data	6
Secure Use of Personal Devices at Work	Employees use company and personal resources for non-approved uses	1
Software Update Best Practices	Employees prevent security patches from being installed on computers	2
Privileged User Security	Privileged users misuse or do not safeguard their heightened level of access	2
Privacy Regulation Awareness	Employees do not adhere to privacy and data protection laws and regulations	14
Compliance and Privacy Readiness	Employees do not understand the benefits of GDPR readiness and compliance	2
Privacy by Design	Employees fail to incorporate privacy principles, practices, or implement privacy controls	8

Based on these classifications, a risk level was assigned to each of the survey responses, as shown in Figure 15.

FIGURE 15:

Classification of Employee Practices and Attitudes by Risk Level



Source: Osterman Research, Inc.

The risk analysis clearly shows that misuse of resources, the inability to properly identify personal information, and compliance issues represent the riskiest behaviors undertaken by employees. Interestingly only one of the 17 risk factors identified above was categorized as more “low risk” than “high risk,” indicating that organizations face a wide range of risky behaviors from their employees across a wide range of issues.

CALCULATING THE RISK ANALYSIS

- Responses that asked for a rating on a scale of 1 (low/poor) to 7 (high/good) were segmented into 1-5s and 6-7s; the 1-5s were considered the risky behaviors or attitudes.
- For responses that asked for a rating on a five-step scale of very poor/not at all confident/have never heard of/strongly disagree to very well/very confident/know very well/strongly agree, the bottom four ratings were considered risky behaviors or attitudes.
- For Yes/No/Not Sure questions, the “Not Sure” responses were considered risky behaviors or attitudes.
- Other questions that did not fall into these categories were classified appropriately to determine what we consider to be risky behaviors or attitudes.

Based on this analysis we determined a percentage score for each of the 17 risk categories, as shown in Figure 15. Among the riskiest behaviors are:

- Employees using company and personal resources for non-approved uses. This has been a perennial problem, but became significantly worse as millions of employees began working from home during 2020.
- Privileged users misusing their heightened level of access or failing to properly safeguard their access.
- Employees who have not been properly trained on how to identify personal information.

Conclusion

Cybersecurity and privacy awareness and training remain an ongoing concern for most organizations. As the COVID-19 pandemic has demonstrated, it's an area that needs continual investment in, and extended periods without ongoing awareness can reduce an employee's ability to make sound risk decisions.

Employees don't need to become security and privacy experts, but their responsibilities with privacy and/or legal matters need to be made clear. If employees know that they have a responsibility, then it becomes easier to ask the question to seek clarification. Without knowing there is an obligation to adhere to laws or regulations, we will continue to see unsafe behavior perpetrate throughout the organization.

Above all, security awareness training needs to be made relevant and memorable. Despite the extensive digitization of organizations and society at large, most employees still struggle with the fundamental basics. Organizations need to focus not just on providing information but making it actionable and foster a culture of security. Only then can long-lasting changes be made that can reduce risk by having employees make informed choices.

About the Survey

This report discusses the results of an in-depth survey conducted with more than 1,000 employees in the United States. Percentage totals in each of the figures in this report may not add up to 100% because the data have been rounded to the nearest whole number.

Osterman Research developed an in-depth questionnaire about cybersecurity and privacy awareness issues. The focus was to develop questions that would help us understand how U.S.-based full-time and part-time employees working at companies, government entities, and educational institutions perceive various types of cybersecurity and privacy practices, and the disconnects that exist between their understanding and behavior in a number of areas. Moreover, given that we conducted this survey roughly ten months into the pandemic, we wanted to understand how employees were dealing with the new realities of work-from-home. Ultimately, our goal was to determine what types of risk organizations face when employees do not appreciate, and/or have not been appropriately trained with regard to, cybersecurity and privacy practices. The survey had a margin of error of 3.1% at a 95% confidence level.

Osterman Research established the following criteria for participants to be able to take part in the survey conducted for this report. Respondents had to be:

- At least 18 years old.
- Employed full-time or part-time at a company or some other organization. Self-employed individuals, students, retired individuals, and those who are not currently employed were not qualified to participate in the survey.
- They had to live in the United States.

The survey was conducted completely online using the Alchemer (formerly SurveyGizmo) platform with 1,055 individuals. The demographics of the survey participants broke out as follows:

GENDER

- Male: 51.0%
- Female: 48.5%
- Prefer not to say: 0.5%

EMPLOYMENT STATUS

- Full-time: 93.6%
- Part-time: 6.4%

AGE

- 18-24 years: 9.1%
- 25-34 years: 27.2%
- 35-44 years: 31.8%
- 45-54 years: 18.2%
- 55-64 years: 10.3%
- 65+ years: 3.4%

JOB ROLES

- Entry-level: 16.5%
- Mid-level: 38.5%
- Management: 29.4%
- Executive or above: 15.6%

ORGANIZATION SIZES

- 1 to 1,000 employees: 51.2%
- 1,001 to 5,000 employees: 19.8%
- 5,001 to 20,000 employees: 14.9%
- 20,001 to 50,000 employees: 4.6%
- More than 50,000 employees: 9.5%

LOCATIONS AND INDUSTRIES

Respondents were surveyed in all 50 states and in a cross-section of industries. We conducted surveys with the goal of completing a near-equal number of surveys in seven industry groups: finance, technology, healthcare, professional services, retail, education and government. The employees in various industries broke out as follows:

- **Finance:** 49.2% are customer-facing, 50.8% are business-facing.
- **Healthcare:** 57.4% were providers or practitioners; 50.0% work in a public healthcare institution and 50.0% work in a private institution.
- **Retail:** 71.4% are customer-facing and 28.6% are business-facing; 96.0% are full-time and 4.0% are temporary.
- **Education:** 47.7% are faculty and 52.3% are staff; 74.2% work in a public institution and 25.8% work in a private one.

ABOUT KNOWBE4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind. Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Info@KnowBe4.com