The Economic Risk of Confidential Data on Mobile Devices in the Workplace

Sponsored by Lookout

Independently conducted by Ponemon Institute LLC

Publication Date: February 2016

The Economic Risk of Confidential Data on Mobile Devices in the Workplace

Ponemon Institute, February 2016

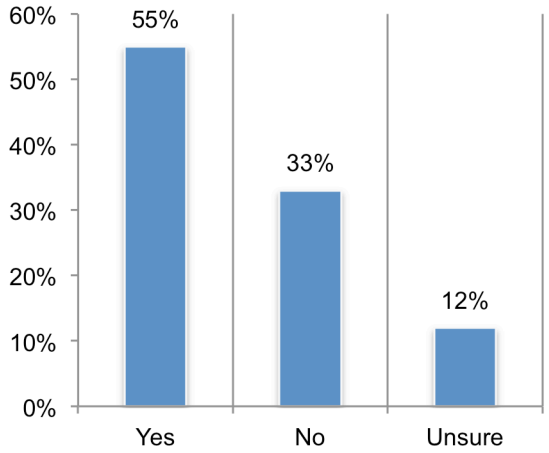
Part 1. Introduction

The purpose of this research, sponsored by Lookout, is to understand the economic risk due to the explosive use of mobile devices with access to sensitive and confidential information in the workplace. In this study, the financial consequences of malware infections and hackers that target employees' devices can be enormous.

As discussed in this report, just one mobile device infected with malware can cost an organization on average $9,485. The potential financial consequences if a hacker compromises an employee's mobile device to steal their credentials and access sensitive and confidential company data can cost an average of $21,042 to investigate, contain and remediate from the attack. These costs are based on the steps that need to be taken following an attack or compromise of a mobile device such as help desk support, IT security support, loss of productivity and the value of the data on the device. Tables 2 and 3 on pages 14 and 15 of this report details how these costs are calculated.

We surveyed 588 IT and IT security professionals in the U.S. who are employed in Global 2000 companies and are familiar with their organization's management and security of mobile devices used in the workplace. In addition, they have responsibility for monitoring or enforcing the security of mobile devices used in the workplace, including employee-owned devices (a.k.a. BYOD).

Figure 1. Do you believe employees have too much work-related data on their mobile devices?



As shown in Figure 1, 55 percent of respondents believe there is too much company data on employees' mobile devices and this shows no sign of decreasing. In fact, respondents estimate that in the past 12 months, work-related data on employees' mobile devices increased by an average of 43 percent.

Other key takeaways in this research include the following:

The root cause of many of today's data breaches is an employee's mobile device. Eighty-three percent of respondents say mobile devices are susceptible to hacking. It is, therefore, not surprising that 70 percent of respondents believe the failure to secure company data on mobile devices has likely resulted in a data breach. In fact, 67 percent of respondents say it was certain or likely that their organization had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information.

Companies are not keeping up with the risk of mobile devices in the workplace. Seventy-four percent of respondents say in the past two years employees' storage of or access to sensitive or confidential data has increased significantly. Despite this increase, only 33 percent of respondents say their organization is vigilant in protecting sensitive or confidential data from unauthorized employee access. Similarly, only 36 percent of respondents say their organization is

vigilant in protecting sensitive or confidential data stored or accessed on employees' mobile devices. Only 39 percent of respondents consider the protection of confidential information accessed by employees with their mobile devices a priority.

The majority of organizations are not providing guidelines for employees' access or storage of company data. Only 41 percent of respondents say their organization has a policy that specifies the types of company data that employees can or cannot access with mobile devices and only 30 percent of respondents say there is a policy specifying the types of company data that can be stored on their mobile devices.

Malware on mobile devices often goes undetected. On average, organizations represented in this study have 53,844 mobile devices in use by employees. An average of 3 percent of employees' mobile devices or approximately 1,723 devices are believed to be infected with malware at any point in time. However, only an average of 26 percent of infected mobile devices (448) are investigated or triaged. The average total direct cost companies are spending on these 448 devices is $12.8 million. If all 1,723 infected devices were investigated or triaged the average cost could be as high as $26.4 million.

On a positive note, budgets for mobile security are expected to increase in the next year. The average annual IT budget in organizations represented in this research is $195 million and an average of 14 percent is dedicated to security. In the next 12 months, the average IT security budget is expected to increase to $32,760,000 and the average budget allocated for mobile security is expected to increase to $5,984,160.

Employees have access to more sensitive and confidential work-related data than IT security thinks. The 56 percent of IT security respondents who believe they do know what employees access say the data types most often accessed are email and texts. However, based on findings in a companion study, IT security is in the dark about what employees are really accessing. The largest gaps between IT security and employees concern sensitive work-related data such as employee's PII (52 percent of employees vs. 18 percent of IT security), customer records (43 percent of employees vs. 19 percent of IT security), and confidential or classified documents (33 percent vs. 8 percent of IT security).

Part 2. Key findings

The key findings are discussed in this section of the report. The complete audited findings are presented in the appendix of this report.

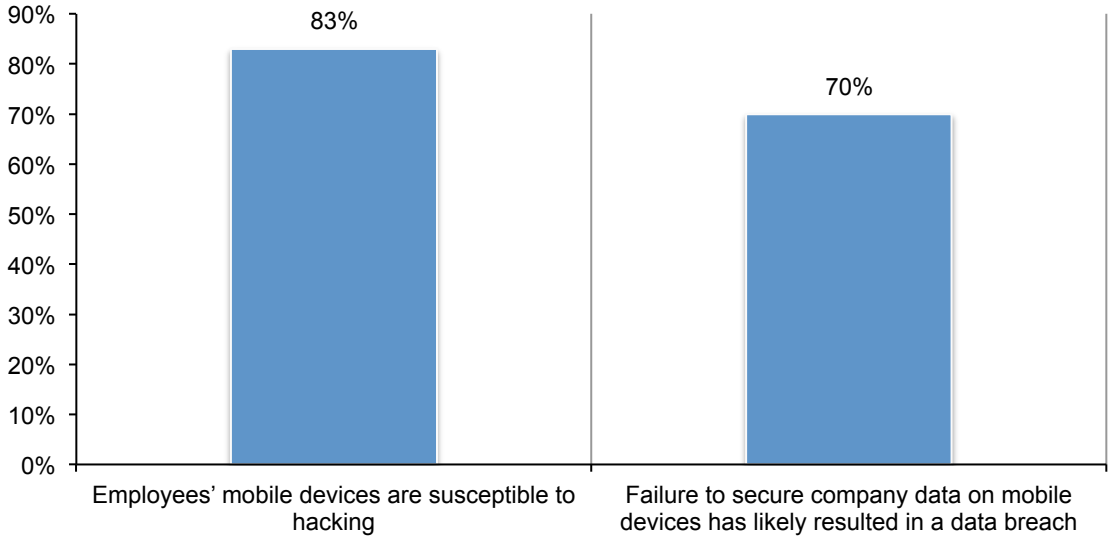
We have organized the report according to the following topics:

- Employees' mobile devices in the workplace increase the risk of a data breach
- Employees have easy access to sensitive and confidential information
- Malware infections and hackers can create significant economic risk

Employees' mobile devices in the workplace increase the risk of a data breach

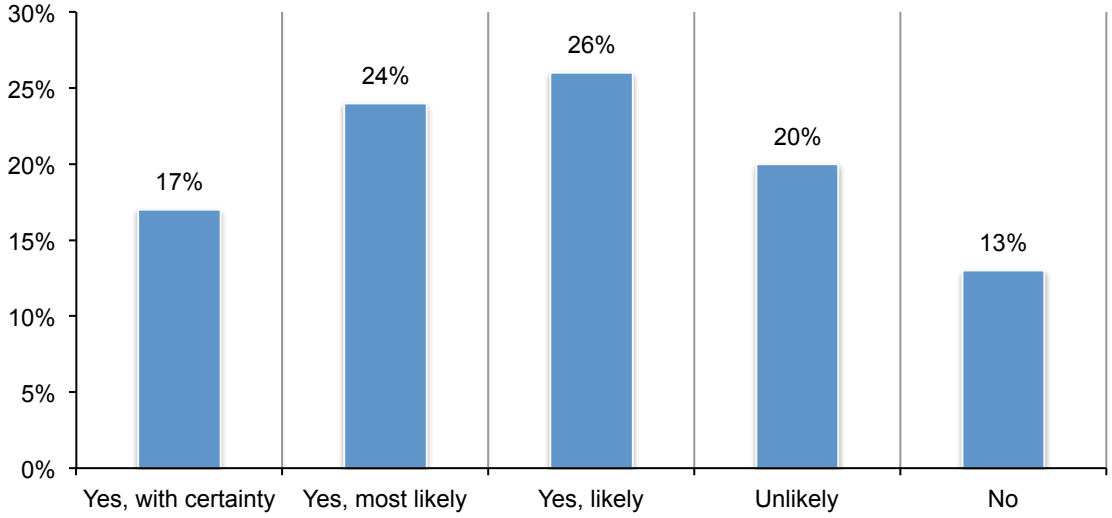
The root cause of many data breaches is an employee's mobile device. According to Figure 2, 83 percent of respondents say mobile devices are susceptible to hacking. It is, therefore, understandable that 70 percent of respondents believe the failure to secure company data on mobile devices has likely resulted in a data breach.

