The Security Impact of Mobile Device Use by Employees

Sponsored by Accellion

Independently conducted by Ponemon Institute LLC

Publication Date: December 2014

The Security Impact of Mobile Device Use by Employees

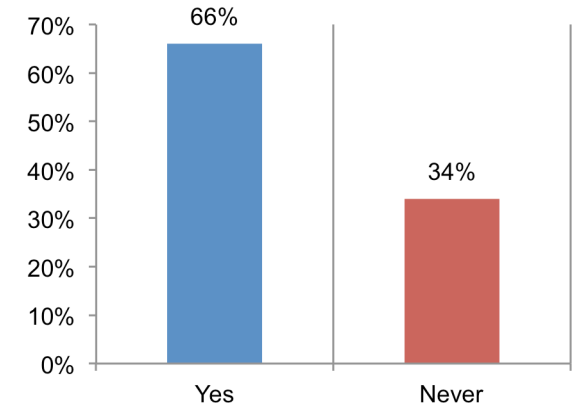
Ponemon Institute, December 2014

Part 1. Executive Overview

What do employees think about the use of mobile devices in the workplace? Are they concerned about the security of their devices? Are they aware of potential risks to corporate information when using smartphones and tablets?

The Security Impact of Mobile Device Use by Employees study sponsored by Accellion and conducted by Ponemon Institute examines employees' perceptions about the secure use of mobile devices to access corporate information. We surveyed 709 individuals in the United States who work in such areas as sales, finance and accounting, corporate IT, business operations and other functions.

Figure 1. Did you download mobile apps without your company's permission?



Overall, this report shows that employees have a growing dependency on mobile devices to access corporate information of all kinds, which impacts their productivity. However, companies seem to ignore the risk created by a mobile workforce, which may come from a lack of training and awareness, as well as employees underestimating the risk of their mobile actions.

Mobile devices such as a smartphone or tablet are used an average of 52 percent of the time mostly to access customer information, including client lists and email lists. On average, respondents say they spend about 25 hours in the office and almost the same amount of time (24 hours) working at home or other locations.

As more of the workday is spent away from the office, employees rely upon mobile devices to complete their work. However, the findings reveal that companies may not be taking mobile security seriously.

For example, training on the secure use of mobile devices hardly exists, very few have a corporate app store so employees can download approved apps and employees believe their company values productivity over security. As a consequence, respondents do not understand how routine tasks such as sharing files, using the cloud and downloading apps that might be infected can create huge risks for their companies. Figure 1 reveals that 66 percent of respondents admit to downloading mobile apps without their employers' approval.

Key takeaways from this research include the following:

Whether in the office or elsewhere, employees have access to sensitive company information. Eighty-eight percent of respondents are accessing such confidential information as email lists, customer data, including contact lists, non-financial and financial business information as well as other intellectual properties. Most time is spent on business email, calendars, contact lists and texting.

Employees say they need mobile access to corporate information to be productive. Sixty-two percent say direct and convenient mobile access to corporate information is essential if they

are to be productive. Further, 38 percent say the use of mobile devices makes them more efficient and the time it takes to do their job is reduced by an average of 30 minutes.

How concerned are companies about mobile security? Only 20 percent of respondents say they have received training on the security of mobile content access and management in the workplace. If they did receive training, 74 percent of respondents say it was not effective in reducing the security risks created by the use of mobile devices.

Employees are clueless about the risk of using unapproved mobile apps. Sixty-six percent of respondents say they have either frequently (23 percent) or sometimes (43 percent) downloaded and used mobile apps that do not have the approval of their company. Only 19 percent say they made sure the apps did not contain viruses or malware. Only 22 percent of respondents say they think such behavior puts their company at risk.

Few companies have an app store for approved mobile device applications. Only 23 percent of respondents say their company has an app store. However, 70 percent of these respondents say they only download apps from the corporate app store.

BYOD is credited with making employees more productive but there is worry about companies controlling their devices. Among BYOD users in this study, 70 percent say that BYOD makes them more productive because they can have both personal and work content on one device.

Employees deny putting sensitive information when using their own devices or accessing public clouds. While many employees say they do not knowingly put their company's sensitive or confidential information at risk with BYOD and BYOC, others are doing so. Companies are allowing such risky practices as using mobile devices when emailing attachments, syncing to desktops and using consumer cloud content services.

Reducing the risk

Employees in this study admit they are not careful when using mobile devices to access sensitive information. Downloading mobile apps without the approval of their organization or making sure these apps do not contain viruses or malware are just some of the behaviors that could result in data leakage. However, taking a few basic actions will help enterprises address these risks:

- Educate employees through training programs that communicate the importance of how to securely use mobile devices for work functions.
- Support both productivity and security by providing enterprise mobile applications that are specially developed for enterprise use.
- Establish guidelines for such practices as the use of commercial grade file sharing applications, public cloud services and enterprise content services.

Part 2. Key findings

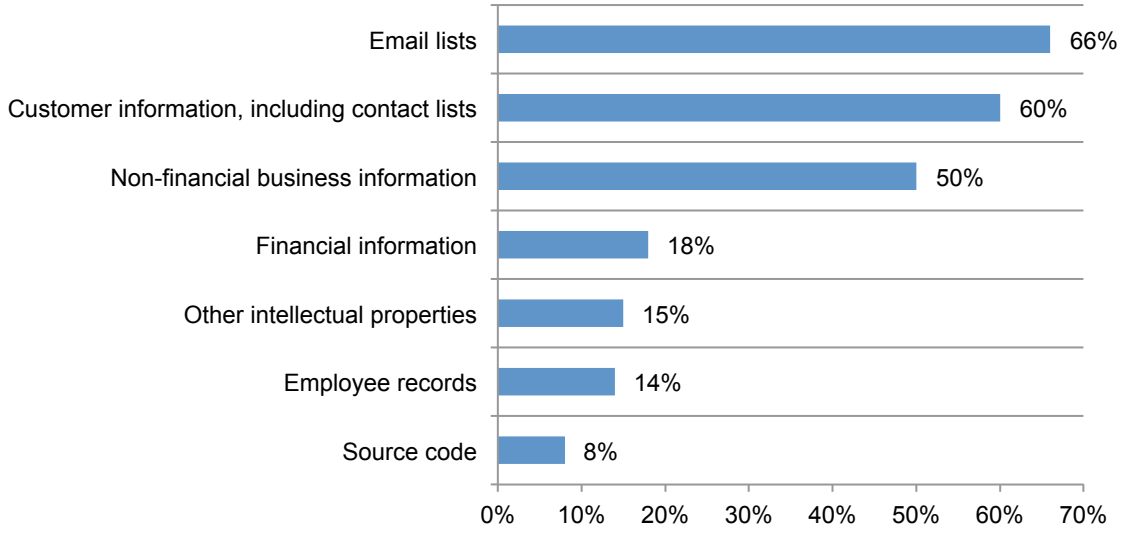
In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of this report. The report is organized according to the following themes:

- Employees have a growing dependency on mobile devices to access corporate information.
- Companies seem to ignore the risk created by a mobile workforce.
- What risk? It may be a lack of training and awareness but employees underestimate the risk of not using their mobile devices securely.

