zix™

BYOD SECURITY: A Fresh Perspective

Conducted by Ponemon Institute LLC
Publication Date: 2013

Sponsored by Zix Corporation

Bring-Your-Own-Device (BYOD) is here to stay. Companies are excited about the potential cost savings and added productivity. Employees are happy to use the personal devices they love and gain the flexibility of working away from the office. But before companies and their employees can enjoy all the benefits, significant hurdles lay in the way. So we partnered with Ponemon Institute to study the BYOD market and better understand the challenges companies face in taking advantage of this new phenomenon.

In total, we surveyed 895 IT and IT security specialists primarily at supervisor level or higher. Respondents represented enterprises of all sizes (with the majority in large organizations) and across a diverse range of industries including finance, healthcare, retail, government and industrial. Overall, the main conclusion that we've drawn from the findings of this study is: while companies are open to implementing a BYOD strategy within their business, the security solutions to fully enable adoption are in their infancy.

Grasping for More
More than 60 percent of respondents say their companies support BYOD; however, 46 percent of those companies do not use tools or policies to protect corporate data. Of the companies with current BYOD security products in place, 60 percent of respondents are unsatisfied mostly due to cost and inadequate security, and 56 percent are looking to replace their current solutions.

In addition, more than 40 percent of respondents say their companies have limited deployment of BYOD. The top reasons include employee resistance to loading security products on personal devices (35 percent), inadequate security solutions (28 percent) and cost of security products (13 percent).

These findings are valuable in understanding companies' BYOD needs and provide a great opportunity to evolve BYOD security into solutions that will enable confident adoption among the entire employee base. Whether the top priority is data security or employee enablement, a new approach is required to meet company data security needs and employee demands of control, convenience and privacy. We have developed that fresh approach.

Making the Most of BYOD
By streaming Exchange data to mobile devices, instead of controlling the devices themselves, employees experience convenient access to the office from their personal devices without allowing sensitive information like customer data and intellectual property from being stored on the device. When a device is lost or stolen, IT departments don't have to scramble to wipe the device, because the data never resides on the device. Better yet, employees can use their devices for work without ever losing control, convenience or privacy.

We invite you to review the detailed report to learn more about the current BYOD market, to better understand the state of BYOD security and to consider how our unique approach, which never allows corporate data to be stored on the device and allows employees to maintain privacy and control, may better meet your BYOD requirements.

Sincerely,

Rick Spurr
Chief Executive Officer and Chairman of the Board
Zix Corporation

BYOD Security: A Fresh Perspective

Prepared by Ponemon Institute

Part 1. Introduction

We are pleased to present the findings of *BYOD Security: A Fresh Perspective* sponsored by ZixCorp. The study focuses on whether companies are losing the ability to safeguard their sensitive and confidential data because of the increasing use of mobile devices in the workplace.

In this study we surveyed 895 IT and IT security specialists in the United States about their organizations' policies for permitting employees to access corporate applications with mobile devices and the security tools used to protect company data on both employee-owned and company provided mobile devices. We also asked what solutions are most desirable for secure access of corporate applications with mobile devices.

Following are the most salient findings.

- **BYOD is permitted in most organizations**. Only 25 percent of respondents say their organizations require employees to use company provided devices exclusively when accessing corporate applications such as email and calendars over the Internet.

- **BYOD security leaves corporate data vulnerable**. Forty-six percent of respondents say no tools or policies are used to protect company data on employee-owned mobile devices. If they do have security it is mostly likely to be company defined mobile device password policies, according to 37 percent of respondents. Thirty-two percent of respondents say secure container is their solution, and 30 percent use mobile device management (MDM) software.

  There is more protection for company owned mobile devices. Thirty-three percent of respondents say no tools are used in contrast to the 46 percent of respondents who say no tools are used for BYOD. Also a higher percentage of respondents (43 percent) say their organizations use company defined mobile device password policies only. This is also the case for MDM software where 36 percent of respondents say this is the solution used.

- **Employee concerns about privacy have limited BYOD deployment.** Thirty-seven percent of respondents say worries about privacy and retention of personal data is a big concern, and 23 percent say it is an occasional concern. Forty percent say it is not an issue.

- **Satisfaction with MDM or secure container solutions is similar for both employee and company provided devices**. Forty percent are satisfied with these solutions for employee owned mobile devices, and 41 percent are satisfied with their protection of data on company provided devices. The primary reasons for dissatisfaction with these solutions are the cost and inadequate security.

- **Employee resistance to security tools on their personal devices is limiting BYOD**. Forty-three percent of respondents say their organizations limit the number of employees allowed to access corporate applications with their own mobile devices. The reason for limited deployment, according to 35 percent of respondents, is employees' resistance to loading security tools on personal device. Another reason is existing security tools are inadequate, according to 28 percent of respondents.

- **There is interest in mobile device solutions that allow access but do not store corporate data.** Fifty-four percent of respondents say they are interested in this solution for all mobile devices, and 12 percent are interested for employees who only need to access their corporate email, calendar and contacts. Fifty-seven percent say this is desirable for all mobile device owners.

