Managing Insider Risk through Training & Culture

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: May 2016

Managing Insider Risk through Training & Culture

Ponemon Institute, May 2016

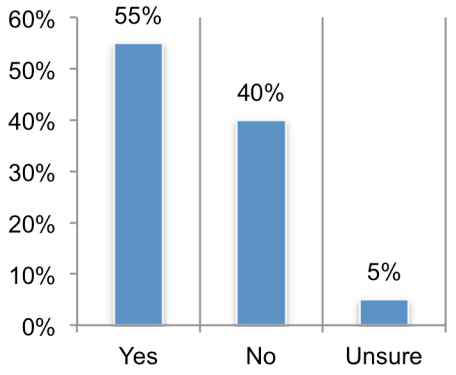
Part 1. Executive summary

Employees and other insiders inadvertently exposing sensitive or confidential information is a nightmare scenario for companies. *Managing Insider Risk through Training & Culture,* sponsored by Experian® Data Breach Resolution, reveals why this security risk persists, despite millions of dollars spent on investments in employee training and other efforts to reduce careless behavior in the handling of sensitive and confidential information. Ponemon Institute surveyed 601 individuals in companies that have a data protection and privacy training (DPPT) program and who are knowledgeable about the program.

Companies understand the risk

Sixty-six percent of respondents admit employees are the weakest link in their efforts to create a strong security posture. As shown in Figure 1, 55 percent of respondents say their organization had a security incident or data breach due to a malicious or negligent employee.

Figure 1. Did your organization have a security incident or data breach due to a malicious or negligent employee?



The top two insider risks, according to respondents, are a data breach caused by a careless or negligent employee who exposes sensitive information or succumbs to a targeted phishing attack. Companies also understand that security risks involve behaviors that could lead to a data breach or other security incident. These concerns are:

- Unleashing malware from an insecure website or mobile device
- Succumbing to targeted phishing attacks
- Using unapproved cloud or mobile applications to send sensitive company information

Current state of employee security awareness

Awareness of the insider risk, however, is not influencing many companies represented in this study to put practices in place that will improve the security culture and training of employees. Only 35 percent of respondents say senior executives believe it is a priority that employees are knowledgeable about how data security risks affect their organizations. As a result, 60 percent of respondents believe employees are not knowledgeable or have no knowledge of the company's security risks.

Employee training programs falling short

While every company surveyed has a training program, many of these programs do not have the depth and breadth of content to drive significant behavioral changes and reduce the insider risk. Only half of the companies agree or strongly agree that current employee training actually reduces noncompliant behaviors.

Forty-three percent of respondents say that training consists of only one basic course for all employees. These basic courses often do not provide training on the risks that lead to data breaches. The following are critical areas that are often ignored:

- Less than half (49 percent of respondents) say the course includes phishing and social engineering attacks
- Only 38 percent of respondents say the course includes mobile device security
- Only 29 percent of respondents say the course includes the secure use of cloud services

Further, only 45 percent of respondents say their organizations make training mandatory for all employees. Even when mandatory, exceptions are made for certain individuals. Specifically, 29 percent of respondents say the CEO and C-level executives in their companies are not required to take the course. Not only does this set a poor example for other employees, it puts high value and sensitive information at risk due to the potential carelessness of senior executives.

Missing a valuable learning opportunity

Following a data breach, companies have a unique opportunity to affirm through training the importance of being conscientious when handling sensitive and confidential information as well as having a real example of the consequences of a data breach. Unfortunately, 60 percent of companies do not require employees to retake security training courses following a data breach, missing a key opportunity to emphasize security best practices.

Conclusion: Creating a culture of security

Mitigating the insider risk should include both culture and training. Sixty-seven percent of respondents say their organizations do not provide incentives to employees for being proactive in protecting sensitive information or reporting potential issues. Only 19 percent of respondents say their organizations provide a financial reward and 29 percent of respondents say they include such information in performance reviews.

Another approach to changing behavior is to have clear consequences for negligent behavior. Unfortunately, the survey found that one-third of respondents say there are no consequences if an employee is found to be negligent or responsible for causing a data breach. The most common type of follow-up with the employee is a one-on-one meeting with a superior. Only 16 percent of respondents say the employee's salary would be reduced and 33 percent say the employee would be terminated.

In conjunction with culture, DPPT programs are critical to reducing the insider risk. Programs should have content that addresses the security risks facing the organization. Following are two recommendations that will improve both training and culture.

Training. Gamify training to make learning about potential security and privacy threats fun. Interactive games that illustrate threats for employees can make the educational experience enjoyable and the content easier to retain. For example, new technologies that simulate real phishing emails and provide simple ways to report potentially fraudulent messages are gaining traction. These types of real-time and interactive activities can be effective in changing user behavior.

Culture. Apply the carrot and stick approach to reducing the insider risk. Provide employees with incentives to report security issues and safeguard confidential and sensitive information. Companies should establish and communicate the consequences of a data breach or security incident caused by negligent or careless behavior. The tone at the top is critical to strengthening an organization's security culture. Senior executives should set an example by participating in the DPPT program and emphasizing the importance of reducing the risk of a data breach or security incident.

Part 2. Key findings

In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of the report.

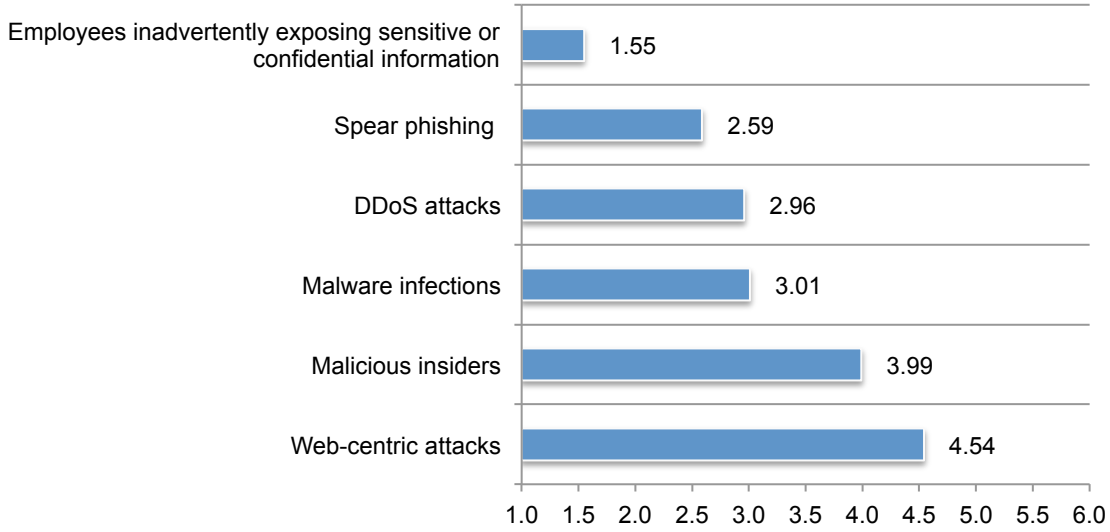
We have organized the report according to these topics:

- Insider risk & data breaches
- Organizational culture & insider risk
- Training programs & technologies to reduce insider risk