Employees have a growing dependency on mobile devices to access corporate information.

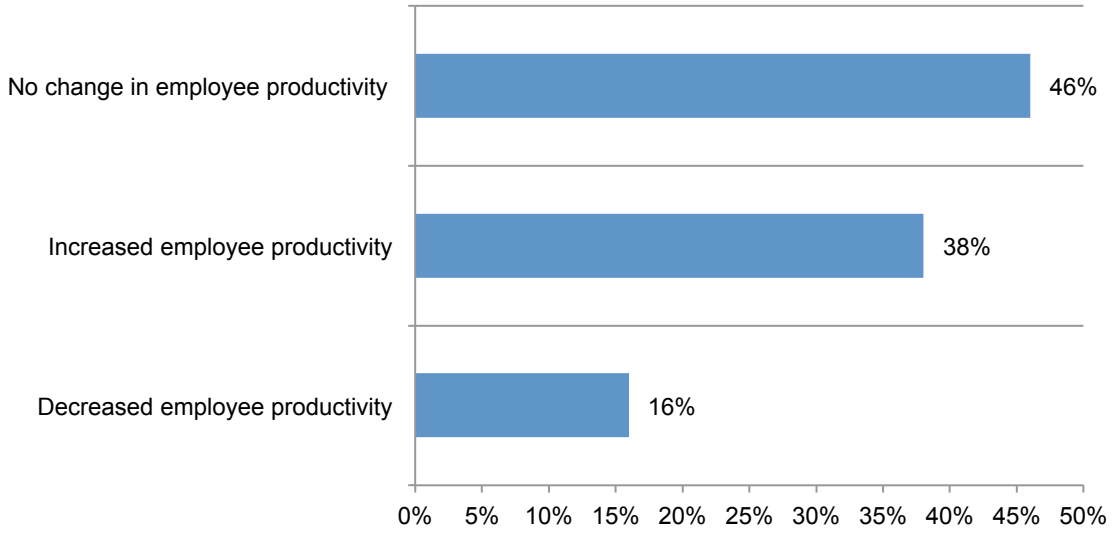
Whether in the office or elsewhere, employees say they need access to sensitive company information. Sixty-two percent of respondents say direct and convenient mobile access to corporate information is essential if they are to be productive. As shown in Figure 2, 66 percent of respondents are accessing such confidential information as email lists, customer data, including contact lists, non-financial and financial business information as well as other intellectual properties. Most time is spent on business email, calendars, contact lists and texting.

Figure 2. What types of sensitive company information do employees access?
More than one response permitted



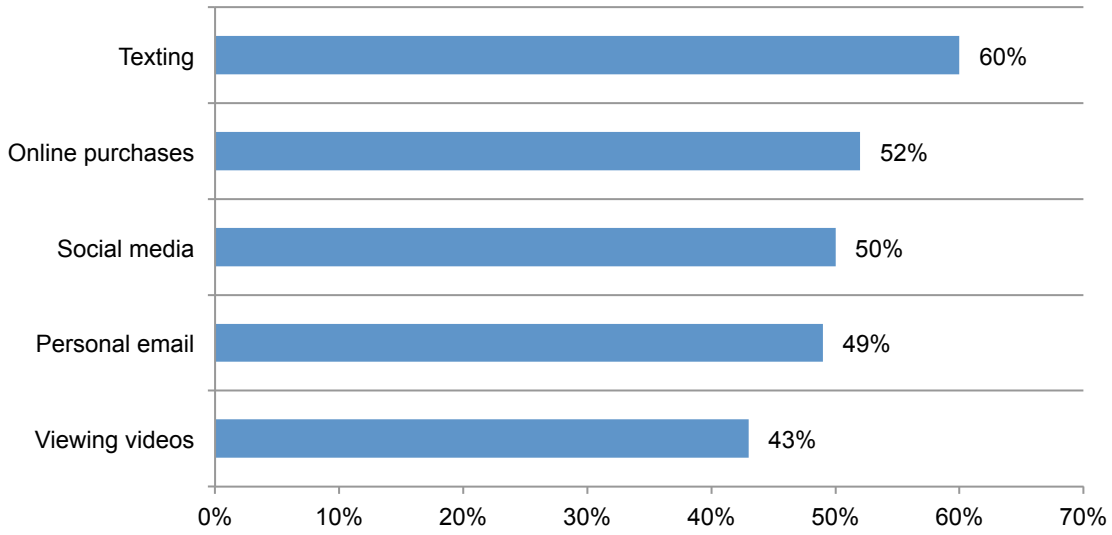
Workplace productivity improves or stays the same with the use of mobile devices. According to Figure 3, 38 percent of respondents say the use of mobile devices makes them more efficient and they save about a half hour on their workplace activities. A higher percentage of respondents (46 percent) say it has had no impact. Only 16 percent actually say mobile devices decrease their productivity and on average they spend an extra 19 minutes on workplace activities because they are less efficient.

Figure 3. How has the use of mobile devices in the workplace affected employees' productivity?



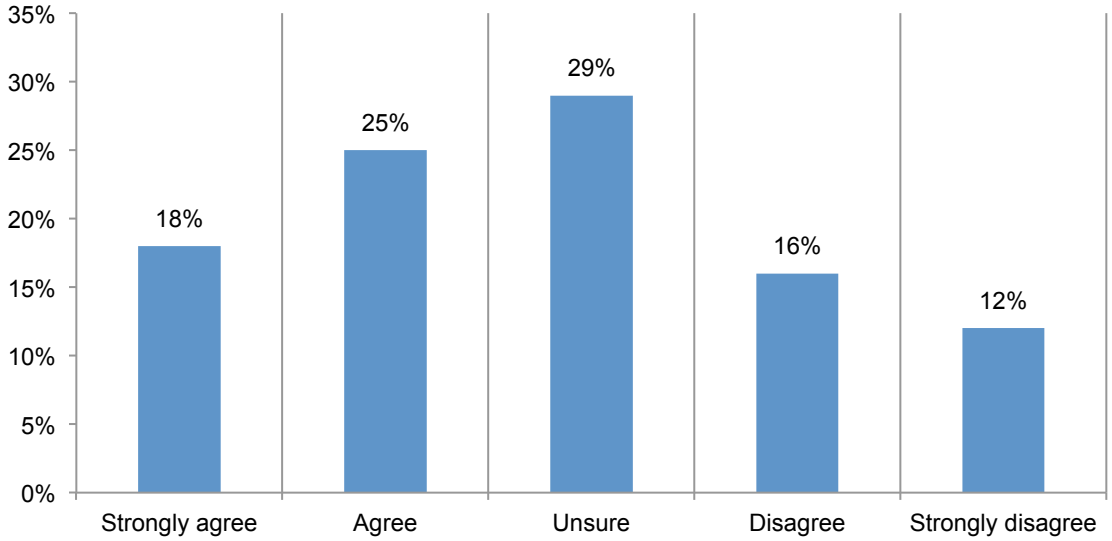
Fifty-nine percent of respondents say they bring their own devices to the workplace and 61 percent say they use mobile devices for both personal and work-related tasks. Such personal tasks include texting, online purchases and social media. Figure 4 shows the top 5 personal tasks respondents do with their mobile device in the workplace.

