MediaPRO
Cybersecurity & Privacy Education

2020 State of Privacy and Security Awareness Report

OSTERMAN RESEARCH

EXECUTIVE SUMMARY

Osterman Research conducted a survey on behalf of MediaPRO during October 2019. The goal of this research was to determine the level of awareness about cybersecurity and privacy best practices among employees in a wide variety of organizations serving various industries in the United States. We wanted to determine not only what employees know (or don't know) about these best practices, but also the extent to which they put their knowledge into action.

About This Report

This report was produced via a partnership between Osterman Research and MediaPRO. MediaPRO sponsored Osterman Research to design and conduct the survey, collect responses, and produce a written report based on analysis of the results. MediaPRO managed the layout and design of the report.

Key Takeaways

More efforts are needed in security awareness training

We discovered that many employees are unaware of several key risk factors as they relate to cybersecurity and privacy. For example, more than two in five employees do not think that clicking a suspicious link or opening a suspicious attachment in an email is likely to lead to a malware infection.

Some employees are misinformed about cybersecurity risks

Many employees think it's safe to plug unknown USB sticks into their work computer, most think there is little risk in leaving unencrypted data on their laptop or mobile device, and many believe that they should respond to the sender of a suspected social engineering attack to determine if the attack is real.

Many employees don't believe that cybersecurity is their personal responsibility

While many users are well-informed about key cybersecurity issues like malware risks, how to create strong passwords, and the necessity of upgrading software, many will not report security incidents, nor do they consider it their responsibility to take additional security safeguards within their corporate systems.

Privacy best practices seem to be less well understood than cybersecurity best practices

Most employees do not know whether or not their organization needs to comply with a variety of key privacy regulations and guidelines, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the Payment Card Industry Data Security Standard (PCI DSS).

TABLE OF CONTENTS

Awareness of Key Issues Is Lacking

Cybersecurity Knowledge Could Use Improvements

A large proportion of employees self-report that they cannot perform a variety of key tasks that would enable them to protect their organizations from various cyberthreats. For example:

- Only 17% of employees are "very confident" that they can identify a "social engineering attack," while more than one-quarter of employees (28%) admitted a lack of confidence in identifying a phishing email.
- One in five employees were unsure if they could describe to their senior management the security risks created by storing work information in personal cloud applications, while only 22% said they'd be very confident doing so.
- Only 27% can identify at least two warning signs that malware has infected their computing platform.

A summary of the confidence that employees have (or typically don't have) about key cybersecurity best practices is shown in Figure 1.

FIGURE 1:

Employee Confidence About Key Cybersecurity Best Practices

Issue	Very Confident	Confident	Not Sure	Somewhat Confident	Not at all Confident
Your current set of passwords is both strong and has not been previously compromised	39%	37%	11%	10%	3%
Identifying a phishing email	37%	35%	12%	12%	4%
Identifying at least two warning signs that malware has infected your desktop/laptop computer or mobile device	27%	34%	17%	15%	7%
Describing the steps needed to actively secure work information and resources while working remotely	27%	35%	17%	13%	8%
Describing to your senior management the negative impacts to your organization posed by cybersecurity risks	25%	33%	18%	13%	11%
Describing to your senior management the security risks created by storing work information in personal cloud applications	22%	34%	20%	12%	13%
Describing to your senior management the security risks created by employees working from home	22%	33%	19%	15%	12%
Describing to your senior management how security expectations for privileged users differ from those for standard users	21%	30%	24%	11%	13%
Identifying a social engineering attack	17%	25%	33%	12%	14%

Source: Osterman Research, Inc.

Many Employees Are Not Aware of Some Key Risk Factors

Our research also discovered that many employees lack awareness of a variety of key risk factors that could lead to data breaches, ransomware or other malware infections, or other security threats. For example:

- 43% of employees are not aware that clicking a suspicious link or opening an unknown attachment in an email is likely to lead to a malware infection.
- More than one-half of employees (55%) are not convinced that connecting their laptop, smartphone or tablet to a public Wi-Fi network, such as in a coffee shop or an airport, is likely to lead to a malware infection.
- One-quarter (25%) of employees believe it's acceptable to use a personal cloud server to transfer work home so as long as their cloud service performs a virus scan before downloading any files.

Why Is This Important?

Employee awareness of cybersecurity and privacy issues is an essential element of any organization's cybersecurity posture. The better informed that employees are about key issues, the more likely they are to be better able to defend against social engineering and other attacks. It's that simple. Awareness is the critical first step to enabling employees to become a valuable defensive layer of their organization's security posture.

However, our research found that awareness of some seemingly basic cybersecurity threats and best practices —let alone putting this awareness into action—is lacking among many employees. For example, more than one-quarter of employees admitted they'd struggle identifying a phishing email, two in five cannot describe to their senior management the negative impacts posed by cybersecurity risks, and three in five cannot identity a social engineering attack.

Our research strongly suggests many organizations are putting themselves at risk from potentially devastating incidents by ignoring the benefits of security awareness training.

Some Users Are Misinformed About Cybersecurity Risks

One of the more interesting set of findings from the research is that employees “know” a variety of things about cybersecurity, but many of these things simply aren’t accurate, as shown in Figure 2. Let’s dive deeper into these findings.