Part 2. Key findings

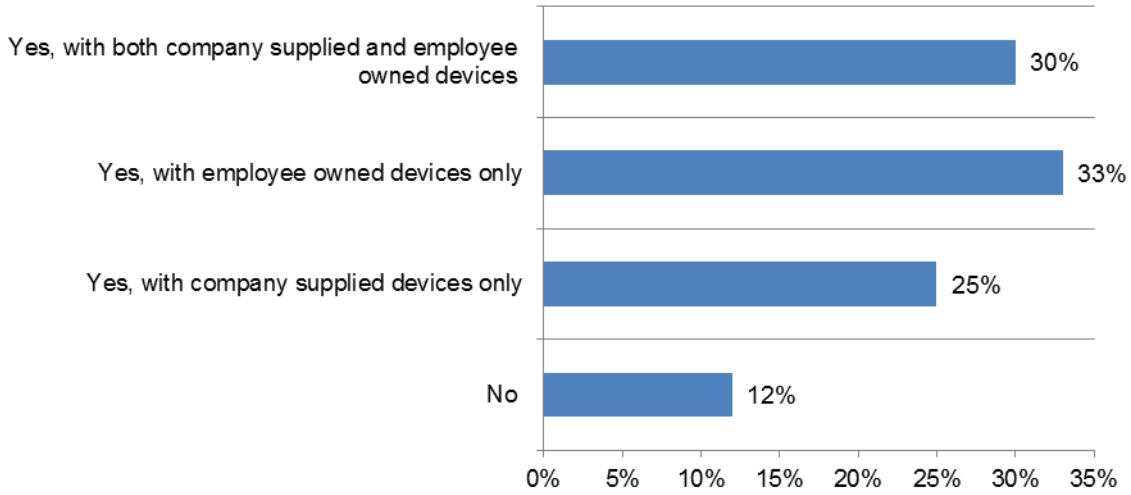
The complete audited findings are presented in the appendix of this report. We have organized the findings according to the following topics:

- Policies for permitting employees to access corporate applications with mobile devices
- Security tools used to protect company data accessed by employees
- Solutions considered desirable for secure access of corporate applications

Policies for permitting employees to access corporate applications with mobile devices

BYOD is permitted in most organizations. According to Figure 1, only 25 percent of respondents say their organizations require employees to use company provided devices exclusively when accessing corporate applications such as email over the Internet. Most organizations allow employees to use their own mobile devices or both company supplied and employee-owned devices. Thirty percent say their organizations allow both company supplied and employee-owned devices and 33 percent say they can use their own mobile devices.

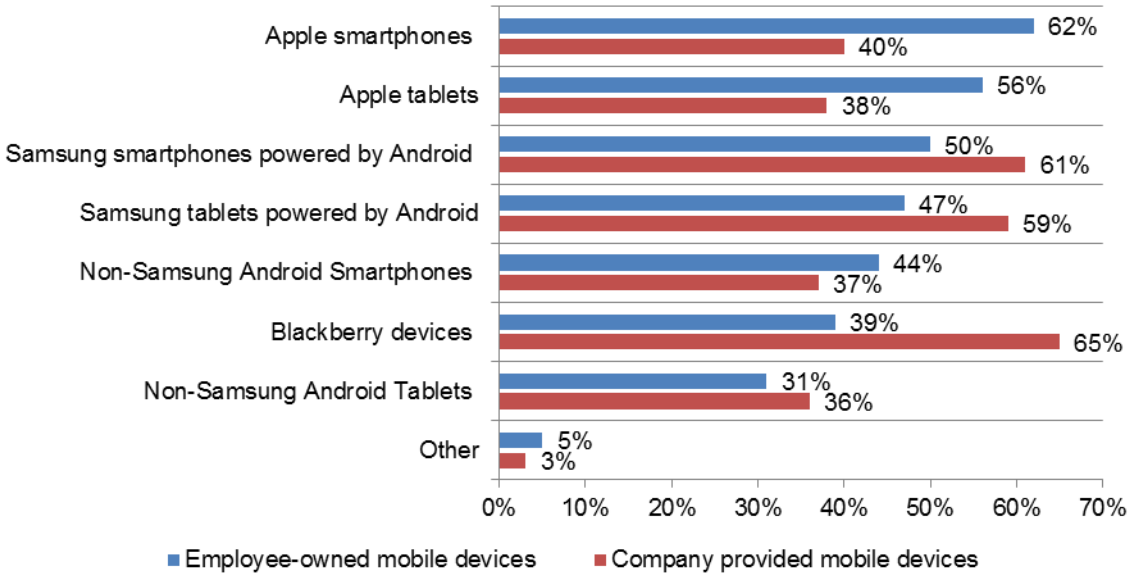
Figure 1. Are employees allowed to access corporate applications with mobile devices?



For convenience and productivity reasons, many employees are using mobile devices to access corporate applications over the Internet. Based on the findings, an average of 57 percent of employees in the organizations represented in this research are using mobile devices, either their own or provided by the company. An average of 44 percent of an organization's employees are using their own devices.