Figure 4. What types of personal tasks are employees doing in the workplace?



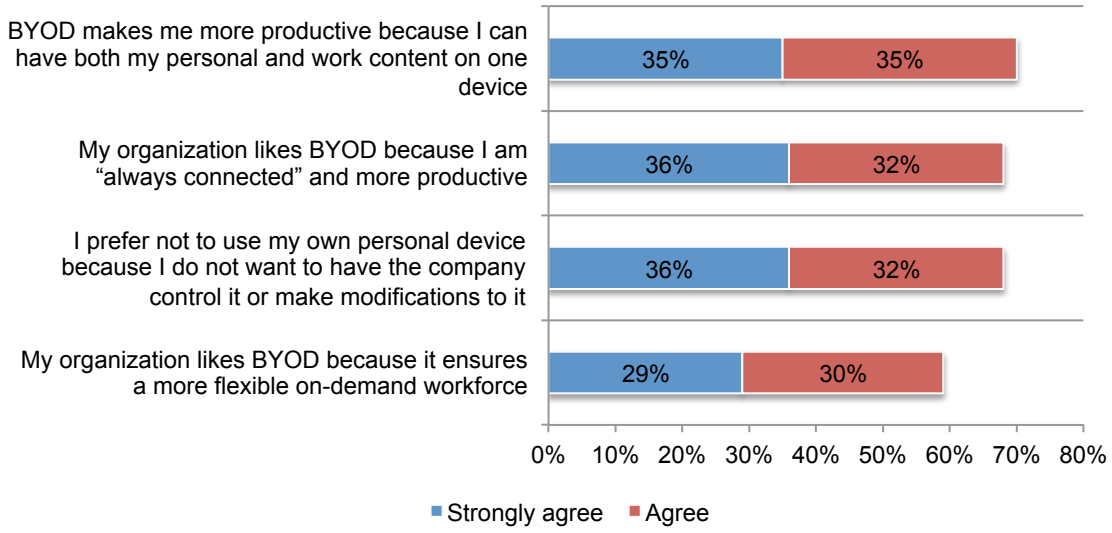
Not allowing the use of personal mobile devices and favorite apps in the workplace would make some quit their job. Many employees do not seem to understand the risk of using insecure mobile devices and apps in the workplace and why an employer may ban them. According to Figure 5, 43 percent of respondents say such a policy would make them look for another job and 29 percent are unsure if they would take such action.

Figure 5. Would you quit your job if you could not use your personal mobile device and favorite apps in the workplace?



BYOD is credited with making employees more productive but there is worry about companies controlling devices. Among BYOD users in this study, 70 percent say that BYOD makes them more productive because they can have both personal and work content on one device, as shown in Figure 6. Further, 68 percent say their employers are happy because they are always connected and as a result can be more productive and 59 percent say their organization likes BYOD because it ensures a more flexible on-demand workforce. However, 68 percent prefer not to use their own device because of concerns that the company will control or modify their devices.

Figure 6. Employees worry about their privacy when using BYOD

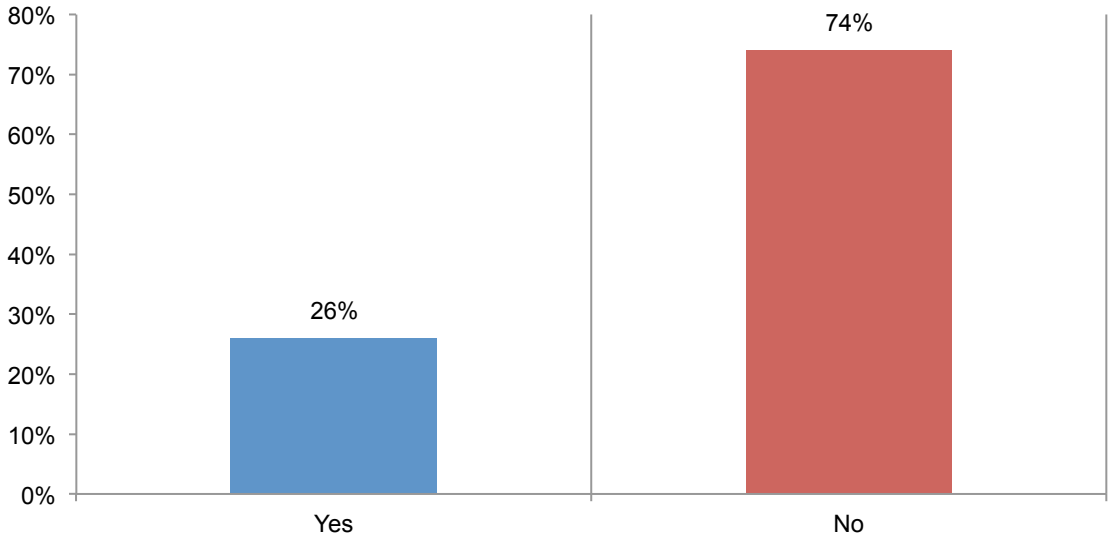


Companies seem to ignore the risk created by a mobile workforce.

Training on the security of mobile content access is rare. Only 20 percent of respondents say they have received training on the security of mobile content access and management in the workplace. As shown in Figure 7, if they did receive training, 74 percent of respondents say it was not effective in reducing the security risks created by the use of mobile devices.