Insider risk & data breaches

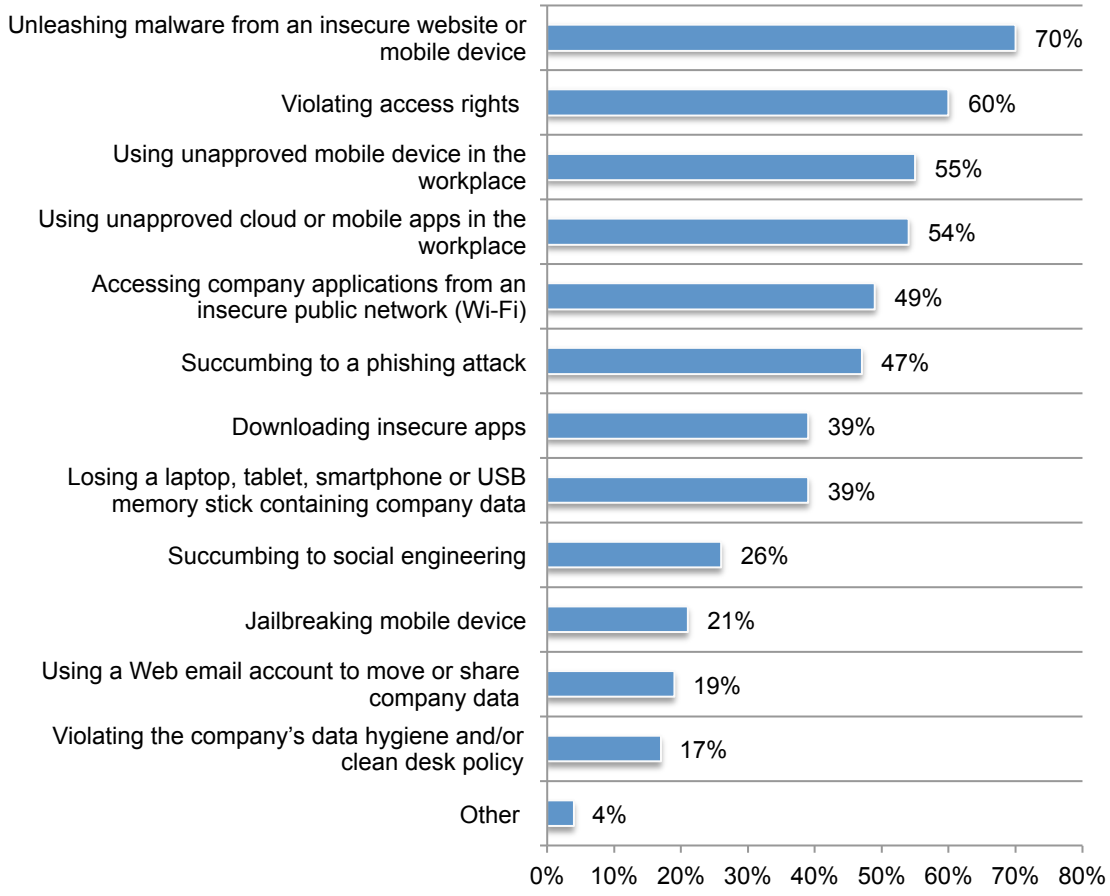
The number one security risk is employee carelessness. We asked respondents to rank their concern regarding six security risks. As shown in Figure 2, the number one concern is employees inadvertently exposing sensitive or confidential information followed by spear phishing and DDoS attacks.

Figure 2. Which security risks are you most concerned about?
1 = most concern to 6 = least concern



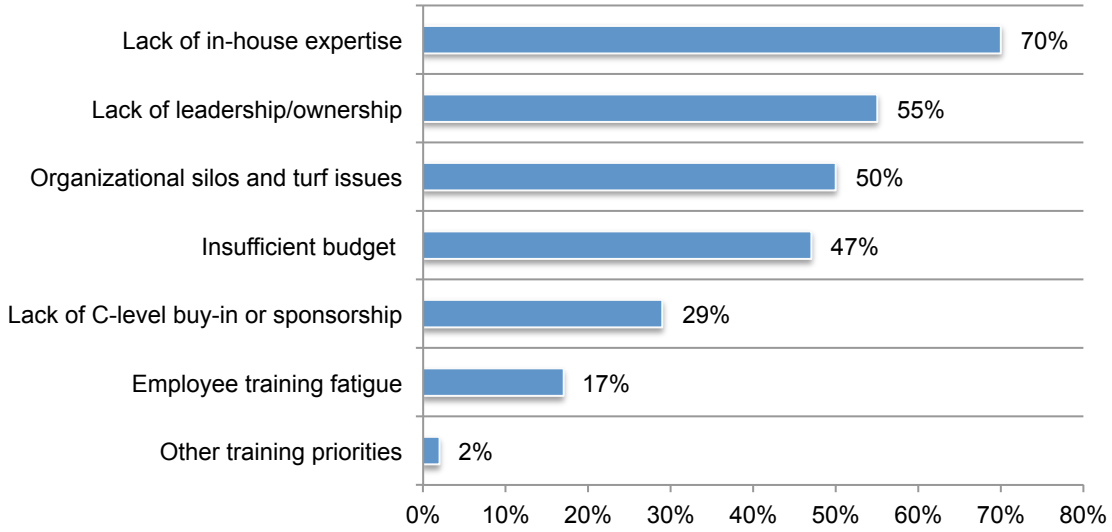
According to Figure 3, the negligent and malicious behaviors companies are most concerned about are: unleashing malware from an insecure website or mobile device (70 percent of respondents), violating access rights (i.e. using someone else's authentication or password) (60 percent of respondents), using an unapproved mobile device in the workplace (55 percent of respondents) and using unapproved cloud or mobile apps in the workplace (54 percent of respondents).

Figure 3. Negligent and malicious behaviors of most concern to organizations
More than one choice permitted



The majority of companies have had a data breach due to a malicious or negligent employee. As discussed, 55 percent of respondents say an insider caused a security incident or data breach. The two primary reasons for not being able to reduce the risk of a data breach are the lack of in-house expertise and a lack of leadership or ownership to address this risk (70 percent and 55 percent of respondents, respectively).

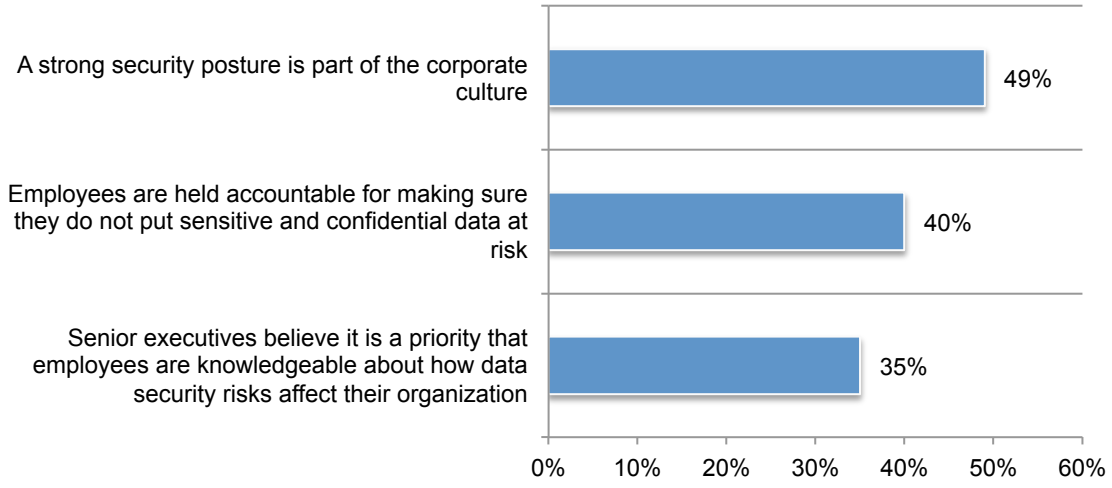
Figure 4. Why reducing the risk of a data breach due to negligent or malicious employees is difficult
More than one response permitted



Organizational culture & the insider risk

Senior management does not make privacy and security training a priority. As shown in Figure 5, only 35 percent of respondents say senior management believes it is a priority that employees are knowledgeable about how data security risks affect their organization. Further, only 40 percent of respondents say the organization holds employees accountable for making sure they do not put sensitive and confidential data at risk. Almost half (49 percent of respondents) do agree that a strong security posture is part of the corporate culture.