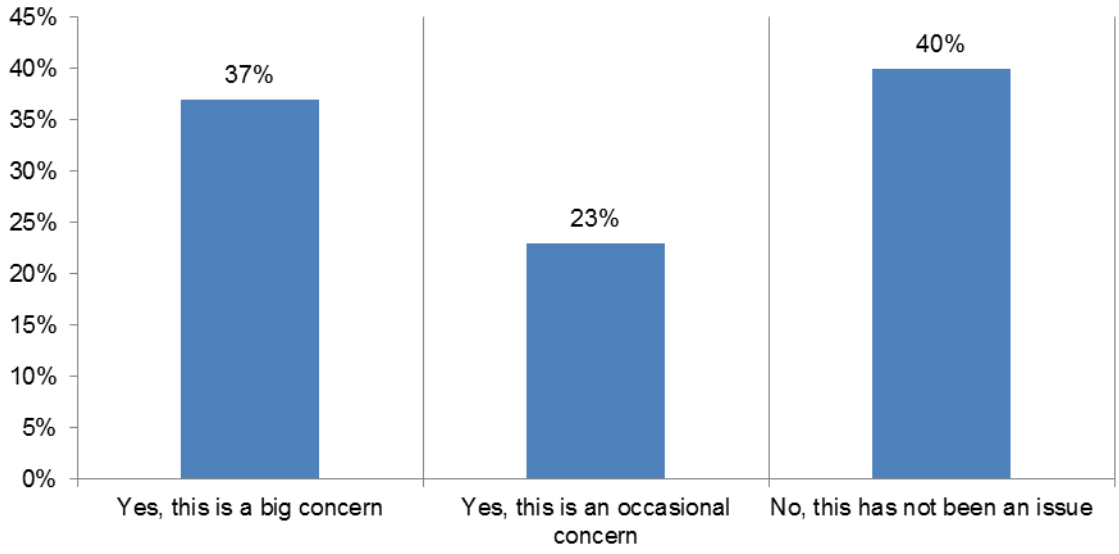
Most popular devices differ for those owned by employees and those provided by the company. Figure 2 reveals Apple smartphones and Apple Tablets are the most popular employee-owned devices supported by companies. For company provided mobile devices, it is the Blackberry device followed by Samsung smartphones powered by Android.

Figure 2. Mobile devices most often supported and used in the workplace



Employee concerns about privacy have limited BYOD deployment. According to Figure 3**,** 37 percent of respondents say worries about privacy and retention of personal data is a big concern, and 23 percent say it is an occasional concern. Forty percent say it is not an issue.

Figure 3. Employee concerns about privacy limits use of employee owned devices



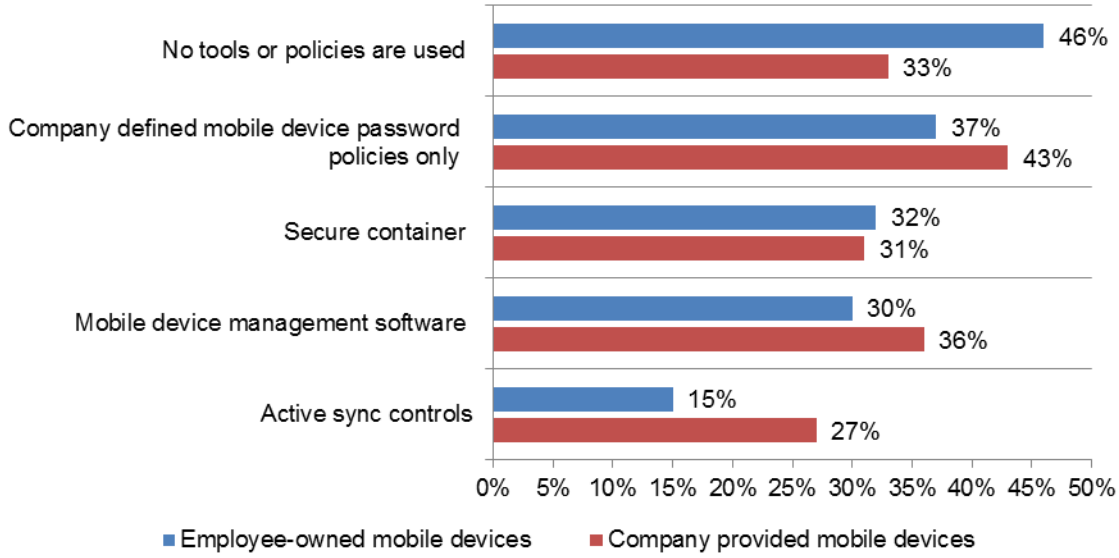
Security tools used to protect company data accessed by employees

BYOD security leaves corporate data vulnerable. According to Figure 4, 46 percent of respondents say no tools or policies are used to protect company data on employee-owned mobile devices. Company defined mobile device password policies are used, according to 37 percent of respondents. Thirty-two percent of respondents say secure container is their solution and 30 percent use mobile device management (MDM) software.

There is more protection for company owned mobile devices. As shown, 33 percent of respondents say no tools are used in contrast to the 46 percent of respondents who say no tools are used for BYOD. A higher percentage of respondents (43 percent) say their organizations use company defined mobile device password policies only. This is also the case for MDM software. Thirty-six percent of respondents say this is the solution used