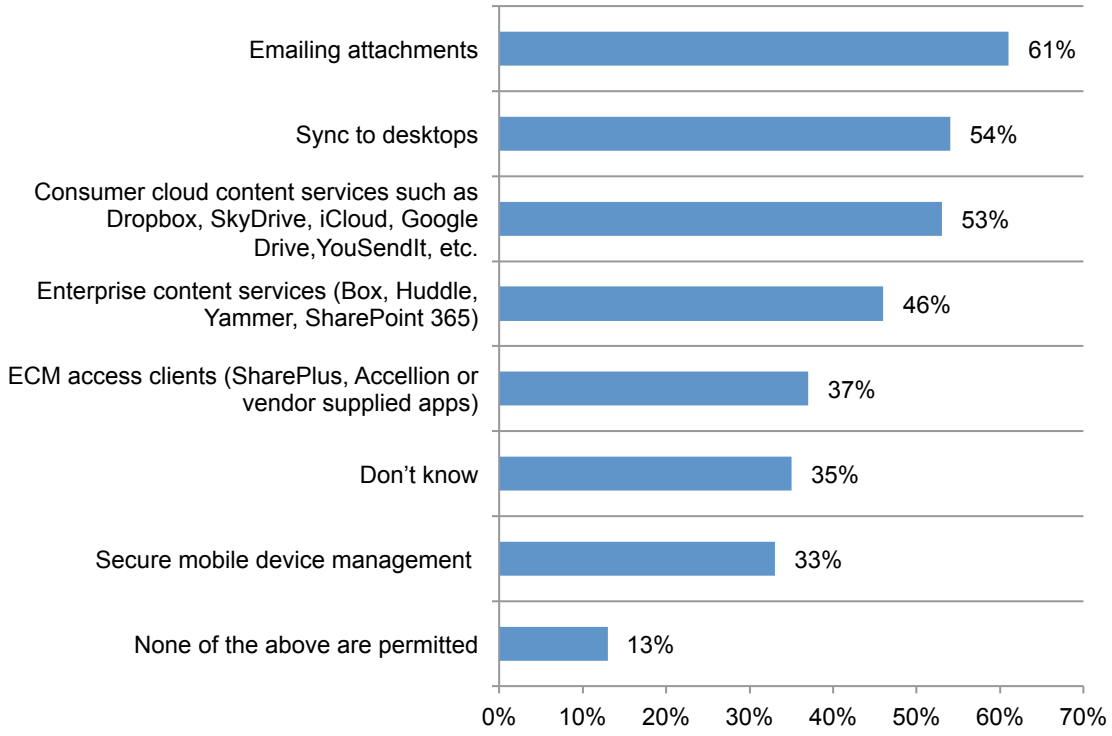
Further, few companies have an app store for approved mobile device applications. Only 23 percent of respondents say their company has an app store. However, 70 percent of these respondents say they only download apps from the corporate app store.

Figure 7. Do you believe training is effective in reducing the security risks created by the use of mobile devices?



Companies are not establishing guidelines for the access of corporate information on mobile devices. As shown in Figure 8, companies are allowing such risky practices as using mobile devices when emailing attachments, syncing to desktops and using consumer cloud content services. Only 13 percent of respondents say these practices are not permitted.

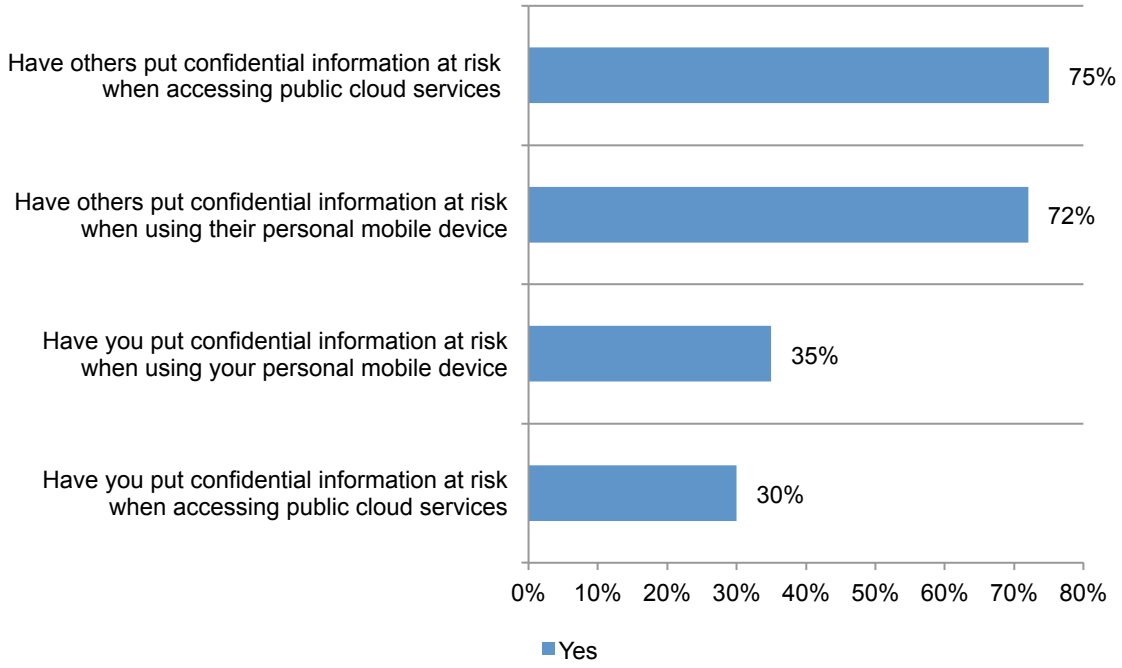
Figure 8. Are the following ways of accessing content on mobile devices permitted by your company?
More than one response permitted



What risk? It may be a lack of training and awareness but many employees underestimate the risk of not using their mobile devices securely.

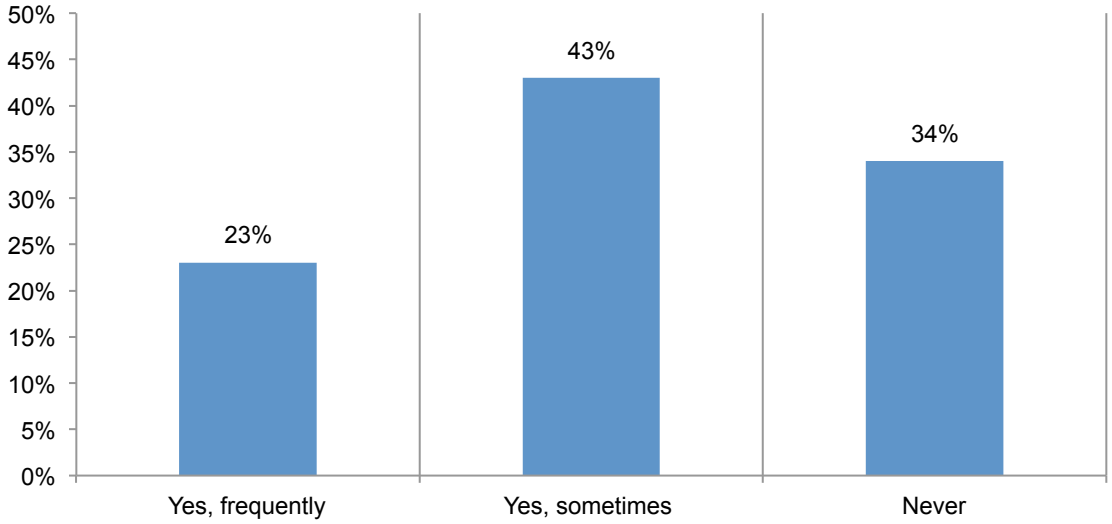
Employees deny putting sensitive information at risk when using their own devices or accessing public clouds. According to Figure 9, while many employees say they do not knowingly put their company's sensitive or confidential information at risk with BYOD and BYOC, others are doing so.