Figure 2. The risk of confidential data on mobile devices used in the workplace
Strongly agree and agree responses combined



As shown in Figure 3, 67 percent of respondents (17 percent + 24 percent + 26 percent) say it was certain, most likely, or likely that their organization had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information.

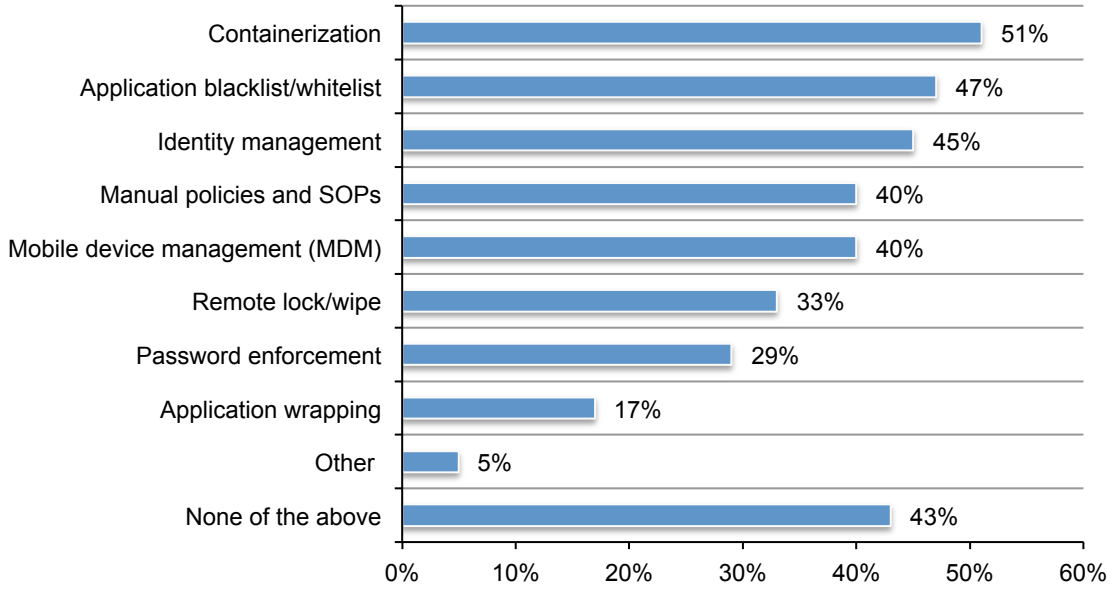
Figure 3. Do you believe your organization has had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information?



Are solutions to manage and secure data accessible on employees' mobile devices sufficient? Figure 4 presents the measures taken to manage data accessible on employees' mobile devices. Most companies use containerization (51 percent of respondents), application blacklist/whitelist (47 percent of respondents), identity management (45 percent of respondents), mobile device management (40 percent of respondents), and manual policies and SOPs (40 percent of respondents). However, 43 percent of respondents say none of these measures are used.

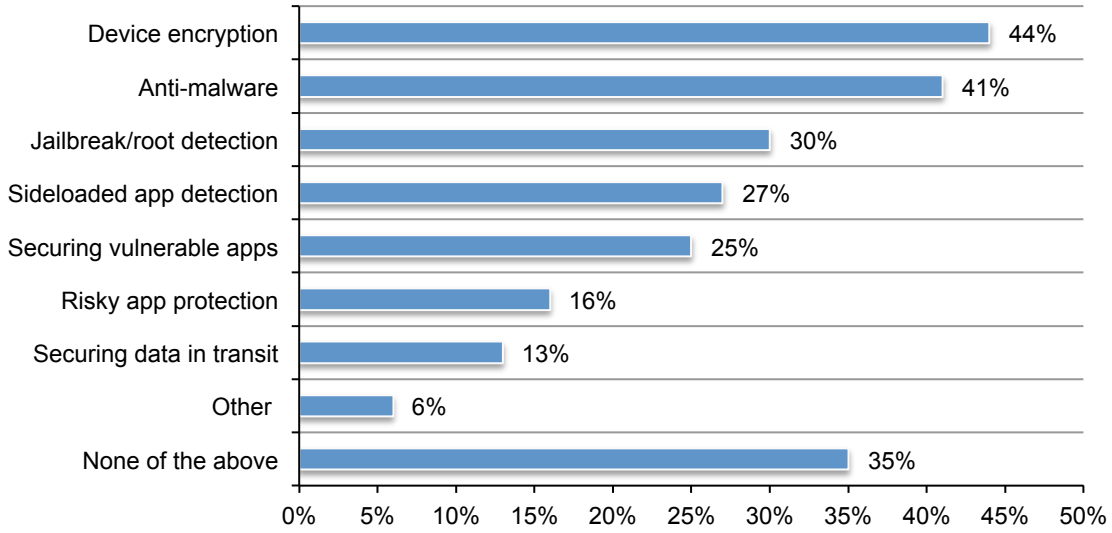
Seventy-four percent of respondents in companies that use containerization, say with certainty (20 percent), most likely (27 percent), or likely (27 percent) their organization had a data breach as a result of employees using mobile devices to access the company's sensitive and confidential information. Sixty percent of respondents in organizations that do not use containerization say with certainty (14 percent), most likely (21 percent) or likely (25 percent) their organization had a data breach due to employees accessing such information.

Figure 4. Measures taken to manage data accessible on employees' mobile devices
More than one response permitted



To secure the data, as shown in Figure 5, most companies use device encryption (44 percent of respondents), anti-malware (41 percent of respondents), jailbreak/root detection (30 percent of respondents), and sideloaded app detection (27 percent of respondents). However, 35 percent of respondent say none of these measures are taken.

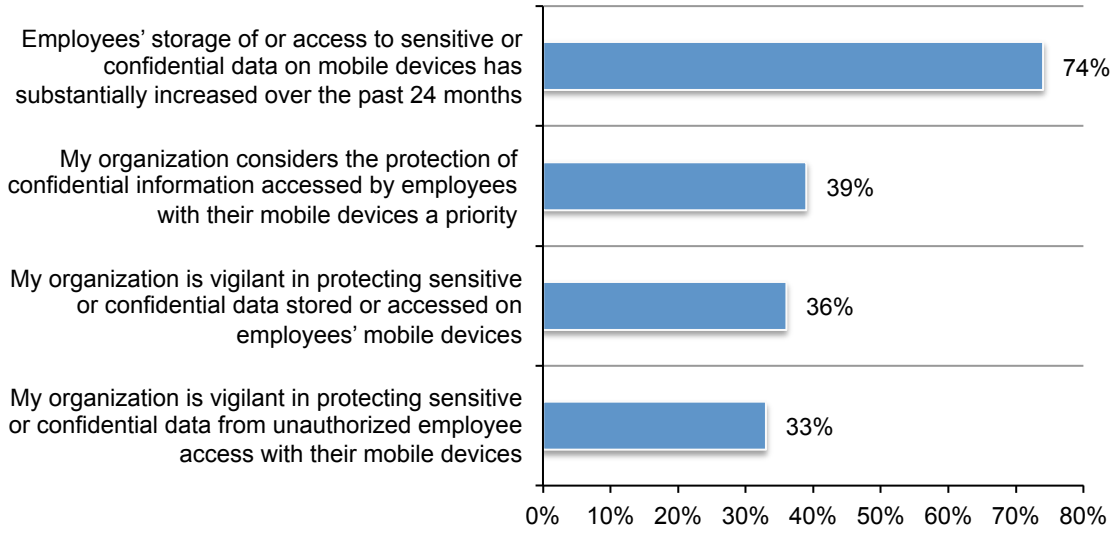
Figure 5. Measures taken to secure data accessible on employees' mobile devices
More than one response permitted



Companies are not keeping up with the risk of mobile devices in the workplace. Seventy-four percent of respondents say in the past two years employees' storage of or access to sensitive or confidential data on mobile device has increased significantly. Despite this increase, only 33 percent of respondents say their organization is vigilant in protecting sensitive or confidential data from unauthorized employee access via mobile devices, as shown in Figure 6.