Proximity does not lead to infection

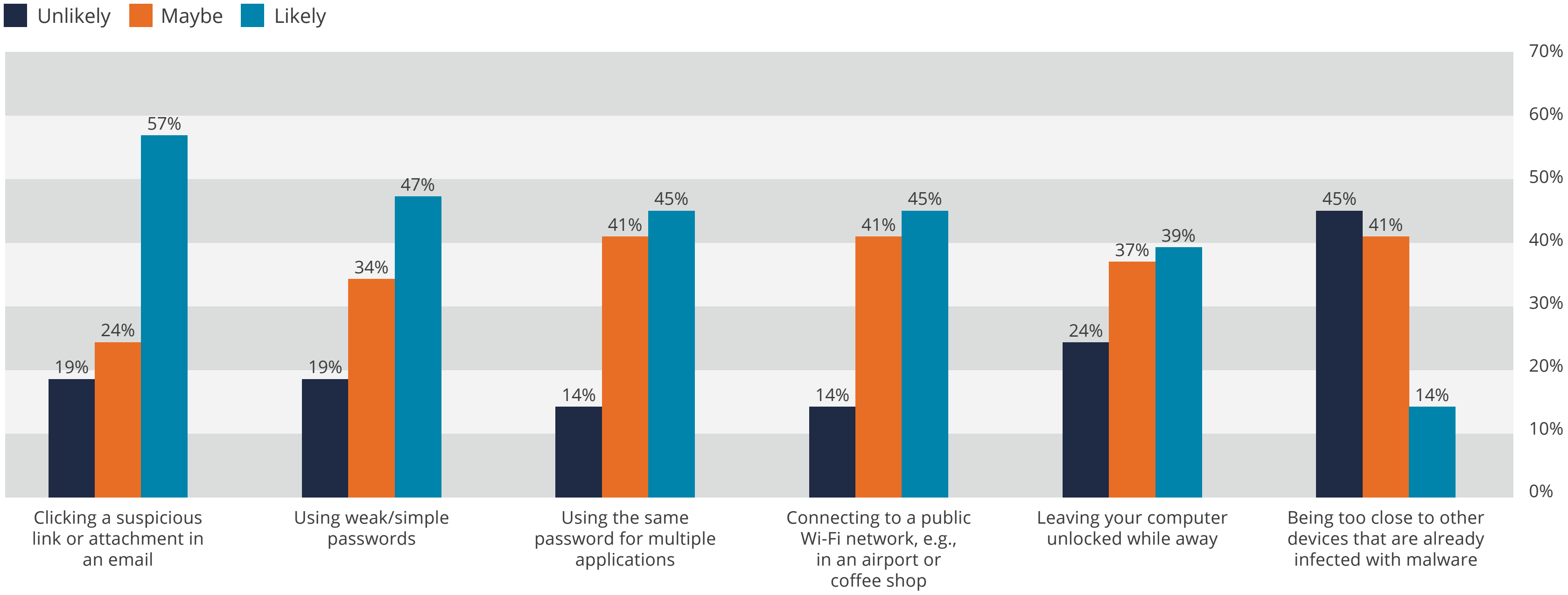
Our research found that one in seven employees (14%) believe that if their computer or mobile device is kept too close to a device that is already infected with malware, their device could also become infected with the same malware.

Leaving computers unlocked does not lead to malware infection

Leaving computers unlocked while they are unattended is a bad idea because unauthorized users could gain access to sensitive or confidential data. However, 39% of employees mistakenly believe that leaving their computer unlocked can also result in a malware infection.

FIGURE 2:

Employee Perceptions About the Likelihood that Computers or Mobile Devices Could Become Infected with Malware as a Result of Various Actions



Source: Osterman Research, Inc.

Many don't believe that checking the "To:" field is necessary

The "type-ahead" feature in many email clients, such as Microsoft Outlook, provides a convenient shortcut for users when sending an email. However, it also creates a security risk by enabling users to more easily send an email to the wrong party.

For example, typing the first few letters of the intended recipient's first name into the "To:" field in an email might bring up a number of potential recipients, and many users will hit the return key on the wrong recipient.

While it's a best practice to always check that the right recipients are specified in the "To:" field, we found that 20% of those surveyed disagree or are unsure if they would.

Responding to social engineering attacks is not a good idea

A cybercriminal who steals a user's login credentials and takes over an email account can then use that account to send phishing and other types of social engineering attacks. This poses a huge problem for recipients of these malicious emails because they look genuine and are, in fact, are coming from a valid email account.

The one thing that recipients of these social engineering attacks should never do after receiving such an email is to respond back to the sender asking for clarification or more information. However, 39% of those we surveyed disagree—they think that replying back to the sender is a good idea.

What about random USB drives?

Should you plug just any USB drive into your computer? The answer is a resounding "No," because cybercriminals use this technique to install malware into targeted networks or computers. But people seem to do it anyway.

For example, a study by researchers at the University of Illinois in 2016 found that 48% of 297 USB sticks dropped around the campus were picked up and plugged into various computers.

Our own research found that 14% of employees believe it's safe to plug random USB drives into their work computer.

Unencrypted data is not risk free

We also found that 51% of those surveyed believe there is relatively little risk in having unencrypted data on their laptop or mobile device, despite the fact that this is one of the primary methods by which data breaches occur.

Authenticating mobile devices is key

32% of employees believe that not securing their laptop or mobile device with a password represents little to no security risk.

Why Is This Important?

Awareness of what constitutes a cyberthreat is key for employees, but the inverse is also true. Misinformation is another enemy of a strong cybersecurity posture.

Our research found that many employees have perceptions about cybersecurity that just aren't true: many believe that simply being in physical proximity to a malware-infected computer or mobile device, or leaving a computer unlocked while away, can lead to a malware infection. A key element of a good security awareness training program is helping employees to distinguish cybersecurity fact from fiction.

Most Users Are Somewhat Informed

Despite the findings discussed in the previous section indicating that employees are not as well-versed in cybersecurity as they perhaps should be, there were some encouraging findings about the current state of employees' cyber know-how:

Most know how to identify a malware infection

The majority of employees seem to be well-versed in identifying the telltale signs of a malware infection: 58% of the employees we surveyed correctly identified "popups rapidly interrupting other programs" as the most likely indicator that their desktop or laptop computer has become infected with malware.

Most are reasonably password-savvy

Our research found that the majority of employees have at least some knowledge about password best practices.

For example, we found that 52% of employees know it's important to use a unique password for every device and application; 37% consider it important to always include a special character (e.g., , $, & or *) in their password; and 91% consider the password "D0nt5top&elie^n" to be either "strong" or "very strong."

Software upgrades are key

The vast majority of employees (84%) understand that they should install software upgrades in order to help protect against cybersecurity threats.

Changing the home router's default password

Routers come with default passwords that are often quite easy to guess, and so these should be changed when the router is configured.