Figure 9. Employees are putting confidential company at risk with BYOD and BYOC



Employees are clueless about the risk of using unapproved mobile apps. Sixty-six percent of respondents say they have either frequently (23 percent) or sometimes (43 percent) downloaded and used mobile apps that do not have the approval of their company as shown in Figure 10. Only 19 percent say they made sure the apps did not contain viruses or malware. Only 22 percent of respondents say they think such behavior puts their company at risk.

Figure 10. Have you downloaded and used mobile apps that do not have the approval of your company?



Part 3. Risky Scenarios

Respondents were asked to indicate if the following 5 scenarios were likely to happen in their organization and what the level of risk is to confidential and sensitive information. A scale from 1= low likelihood/low risk to 10=high likelihood/high risk. The findings reveal that respondents believe all scenarios are very likely to happen but do not believe that they pose a great risk.

While all scenarios illustrate how confidential and sensitive information can be at risk, the areas that companies need to be most aware of are those that are most likely to occur but the employees' awareness of the risk is lower than the likelihood of an occurrence. The following are the most risky practices:

- The use of consumer file-sharing applications to move confidential business information without the employer's permission (scenario 3).

- The use of an unauthorized public cloud service to circumvent file-size limits prescribed for work email (scenario 4).

Table 1. Risky scenarios 1 = low likelihood to 10 = high likelihood	Likelihood of happening?	How risky is this?
Employee fails to use remote wipe on a lost mobile device with corporate information	7.54	5.62
Employee uses an unapproved cloud-based note taking and clipping service and stores unencrypted sensitive company information on his mobile device	8.06	5.40
Employee transfers confidential company information to a commercial file-sharing application	8.22	5.54
Employee uses unauthorized public cloud service to store company information for easy access	8.52	5.30
An employee copies confidential information from SharePoint to her USB stick because she wants to be able to send this information to people without SharePoint access	7.42	5.89

Scenario 1 An employee uses her mobile device for both personal and company purposes. In addition to company documents, the mobile device has personal photos. The device is lost. The employee does not use remote wipe because she doesn't want to lose her photos. The average is 7.5 for likelihood but the average risk is 5.6.

Scenario 2 To be more productive, an employee uses an unapproved cloud-based note taking and clipping service that lets him create and store information for easy access. The employee has sensitive company information but does not encrypt it so it can be easily accessed from his iPad or iPhone. He ignores the potential risk of having a cybercriminal steal this information. The average is 8.1 for likelihood but the average for risk is only 5.4.

Scenario 3 After registering with a consumer file-sharing application, an employee moves several large files containing business confidential information to this file sharing application. The employee did not obtain permission from the employer to use this application. The average likelihood is 8.2 and the risk is 5.5.

Scenario 4 To circumvent file-size limits prescribed for work email, an employee transfers company information to an unauthorized public cloud service. She does this frequently to avoid difficulties in connecting to work email when outside the office. Moreover, she is assured that IT is not monitoring what she is sending via personal email. The average likelihood is 8.5 and the average risk is 5.3

Scenario 5 An employee copies confidential information from SharePoint to her USB stick because she wants to be able to send this information to people without SharePoint access. She also wants to be able to work on these documents from home without needing access to the company's network. The average likelihood is 7.4 and the average risk is 5.9.

Part 4. Conclusion

Employees are spending almost as much time working outside the office as they do behind their desks. To be productive no matter where they are, employees want direct and convenient mobile access to corporate information. However, without appropriate training and security procedures in place such access puts confidential corporate information at risk.

This study highlights the behaviors that companies must address to prevent the misuse and abuse of their sensitive information. Recommendations to mitigate the risks created by these behaviors include the following:

- Communicate the importance of the secure use of mobile devices in training programs.
- Support both productivity and security by providing an app store for approved mobile device applications.
- Educate employees about the need to make sure apps they use in the workplace do not contain viruses or malware.
- Establish guidelines for such practices as the use of commercial grade file sharing applications, public cloud services and enterprise content services.

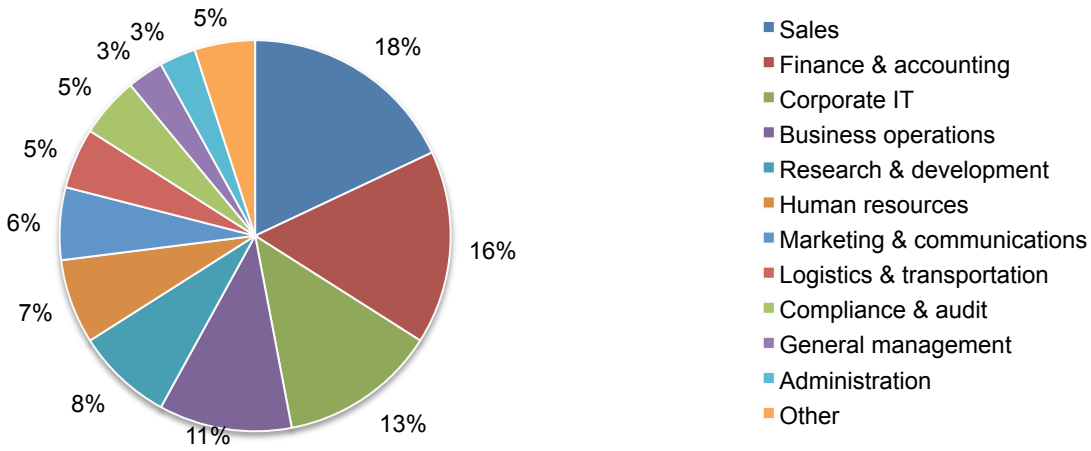
Part 5. Methods

A sampling frame composed of 19,901 individuals in the United States who work in such areas as sales, finance and accounting, corporate IT, business operations and other functions were selected for participation in this survey. As shown in the following table, 798 respondents completed the survey. Screening removed 89 surveys. The final sample was 709 surveys (or a 3.6 percent response rate).

Table 2. Sample response	Freq	Pct%
Total sampling frame	19,901	100.0%
Total returns	798	4.0%
Rejected or screened surveys	89	0.4%
Final sample	709	3.6%

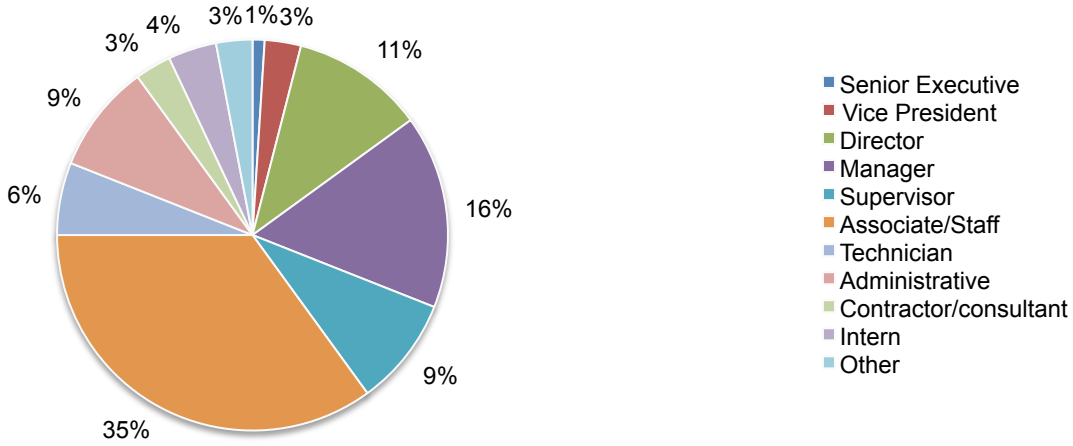
Pie chart 1 reports the current department or job function of respondents. As shown in Pie Chart 1, 18 percent of respondents reported their current job function is in sales, 16 percent indicated finance and accounting and 13 percent responded corporate IT.