Figure 4. Security used for employee-owned and corporate provided mobile devices

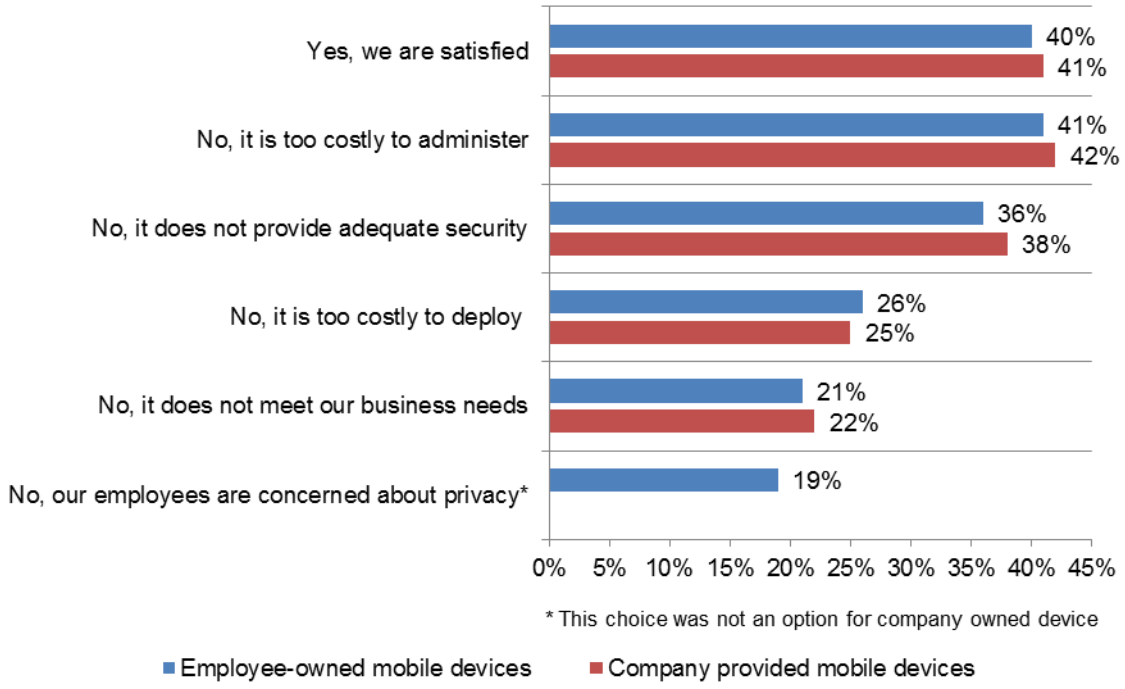
More than one response permitted



Satisfaction with MDM or secure container solutions is similar for both employee-owned and company provided devices. According to Figure 5, 40 percent are satisfied with these solutions for employee-owned mobile devices, and 41 percent are satisfied with their protection of data on company provided devices. The primary reasons for dissatisfaction with these solutions, both employee-owned and company provided mobile devices, are the cost and inadequate security.

Figure 5. Satisfaction with MDM or secure container solution

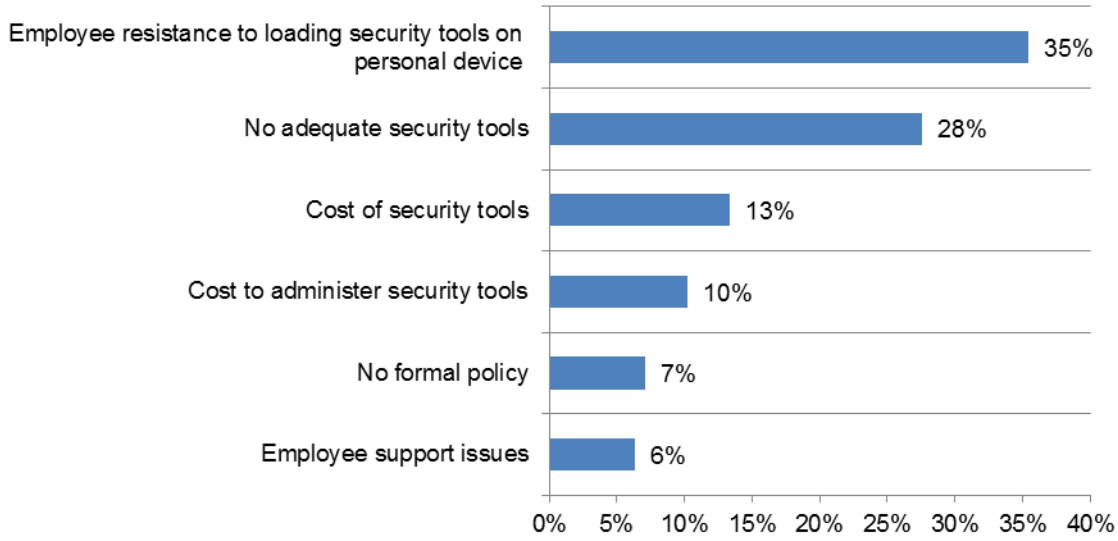
More than one response permitted



Employee resistance to security tools on their personal devices is limiting BYOD. Forty-three percent of respondents say their organizations limit the number of employees allowed to access corporate applications with their own mobile devices.

As shown in Figure 6, the reason for limited deployment, according to 35 percent of respondents, is employees' resistance to loading security tools on personal device. Twenty-eight percent of respondents say there are no adequate security tools.