We found that 61% of employees agree or strongly agree that when working from home they should change their router's default password before accessing corporate data or email.

Most can identify ways to maintain physical security

While cybersecurity threats pose significant risks to any organization, so do physical risks, such as letting unbadged individuals through secure doors or leaving confidential documents in plain view on a desk.

We found that 69% of employees are confident or very confident that they can identify at least four ways to keep work areas and resources safe from various physical security threats.

Employees' views on various cybersecurity issues are shown in Figure 3 (page 9).

[1] *https://www.vice.com/en_us/article/pgkgxb/study-finds-48-percent-people-will-plug-a-random-usb-into-their-computer*

FIGURE 3:

Agreement with Various Statements About Cybersecurity Issues

Threat	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
Whenever I send important company data through our secure email system, I should always double-check the “To:” field to ensure that each recipient is authorized to view the data	45%	34%	16%	3%	1%
I should install software upgrades to protect my devices from cybersecurity threats	44%	40%	11%	3%	1%
If I work from home, I should change my router’s default password before accessing corporate data or email	27%	34%	32%	7%	1%
A coworker’s credentials mistakenly give them access to corporate systems. You mention it to them and they seem honestly confused and don’t seem to be using their access with malicious intent. Nevertheless, they should be considered an insider threat	16%	44%	29%	9%	1%
If I delete a phishing email without clicking on or opening anything it means that I’m completely safe	15%	27%	27%	26%	5%
When I receive a strange request through email which might be a social-engineering attempt, it’s a good idea to reply with a new email to verify the request before taking any action	15%	24%	22%	19%	21%
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	11%	23%	21%	28%	17%
We have important documents on our company’s cloud server, but I save a working copy on my local computer instead of struggling with the cloud service’s live editing feature. As long as I upload my copy, things will stay safe	9%	18%	29%	32%	13%
It’s OK if I use a personal cloud server to transfer data between work and my home office, so long as I ensure that the cloud performs a virus scan before downloading any files	8%	18%	25%	30%	20%
It’s safe to download third-party apps, such as games, to my mobile device that don’t access corporate data	7%	17%	21%	30%	24%
If I get a USB thumb drive from a trade show, it’s safe to plug it into my work computer	5%	9%	16%	32%	38%

Source: Osterman Research, Inc.

Why Is This Important?

Although our research demonstrates that a good portion of employees are more or less on the right track when it comes to cybersecurity awareness, it only takes one mistake to cause a potentially devastating cybersecurity incident.

In an organization of several thousand employees, it's highly likely that at least one person – even among those who are fairly well-versed in cybersecurity issues – will make a mistake. This demonstrates how even a small percentage of employees – sometimes only one – can make a big difference in the end because of the ease in which incidents can occur.

More Engagement in Overall Cybersecurity Process Is Needed

Cybersecurity is not a task simply for "IT," though a variety of TV shows and other media may suggest otherwise. It needs to be an integral component of everything that every employee does in order to minimize corporate risk.

Unfortunately, we found that many users are not fully engaged in the security process, underscoring the idea that even just a small proportion of employees who are not following security best practices can wreak havoc in an organization:

Many won't go the extra mile

We asked employees the extent to which they agree with the following scenario: *you're a privileged user, but you don't work in the IT department. Consequently, that means you have a responsibility to perform your job duties carefully, but that's it—it would not be appropriate to take additional safeguards within your corporate systems.* 34% agree or strongly agree with that sentiment.

Some won't report security incidents

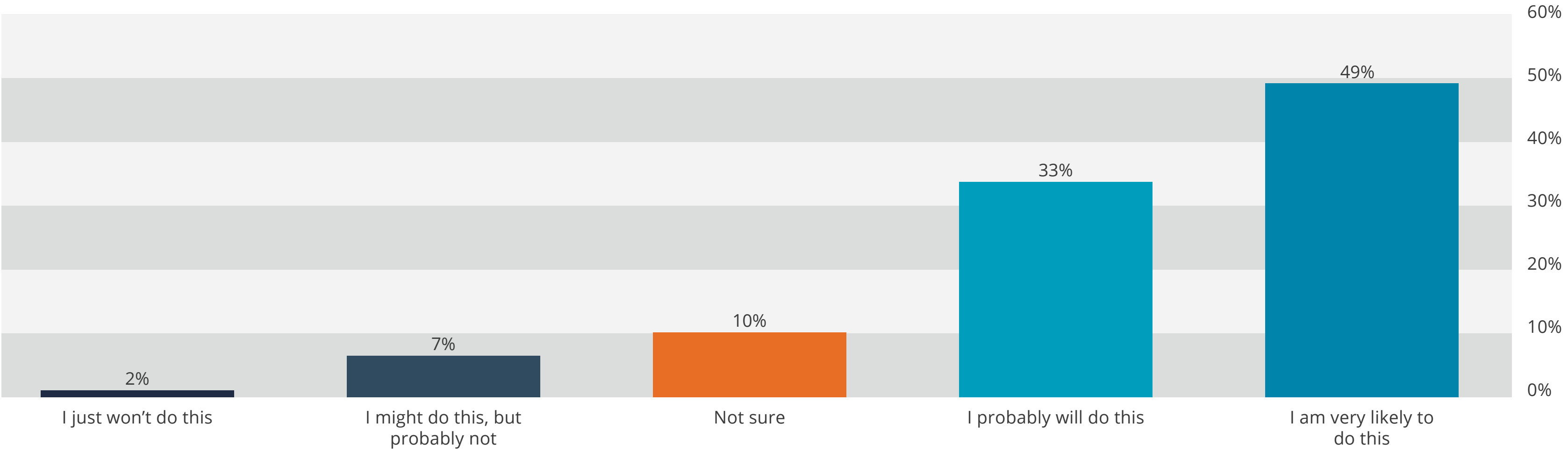
Almost half (49%) of employees said they were "very likely" to report a security incident. While this percentage is high, it still leaves a third of employees who would "probably" report and almost one in five (19%) who were unsure or *simply would not.* Even one serious incident gone unreported can have dire consequences for an organization of any size.