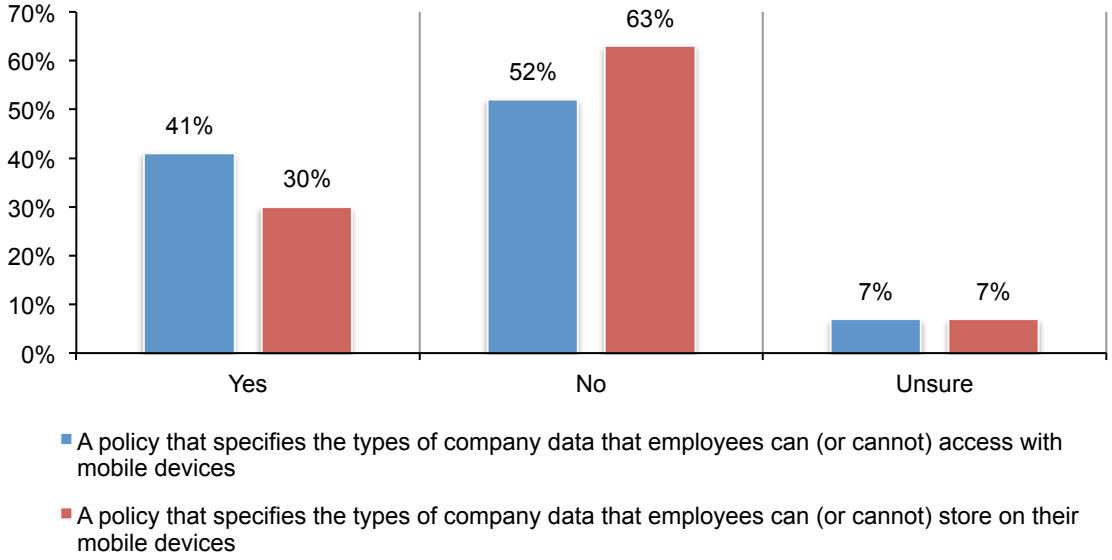
Similarly, only 36 percent of respondents say their organization is vigilant in protecting sensitive or confidential data stored or accessed on employees' mobile devices. Only 39 percent of respondents consider the protection of confidential information accessed by employees with their mobile devices a priority.

Figure 6. Why mobile devices pose a risk in the workplace
Strongly agree and agree responses combined



The majority of organizations are not providing guidelines for employees' access or storage of company data. According to Figure 7, only 41 percent of respondents say their organization has a policy that specifies the types of company data that employees can or cannot access with mobile devices and only 30 percent of respondents say there is a policy specifying the types of company data that can be stored on their mobile devices.

Figure 7. Does your organization have a policy that specifies the types of company data that employees can or cannot access or store?



Budgets for mobile security are expected to increase in the next year. As shown in Table 1, the average annual IT budget in organizations represented in this research is $195 million and an average of 14 percent is dedicated to security. The average IT security budget is expected to increase to $32,760,000 and the average budget allocated for mobile security is expected to increase to $5,984,160.

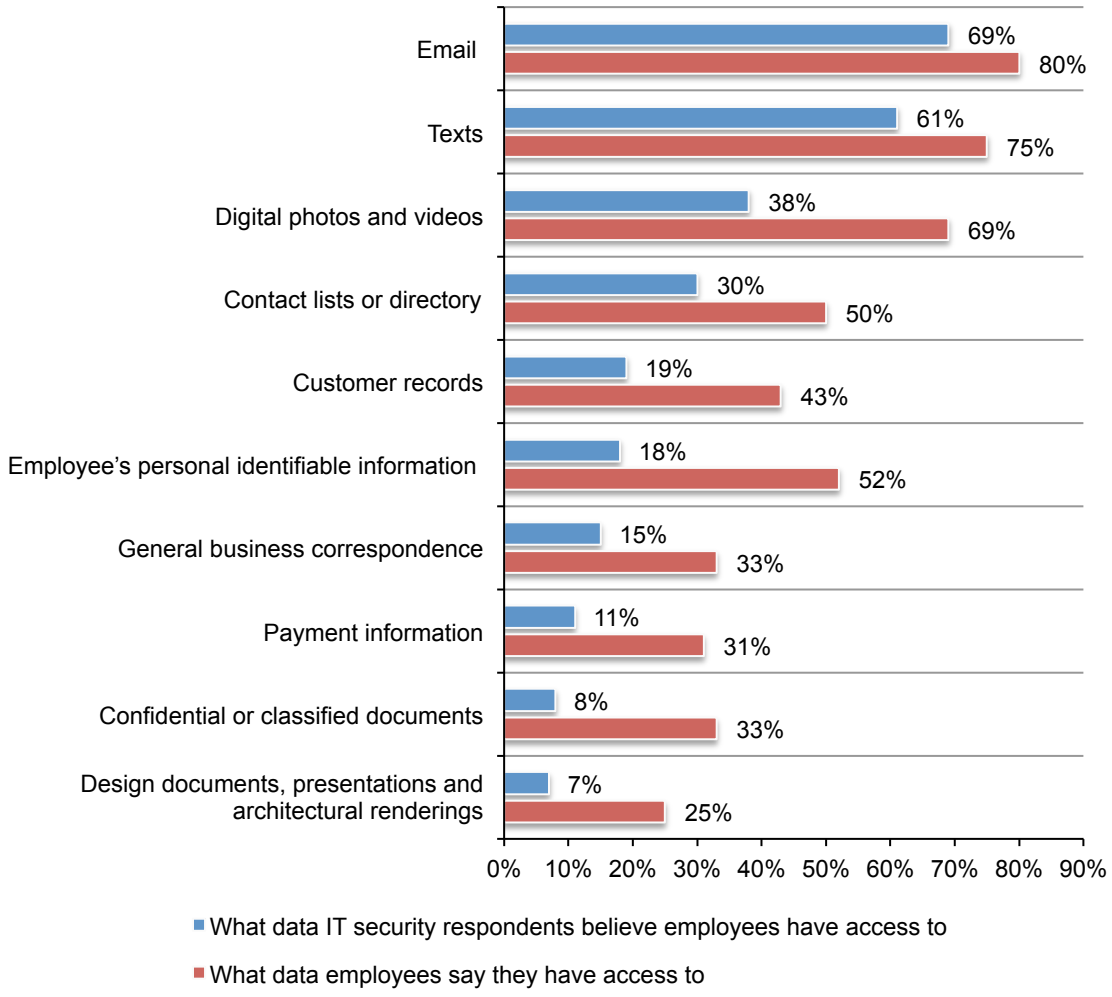
Table 1. Budgets for IT, IT security & Mobile Security	**Extrapolated value**
Average annual IT budget	$195,000,000
Average annual budget for IT security (14 percent of IT budget)	$27,300,000
Increase to IT security budget in the next 12 months (20 percent)	$32,760,000
Average annual budget for mobile security (16 percent of IT security budget)	$4,368,000
Increase to mobile security budget over the next 12 months (37 percent)	$5,984,160

Employees have easy access to sensitive and confidential information

Employees have access to more sensitive and confidential work-related data than IT security thinks. Forty-four percent of respondents do not know the types of company-related data employees can access with their mobile devices.

Figure 8 shows significant gaps between what employees[1] can access and what IT security believes they can access. The 56 percent of respondents who believe they do know say the most frequently accessed data types are email and texts. However, the largest gaps concern sensitive work-related data such as employee's PII (52 percent of employees vs. 18 percent of IT security), confidential or classified documents (33 percent vs. 8 percent of IT security) and customer records (43 percent of employees vs. 19 percent of IT security).

Figure 8. The company-related data employees have access to with their mobile devices versus what data IT security thinks they can access
More than one response permitted