Figure 6. Why organizations limit access to corporate data

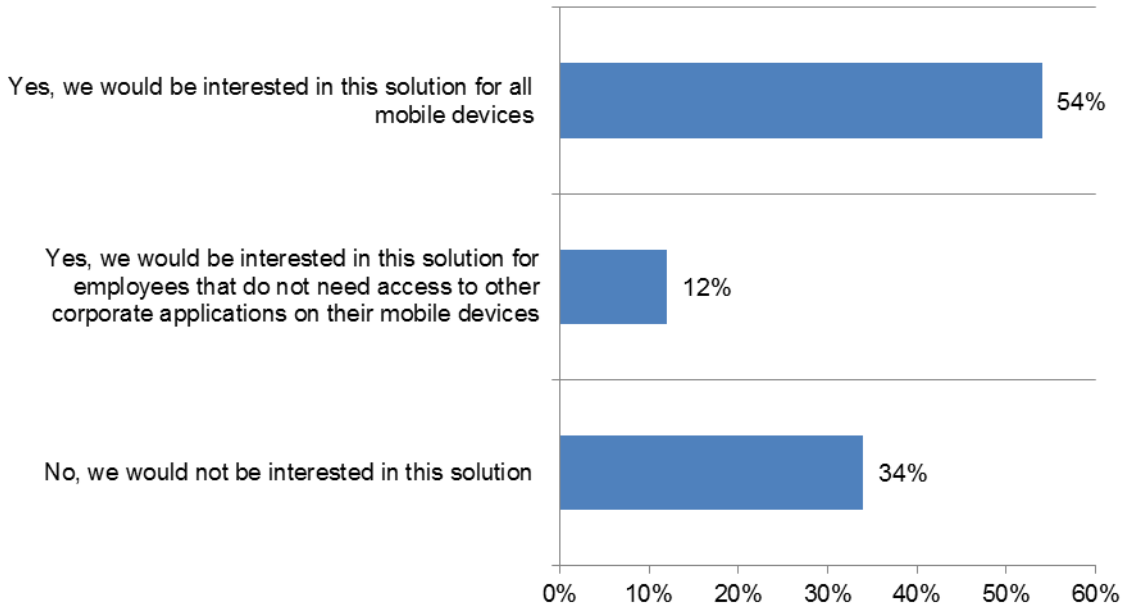


Solutions considered desirable for secure access of corporate applications

Most employees only need access to corporate email, calendar and contacts on mobile devices. Our analysis revealed that on average 62 percent of employees in small and medium-sized organizations only need this type of access. In larger organizations, an average of 51 percent of respondents need such access.

As shown in Figure 7, 54 percent of respondents say they would be interested in a mobile device security solution for all mobile devices that enables employees to access their corporate email, calendar and contacts but never stores any corporate data on their employees' mobile devices. Twelve percent would like the solution for employees that do not need to access sensitive data.

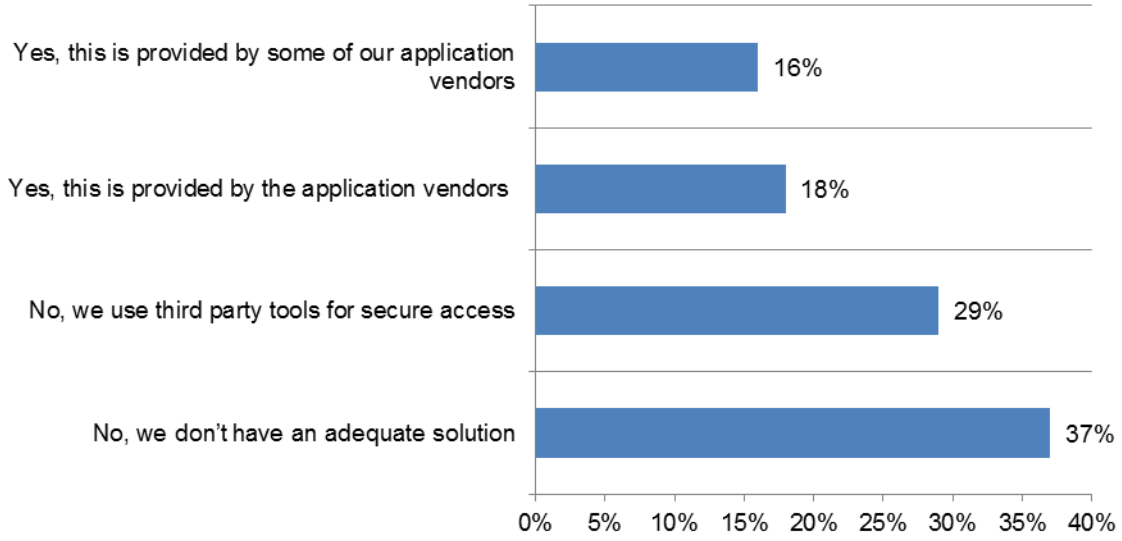
Figure 7. Is there interest in a solution that allows access but does not store data?



Most companies do not have security solutions for devices that have access to corporate applications with sensitive corporate data. According to respondents, an average of 47 percent of employees currently need access to applications other than email, calendar and contacts on mobile devices. These could have sensitive or confidential information in document repository, product pricing, sales order entry, customer and financial data.

Thirty-four percent of respondents (16 percent + 18 percent) say all or some of the application vendors provide security solutions, as shown in Figure 8. Twenty-nine percent say they use third party tools for secure access, and 37 percent say they have no adequate solutions.

Figure 8. Application vendors provide an acceptable way to securely access their application on mobile devices