Many won't confront workers openly discussing sensitive information

When employees were asked what they would do if co-workers were routinely discussing sensitive data in the open, 11% responded that they would discretely leave the room (instead of asking their co-workers to discuss sensitive matters only in a private location as they should), and 4% were not sure what they would do.

FIGURE 4:

"If you notice what you think is a security incident, how likely are you to report it?"



Source: Osterman Research, Inc.

Why Is This Important?

Cybercriminals typically don’t go after security professionals or ”IT” in a department. They go after people who control or process data, who have access to databases with sensitive information, or who have access to corporate financial accounts.

Consequently, cybersecurity is not just for security or IT professionals—it’s the responsibility of every employee at every level, all of the time. Employees need to be engaged in the cybersecurity process through a comprehensive security awareness training program that includes regular reminders that their awareness and diligence are an integral component of their organization’s security infrastructure.

Our research found that a significant proportion of employees just are not sufficiently engaged in the cybersecurity process, and so represent the weak link in the security chain that can be easily exploited by cybercriminals.

Common Privacy Regulations Are Not Well Understood

We found that many employees lack confidence in their understanding of privacy regulations, conveying privacy guidelines, and taking steps to protect data, as evidenced by the following:

Lack of knowledge about key privacy regulations

Most employees don't know whether or not their organization needs to comply with a variety of important privacy requirements.

For example, the GDPR had been in effect for 17 months at the time of the survey, but 61% of those surveyed did not know whether their organization needs to comply with it.

Similarly, 62% don't know if their organization needs to be compliant with the CCPA, 66% did not know if their organization needs to be compliant with PCI DSS, and 61% don't know if they need to be compliant with the Family Educational Rights and Privacy Act (FERPA).

The only privacy regulation about which there is significant understanding is the Health Insurance Portability and Accountability Act (HIPAA) —only 25% of employees weren't sure if their organization needs to be compliant with it. Employees' understanding about their organizations' need to comply with various privacy regulations is shown in Figure 5 (page 14).

Explaining corporate privacy would be a challenge

When asked if they could explain their organization's privacy statement to their senior management, 43% of employees have little or no confidence in their ability to do so. Only one in six (17%) told us they are "very confident" they could explain the privacy policy to their senior managers.

Storing sensitive data in an unsecured location is not a good idea

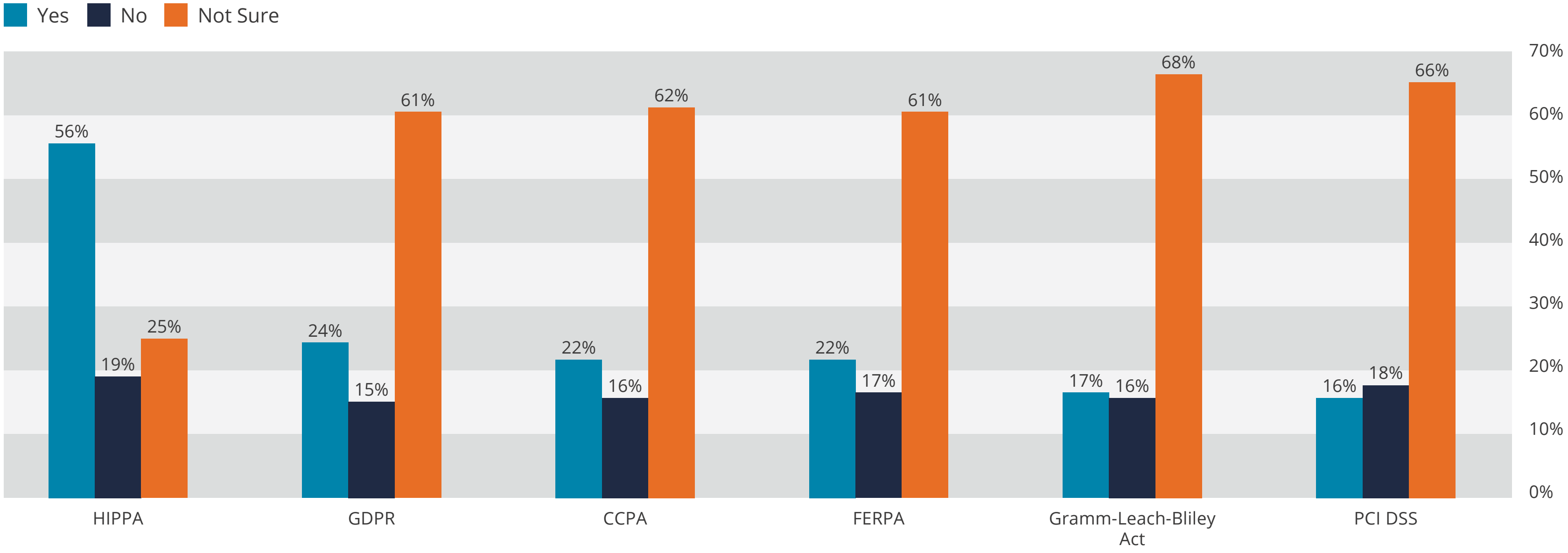
Could customer information collected from an on-site event and then stored in an unsecured location constitute a potential policy violation? Nearly three in five employees (58%) don't think this would create a policy violation.

Should employees store personal data on their work computers?

We found that 69% of employees don't believe that storing their personal data on their desktop and laptop computers, as well as their mobile devices, could create a policy violation.

FIGURE 5:

Employee Understanding of Privacy Regulations with which Their Organization Must Comply



Why Is This Important?

Privacy regulations are becoming much more common in a growing number of jurisdictions around the world. The consequences of violating them—such as the fines for non-compliance—can be significant in some cases. For example, under the GDPR the European Union can impose fines of up to 4% of an organization's annual revenue, meaning that a single fine could total several billion dollars.