Pie Chart 1. Current department or job function



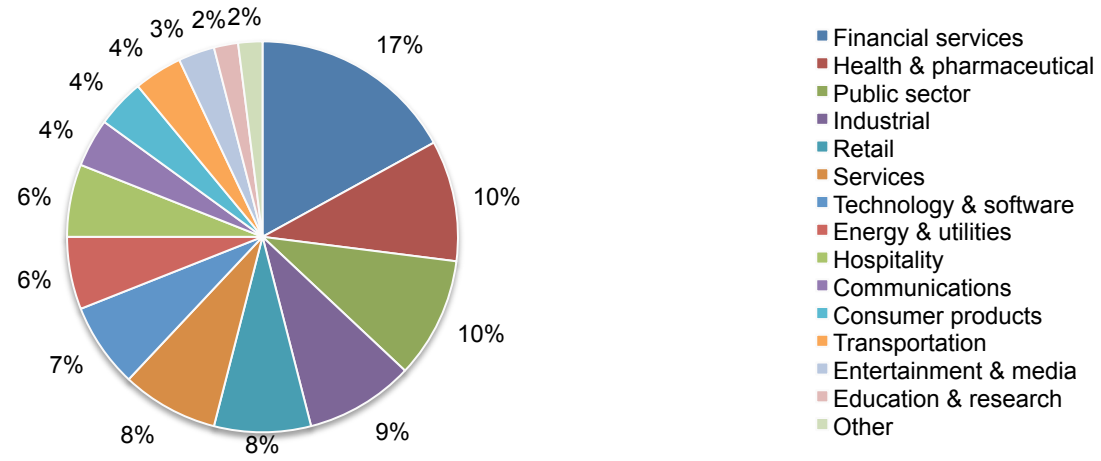
Pie Chart 2 reports the organizational level for survey participants. Forty percent of respondents are at or above the supervisory level.

Pie Chart 2. Position level within the organization



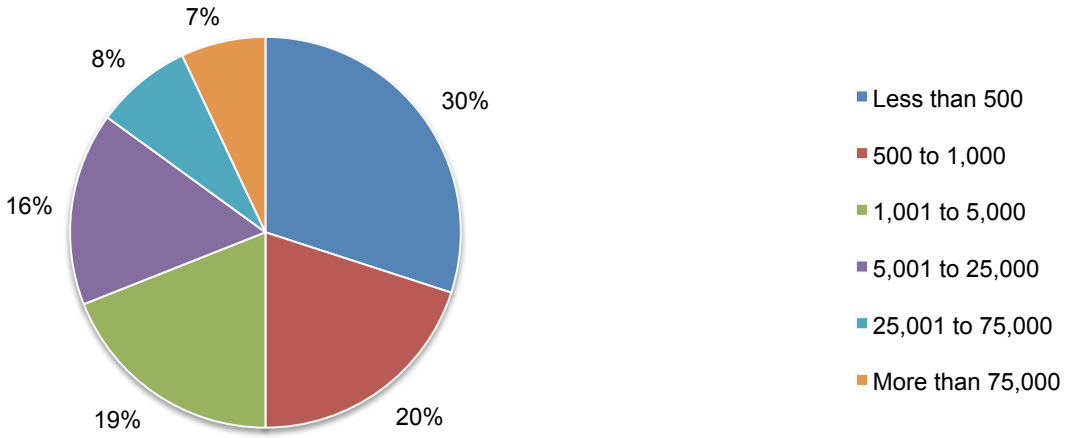
Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by health & pharmaceutical (10 percent) and public sector (10 percent).

Pie Chart 3. Primary industry focus



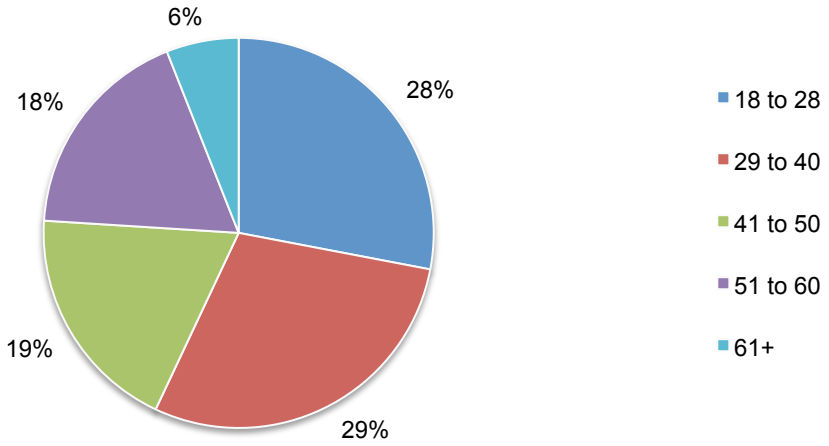
According to Pie Chart 4, half of the respondents are from organizations with a global headcount of over 1,000 employees.

Pie Chart 4. Worldwide headcount of the organization



As shown in Pie Chart 5, more than half (57 percent) of respondents are between the ages of 18 and 40 years. The extrapolated value of the sample is 38.9 years.

Pie Chart 5. Age range



Part 6. Caveats

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 work in such areas as sales, finance and accounting, corporate IT, business operations and other functions in various organizations in the United States. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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 October 2014.