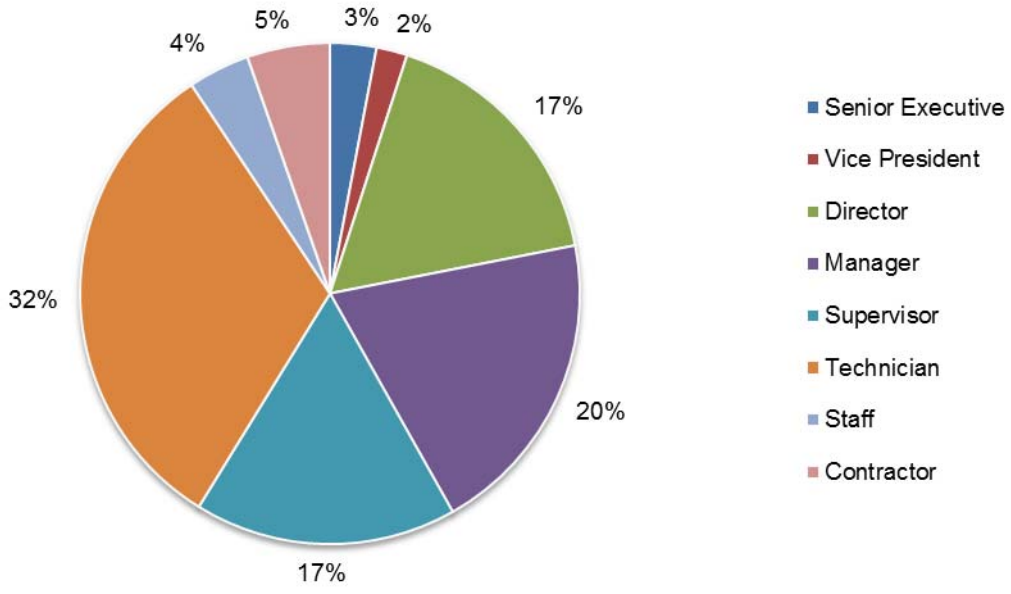
Part 3. Methods

A random sampling frame of 29,839 IT and IT security specialists located in all regions of the United States were selected as participants to this survey. As shown in Table 1, 1,043 respondents completed the survey. Screening and reliability checks removed 148 surveys. The final sample was 895 surveys (or a 3.0 percent response rate).

Table 1. Sample response	Freq	Pct%
Sampling frame	29,839	100.0%
Total returns	1,043	3.5%
Rejected and screened surveys	148	0.5%
Final sample	895	3.0%

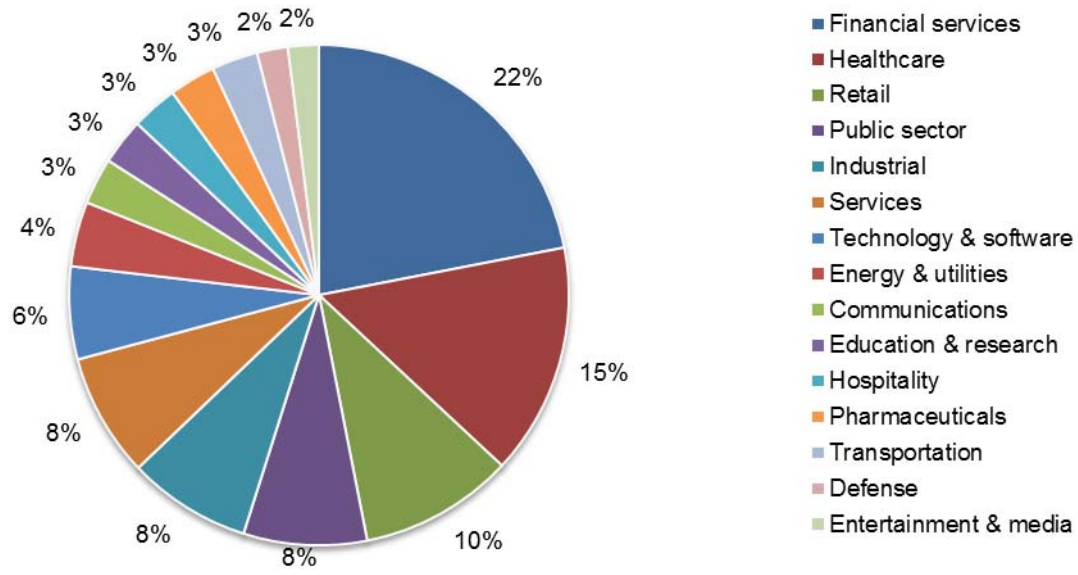
Pie Chart 1 reports the respondent's position level within the organization. By design, 59 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



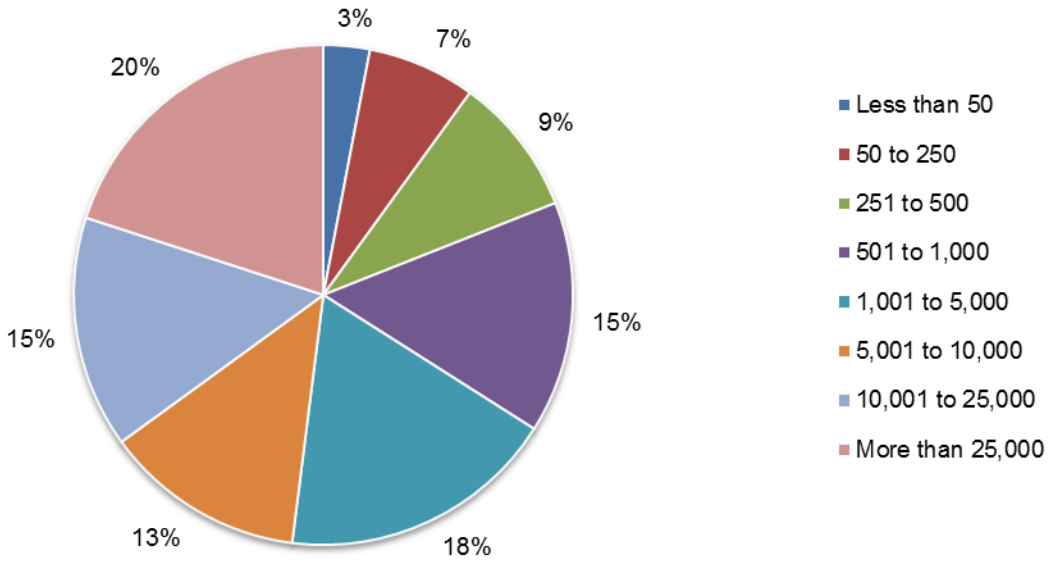
Pie Chart 2 reports a total of 15 industry segments of respondents' organizations. This chart identifies financial services (22 percent) as the largest segment, followed by healthcare (15 percent) and retail (10 percent).