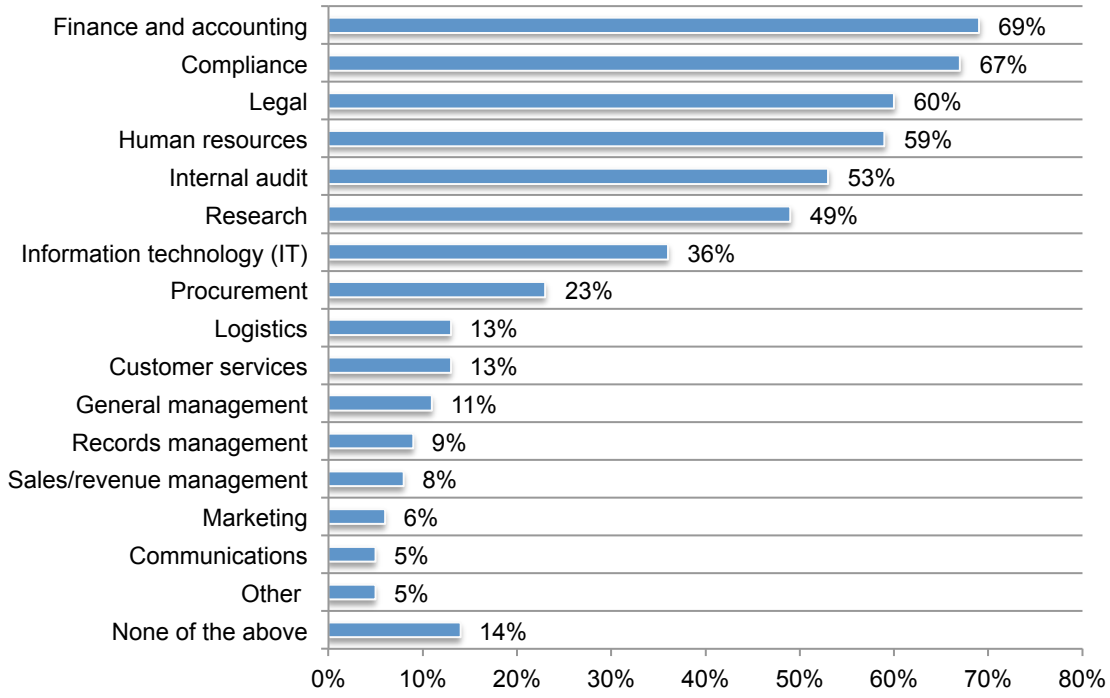
Figure 5. What senior management thinks about the insider risk
Strongly agree and agree responses combined



The departments most conscientious about safeguarding sensitive information are finance and accounting and compliance. Respondents consider certain departments more careful than others in the handling of sensitive and confidential information.

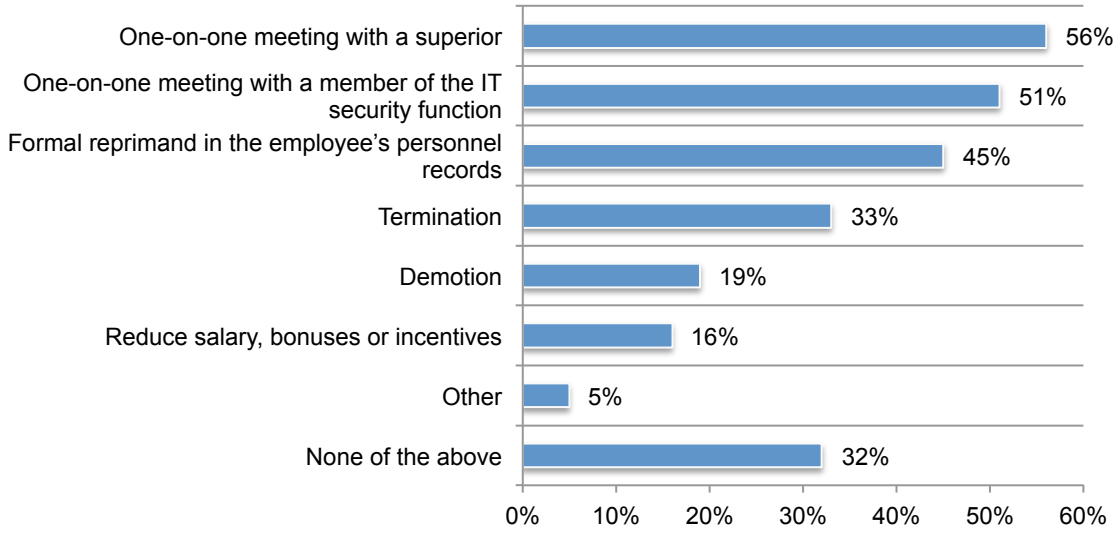
As shown in Figure 6, the most conscientious are: finance and accounting (69 percent of respondents), compliance (67 percent of respondents), legal (60 percent of respondents), human resources (59 percent of respondents) and internal audit (53 percent of respondents). The least conscientious are: sales, marketing and communications (8 percent of respondents, 6 percent of respondents and 5 percent of respondents, respectively).

Figure 6. Which departments are most conscientious about protecting your organization's sensitive and confidential information?
Five choices permitted



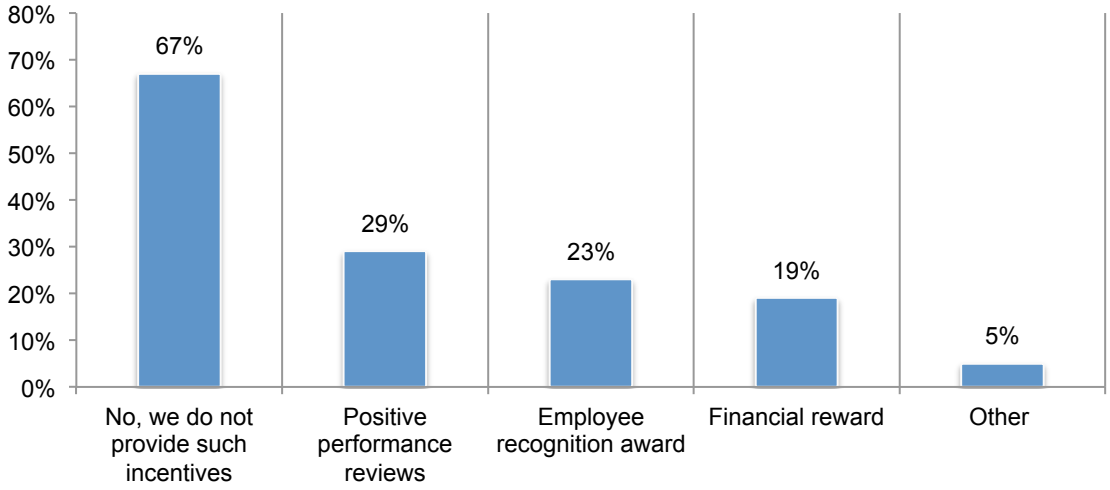
How do organizations address negligent employees or reward good behavior? As shown in Figure 7, the primary methods of dealing with an employee who is careless with sensitive and confidential information are to have a one-on-one meeting with a superior (56 percent of respondents), a one-on-one meeting with a member of the IT security function (51 percent of respondents) or a formal reprimand in the employee's personnel records (45 percent of respondents). Only 19 percent of respondents say their organizations demote employees or reduce salary, bonuses or incentives (16 percent of respondents).

Figure 7. Does your organization take any of the following actions if an employee is found to be negligent?
More than one choice permitted



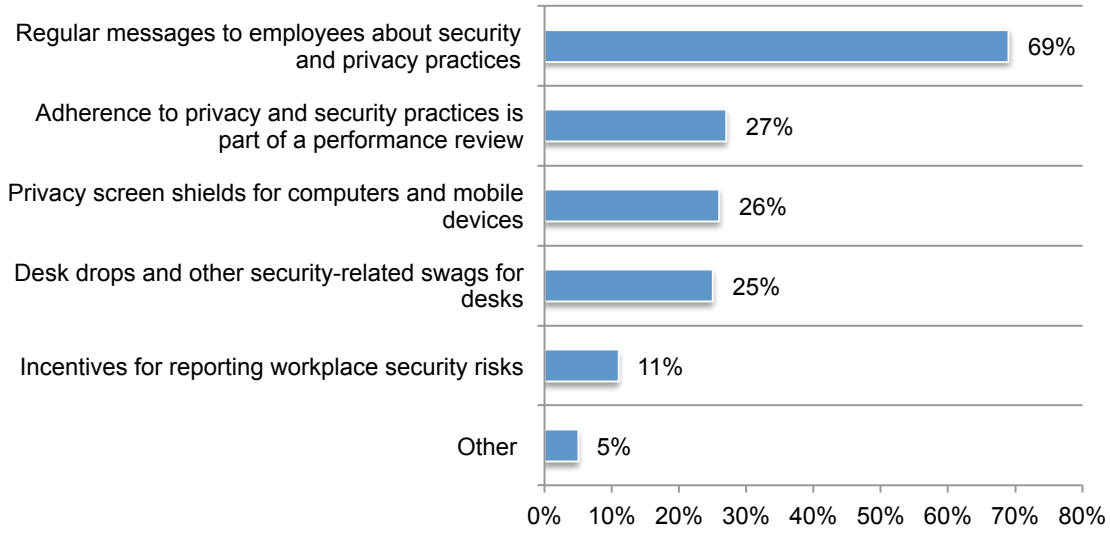
Sixty-seven percent of respondents say their organizations do not offer any incentives to employees for being proactive in protecting sensitive and confidential information. If they do offer incentives, it is most likely to be a positive performance review (29 percent of respondents) or employee recognition award (23 percent of respondents).