This means employee needs to understand the privacy regulations to which its employer is subject so that they can manage data properly and in compliance with these regulations. However, our research found that most employees are unaware whether their employer is subject to a variety of key privacy regulations, rendering them unable to be part of addressing their employer's privacy obligations. We're not talking about each employee being a privacy expert. But every employee needs a basic understanding of their company's requirements under their respective privacy regulations and guidelines.

Our research suggests employers need to do a better job at training its employees about the compliance obligations, guidelines and best practices that they should follow to safeguard company data and other assets.

Source: Osterman Research, Inc.

Many Users Are Aware of Good Privacy Practices

Despite their relative lack of knowledge about privacy regulations, many understand that the consequences of privacy breaches could be severe. For example, 46% of employees believe that a privacy breach would likely or very likely damage their employer's reputation, 40% believe that their employer would experience lost opportunities for revenue, and 29% believe the organization would receive significant fines from regulators. Let's look a little more in-depth at these findings:

Most understand that oversharing on social media is a bad idea

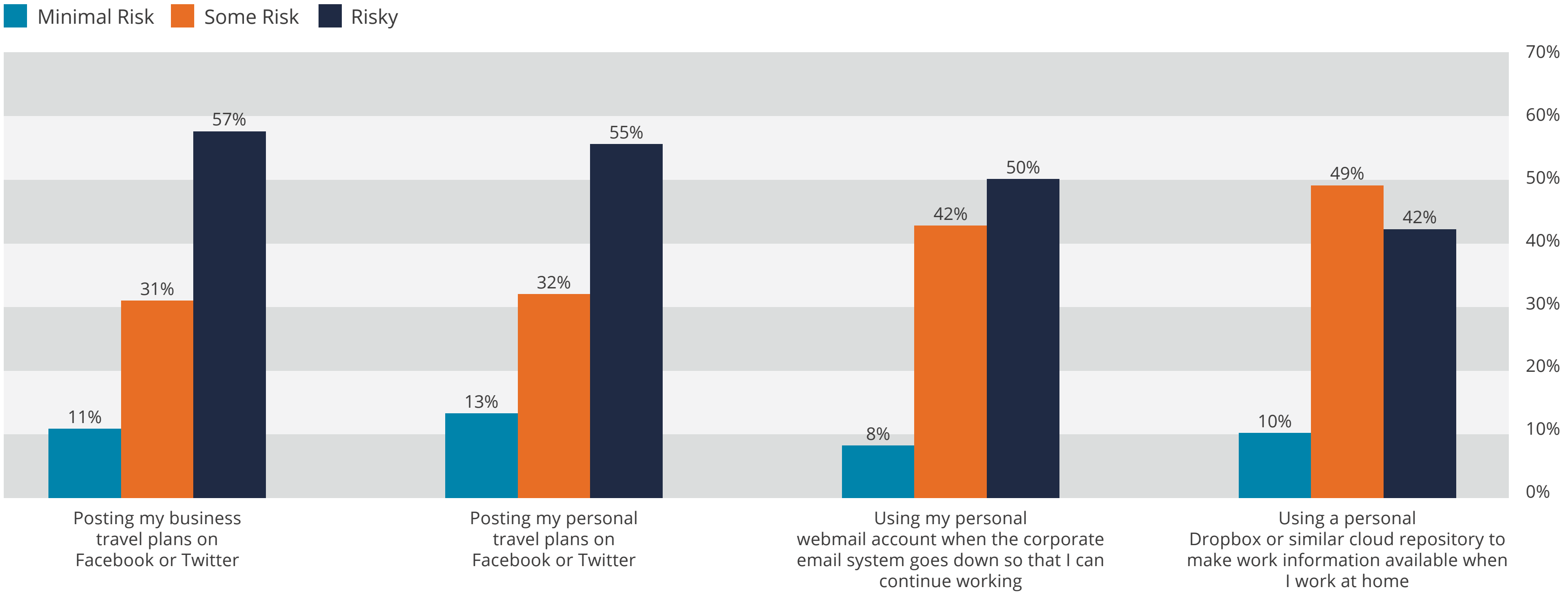
When employees share too much information on Facebook, Twitter or other social media venues, they provide fodder for cybercriminals to craft social engineering attacks like phishing and spear phishing attempts. The good news is that most employees understand that: 55-57% of those surveyed consider it to be risky or very risky to share personal or business travel plans on Facebook or Twitter.

Use of personal webmail is considered risky

Some employees will use personal webmail at work not only for sending or receiving their own email, but also to have access to email when the corporate system goes down or when it won't support sending a very large file. Our research found that one-half (50%) of employees consider that using personal webmail for work purposes poses a risk to their organization, but the other half don't consider this to be a serious risk.

FIGURE 6:

Employees' Risk Perceptions About Various Day-to-Day Tasks



Source: Osterman Research, Inc.

Why Is This Important?

Most employees have at least a reasonable understanding about data privacy best practices as they relate to many of their day-to-day tasks.

For example, 90% of employees understand that there is at least some risk associated with using a personally managed file-sharing solution or a similar cloud repository to make information available when they're working at home. Most know that sharing travel plans on social media—which could provide useful information for spear phishing and BEC messages—is a risky behavior.

Mapping Responses Across Multiple Risk Areas

Osterman Research and MediaPRO 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):

- Incident Reporting (64)
- Physical Security (24)
- Identifying Malware (46)
- Cloud Computing (17)
- Identifying Personal Information (11)
- Phishing and Social Engineering Awareness (23)
- Working Remotely (17)
- Responsible Use of Social Media (11)
- Password Best Practices (11)
- Mobile Device Safety (33)
- Secure Data Handling (21)
- Secure Use of Personal Devices at Work (5)
- Software Update Best Practices (7)
- Privileged User Security (7)
- Privacy Regulation Awareness (41)
- GDPR Readiness (7)
- Privacy by Design (21)