Pie Chart 2. Industry distribution of respondents' organizations



As shown in Pie Chart 3, 66 percent of respondents are from organizations with a global headcount greater than 1,000 employees.

Pie chart 3. Worldwide headcount



Part 4. 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 are IT or IT security specialists. 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 holdout 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 a truthful response.

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 2013.

Sample response	Freq	Pct%
Sampling frame	29,839	100.0%
Total returns	1,043	3.5%
Total screened or rejected surveys	148	0.5%
Final sample	895	3.0%

Part 1. Your role and organization

Q1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	2%
Director	17%
Manager	20%
Supervisor	17%
Technician	32%
Staff	4%
Contractor	5%
Total	100%

Q2. What industry best describes your organization's focus?	Pct%
Financial services	22%
Healthcare	15%
Communications	3%
Defense	2%
Education & research	3%
Energy & utilities	4%
Entertainment & media	2%
Public sector	8%
Hospitality	3%
Industrial	8%
Pharmaceuticals	3%
Retail	10%
Services	8%
Technology & software	6%
Transportation	3%
Other	0%
Total	100%

Q3. What is the worldwide headcount of your organization?	Pct%
Less than 50	3%
50 to 250	7%
251 to 500	9%
501 to 1,000	15%
1,001 to 5,000	18%
5,001 to 10,000	13%
10,001 to 25,000	15%
More than 25,000	20%
Total	100%

Q4. Does your organization allow employees to access corporate applications (email,	Pct%
No (go to Q22)	12%
Yes, with company supplied devices only (go to Q15)	25%
Yes, with employee owned devices only (answer questions Q6-Q14, then go to Q26)	33%
Yes with both company supplied and employee owned devices (go to Q5)	30%
Total	100%

Q5. What percentage of your employees currently access your corporate applications	Pct%
1-10%	9%
11-25%	11%
26- 50%	13%
51-75%	34%
76-100%	33%
Total	100%

Part 2: Employee owned devices

Q6. Which device types do you support for employee owned mobile devices used to	Pct%
Apple smartphones	62%
Apple tablets	56%
Non-Samsung Android Smartphones	44%
Non-Samsung Android Tablets	31%
Samsung smartphones powered by Android	50%
Samsung tablets powered by Android	47%
Blackberry devices	39%
Other	5%
Total	334%

Q7. What percentage of your employees access your corporate applications with	Pct%
1-10%	10%
10-25%	19%
25- 50%	34%
50-75%	19%
75-100%	18%
Total	100%

Q8, How do you protect company data on employee owned mobile devices?	Pct%
Company defined mobile device password policies only (go to Q11)	37%
Mobile device management (MDM) software	30%
Secure container	32%
Active sync controls (go to Q11)	15%
No tools or policies are used (go to Q11)	46%
Total	160%

Q9. Who do you use for MDM or secure container solutions?	Pct%
Good Technology	39%
Mobile Iron	27%
Airwatch	23%
Citrix	31%
FiberLink (MaaS 360)	16%
Other	3%
Total	139%

Q10. Are you satisfied with your MDM or secure container solution?	Pct%
No, it does not meet our business needs	21%
No, it does not provide adequate security	36%
No, our employees are concerned about privacy	19%
No, it is too costly to administer	41%
No, it is too costly to deploy	26%
Yes we are satisfied (go to Q12)	40%
Total	183%

Q11. Are you actively looking for a new mobile device security solution for employee	Pct%
No	44%
Yes, we are looking now	35%
Yes, in the next 6-12 months	11%
Yes, in the next 12-24 months	10%
Total	100%

Q12. Has the use of employee owned mobile devices been limited due to employee	Pct%
Yes, this is a big concern	37%
Yes this is an occasional concern	23%
No, this has not been an issue	40%
Total	100%

Q13. Do you limit the number of employees that are allowed to access your corporate	Pct%
Yes	43%
No (go to Q15)	57%
Total	100%

Q14. What is the primary reason you limit the number employees allowed to access	Pct%
No formal policy	7%
No adequate security tools	28%
Cost of security tools	13%
Cost to administer security tools	10%
Employee support issues	6%
Employee resistance to loading security tools on personal device	35%
Other	0%
Total	100%

Part 3: Company owned devices

Q15. What device types do you support for company owned mobile devices used to	Pct%
Apple smartphones	40%
Apple tablets	38%
Non-Samsung Android Smartphones	37%
Non Samsung Android Tablets	36%
Samsung smartphones powered by Android	61%
Samsung tablets powered by Android	59%
Blackberry devices	65%
Other	3%
Total	339%

Q16. What percentage of employees access your corporate applications with company	Pct%
1-10%	8%
11-25%	9%
26- 50%	11%
51-75%	33%
76%- 100%	39%
Total	100%

Q17. How do you protect company data on company owned mobile devices?	Pct%
Company defined mobile device password policies only (go to Q20)	43%
Mobile device management (MDM) software	36%
Secure container	31%
Active sync control (go to Q20)	27%
No tools are used (go to Q20)	33%
Total	170%

Q18. Who do you use for MDM or secure container solutions?	Pct%
Good Technology	42%
Mobile Iron	30%
Airwatch	21%
Citrix	33%
Fiberlink (MaaS 360)	20%
Other	2%
Total	148%

Q19. Are you satisfied with your MDM or secure container solutions?	Pct%
No, it does not meet our business needs	22%
No, it does not provide adequate security	38%
No, it is too costly to administer	42%
No, it is too costly to deploy	25%
Yes we are satisfied (go to Q21)	41%
Total	168%

Q20. Are you actively looking for a new mobile device security solution for company	Pct%
No	35%
Yes, we are looking now	50%
Yes, in the next 6-12 months	8%
Yes, in the next 12-24 months	7%
Total	100%

Q21. Does your organization intend to promote the increased use of employee owned	Pct%
Yes, we are doing that now	19%
Yes we plan to start in the next 6-12 months	8%
Yes we plan to start in the next 12-24 months	9%
No, we are happy with the current usage	20%
No we don't intend to permit employees to use personal mobile devices	44%
Total	100%

Go to Q26

Part 4: No access with mobile devices.