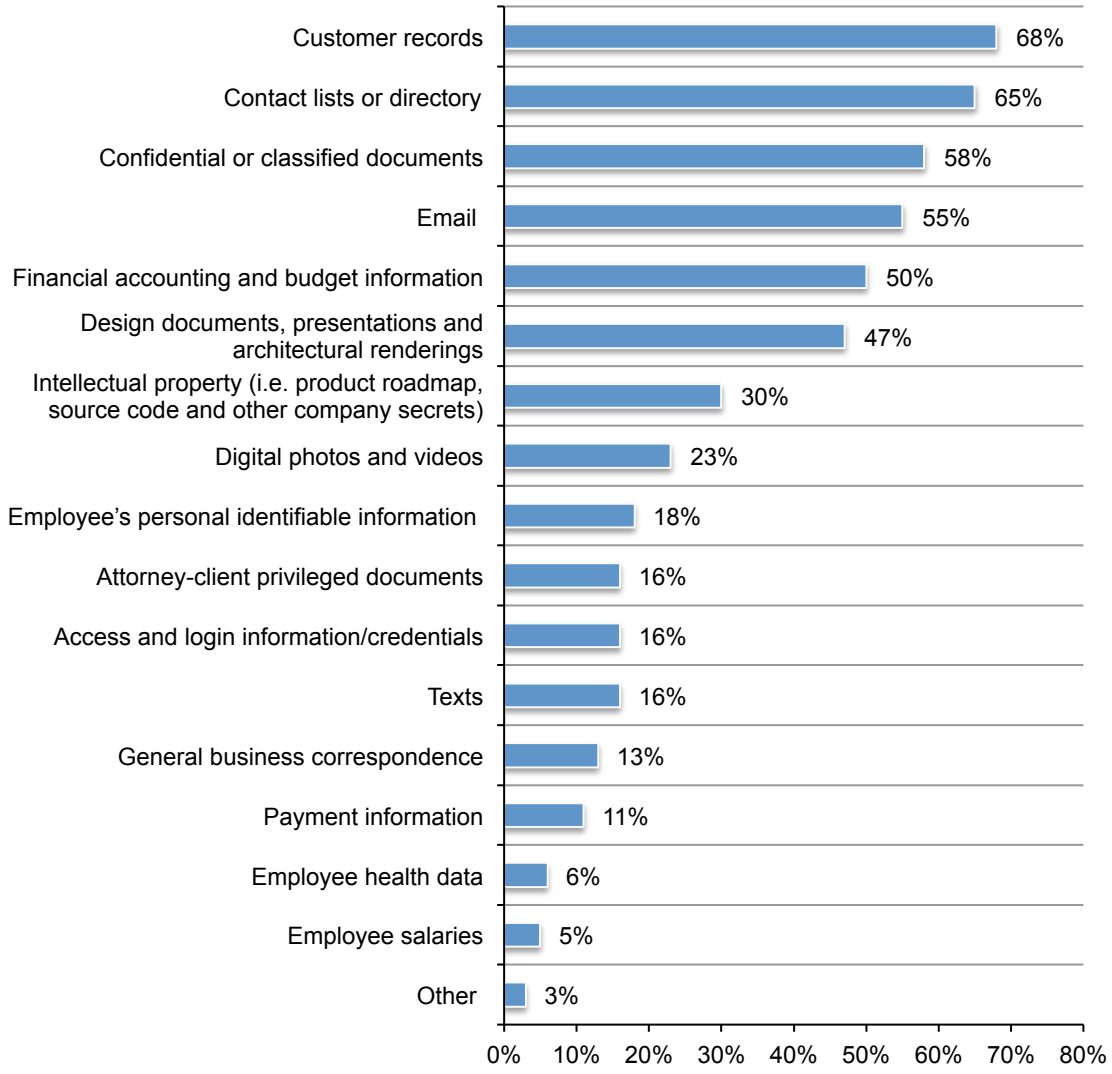


[1] See: *How Much Is the Data on Your Mobile Device Worth?* sponsored by Lookout and conducted by Ponemon Institute, February 2016

Certain data is considered more at risk because of employees' ability to access it on mobile devices. According to Figure 9, 68 percent of respondents say customer records are at the greatest risk due to employees' ability to access and store them on mobile devices. Other data types that could put companies most at risk are: contact lists or directories (65 percent of respondents), confidential or classified documents (58 percent of respondents), email (55 percent of respondents) and financial accounting and budget information (50 percent of respondents).

As previously reported in Table 8, the data considered by IT security to be most at risk--customer records, contact lists, directories, and classified documents--can be accessed via mobile devices, according to 43 percent of respondents, 50 percent of respondents and 33 percent of respondents respectively.

Figure 9. Company data types most at risk because of employees' ability to access and store them on their mobile devices.
More than one response permitted

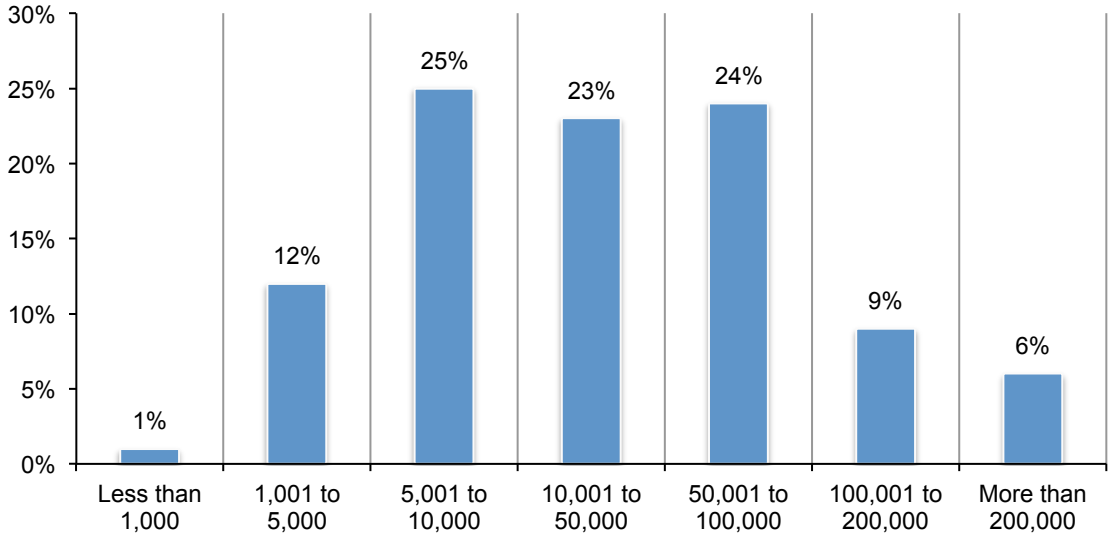


Determining the cost of mobile malware infections. In this study, we examined two common scenarios that can put company data at risk. The first one involves malware infections on mobile devices and the second scenario involves stolen credentials.

When employees download mobile apps for business and personal use, these mobile apps may contain malware sometimes infecting devices that go undetected for months or even years. When activated, malware can disrupt business processes, cause IT downtime and result in the exfiltration of sensitive or confidential data.

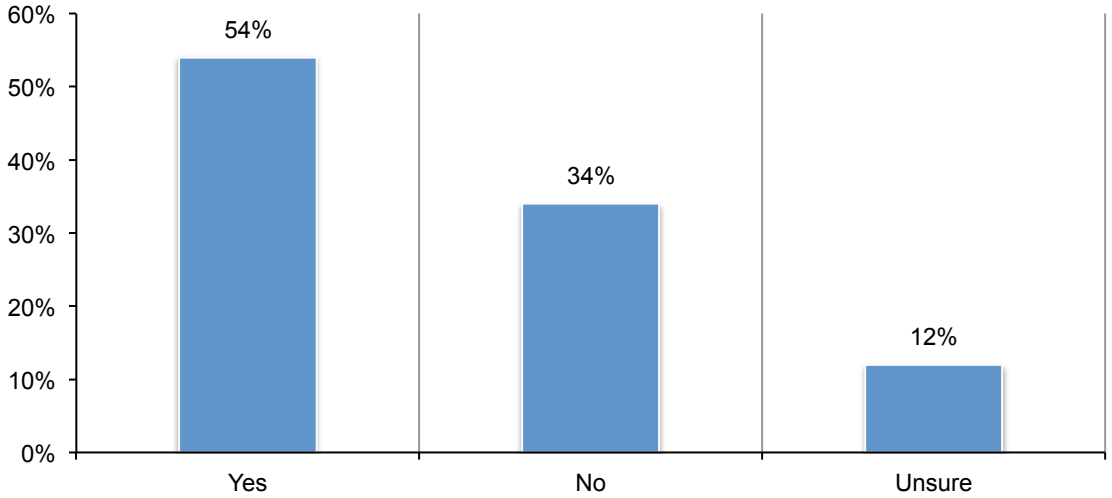
As shown in Figure 10, on average, organizations represented in this study have 53,844 mobile devices in use by employees.

Figure 10. How many mobile devices are in use by employees within your organization?



As shown in Figure 11, 54 percent of respondents say a mobile malware infection occurred in their organization over the past 24 months. However, 12 percent are uncertain. Sixty-six percent of respondents expect a malware infection could occur in their organization in the future.

Figure 11. Has a mobile malware infection occurred in your organization sometime over the past 24 months?



At any point in time, an average of 3 percent of employees' mobile devices (53,844) or approximately 1,723 devices are believed to have malware infections. However, only an average of 26 percent of infected mobile devices (448) are investigated and/or triaged. What is the cost if 26 percent of these devices are investigated and/or triaged? Or, what would be the cost if 100 percent of all infected devices were investigated or triaged? Following are two calculations that show the costs (based on the calculations in Table 2) for both scenarios:

Assume 26 percent of infected devices are investigated and/or triaged: $3,530,240 (total direct cost) + $12,812,017 (total indirect cost) = $16,342,257.

Assume 100 percent of devices are investigated and/or triaged: $13,577,846 (total direct cost) + $12,812,017 (total indirect cost) = $26,389,863

How we calculate the cost of mobile malware. Our analysis of the cost of mobile malware is summarized in Table 2. All figures are extrapolated values defined for the average-sized organization that participated in this research. As shown, we calculate the cost of helpdesk including device replacement, IT security support including investigations and forensics and diminished productivity or idle time. The sum of these costs equals $7,880 per malware-infected mobile device. To determine the total average direct cost of $3,530,240 per year, we formulate the following calculation:

$3,530,240 = $7,880 X 53,844 [number of network-connected mobile devices] X 3.2% [percent of devices infected with malware at least once per year] X 26% [percent of infected devices investigated and triaged]

The second part of our analysis is the determination of indirect costs – which is the cost of data breach, the cost of non-compliance and diminished reputation. Here we use an expected value approach. That is, we first determine the potential maximum loss (PML) or "worst case" scenario from survey extrapolations. As can be seen in the table, we estimate $50,440,000 as the PML for data breach, $19,279,780 as the PML for non-compliance, and $61,015,000 as the PML for diminished reputation. Then we multiply total PML by the perceived likelihood of occurrence per annum, which is estimated at 9.8%. Following is our calculation:

$12,812,017 = 9.8% X $50,440,000 {[PML for data breach] + $19,279,780 [PML for non-compliance] + $61,015,000 [PML for diminished reputation]}