Survey response	Freq	Pct%
Total sampling frame	19901	100.0%
Total returns	798	4.0%
Rejected or screened surveys	89	0.4%
Final sample	709	3.6%

Part 1. Background

Q1a. In a typical week, how much time do you spend working in the office?	Pct%
10 hours or less	25%
Between 11 hours and 20 hours	15%
Between 21 hours and 30 hours	17%
Between 31 hours and 40 hours	21%
More than 40 hours	22%
Total	100%
Extrapolated hours	24.8

Q1b. In a typical week, how much time do you spend working outside the office?	Pct%
10 hours or less	23%
Between 11 hours and 20 hours	18%
Between 21 hours and 30 hours	18%
Between 31 hours and 40 hours	27%
More than 40 hours	14%
Total	100%
Extrapolated hours	24.0

Q2a. How much time is spent using a mobile device such as a smartphone or tablet both at the office and outside the office?	Pct%
Less than 20 percent of the work week	10%
20 percent to 39 percent of the work week	23%
40 percent to 59 percent of the work week	30%
60 percent to 79 percent of the work week	21%
80 percent to 100 percent of the work week	16%
Total	100%
Extrapolated value	52%

Q2b. In the next year, how much time will be spent using mobile devices such as smartphones and tablets to complete your work?	Pct%
Less than 20 percent of the work week	5%
20 percent to 39 percent of the work week	14%
40 percent to 59 percent of the work week	23%
60 percent to 79 percent of the work week	29%
80 percent to 100 percent of the work week	29%
Total	100%
Extrapolated value	63%

Q3. What mobile device do you rely most upon to complete your work?	Pct%
Smart phone	33%
Tablet	18%
Laptop	49%
Total	100%

Q4a. Do you have access to your organization's sensitive and confidential work-related information?	Pct%
Yes	88%
No	12%
Total	100%

Q4b. If yes, what types of sensitive company information do you access? Please select all that apply	Pct%
Customer information, including contact lists	60%
Email lists	66%
Employee records	14%
Non-financial business information	50%
Financial information	18%
Source code	8%
Other intellectual properties	15%
Total	231%

Q5. Do you use your own personally owned mobile device (BYOD) to access corporate data?	Pct%
Yes	59%
No	41%
Total	100%

Part 2: Productivity issues in the use of mobile devices to access and use corporation information

Q6a. How has the use of mobile devices in the workplace affected employees' productivity?	Pct%
Increased employee productivity	38%
Decreased employee productivity	16%
No change in employee productivity (skip to Q7)	46%
Total	100%

Q6b. [If you selected increase] On average, how many minutes per employee **are saved** each day as a result of using mobile devices in the workplace?	Pct%
10 minutes or less	10%
Between 11 minutes and 20 minutes	13%
Between 21 minutes and 30 minutes	26%
Between 31 minutes and 40 minutes	31%
More than 40 minutes	20%
Total	100%
Extrapolated value	29.8

Q6c. [If you selected decrease] On average, how many additional minutes per employee **are incurred** each day as a result of using mobile devices in the workplace?	Pct%
10 minutes or less	31%
Between 11 minutes and 20 minutes	35%
Between 21 minutes and 30 minutes	14%
Between 31 minutes and 40 minutes	11%
More than 40 minutes	9%
Total	100%
Extrapolated value	18.7

Q7. As part of your job role and responsibilities, please select all the tasks you do on your smart phones or tablets.	Pct%
Business email	89%
Calendar	85%
Contact lists	80%
Texting	79%
Document collaboration & management (i.e. SharePoint)	56%
Document creation	49%
Store work data locally on the device	47%
Document sharing	40%
Video conferencing	40%
Photos and videos	26%
Location services	26%
Social media	25%
Content management	16%
CRM (i.e. Salesforce.com)	16%
Mobile payments	15%
Maps and navigation	12%
Other (please specify)	5%
Total	706%

Q8a. Do you use your mobile device for both personal and work-related tasks?	Pct%
Yes	61%
No	39%
Total	100%

Q8b. If yes, below please select all the personal tasks you do with your mobile device in the workplace from the list below.	Pct%
Texting	60%
Online purchases	52%
Social media	50%
Personal email	49%
Viewing videos	43%
Document sharing	38%
Photos and videos	37%
Calendar	26%
Contact lists	23%
Maps and navigation	22%
Mobile payments	19%
e-Health	16%
Other (please specify)	4%
Total	439%

Please rate the following statements from strongly agree to strongly disagree using the scale below each item.	
Q9a. Direct and convenient mobile access to corporate information is essential if I am to be productive.	Pct%
Strongly agree	29%
Agree	33%
Unsure	18%
Disagree	16%
Strongly disagree	4%
Total	100%

Q9b. I would quit my job if I could not use my personal mobile device and favorite apps in the workplace.	Pct%
Strongly agree	18%
Agree	25%
Unsure	29%
Disagree	16%
Strongly disagree	12%
Total	100%

Q9c. My company's mobile security polices and procedures diminish my ability to be productive.	Pct%
Strongly agree	29%
Agree	26%
Unsure	11%
Disagree	24%
Strongly disagree	10%
Total	100%

Q9d. My organization places more emphasis on mobile productivity than security when accessing content and using collaboration tools in my work.	Pct%
Strongly agree	30%
Agree	26%
Unsure	13%
Disagree	25%
Strongly disagree	6%
Total	100%

Q9e. BYOD makes me more productive because I can have both my personal and work content on one device (only tabulated for BYOD users).	Pct%
Strongly agree	35%
Agree	35%
Unsure	12%
Disagree	10%
Strongly disagree	8%
Total	100%

Q9f. My organization likes BYOD because I am "always connected" and more productive (only tabulated for BYOD users).	Pct%
Strongly agree	36%
Agree	32%
Unsure	20%
Disagree	8%
Strongly disagree	4%
Total	100%

Q9g. My organization likes BYOD because they do not have to provide me with a mobile device (only tabulated for BYOD users);	Pct%
Strongly agree	25%
Agree	23%
Unsure	20%
Disagree	15%
Strongly disagree	17%
Total	100%

Q9h. My organization likes BYOD because it ensures a more flexible on-demand workforce (only tabulated for BYOD users).	Pct%
Strongly agree	29%
Agree	30%
Unsure	19%
Disagree	15%
Strongly disagree	7%
Total	100%

Q9i. I prefer not to use my own personal device because I do not want to have the company control it or make modifications to it (only tabulated for BYOD users).	Pct%
Strongly agree	36%
Agree	32%
Unsure	10%
Disagree	17%
Strongly disagree	5%
Total	100%

Part 3. Security issues in the use of mobile devices to access and use corporation information	
Q10a. Have you received training on the security of mobile content access and management in the workplace?	Pct%
Yes	20%
No	80%
Total	100%

Q10b. If yes, do you believe the training was effective in reducing the security risks created by the use of mobile devices?	Pct%
Yes	26%
No	74%
Total	100%

Q11a. Have you ever knowingly put your company's sensitive or confidential information at risk when using your mobile device in the workplace (BYOD)? Only tabulated for BYOD users.	Pct%
Yes	35%
No	65%
Total	100%

Q11b. Have others put your company's sensitive or confidential information at risk when using their mobile device in the workplace (BYOD)?	Pct%
Yes	72%
No	28%
Total	100%

Q12a. Have you ever knowingly put your company's sensitive or confidential information at risk when accessing public cloud services in the workplace (BYOC)?	Pct%
Yes	30%
No	70%
Total	100%

Q12b. Have others put your company's sensitive or confidential information at risk when accessing public cloud services in the workplace (BYOC)?	Pct%
Yes	75%
No	25%
Total	100%