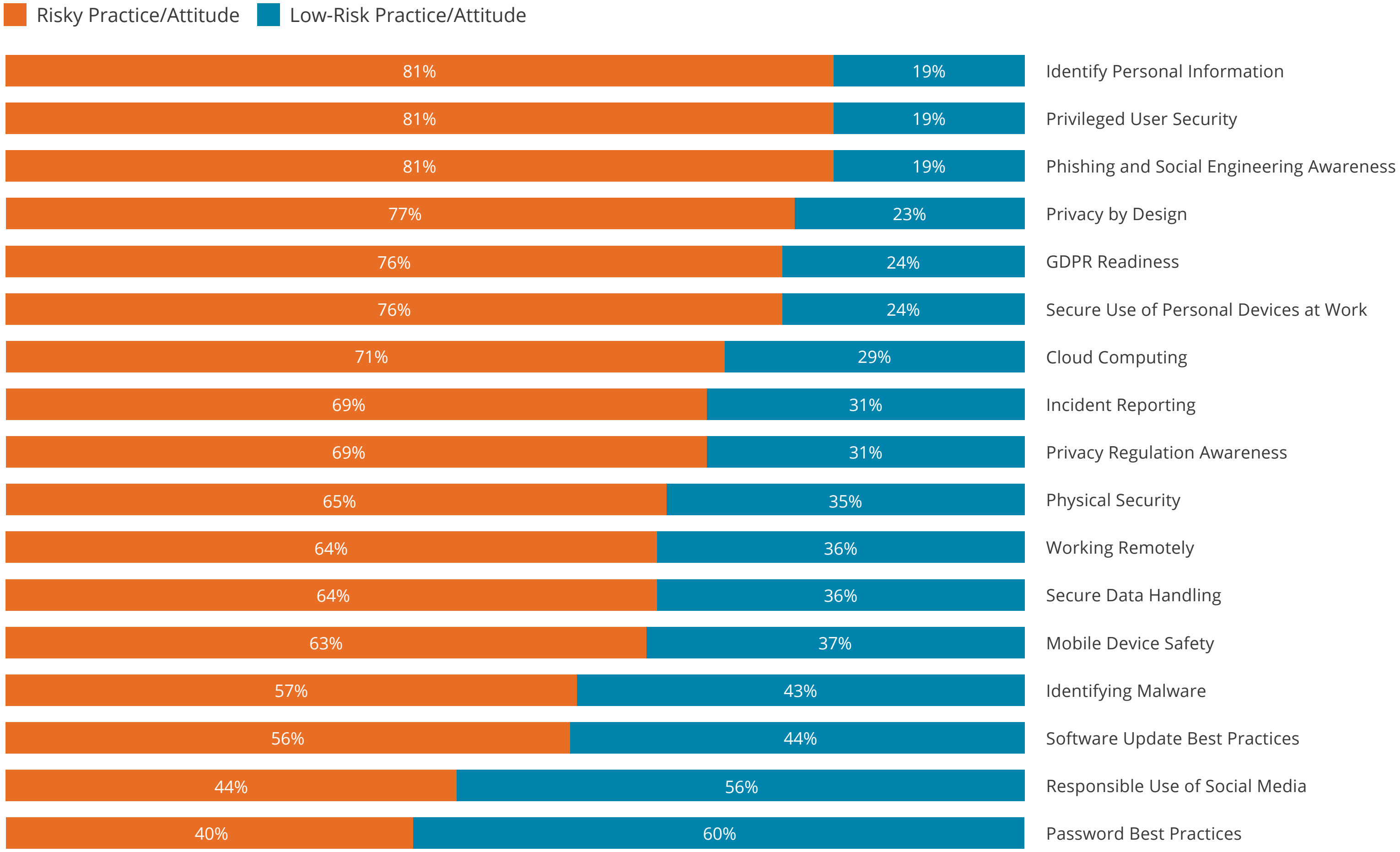
Based on these classifications, a risk level was assigned to each of the survey responses on the following:

- 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 attitude.
- 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 score percentage for each of the 17 risk categories, as shown in Figure 7 (page 18).

FIGURE 7:

Classification of Employee Practices and Attitudes by Risk Level



As shown in Figure 7, for 15 of the 17 risky behaviors and practices we identified, more than 50% of the employees we surveyed fall onto the "risky" side of the spectrum. The only behaviors and attitudes for which more than half of employees are in the "low risk" category are a) disclosures of information through social media or public forums and b) following guidelines for password use and management.

Source: Osterman Research, Inc.

Why Is This Important?

The at-a-glance risk-based analysis on the previous page presents a mixed bag of results, with an overall trend toward “needs improvement.” One of two main conclusions can be drawn from this analysis:

- Employees know how to protect themselves and their organization from various cybersecurity and privacy risks and are simply not acting upon what they know, or
- Employees have not been given the appropriate level of cybersecurity and privacy awareness education and so don’t know how to deal with all the threats and risks that they face.

We’re willing to bet it’s highly unlikely most employees are intentionally disregarding what they know. Anyone doing that for too long won’t be employed after a while. That said, this analysis shows work is still needed to disseminate information on cybersecurity and data privacy best practices for the “average employee.”

Conclusion

This survey was a test. Not a test of the users we surveyed, but a test of you, the professional working in cybersecurity and privacy awareness.

Let me explain.

How did you feel when you read this survey? Were you irritated at all the things people still didn't know? Frustrated that despite how widely the world has embraced digital technology, so many users remain deeply confused how to navigate our digital world safely? If so, you aren't alone in this feeling: many of you moved into the IT profession because you love to work with systems that behave with order, logic, and rigor.

But this survey (like so many others) reveals something fundamentally true about the humans who operate and interact with the systems that enable our digital world: Humans think one thing and do the other. They hold mutually contradictory thoughts in their minds. They are illogical, contradictory, and maddeningly complex.

Humans are also the dynamic and creative force that creates value in our companies. So, if you read this survey and were inspired by the challenge of helping your fellow employees resolve their confusion around data protection and align their behaviors to their knowledge, there's a great job waiting for you! You can be an awareness program manager (or some variation on that title).

Working on the human side of cybersecurity assumes that you understand both the systems we use to process information and the laws, regulations, and policies we use to guide that information's use—but those are just prerequisites. The real meat of this job lies in conveying all that you know to your fellow employees with such clarity and consistency and regularity that they will reliably protect the information that your company depends upon. And by the way, it's not enough for employees to know the right thing, they've got to consistently do the right thing. That's right: you've got to shape what employees know and do, even though those employees may not give a damn about security and privacy.