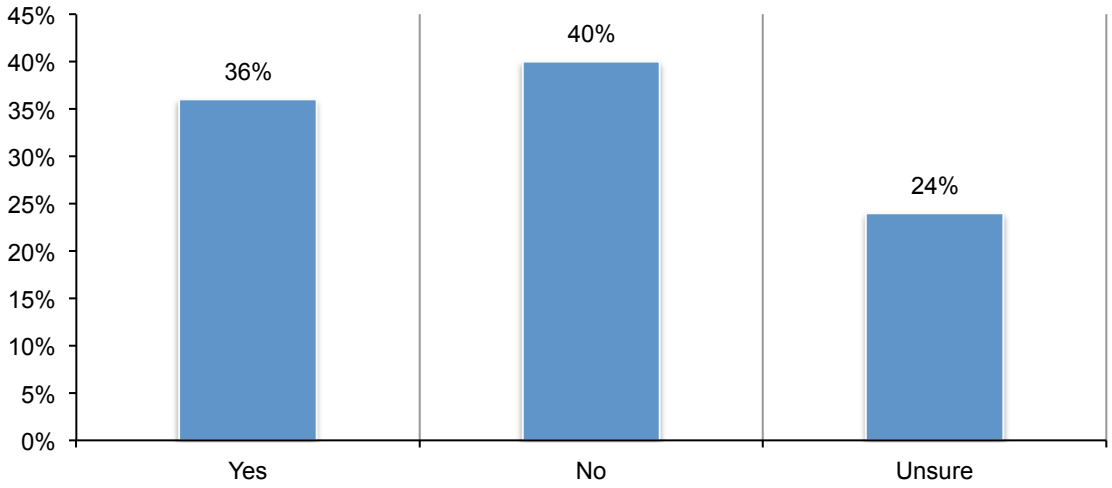
Combining direct and indirect costs results in a total average cost of mobile malware at $16,342,257 or an average cost per successful (weaponized) mobile malware attack is $9,485

Table 2: Analysis of the Cost of Mobile Malware

Cost Calculus	Source	Estimates
IT helpdesk including replacement	Extrapolated value	1,334
IT security support including investigations and forensics	Extrapolated value	4,289
Diminished productivity or idle time	Extrapolated value	2,257
Sum of direct costs per device	Sub-total	$7,880
Percent of devices infected with malware at least once per year	Extrapolated value	3.2%
Number of network-connected mobile device	Extrapolated value	53,844
Number of device compromises	Calc: 3.2% X 53,844	1,723
Percent of infected devices investigated and/or triaged	Extrapolated value	26%
Number of infected devices investigated and/or triaged	Calc: 26% X 1,723	448
Total direct average cost	Calc: 7,880 X 448	$3,530,240
Potential maximum loss (PML) per year		
Cost of data loss or breach	Extrapolated value	50,440,090
Cost of non-compliance	Extrapolated value	19,279,780
Lost or diminished reputation	Extrapolated value	61,015,000
Total PML	Sub-total	$130,734,870
Perceived likelihood of occurrence per annum	Extrapolated value	9.8%
Total indirect average cost	Calc: $130,734,870 X 9.8%	$12,812,017
Total average cost	Calc: $12,812,017 + $3,530,240	$16,342,257
Average cost per network connected device	Calc: $16,342,257 ÷ 53,844	$304
Average cost per malware-infected device	Calc: $16,342,257 ÷ 1,723	$9,485

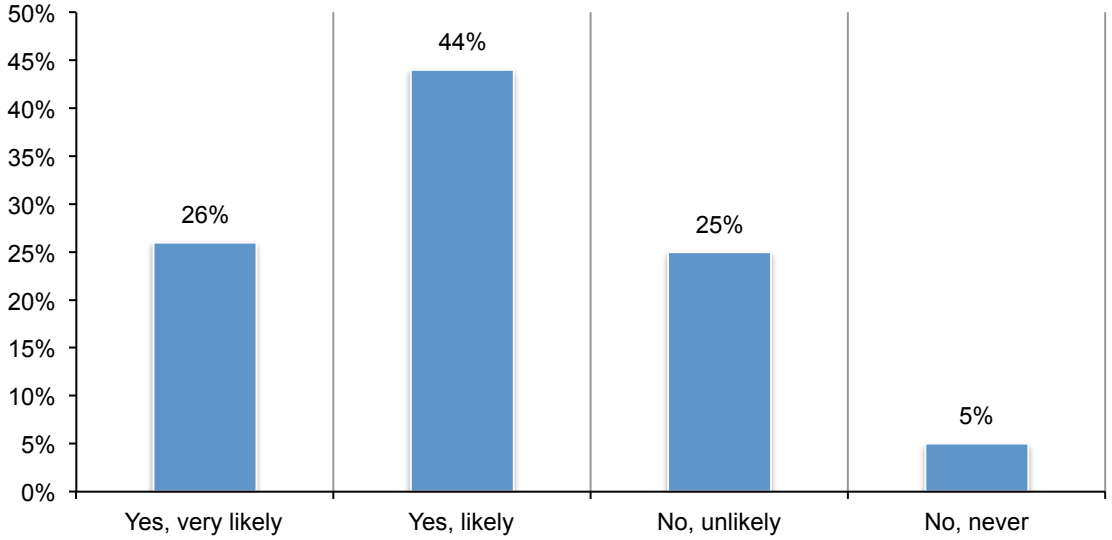
What can a hacker cost a company? In the second scenario, we looked at the potential financial consequences if a hacker targets employees' mobile devices to steal their credentials and access sensitive and confidential company data? According to Figure 12, 36 percent of respondents say this type of incident occurred in their organization over the past 24 months. However, 24 percent of respondents say they are unsure if such a scenario occurred in their organization.

Figure 12. Has a hacker accessed and compromised employees' mobile devices in order to steal credentials and access company data?



According to Figure 13, 72 percent of respondents (26 percent + 46 percent) say it is possible that the enterprise data accessible on the mobile device was compromised. Fifty-nine percent of respondents believe such an incident could occur in their organization.

Figure 13. Is it possible that the enterprise data accessible by the infected mobile device was compromised?



At any point in time, an average of 1.2 percent of employees' mobile devices (53,844) or approximately 646 devices are compromised. However, only an average of 19 percent of compromised mobile devices (123) are investigated and/or triaged. What is the cost if 19 percent of these devices are investigated and/or triaged? Or, what would be the cost if 100 percent of all

compromised devices were investigated or triaged? Following are two calculations that show the costs (based on the calculations in Table 3) for both scenarios:

Assume 19 percent of infected devices are investigated and/or triaged: $2,225,717 (total direct cost) + $11,369,920 (total indirect cost) = $13,595,637.

Assume 100 percent of devices are investigated and/or triaged: $11,711,980 (total direct cost) + $11,369,920 (total indirect cost) = $23,081,900.

How we calculate the cost of mobile device compromises. We follow the same two-step process (as above) to extrapolate the total average cost of mobile device compromises. Again, all data points are calculated values derived for the average organization that participated in this survey research. Table 3 shows three categories of direct total costs – which are the cost of helpdesk including device replacement, IT security support including investigations and forensics and diminished productivity or idle time. The sum of this cost equals $18,130 per compromised mobile device. To determine the total average direct cost of $2,225,717 per year, we formulate the following calculation:

$2,225,717 = $18,130 X 53,844 [number of network-connected mobile devices] X 1.2% [percent of devices compromised] X 19% [percent of compromised devices investigated and triaged]

Similar to our previous analysis, indirect cost consists of three components; that is, the cost of data breach, the cost of non-compliance and diminished reputation. Using an expected value approach per annum, we formulate the following calculation for indirect cost:

$11,369,920 = 8.7% X {$54,313,750 [PML for data breach] + $18,228,640 [PML for non-compliance] + $58,146,340 [PML for diminished reputation]}

Combining direct and indirect costs results in a total average cost of mobile device compromise at $13,595,637 or an average cost per compromised mobile device of $21,042.

Table 3: Analysis of the Cost of Mobile Device Compromise

Cost Calculus	Source	Estimates
IT helpdesk including replacement	Extrapolated value	4,208
IT security support including investigations and forensics	Extrapolated value	10,926
Diminished productivity or idle time	Extrapolated value	2,996
Sum of direct costs per device	Sub-total	$18,130
Percent of compromised devices at least once per year	Extrapolated value	1.2%
Number of network-connected mobile device	Extrapolated value	53,844
Number of device compromised	Calc: 1.2% X 53,844	646
Percent of compromised devices investigated and/or triaged	Extrapolated value	19%
Number of compromised devices investigated and/or triaged	Calc: 19% X 646	123
Total direct average cost	Calc: $18,130 X 123	$2,225,717
Potential maximum loss (PML) per year		
Cost of data loss or breach	Extrapolated value	54,313,750
Cost of non-compliance	Extrapolated value	18,228,640
Lost or diminished reputation	Extrapolated value	58,146,340
Total PML	Sub-total	$130,688,730
Perceived likelihood of occurrence per annum	Extrapolated value	8.7%
Total indirect average cost	Calc: $130,688.730 X 8.7%	$11,369,920
Total average cost	Calc: $11,389,920 + $2,225,717	$13,595,637
Average cost per all network connected device	Calc: $13,595,637 ÷ 53,844	$253
Average cost per compromised device	Calc: $13,595,637 ÷ $646	$21,042