Figure 8. Does your organization offer any of the following incentives to employees for being proactive in protecting sensitive and confidential information?
More than one choice permitted



To support training, organizations send regular messages to employees about security and privacy practices. In addition to training, the primary step taken by companies is to send regular messages to employees about security and privacy practices, according to 69 percent of respondents. This is followed by 27 percent of respondents who say the company makes adherence to privacy and security practices part of a performance review and 26 percent of respondents who say their company provides privacy screen shields for computers and mobile devices.

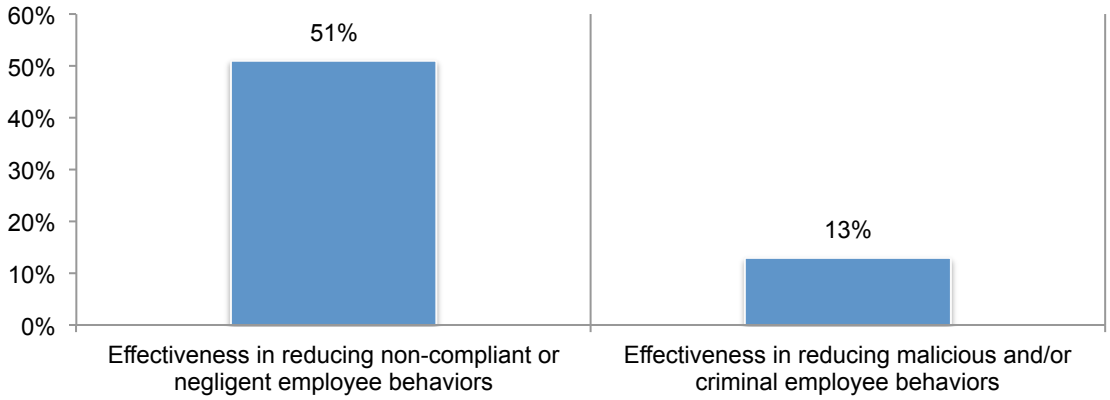
Figure 9. In addition to training, what steps do you take to reduce the risk of employee negligence?
More than one choice permitted



Training programs & technologies to reduce insider risk

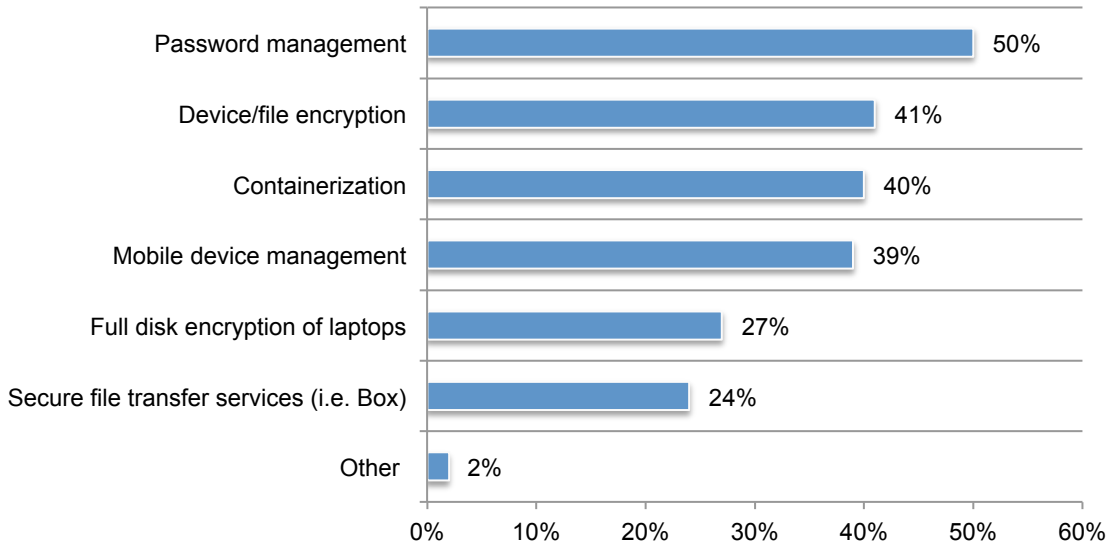
Training programs need to become more effective. As discussed previously, only 25 percent of respondents say their employees have a deep knowledge about privacy and data protection. According to Figure 10, 51 percent of respondents rate the effectiveness of their organization's DPPT in reducing noncompliant or negligent employee behaviors in the workplace as highly effective but not highly effective in reducing malicious behavior.

Figure 10. How effective is your DPPT program in reducing negligent or malicious behaviors?
1 = low to 10 = high, 7+ responses reported



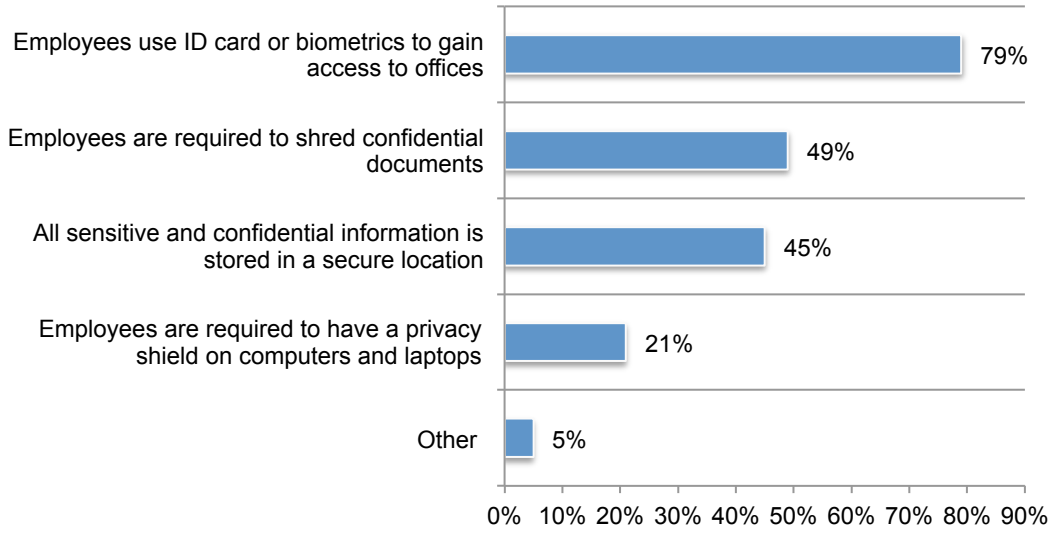
Technologies are used to supplement training to reduce insider risk. To address the risks of malicious and careless employees, many companies are turning to such solutions as data-loss prevention technologies, according to 59 percent of respondents. As shown in Figure 11, companies represented in this study also use password management (50 percent of respondents), device/file encryption (41 percent of respondents), containerization (40 percent of respondents) and mobile device management (39 percent of respondents).

Figure 11. Does your organization use any of the following device management solutions?
More than one choice permitted



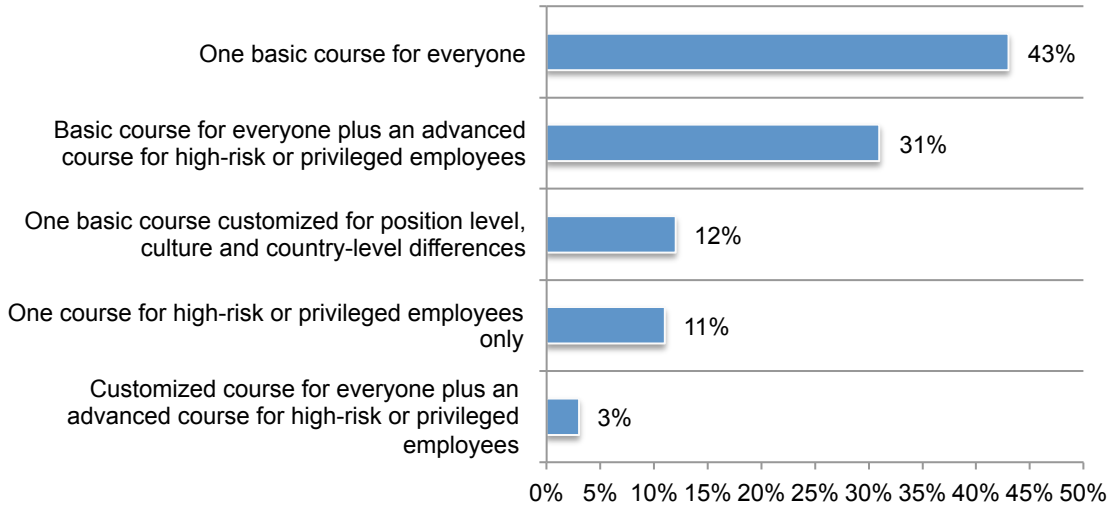
Physical security is also used to reduce insider threats. As shown in Figure 12, 79 percent of respondents say their companies require employees to use ID cards or biometrics to gain access to offices. Other requirements for employees are: shredding confidential documents (49 percent of respondents), storing all sensitive and confidential information in a secure location (45 percent of respondents) or having a privacy shield on computers and laptops (21 percent of respondents).