Q13. Are any of the following ways of accessing content on mobile devices permitted by your company? Please select all that apply.	Pct%
Emailing attachments	61%
Sync to desktops	54%
Consumer cloud content services such as Dropbox, SkyDrive, iCloud, Google Drive,YouSendIt, etc.	53%
Enterprise content services (Box, Huddle, Yammer, SharePoint 365)	46%
ECM access clients (SharePlus, Accellion or vendor supplied apps)	37%
Secure mobile device management (basic MDM)	33%
None of the above are permitted	13%
Don't know	35%
Total	332%

Q14a. Does your organization have a corporate app store for approved mobile device applications?	Pct%
Yes	23%
No	65%
Under development	12%
Total	100%

Q14b. If yes, do you only download apps from the corporate app store?	Pct%
Yes	70%
No	30%
Total	100%

Q15a. Have you downloaded and used mobile apps that do not have the approval of your company?	Pct%
Yes, frequently	23%
Yes, sometimes	43%
Never	34%
Total	100%

Q15b. If yes, did you check to make sure the apps did not contain viruses or malware?	Pct%
Yes	19%
No	81%
Total	100%

Q15c. If yes [Q15a], do you think you put your organization at risk?	Pct%
Yes	22%
No	78%
Total	100%

Part 4. Scenarios:

Scenario 1: An employee uses her mobile device for both personal and company purposes. In addition to company documents, the mobile device has personal photos. The device is lost. The employee does not use remote wipe because she doesn't want to lose her photos.	
Q16a. What is the likelihood of this happening in your organization?	Pct%
1 or 2 [Low likelihood]	5%
3 or 4	10%
5 or 6	16%
7 or 8	16%
9 or 10 [High likelihood]	53%
Total	100%
Extrapolated value	7.5

Q16b. How much of a risk is this to your organization?	Pct%
1 or 2 [Low risk]	21%
3 or 4	24%
5 or 6	10%
7 or 8	18%
9 or 10 [High risk]	27%
Total	100%
Extrapolated value	5.6

Scenario 2: To be more productive, an employee uses an unapproved cloud-based note taking and clipping service that lets him create and store information for easy access. The employee has sensitive company information but does not encrypt it so it can be easily accessed from his iPad or iPhone. He ignores the potential risk of having a cybercriminal steal this information.	
Q17a. What is the likelihood of this happening in your organization?	Pct%
1 or 2 [Low likelihood]	3%
3 or 4	5%
5 or 6	12%
7 or 8	21%
9 or 10 [High likelihood]	59%
Total	100%
Extrapolated value	8.1

Q17b. How much of a risk is this to your organization?	Pct%
1 or 2 [Low risk]	22%
3 or 4	23%
5 or 6	16%
7 or 8	16%
9 or 10 [High risk]	23%
Total	100%
Extrapolated value	5.4

Scenario 3: After registering with a consumer file-sharing application, an employee moves several large files containing business confidential information to this file sharing application. The employee did not obtain permission from the employer to use this application.	
Q18a. What is the likelihood of this happening in your organization?	Pct%
1 or 2 [Low likelihood]	2%
3 or 4	6%
5 or 6	10%
7 or 8	18%
9 or 10 [High likelihood]	64%
Total	100%
Extrapolated value	8.2

Q18b. How much of a risk is this to your organization?	Pct%
1 or 2 [Low risk]	26%
3 or 4	19%
5 or 6	11%
7 or 8	15%
9 or 10 [High risk]	29%
Total	100%
Extrapolated value	5.5

Scenario 4: To circumvent file-size limits prescribed for work email, an employee transfers company information to an unauthorized public cloud service. She does this frequently to avoid difficulties in connecting to work email when outside the office. Moreover, she is assured that IT is not monitoring what he is sending via personal email.	
Q19a. What is the likelihood of this happening in your organization?	Pct%
1 or 2 [Low likelihood]	3%
3 or 4	4%
5 or 6	6%
7 or 8	13%
9 or 10 [High likelihood]	74%
Total	100%
Extrapolated value	8.5

Q19b. How much of a risk is this to your organization?	Pct%
1 or 2 [Low risk]	32%
3 or 4	15%
5 or 6	12%
7 or 8	13%
9 or 10 [High risk]	28%
Total	100%
Extrapolated value	5.3

Scenario 5: An employee copies confidential information from SharePoint to her USB stick because she wants to be able to send this information to without SharePoint access. She also wants to be able to work on these documents from home without needing access to the company's network.	
Q20a. What is the likelihood of this happening in your organization?	Pct%
1 or 2 [Low likelihood]	6%
3 or 4	12%
5 or 6	13%
7 or 8	18%
9 or 10 [High likelihood]	51%
Total	100%
Extrapolated value	7.4

Q20b. How much of a risk is this to your organization?	Pct%
1 or 2 [Low risk]	5%
3 or 4	16%
5 or 6	19%
7 or 8	16%
9 or 10 [High risk]	44%
Total	100%
Extrapolated value	5.9

Recap	Likelihood	Risk level
Scenario 1	7.54	5.62
Scenario 2	8.06	5.40
Scenario 3	8.22	5.54
Scenario 4	8.52	5.30
Scenario 5	7.42	5.89

Part 5: Organizational characteristics and demographics

D1. Check the department or function you are in.	Pct%
Sales	18%
Finance & accounting	16%
Corporate IT	13%
Business operations	11%
Research & development	8%
Human resources	7%
Marketing & communications	6%
Logistics & transportation	5%
Compliance & audit	5%
General management	3%
Administration	3%
Other (please specify)	5%
Total	100%

D2. What organizational level best describes your position level?	Pct%
Senior Executive	1%
Vice President	3%
Director	11%
Manager	16%
Supervisor	9%
Associate/Staff	35%
Technician	6%
Administrative	9%
Contractor/consultant	3%
Intern	4%
Other (please specify)	3%
Total	100%

D3. What is your organization's primary industry sector?	Pct%
Agriculture & food services	1%
Communications	4%
Consumer products	4%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	3%
Financial services	17%
Health & pharmaceutical	10%
Hospitality	6%
Industrial	9%
Public sector	10%
Retail	8%
Services	8%
Technology & software	7%
Transportation	4%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 500	30%
500 to 1,000	20%
1,001 to 5,000	19%
5,001 to 25,000	16%
25,001 to 75,000	8%
More than 75,000	7%
Total	100%
Extrapolated value	12,795

D5. What defines your age range?	Pct%
18 to 28	28%
29 to 40	29%
41 to 50	19%
51 to 60	18%
61+	6%
Total	100%
Extrapolated value	38.9

D6. What defines your US regional location?	Pct%
Northeast	20%
Mid-Atlantic	19%
Midwest	17%
Southeast	13%
Southwest	12%
Pacific-West	19%
Total	100%

D7. Gender	Pct%
Female	46%
Male	54%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

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.