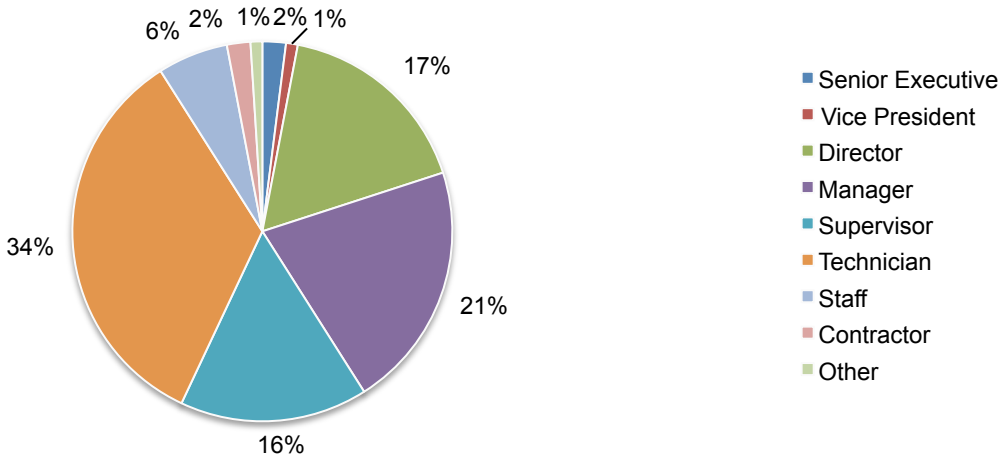
Part 3. Methods

A sampling frame of 15,507 IT and IT security professionals located in the United States was selected as participants to this survey. Table 1 shows 647 total returns. Screening and reliability checks required the removal of 59 surveys. Our final sample consisted of 588 surveys or a 3.8 percent response.

Table 4. Sample response	Freq	Pct%
Sampling frame	15,507	100.0%
Total returns	647	4.2%
Rejected or screened surveys	59	0.4%
Final sample	588	3.8%

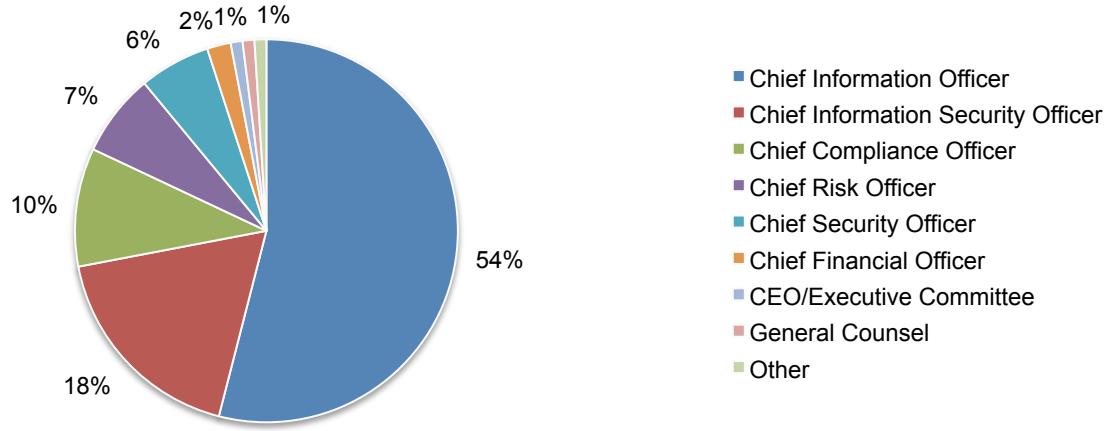
Pie Chart 1 reports the respondent's organizational level within the organization. By design, more than half of respondents (57 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



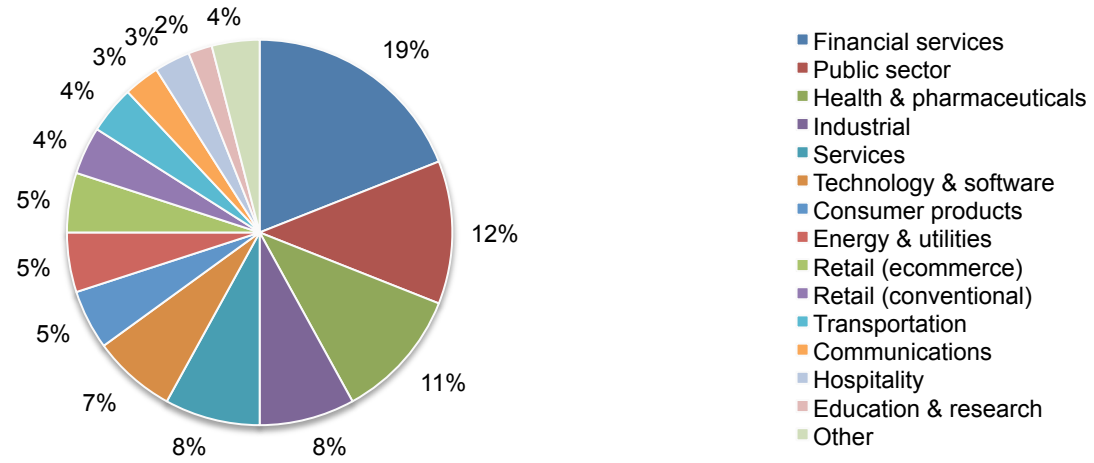
As shown in Pie Chart 2, more than half (54 percent) of the respondents indicated they report directly to the CIO and another 18 percent report to the CISO.

Pie Chart 2. Primary person you or your IT security leader reports to



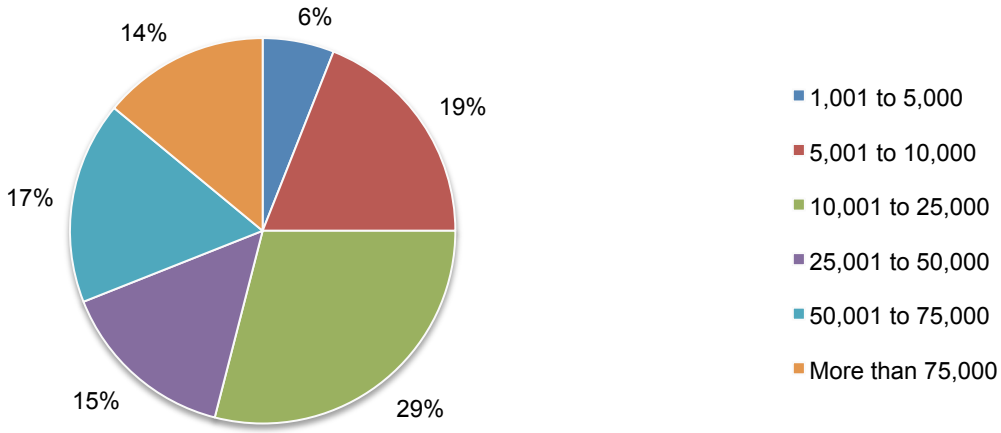
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (12 percent) and health & pharmaceutical (11 percent).

Pie Chart 3. Primary industry focus



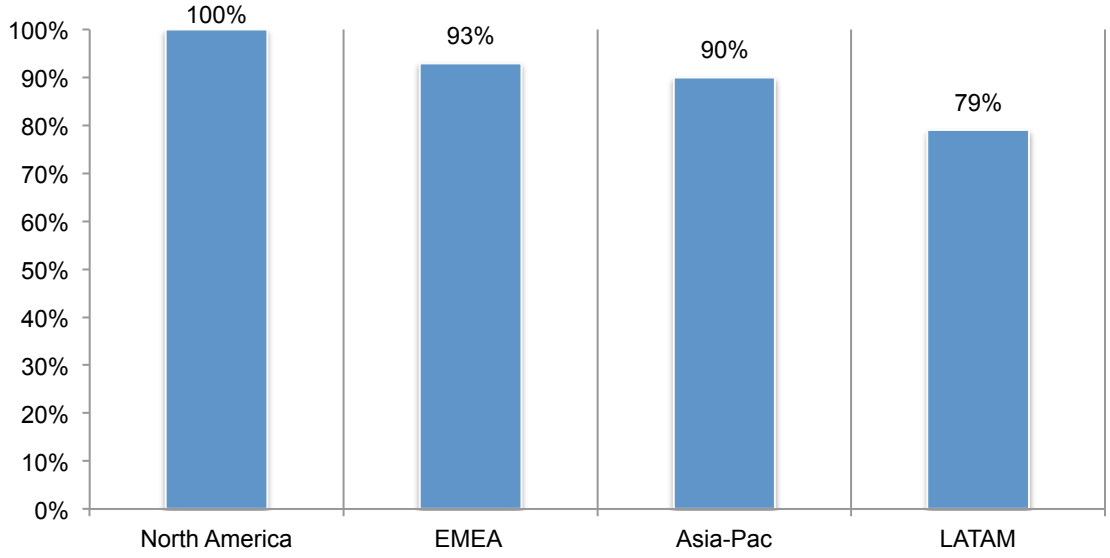
As shown in Pie Chart 4, 75 percent of respondents are from organizations with a global headcount of more than 10,000 employees.

Pie Chart 4. Global employee headcount



In addition to having operations in North America, 93 percent of respondents indicated their organization has operations in Europe, the Middle East and Africa and 90 percent responded Asia-Pacific, as shown in Figure 15.

Figure 15. Global location of operations
More than one response permitted



Part 4. Caveats to this study

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

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

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in the United States. 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 September 2015.