Figure 12. Does your organization have any of the following physical security precautions in place?
More than one choice permitted



Most DPPT programs are basic in content. According to Figure 13, 43 percent of respondents say their organizations have one basic course for everyone, followed by 31 percent of respondents who say it is one basic course for everyone plus an advanced course for high-risk or privileged employees. Only 3 percent of respondents say they offer a customized course for everyone plus an advanced course for high-risk or privileged employees.

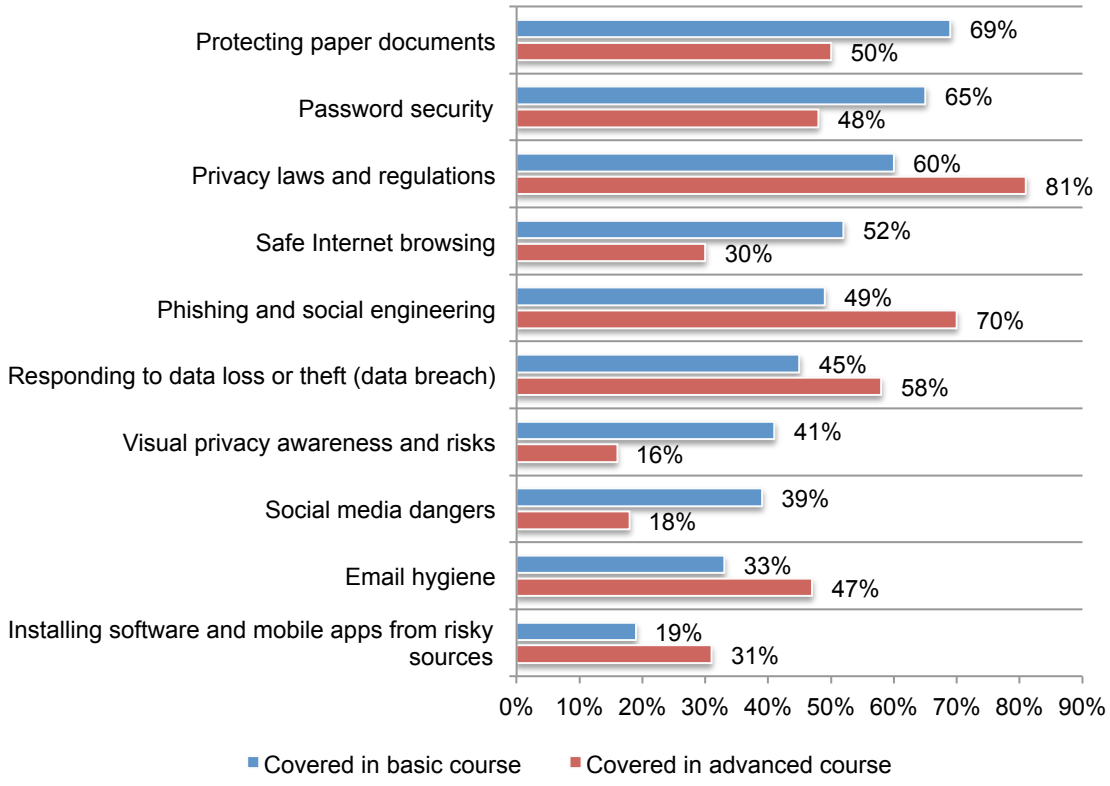
Figure 13. What best describes the structure of your organization's DPPT program?



Basic courses typically cover these topics: protecting paper documents, securing protected data, password security, privacy laws and regulations, and data classification. Advanced courses are more likely to cover phishing and social engineering, responding to a data loss or theft, mobile device security, and email hygiene.

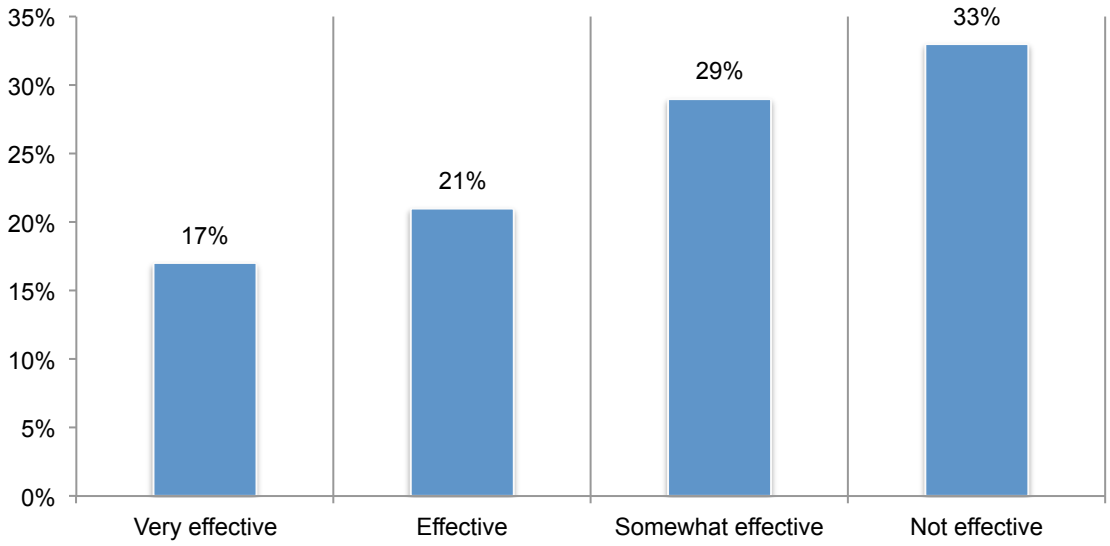
The biggest differences between the two programs are: protecting paper documents, password security, privacy laws and regulations, safe Internet browsing, phishing and social engineering, visual privacy awareness and risks, and social media dangers, responding to data loss or theft (data breach), email hygiene, and installing software and mobile apps from risky sources.

Figure 14. Topics covered in basic and advanced DPPT courses
More than one choice permitted



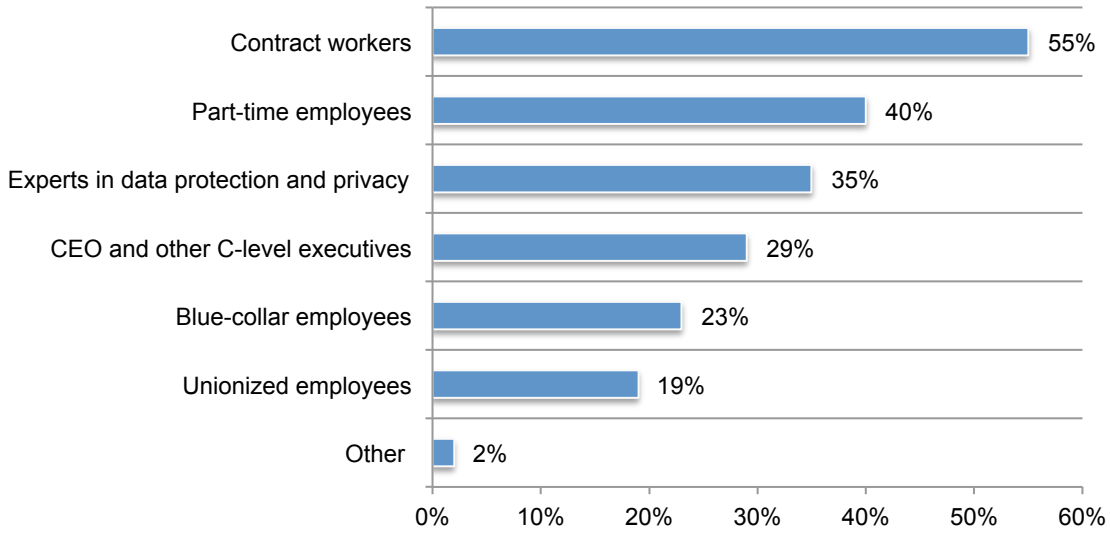
Purchased training products are given low marks. Fifty-five percent of respondents say their companies purchase products for their DPPT program. However, as shown in Figure 15, 62 percent of respondents say these products are only somewhat effective or not effective (29 percent + 33 percent).