Q22. Do you not allow employees to use mobile devices to access any of your corporate applications due to lack of security?	Pct%
Yes	61%
No (go to Q24)	39%
Total	100%

Q23. What is your primary concern about securing corporate data on mobile devices?	Pct%
Cost of security solutions	22%
Deployment and administration of security solutions	12%
No business requirement	9%
Effectiveness of available security solutions	6%
Not a business priority	51%
Total	100%

Q24. Does your organization plan to allow employees to access your corporate applications with mobile devices in the future?	Pct%
No, we have no plans (End)	44%
Yes, in the next 12 months	11%
Yes in the next 24 months	8%
Yes, but don't a have a plan yet	37%
Total	100%

Q25. Which mobile devices will you allow employees to use to access corporate applications over the Internet?	Pct%
Employee owned mobile devices	35%
Company owned devices	37%
Both employee and company owned mobile devices	28%
Total	100%

Part 5: Secure access to email, calendar and contacts solution

Q26. What percentage of your employees need access only to corporate email, calendar and contacts on mobile devices?	Pct%
0% (go to Q34)	9%
1-20%	10%
21-40%	16%
41-60%	19%
61-80%	12%
81-100%	34%
Total	100%

Q27. Would your company be interested in a mobile device security solution that enables employees to access their corporate email, calendar and contacts, but never stores any corporate data on your employee's mobile devices?	Pct%
Yes we would be interested in this solution for all mobile devices (go to 29)	54%
Yes we would be interested in this solution for employees that do not need access to other corporate applications on their mobile devices (go to 29)	12%
No we would not be interested in this solution for my organization	34%
Total	100%

Q28. Why would your organization not be interested in this type of security solution? Please select all that apply.	Pct%
Our employees need access to email and calendar on their mobile devices when not connected to the internet	12%
We need a security solution that provides secure access to other corporate applications	14%
We are happy with our current mobile device security solution	36%
We have just signed a long term contract with a mobile device security vendor	25%
We don't think we need security for email and calendar on mobile devices	9%
We don't want to have to manage a security solution that is only for email, calendar and contacts on mobile devices	19%
We don't have any budget allocated	50%
Other (please specify)	0%
Total	165%

Q29. Would this security solution be acceptable for all mobile device owners?	Pct%
Employees owned devices only	13%
Company owned devices only	30%
Both company and employee owned devices.	57%
Total	100%

Q30. Would this security solution be acceptable for all types of mobile devices?	Pct%
Smartphones only	18%
Tablets only	9%
Both tablets and smart phones	73%
Total	100%

Q31. What implementation model would be acceptable for this security solution?	Pct%
Cloud based service, which will be used to securely retrieve and display emails to end users, but will not permanently store email.	34%
Virtual appliance solution that is run in your data center by your staff, where email is only ever stored on your internal network	26%
Either solution is acceptable	40%
Total	100%

Q32. Would your organization be interested in purchasing a security solution that provided secure access to email, calendar and contacts on mobile devices, but never stores any of that corporate data on the mobile device?	Pct%
Yes	53%
No	47%
Total	100%

Q33. When would your organization be interested in purchasing a solution that provides secure access to email, calendar and contacts on mobile devices?	Pct%
Now	40%
In the next 6 months	18%
In the next 6- 12 months	16%
In the next 12-24 months	11%
Greater than 24 months	15%
Total	100%

Q34. What percentage of your employees will need access to other applications on mobile devices within the next 24 months?	Pct%
1-20%	5%
21-40%	18%
41-60%	34%
Greater than 60%	43%
Total	100%

Q35. What percentage of your employees currently need access to other apps besides email, calendar and contacts on mobile devices?	Pct%
0% (End)	12%
1-20%	12%
21-40%	19%
41-60%	21%
61-80%	18%
81-100%	18%
Total	100%

Q36. What other applications do your employees need to access with mobile devices (smartphone or tablet)? Please select all that apply.	Pct%
Sales Order entry	46%
Customer data	40%
Product Pricing	49%
Financial data	38%
Document repository	51%
Other	2%
Total	226%

Q37. Do the application vendors provide an acceptable way to securely access their application (other than email, calendar and contacts) on mobile devices)?	Pct%
Yes, this is provided by the application vendors	18%
Yes, this is provided by some of our application vendors	16%
No, we use third party tools for secure access	29%
No, we don't have an adequate solution	37%
Total	100%

Q38. Would employees need to access any of these other applications (besides corporate email, calendar and contacts) on their smartphones?	Pct%
No (End)	51%
Yes	49%
Total	100%

Q39. What other applications do your employees need to access with their smartphones? Please select all that apply.	Pct%
Sales Order entry	44%
Customer data	38%
Product Pricing	39%
Financial data	28%
Document repository	46%
Other	3%
Total	198%

Q40. What percent of your employees need access to other apps besides email, calendar and contacts with their smartphone?	Pct%
0%	10%
1-20%	21%
21-40%	26%
41-60%	20%
61-80%	15%
80-100%	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.