Sample response	Freq	Pct%
Total sampling frame	15,507	100.0%
Total returns	647	4.2%
Rejected or screened surveys	59	0.4%
Final sample	588	3.8%

Screening questions

S1. How familiar are you with your organization's management and security of mobile devices used by employees in the workplace?	Pct%
Very familiar	43%
Familiar	39%
Somewhat familiar	18%
Little or no knowledge (Stop)	0%
Total	100%

S2. Do you have responsibility for monitoring or enforcing the security of mobile devices used in the workplace, including employee-owned devices (a.k.a. BYOD)?	Pct%
Yes, full responsibility	37%
Yes, some responsibility	63%
Minimal or no responsibility (Stop)	0%
Total	100%

Part 2. Attributions

Please rate the following statements using the five-point scale provided below each item. Note that mobile devices include employee-owned (BYOD) and company-assigned devices such as smart phones and tablets.	Strongly agree	Agree
Q1a. Employees' storage of or access to sensitive or confidential data on mobile devices has substantially increased over the past 24 months.	44%	30%
Q1b. Failure to secure company data on mobile devices has likely resulted in a data breach.	39%	31%
Q1c. My organization considers the protection of confidential information accessed by employees with their mobile devices a priority.	19%	20%
Q1d. My organization is vigilant in protecting sensitive or confidential data stored or accessed on employees' mobile devices.	18%	18%
Q1e. My organization is vigilant in protecting sensitive or confidential data from unauthorized employee access with their mobile devices.	17%	16%
Q1f. Employees' mobile devices are susceptible to hacking.	49%	34%

Part 3. General Questions

Q2. Do you believe your organization has had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information?	Pct%
Yes, with certainty	17%
Yes, most likely	24%
Yes, likely	26%
Unlikely	20%
No	13%
Total	100%

Q3a. Approximately, how many mobile devices are in use by employees within your organization today?	Pct%
Less than 1,000	1%
1,001 to 5,000	12%
5,001 to 10,000	25%
10,001 to 50,000	23%
50,001 to 100,000	24%
100,001 to 200,000	9%
More than 200,000	6%
Total	100%
Extrapolated value	53,844

Q3b. What percentage of all mobile devices used by employees are infected with malware at any point in time?	Pct%
Less than 1 percent	9%
1 percent	15%
2 percent	18%
3 percent	21%
4 percent	16%
5 percent	8%
6 percent	5%
7 percent	3%
8 percent	2%
9 percent	2%
10 percent	1%
More than 10 percent	0%
Total	100%
Extrapolated value	3.2%

Q3c. What percentage of all infected mobile devices are investigated and/or triaged?	Pct%
Less than 5%	6%
5 to 10%	9%
11 to 15%	8%
16 to 20%	22%
21 to 30%	28%
31 to 40%	10%
41 to 50%	9%
51 to 75%	6%
76 to 100%	2%
Total	100%
Extrapolated value	26%

Q4. Do you believe employees have too much work-related data on their mobile devices?	Pct%
Yes	55%
No	33%
Unsure	12%
Total	100%

Q5. Approximately, how much has work-related data on employees' mobile devices increased over the past 12 months?	Pct%
No increase	5%
Less than 5%	4%
5 to 10%	5%
11 to 15%	6%
16 to 20%	17%
21 to 30%	14%
31 to 40%	11%
41 to 50%	10%
51 to 75%	7%
76 to 100%	8%
More than 100%	13%
Total	100%
Extrapolated value	43%

Q6a. What percentage of data accessible on PCs is also accessible on employees' mobile device?	Pct%
Less than 5%	2%
5 to 10%	3%
11 to 15%	7%
16 to 20%	8%
21 to 30%	8%
31 to 40%	10%
41 to 50%	9%
51 to 75%	12%
76 to 100%	41%
Total	100%
Extrapolated value	56%

Q6b. How much will such access increase in the next 24 months?	Pct%
No increase	0%
Less than 5%	2%
5 to 10%	2%
11 to 15%	5%
16 to 20%	11%
21 to 30%	10%
31 to 40%	14%
41 to 50%	20%
51 to 75%	17%
76 to 100%	8%
More than 100%	11%
Total	100%
Extrapolated value	50%

Q7a. Does your organization have a policy that specifies the types of company data that employees can (or cannot) **access** with mobile devices?	Pct%
Yes	41%
No	52%
Unsure	7%
Total	100%

Q7b. Does your organization have a policy that specifies the types of company data that employees can (or cannot) **store** on their mobile devices?	Pct%
Yes	30%
No	63%
Unsure	7%
Total	100%

Q8a. Do you know what types of company-related data employees can access with their mobile devices?	Pct%
Yes	56%
No	44%
Total	100%

Q8b. If yes, please select all the company-related data types employees have access to with their mobile devices.	Pct%
Email	69%
Texts	61%
Digital photos and videos	38%
Contact lists or directory	30%
Customer records	19%
Employee's personal identifiable information (i.e Social Security numbers, birth date, home address)	18%
Access and login information/credentials	16%
General business correspondence	15%
Payment information	11%
Financial accounting and budget information	10%
Confidential or classified documents	8%
Design documents, presentations and architectural renderings	7%
Employee health data	6%
Intellectual property (i.e. product roadmap, source code and other company secrets)	5%
Employee salaries	5%
Other (please specify)	2%
Attorney-client privileged documents	1%
Total	321%

Q8c. If yes, which of the following company-related data types are most at risk because of employees' ability to access and store them on their mobile devices? Please select your top 5 choices.	Pct%
Customer records	68%
Contact lists or directory	65%
Confidential or classified documents	58%
Email	55%
Financial accounting and budget information	50%
Design documents, presentations and architectural renderings	47%
Intellectual property (i.e. product roadmap, source code and other company secrets)	30%
Digital photos and videos	23%
Employee's personal identifiable information (i.e Social Security numbers, birth date, home address)	18%
Texts	16%
Access and login information/credentials	16%
Attorney-client privileged documents	16%
General business correspondence	13%
Payment information	11%
Employee health data	6%
Employee salaries	5%
Other (please specify)	3%
Total	500%

Q9a. What measures does your organization take to manage data accessible on employees' mobile devices? Please check all that apply.	Pct%
Application wrapping	17%
Containerization	51%
Password enforcement	29%
Remote lock/wipe	33%
Mobile device management (MDM)	40%
Identity management	45%
Application blacklist/whitelist	47%
Manual policies and SOPs	40%
Other (please specify)	5%
None of the above	43%
Total	350%

Q9b. What measures does your organization take to secure data accessible on employees' mobile devices? Please check all that apply.	Pct%
Anti-malware	41%
Jailbreak/root detection	30%
Device encryption	44%
Securing data in transit	13%
Securing vulnerable apps	25%
Risky app protection	16%
Sideloaded app detection	27%
Other (please specify)	6%
None of the above	35%
Total	237%

Q10a.What is your organization's approximate annual budget for IT?	Pct%
Under $10 million	1%
$10 million to $25 million	5%
$26 million to $50 million	6%
$51 million to $100 million	39%
$101 million to $250 million	23%
$251 million to $500 million	15%
More than $500 million	11%
Total	100%
Extrapolated value	$195
Q10b. What percentage of your organization's IT budget is dedicated to security?	Pct%
Less than 2%	8%
2 to 5%	11%
6 to 10%	19%
11 to 15%	23%
16 to 20%	19%
21 to 25%	12%
More than 25%	8%
Total	100%
Extrapolated value	13.6%

Q10c. Will this percentage increase in the next year?	Pct%
Yes	51%
No	34%
Unsure	15%
Total	100%

Q10d. If yes, how much will it increase?	Pct%
Less than 5%	8%
5 to10%	16%
11 to 20%	28%
21 to 30%	33%
31 to 40%	8%
41 to 50%	5%
More than 50%	2%
Total	100%
Extrapolated value	20.2%

Q11a. What percentage of your organization's IT security budget is dedicated to mobile security?	Pct%
Less than 5%	14%
5 to10%	29%
11 to 20%	28%
21 to 30%	20%
31 to 40%	5%
41 to 50%	3%
More than 50%	1%
Total	100%
Extrapolated value	15.6%

Q11b. Will this percentage increase in the next year?	Pct%
Yes	52%
No	39%
Unsure	9%
Total	100%

Q11c. If yes, how much will it increase?	Pct%
Less than 5%	0%
5 to10%	3%
11 to 20%	9%
21 to 30%	13%
31 to 40%	39%
41 to 50%	23%
More than 50%	13%
Total	100%
Extrapolated value	36.6%

Part 4. Scenarios

Malware infections on insecure mobile devices: Employees download mobile apps for business and personal use. These mobile apps may contain malicious software such as viruses, worms and trojans, sometimes infecting devices that go undetected for months or even years. When activated, malware can disrupt business processes, cause IT downtime and result in the ex-filtration of sensitive or confidential data.

Q12a. Has a mobile malware infection occurred in your organization sometime over the past 24 months?	Pct%
Yes	54%
No	34%
Unsure	12%
Total	100%

Q12b. If no, do you believe this type of incident **could happen** to your organization?	Pct%
Yes, very likely	21%
Yes, likely	45%
No, unlikely	29%
No, never	5%
Total	100%

Q12c. How much did (or could) this incident cost your organization?