If nothing else, this survey presents a thundering argument for the importance of running a security and privacy awareness program. The work of building awareness and changing behavior will not be achieved through once-a-year training, nor by the mere application of simulated phishing attacks. It's going to take an ongoing, creative application of effort designed to instill a privacy- and security-aware culture. It will take diligence and perseverance and most likely a dogged belief that it matters for people to get this right—it matters for their work and it matters for their personal life.

When you succeed at this job, the rewards are huge: you'll see quantitative evidence of your efforts at risk reduction wherever you measure it (whether it's phishing, incident reporting, assessment scores, or other risk indices). You'll hear the thanks from employees who've seen firsthand the benefits of improving their skills at work and at home. Last but not least, you'll receive praise from executives who can sense the ways that you're building a risk-aware culture.

So if you read this survey and were inspired by the work that is still to be done, in your company and in the culture at large, congratulations: there is work for you to do.

Tom Pendergast
MediaPRO Chief Learning Officer

About the Survey

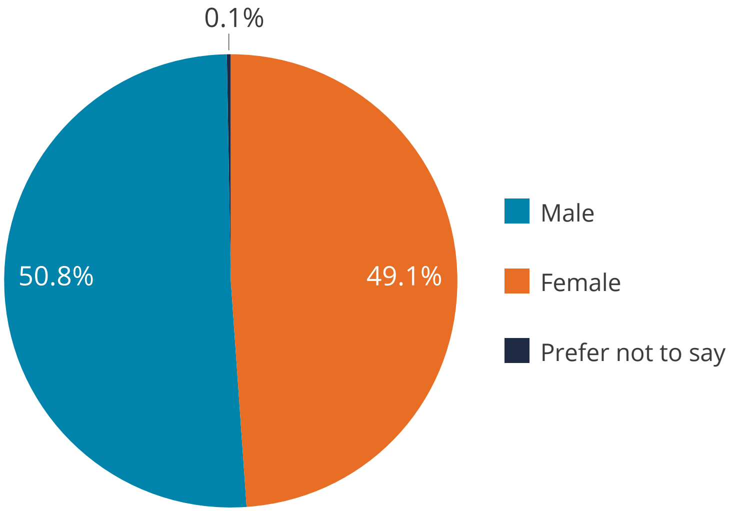
Osterman Research worked with MediaPRO to develop an in-depth questionnaire about cybersecurity and privacy awareness issues. Our focus in developing the questions was to understand how full-time and part-time employees working at companies, government entities and educational institutions, in the U.S. perceived various types of cybersecurity and privacy practices and to gauge how well employees were implementing these practices. Our goal was to determine the level of risk that organizations face when employees do not understand, and have not been appropriately trained about, cybersecurity and privacy practices. The survey had a margin-of-error of 3.1%.

The survey panel was qualified by Osterman Research according to the following criteria:

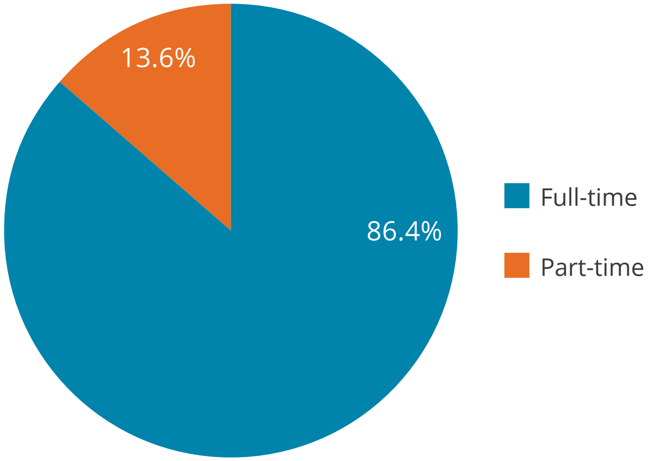
- The individuals surveyed had to be at least 18 years of age
- They had to be employed full-time or part-time by an organization of some kind; self-employed individuals, students, retired individuals and those who are not currently employed did not qualify to participate in the survey
- They had to reside in the United States
- They had to complete the full questionnaire, which consisted of 35 questions and took approximately 14 minutes to complete; 92% of those asked to complete the survey did so

The survey was completed online using the SurveyGizmo platform with 1,015 employees in the United States, broken out as follows:

Gender

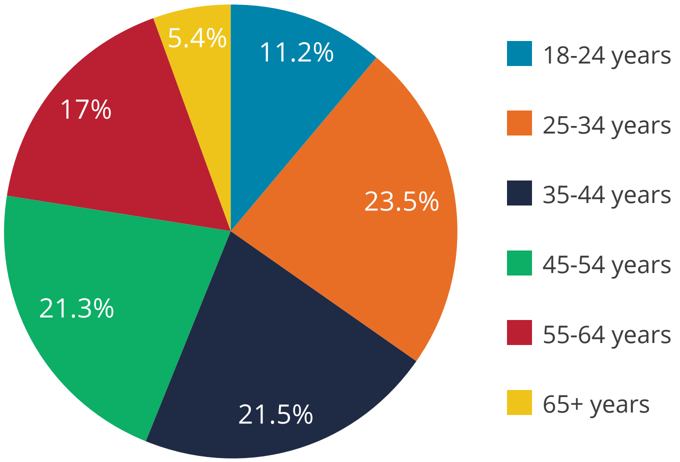


Employment Status

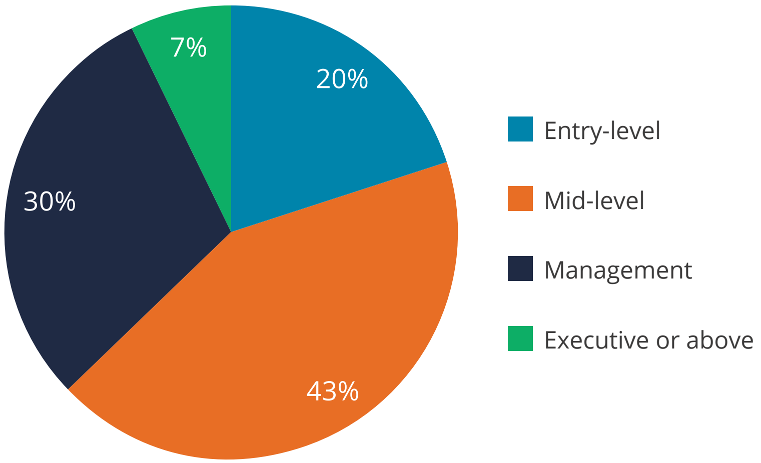


Source: Osterman Research, Inc.