Figure 15. How effective are training products purchased from vendors?



DPPT courses are not mandatory for everyone. Fifty-four percent of respondents say the program is not mandatory for everyone. If DPPT is mandatory, there are exceptions made for certain individuals. According to Figure 16, 55 percent of respondents say contract workers are not required to take the course and 35 percent of respondents say experts in data protection and privacy are exempt. Twenty-nine percent of respondents say the CEO and C-level executives in their organizations are not required to take the course. An average of 60 percent of all employees required to take the course actually complete it.

Figure 16. Who is exempt from taking DPPT courses?
More than one choice permitted

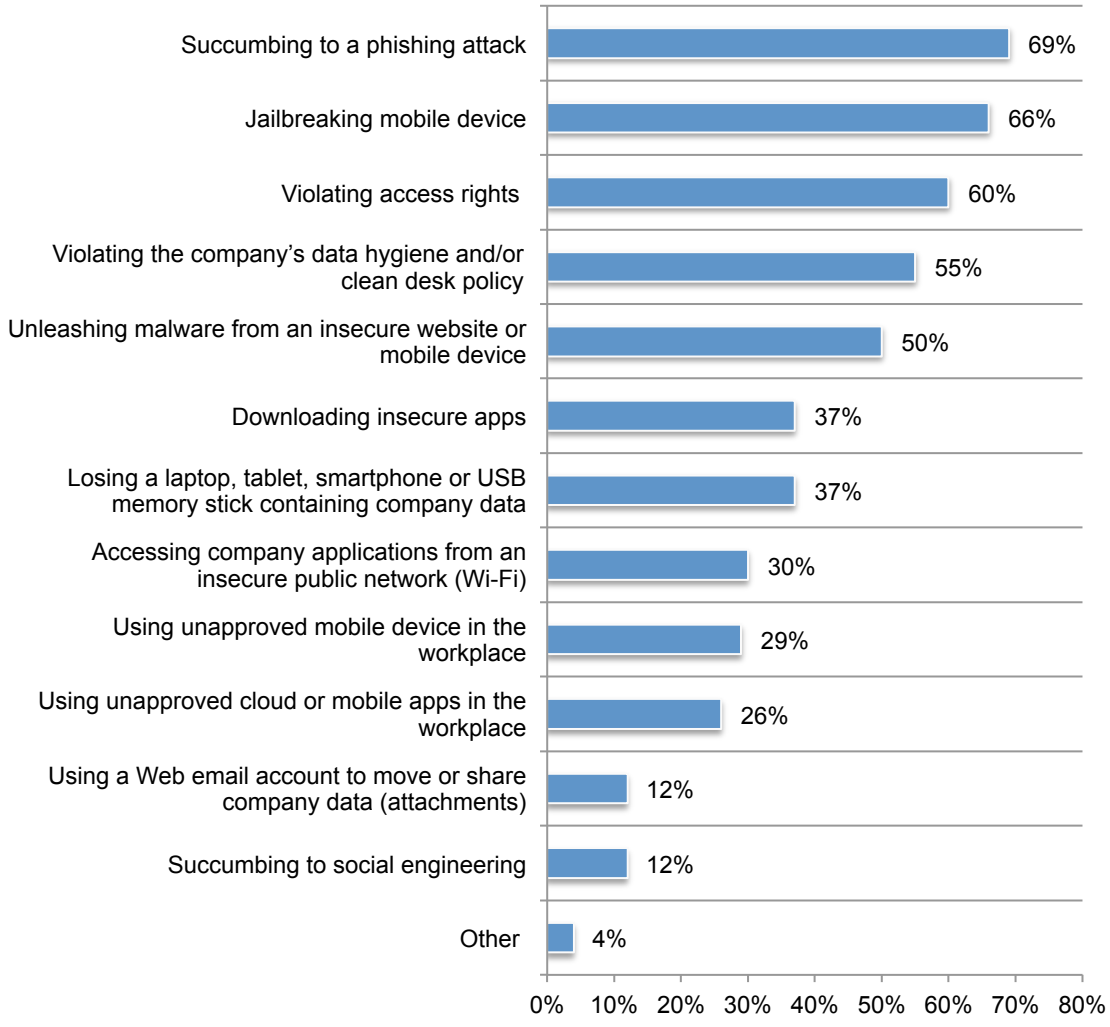


Companies miss a valuable training opportunity. Following a data breach, only 30 percent of respondents say their organization requires employees to take or retake the DPPT course. This would be an excellent time—while the breach is fresh in the minds of employees—to increase their privacy and security knowledge.

Following certain negligent and malicious behaviors, employees are required to retake the DPPT course. According to Figure 17**,** 69 percent of respondents say succumbing to a phishing attack and 66 percent say jailbreaking a mobile device will send the employee back to school.

Other behaviors requiring employees to retake the course are: violating access rights (using someone else's authentication or password) (60 percent of respondents), violating the company's data hygiene and/or clean desk policy (55 percent of respondents) and unleashing malware from an insecure website or mobile device.

Figure 17. Which negligent and malicious behaviors require employees to retake the DPPT course?
More than one choice permitted



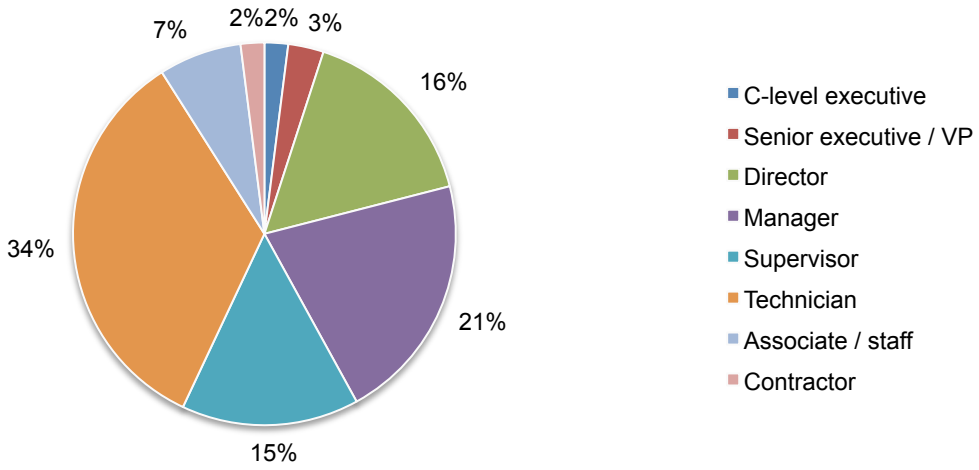
Part 3. Methods

A sampling frame of 16,556 individuals in companies that have a data protection and privacy training program (DPPT) program were selected to participate in this survey. Table 1 shows 651 total returns. Screening and reliability checks required the removal of 50 surveys. Our final sample consisted of 60 surveys or a 3.6 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,556	100.0%
Total returns	651	3.9%
Rejected or screened surveys	50	0.3%
Final sample	601	3.6%

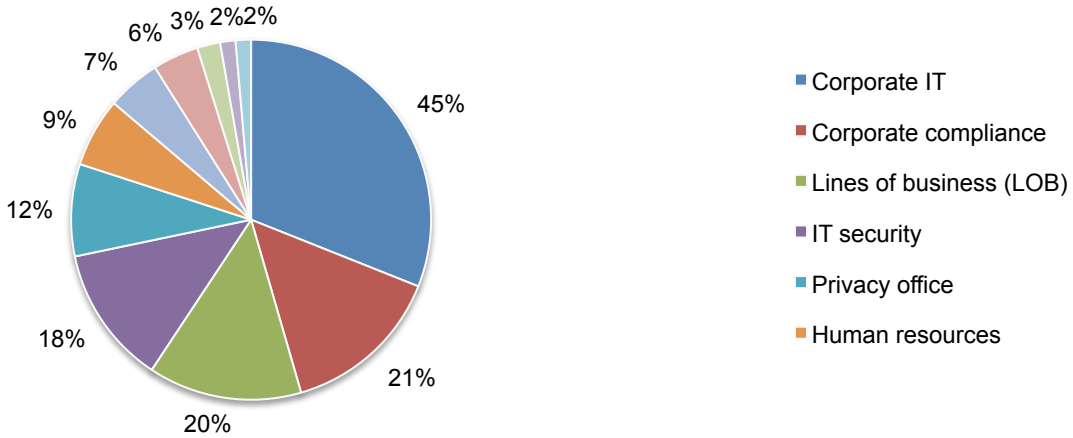
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of respondents (57 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