Q12c-1 IT help desk support (including replacement of the device)	Pct%
Less than $500	34%
$500 to $1,000	47%
$1,001 to $2500	9%
$2,501 to $5,000	7%
$5,001 to $10,000	1%
$10,001 to $25,000	2%
$25,001 to $50,000	0%
More than $50,000	0%
Total	100%
Extrapolated value	$1,334

Q12c-2 IT security support (including investigation and forensics)	Pct%
Less than $500	21%
$500 to $1,000	25%
$1,001 to $2,500	21%
$2501 to $5,000	14%
$5,001 to $10,000	12%
$10,001 to $25,000	2%
$25,001 to $50,000	5%
More than $50,000	0%
Total	100%
Extrapolated value	$4,289

Q12c-3 Diminished productivity or idle time	Pct%
Less than $500	28%
$500 to $1,000	32%
$1,001 to $2,500	16%
$2,501 to $5,000	18%
$5,001 to $10,000	3%
$10,001 to $25,000	2%
$25,001 to $50,000	1%
More than $50,000	0%
Total	100%
Extrapolated value	$2,257

Q12d. Is it possible that the enterprise data accessible by the infected mobile device was compromised?	Pct%
Yes, very likely	26%
Yes, likely	46%
No, unlikely	22%
No, never	6%
Total	100%

Q12e. How much did (or could) this incident cost your organization in terms of the value of the data or device compromised? Please provide a total or maximum exposure here (i.e., worst case scenario).	Pct%
Zero	0%
Less than $10,000	1%
$10,001 to $100,000	0%
$100,001 to $250,000	0%
$250,001 to $500,000	6%
$500,001 to $1,000,000	9%
$1,000,001 to $5,000,000	10%
$5,000,001 to $10,000,000	9%
$10,000,001 to $25,000,000	10%
$25,000,001 to $50,000,000	13%
$50,00,001 to $100,000,000	17%
More than $100,000,000	25%
Total	100%
Extrapolated value	$50,440,090

Q12f. How much did (or could) this incident cost your organization in terms of non-compliance or regulatory violations? Please provide total or maximum exposure here (i.e., worst case scenario).	Pct%
Zero	0%
Less than $10,000	2%
$10,001 to $100,000	12%
$100,001 to $250,000	16%
$250,001 to $500,000	18%
$500,001 to $1,000,000	11%
$1,000,001 to $5,000,000	4%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25,000,000	9%
$25,000,001 to $50,000,000	6%
$50,00,001 to $100,000,000	5%
More than $100,000,000	9%
Total	100%
Extrapolated value	$19,279,780

Q12g. How much did (or could) this incident cost your organization in terms of your organization's reputation and customer goodwill? Please provide total or maximum exposure here (i.e., worst case scenario).	Pct%
Zero	0%
Less than $10,000	0%
$10,001 to $100,000	0%
$100,001 to $250,000	0%
$250,001 to $500,000	2%
$500,001 to $1,000,000	1%
$1,000,001 to $5,000,000	5%
$5,000,001 to $10,000,000	9%
$10,000,001 to $25,000,000	19%
$25,000,001 to $50,000,000	16%
$50,00,001 to $100,000,000	15%
More than $100,000,000	33%
Total	100%
Extrapolated value	$61,015,000

Q12h. How likely do you believe this type of incident will occur again in the next 12 months?	Pct%
Very likely	32%
Likely	49%
Unlikely	17%
No chance	2%
Total	100%

Q12i. From a cost prospective, what is the likelihood that the worst case scenario will prevail in the next 12 months?	Pct%
Less than 5%	41%
5 to10%	26%
11 to 20%	24%
21 to 30%	6%
31 to 40%	2%
41 to 50%	1%
More than 50%	0%
Total	100%
Extrapolated value	9.8%

Stolen credentials. A hacker targets employees' mobile devices to steal their credentials and access sensitive and confidential company data. Using these credentials, the hacker accesses and compromises this data.

Q13a. Has this type of incident occurred in your organization sometime over the past 24 months?	Pct%
Yes	36%
No	40%
Unsure	24%
Total	100%

Q13b. If no, do you believe this type of incident **could happen** to your organization?	Pct%
Yes, very likely	15%
Yes, likely	45%
No, unlikely	31%
No, never	9%
Total	100%

Q13c. How much did (or could) this incident cost your organization?

Q13c-1 IT help desk support (including replacement of the device)	Pct%
Less than $500	12%
$500 to $1,000	25%
$1,001 to $2,500	27%
$2,501 to $5,000	18%
$5,001 to $10,000	11%
$10,001 to $25,000	4%
$25,001 to $50,000	2%
More than $50,000	1%
Total	100%
Extrapolated value	$4,208

Q13c-2 IT security support (including investigation and forensics)	Pct%
Less than $500	2%
$500 to $1,000	11%
$1,001 to $2,500	12%
$2501 to $5,000	22%
$5,001 to $10,000	22%
$10,001 to $25,000	20%
$25,001 to $50,000	8%
More than $50,000	3%
Total	100%
Extrapolated value	$10,926

Q13c-3 Diminished productivity or idle time	Pct%
Less than $500	27%
$500 to $1,000	30%
$1,001 to $2,500	15%
$2,501 to $5,000	14%
$5,001 to $10,000	13%
$10,001 to $25,000	3%
$25,001 to $50,000	1%
More than $50,000	0%
Total	103%
Extrapolated value	$2,996

Q13d. Is it possible that the enterprise data accessible by the compromised mobile device was compromised?	Pct%
Yes, very likely	26%
Yes, likely	44%
No, unlikely	25%
No, never	5%
Total	100%

Q13e. How much did (or could) this incident cost your organization in terms of the value of the data or device compromised? Please provide a total or maximum exposure here (i.e., worst case scenario).	Pct%
Zero	0%
Less than $10,000	0%
$10,001 to $100,000	0%
$100,001 to $250,000	0%
$250,001 to $500,000	5%
$500,001 to $1,000,000	8%
$1,000,001 to $5,000,000	7%
$5,000,001 to $10,000,000	10%
$10,000,001 to $25,000,000	10%
$25,000,001 to $50,000,000	15%
$50,00,001 to $100,000,000	18%
More than $100,000,000	27%
Total	100%
Extrapolated value	$54,313,750

Q13f. How much did (or could) this incident cost your organization in terms of non-compliance or regulatory violations? Please provide total or maximum exposure here (i.e., worst case scenario).	Pct%
Zero	0%
Less than $10,000	1%
$10,001 to $100,000	6%
$100,001 to $250,000	18%
$250,001 to $500,000	19%
$500,001 to $1,000,000	15%
$1,000,001 to $5,000,000	7%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25,000,000	7%
$25,000,001 to $50,000,000	5%
$50,00,001 to $100,000,000	6%
More than $100,000,000	8%
Total	100%
Extrapolated value	$18,228,640

Q13g. How much did (or could) this incident cost your organization in terms of your organization's reputation and customer goodwill? Please provide total or maximum exposure here (i.e., worst case scenario).	Pct%
Zero	0%
Less than $10,000	1%
$10,001 to $100,000	0%
$100,001 to $250,000	0%
$250,001 to $500,000	3%
$500,001 to $1,000,000	4%
$1,000,001 to $5,000,000	6%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25,000,000	16%
$25,000,001 to $50,000,000	17%
$50,00,001 to $100,000,000	13%
More than $100,000,000	32%
Total	100%
Extrapolated value	$58,146,340

Q13h. How likely do you believe this type of incident will occur again in the next 12 months?	Pct%
Very likely	27%
Likely	46%
Unlikely	21%
No chance	6%
Total	100%

Q13i. From a cost prospective, what is the likelihood that the worst case scenario will prevail in the next 12 months?	Pct%
Less than 5%	52%
5 to10%	22%
11 to 20%	19%
21 to 30%	4%
31 to 40%	2%
41 to 50%	1%
More than 50%	0%
Total	100%
Extrapolated value	8.7%

Part 5. Your role and organization (Global 2000 sampling frame)

D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	1%
Director	17%
Manager	21%
Supervisor	16%
Technician	34%
Staff	6%
Contractor	2%
Other	1%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	1%
Chief Financial Officer	2%
General Counsel	1%
Chief Information Officer	54%
Chief Compliance Officer	10%
Human Resources VP	0%
Chief Security Officer	6%
Chief Information Security Officer	18%
Chief Privacy Officer	0%
Chief Risk Officer	7%
Other	1%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Financial services	19%
Health & pharmaceuticals	11%
Hospitality	3%
Industrial	8%
Public sector	12%
Retail (conventional)	4%
Retail (ecommerce)	5%
Services	8%
Technology & software	7%
Transportation	4%
Other (please specify)	2%
Total	100%

D4. Where are your operations located? (check all that apply)	Pct%
North America	100%
LATAM	79%
EMEA	93%
Asia-Pac	90%
Total	362%

D5. What is the worldwide headcount of your organization?	Pct%
1,001 to 5,000	6%
5,001 to 10,000	19%
10,001 to 25,000	29%
25,001 to 50,000	15%
50,001 to 75,000	17%
More than 75,000	14%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

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