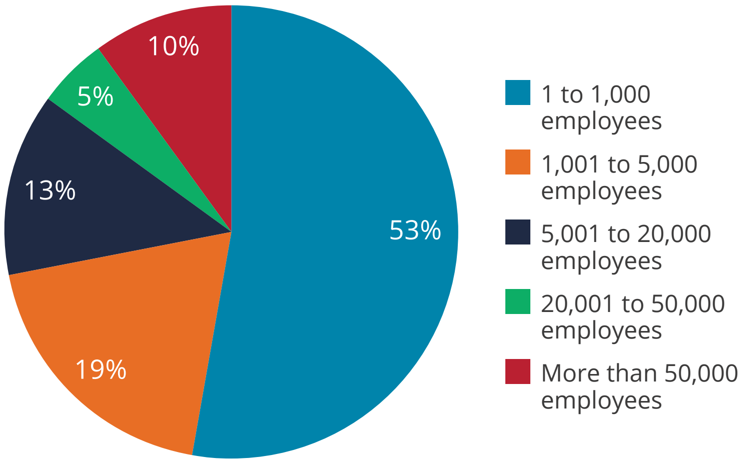
Age



Job Roles



Organization Sizes



Source: Osterman Research, Inc.

Industries

Respondents were surveyed in 49 states and in a cross section of industries. The leading industries represented are shown in the below graph:

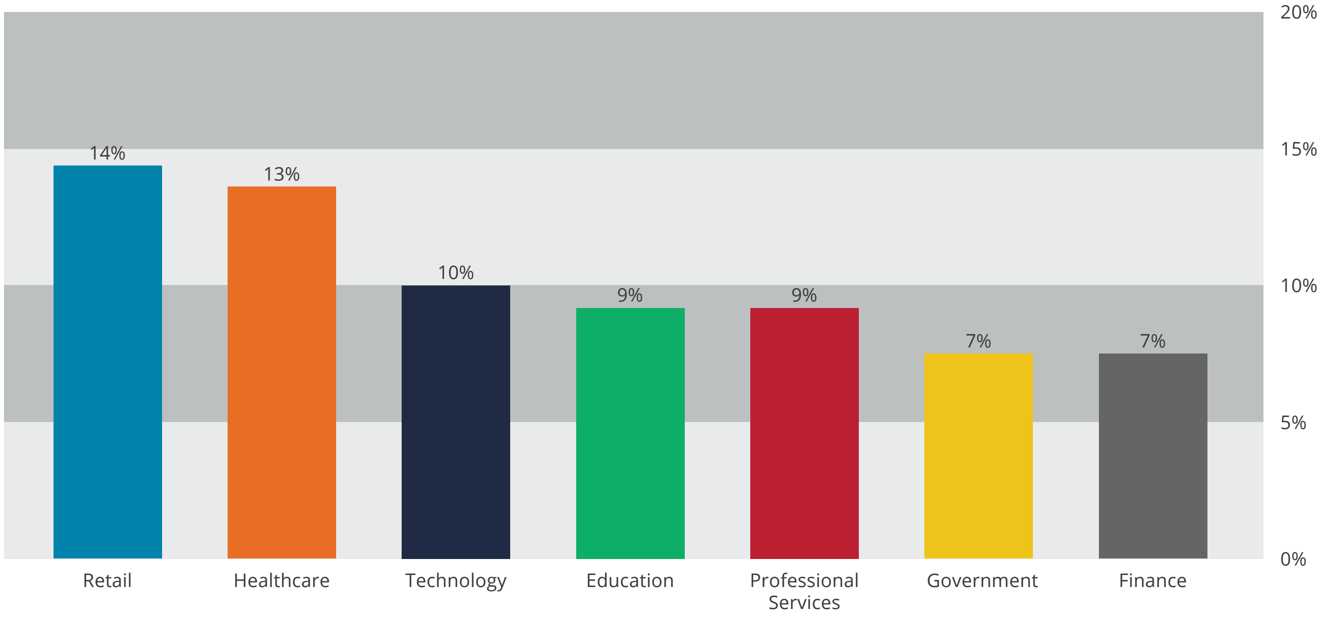
The employees in various industries broke out as follows:

Finance
40% were customer-facing, 60% were business-facing.

Healthcare
43% were providers or practitioners, 51% work in a public healthcare institution and 49% work in a private institution.

Retail
76% of are customer-facing and 24% are business-facing; 91% are full-time and 9% are temporary.

Education
38% are faculty and 62% are staff; 76% work in a public institution and 24% work in a private one.



Source: Osterman Research, Inc.

ABOUT MEDIAPRO

MediaPRO security and privacy training solutions are used by organizations of all sizes to protect sensitive data, demonstrate compliance, and reduce the risk to their reputation and bottom line. Unlike phishing-focused security awareness training solutions, MediaPRO TrainingPacks cover phishing, security, privacy, and compliance. MediaPRO TrainingPacks combine engaging, flexible, out-of-the box courses with reinforcement materials, and great customer support.

OSTERMAN RESEARCH

Osterman Research provides timely and accurate market research, cost data and benchmarking information to technology-based companies. They do this by continually gathering information from IT decision-makers and end-users of information technology. They report and analyze information to help companies develop and improve the products and services they offer to different markets or to internal customers.