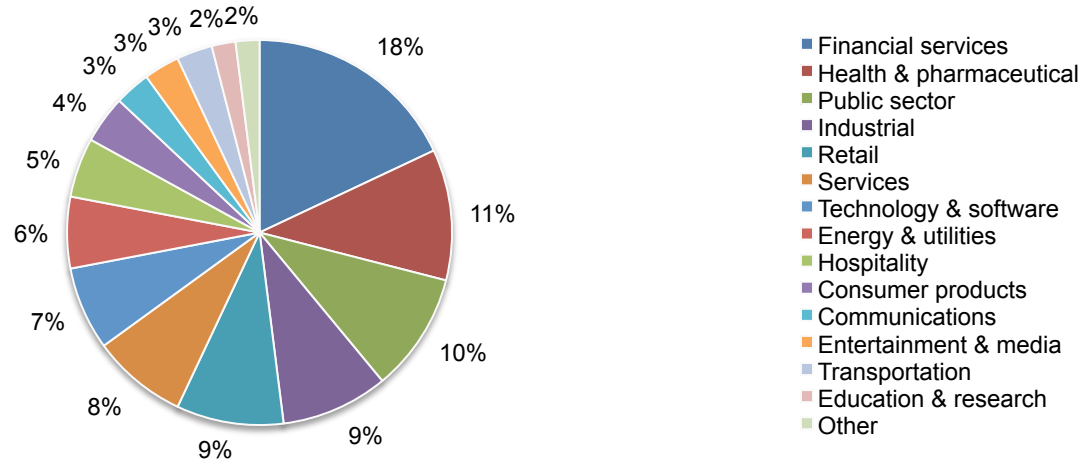
As shown in Pie Chart 2, 45 percent of respondents reported their functional area is within corporate IT, 21 percent responded corporate compliance and 20 percent responded lines of business.

Pie Chart 2. Primary functional area within the organization



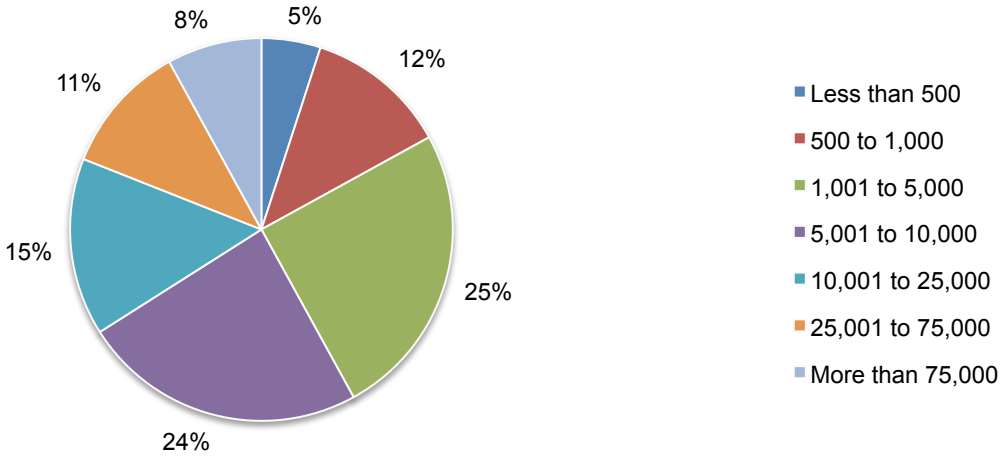
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by and health and pharmaceutical (11 percent) and public sector (10 percent).

Pie Chart 3. Primary industry segment



As shown in Pie Chart 4, 58 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 4. Global employee headcount



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 in companies that have a data protection and privacy training program (DPPT) program. 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 in April 2016.

Survey response	Freq	Pct%
Total sampling frame	16,556	100.0%
Total returns	651	3.9%
Rejected or screened surveys	50	0.3%
Final sample	601	3.6%

Screening Questions

S1. Does your organization have a data protection and privacy training (DPPT) program in place today?	Pct%
Yes, a program that combines data protection and privacy topics	29%
Yes, separate programs for data protection and privacy topics	30%
Yes, a program focused solely on data protection (not privacy)	26%
Yes, a program focused solely on privacy (not data protection)	15%
No (stop)	0%
Total	100%

S2. How knowledgeable are you about your organization's DPPT program?	Pct%
Very knowledgeable	42%
Knowledgeable	30%
Somewhat knowledgeable	28%
No knowledge [stop]	0%
Total	100%

Part 2. General questions

Q1. How knowledgeable are employees about your organization's security risks?	Pct%
Very knowledgeable	8%
Knowledgeable	13%
Somewhat knowledgeable	19%
Not knowledgeable	50%
No knowledge	10%
Total	100%

Q2. Please rank your concern about the following six security risks from 1 = most concern to 6 = least concern	Average rank	Rank order
Employees inadvertently exposing sensitive or confidential information	1.55	1
Malicious insiders	3.99	5
Spear phishing	2.59	2
Web-centric attacks	4.54	6
DDoS attacks	2.96	3
Malware infections	3.01	4

Q3. Did your organization have a security incident or data breach due to a malicious or negligent employee?	Pct%
Yes	55%
No	40%
Unsure	5%
Total	100%

Q4. What makes it difficult to reduce the risk of a data breach due to negligent or malicious employees? Please select all that apply.	Pct%
Insufficient budget	47%
Lack of in-house expertise	70%
Lack of leadership/ownership	55%
Lack of C-level buy-in or sponsorship	29%
Organizational silos and turf issues	50%
Employee training fatigue	17%
Other training priorities	2%
Total	270%

2. Attributions: Please rate each statement using the agreement scale provided below each item.	Strongly agree	Agree
Q5. My organization's DPPT program reduces employees' non-compliant behaviors and negligence.	21%	29%
Q6. My organization's DPPT is effective at minimizing loss or theft of confidential data.	18%	25%
Q7. Senior executives believe it is a priority that employees are knowledgeable about how data security risks affect their organization.	16%	19%
Q8. Employees are the weakest link in our organization's cybersecurity infrastructure.	35%	31%
Q9. My organization's employees have deep knowledge about privacy and data protection.	11%	14%
Q10. My organization holds employees accountable for making sure they do not put sensitive and confidential data at risk.	19%	21%
Q11. A strong security posture is part of the corporate culture.	21%	28%

3. State of Training

Q12. Using the following 10-point scale, please rate the effectiveness of your organization's DPPT in reducing non-compliant or negligent (non-malicious) employee behaviors in the workplace. 1 = low to 10 = high.	Pct%
1 or 2	8%
3 or 4	15%
5 or 6	26%
7 or 8	35%
9 or 10	16%
Total	100%
Extrapolated value	6.22

Q13. Using the following 10-point scale, please rate the effectiveness of your organization's DPPT in reducing malicious and/or criminal employee behaviors in the workplace. 1 = low to 10 = high.	Pct%
1 or 2	44%
3 or 4	28%
5 or 6	15%
7 or 8	8%
9 or 10	5%
Total	100%
Extrapolated value	3.54

Q14. What best describes the structure of your organization's DPPT program?	Pct%
One basic course for everyone	43%
One basic course customized for position level, culture and country-level differences	12%
Basic course for everyone plus an advanced course for high-risk or privileged employees	31%
Customized course for everyone plus an advanced course for high-risk or privileged employees	3%
One course for high-risk or privileged employees only	11%
Other (please specify)	0%
Total	100%

Q15a. Do you purchase training products for your DPPT program?	Pct%
Yes	55%
No	40%
Unsure	5%
Total	100%

Q15b. If yes, how effective are these products?	Pct%
Very effective	17%
Effective	21%
Somewhat effective	29%
Not effective	33%
Total	100%

Q16. Which of the following negligent and malicious behaviors is your organization most concerned about? Please select your top five choices.	Pct%
Unleashing malware from an insecure website or mobile device	70%
Violating access rights (using someone else's authentication or password)	60%
Using unapproved mobile device in the workplace	55%
Using unapproved cloud or mobile apps in the workplace	54%
Accessing company applications from an insecure public network (Wi-Fi)	49%
Succumbing to a phishing attack	47%
Losing a laptop, tablet, smartphone or USB memory stick containing company data	39%
Downloading insecure apps	39%
Succumbing to social engineering	26%
Jailbreaking mobile device	21%
Using a Web email account to move or share company data (attachments)	19%
Violating the company's data hygiene and/or clean desk policy	17%
Other (please specify)	4%
Total	500%

Q17a. Does your organization require employees to take or retake the DPPT course following a data breach?	Pct%
Yes	30%
No	60%
Unsure	10%
Total	100%

Q17b. Which of the following negligent and malicious behaviors require the employee to retake the DPPT course? Please select all that apply.	Pct%
Succumbing to a phishing attack	69%
Succumbing to social engineering	12%
Unleashing malware from an insecure website or mobile device	50%
Jailbreaking mobile device	66%
Losing a laptop, tablet, smartphone or USB memory stick containing company data	37%
Using a Web email account to move or share company data (attachments)	12%
Using unapproved cloud or mobile apps in the workplace	26%
Using unapproved mobile device in the workplace	29%
Downloading insecure apps	37%
Violating the company's data hygiene and/or clean desk policy	55%
Violating access rights (using someone else's authentication or password)	60%
Accessing company applications from an insecure public network (Wi-Fi)	30%
Other (please specify)	4%
Total	487%

Q18. In addition to training, what steps do you take to reduce the risk of employee negligence?	Pct%
Adherence to privacy and security practices is part of a performance review	27%
Incentives for reporting workplace security risks	11%
Desk drops and other security-related swags for desks	25%
Privacy screen shields for computers and mobile devices	26%
Regular messages to employees about security and privacy practices	69%
Other (please specify)	5%
Total	163%

Q19. Which departments are most conscientious about protecting your organization's sensitive and confidential information? Please select the top five choices	Pct%
Finance and accounting	69%
Compliance	67%
Legal	60%
Human resources	59%
Internal audit	53%
Research	49%
Information technology (IT)	36%
Procurement	23%
Customer services	13%
Logistics	13%
General management	11%
Records management	9%
Sales/revenue management	8%
Marketing	6%
Communications	5%
Other (please specify)	5%
None of the above	14%
Total	500%

Q20. Does your organization take any of the following actions if an employee is found to be negligent? Please select all that apply.	Pct%
Reduce salary, bonuses or incentives	16%
Demotion	19%
Termination	33%
Formal reprimand in the employee's personnel records	45%
One-on-one meeting with a member of the IT security function	51%
One-on-one meeting with a superior	56%
Other (please specify)	5%
None of the above	32%
Total	257%

Q21. Does your organization offer any of the following incentives to employees for being proactive in protecting sensitive and confidential information?	Pct%
Positive performance reviews	29%
Financial reward	19%
Employee recognition award	23%
Other (please specify)	5%
No, we do not provide such incentives	67%
Total	143%

Q22. How is the success of the DPPT program measured or determined? Please select all that apply.	Pct%
Coverage (number of employees who completed training)	73%
Employee satisfaction (feedback)	68%
Employee quiz (pass rate)	65%
Third-party assessment	26%
Pre- and post-testing (determine learning gain or retention over time)	25%
Time to complete rollout	25%
Delivery cost per employee	21%
Reduction in non-compliant behaviors and practices	11%
Reduction in the number of data breaches	10%
Other (please specify)	4%
Total	328%

Q23a. Is DPPT mandatory for employees?	Pct%
Yes	46%
No	54%
Total	100%

Q23b. If the DPPT program is mandatory, are there exceptions to participation?	Pct%
Yes	45%
No	40%
Unsure	15%
Total	100%

Q23c. If yes, who are they? Please select all that apply.	Pct%
CEO and other C-level executives	29%
Blue-collar employees	23%
Unionized employees	19%
Experts in data protection and privacy	35%
Part-time employees	40%
Contract workers	55%
Other (please specify)	2%
Total	203%

Q24. Approximately, what percentage of employees who are required to take the DPPT actually completes the course?	Pct%
Less than 5%	0%
5% to 10%	9%
11% to 25%	13%
26% to 50%	15%
51% to 75%	18%
76% to 100%	37%
100% (all)	8%
Total	100%
Extrapolated value	60%

Q25. Does your organization have data-loss prevention technologies and other solutions to monitor employee access and sending of corporate documents?	Pct%
Yes	59%
No	30%
Unsure	11%
Total	100%

Q26. Does your organization use any of the following device management solutions? Please check all that apply.	Pct%
Mobile device management	39%
Containerization	40%
Device/file encryption	41%
Full disk encryption of laptops	27%
Password management	50%
Secure file transfer services (i.e. Box)	24%
Other (please specify)	2%
Total	223%

Q27. Does your organization have any of the following physical security precautions in place? Please check all that apply	Pct%
All sensitive and confidential information is stored in a secure location	45%
Employees are required to shred confidential documents	49%
Employees are required to have a privacy shield on computers and laptops	21%
Employees use ID card or biometrics to gain access to offices	79%
Other (please specify)	5%
Total	199%

Q28. Please select those topics that are covered in your organization's DPPT. Show the basic course and advanced course separately. Leave the advanced course column blank if an advanced course is not provided.	Covered in basic course	Covered in advanced course
Protecting paper documents	69%	50%
Securing protected data	65%	73%
Password security	65%	48%
Privacy laws and regulations	60%	81%
Data classification	59%	68%
Preventing malware infection	57%	55%
Safe Internet browsing	52%	30%
Phishing and social engineering	49%	70%
Responding to data loss or theft (data breach)	45%	58%
Visual privacy awareness and risks	41%	16%
Social media dangers	39%	18%
Mobile device security	38%	45%
Using personal devices in the workplace (e.g., BYOD)	38%	29%
Email hygiene	33%	47%
Using cloud services safely	29%	21%
Managing data clutter	24%	19%
Encryption basics	20%	25%
Installing software and mobile apps from risky sources	19%	31%
Biometrics for authentication	15%	26%
Acceptable use of computers in the workplace	11%	5%
Complying with record retention policy and e-discovery	9%	30%

Q29. Approximately, what is the dollar range that best describes your organization's **IT budget for 2016**?	Pct%
< $1 million	0%
$1 to 5 million	2%
$6 to $10 million	11%
$11 to $50 million	16%
$51 to $100 million	23%
$101 to $250 million	24%
$251 to $500 million	19%
> $500 million	5%
Total	100%
Extrapolated value	163.7

Q30. Approximately, what percentage of the **2016 IT budget** will go to IT security activities and investments?	Pct%
< 2%	0%
2% to 5%	21%
6% to 10%	26%
11% to 20%	23%
21% to 30%	25%
31% to 50%	5%
51% to 75%	0%
75% to 100%	0%
Total	100%
Extrapolated value	14.8%

Q31. What percentage of the IT security budget is allocated to addressing the following employee risk management activities: training and awareness programs, workplace monitoring and (insider) preventive and detective controls?	Pct%
< 2%	1%
2% to 5%	6%
6% to 10%	13%
11% to 20%	26%
21% to 30%	46%
31% to 50%	8%
51% to 75%	0%
75% to 100%	0%
Total	100%
Extrapolated value	20.3%

4. Organizational Characteristics & Role

D1. What best describes your position level?	Pct%
C-level executive	2%
Senior executive / VP	3%
Director	16%
Manager	21%
Supervisor	15%
Technician	34%
Associate / staff	7%
Contractor	2%
Other (please specify)	0%
Total	100%

D2. What best describes your functional area?	Pct%
Corporate compliance	21%
Corporate IT	45%
Corporate training	7%
Enterprise risk management	6%
Finance & accounting	1%
General counsel / legal	3%
General management	1%
Human resources	9%
IT risk management	2%
IT security	18%
Lines of business (LOB)	20%
Privacy office	12%
Procurement / vendor management	2%
Other (please specify)	0%
Total	147%

D3. What best describes your organization's primary industry segment?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	4%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	5%
Industrial	9%
Public sector	10%
Retail	9%
Services	8%
Technology & software	7%
Transportation	3%
Total	100%

D4. What range best describes the global headcount of your organization?	Pct%
Less than 500	5%
500 to 1,000	12%
1,001 to 5,000	25%
5,001 to 10,000	24%
10,001 to 25,000	15%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

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 organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, 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.