



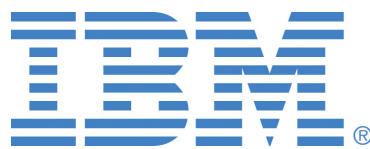
# The State of Mobile Application Insecurity

---

**Sponsored by IBM**

Independently conducted by Ponemon Institute LLC

Publication Date: February 2015



## The State of Mobile Application Insecurity

Ponemon Institute, February 2015

### Part 1. Introduction

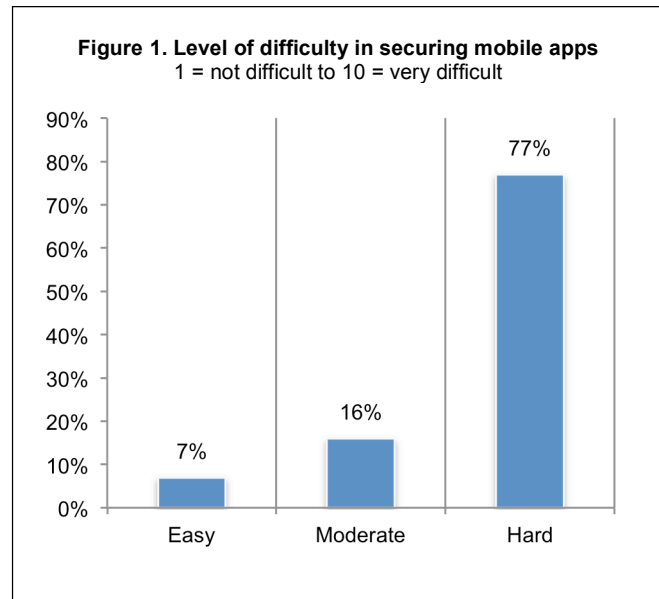
We are pleased to present the findings of *The State of Mobile Application Insecurity* sponsored by IBM. The purpose of this research is to understand how companies are reducing the risk of unsecured mobile apps in the workplace.

Ponemon Institute surveyed 640 individuals involved in the application development and security process in their organizations on the following topics:

- Why mobile application security eludes many organizations.
- The difficulty in controlling employees' risky behaviors.
- Are organizations taking the right steps to secure mobile apps?

As shown in Figure 1, 77 percent of respondents rate the level of difficulty in securing apps as very high. Only 7 percent of respondents believe it is easy or a "piece of cake."

Following are six findings that reveal why the state of mobile application is insecure:



1. The "rush to release" results in mobile apps that can have vulnerabilities. Sixty-five percent of respondents say the security of mobile apps is sometimes put at risk because of customer demand or need. Thirty-eight percent of respondents say their organizations do not scan for vulnerabilities.
2. Mobile apps are often tested infrequently and too late. Most respondents (55 percent) say they do not test apps or they are unsure. Mobile apps are rarely tested in production. Most often they are tested in development or post-development.
3. Malware-infected mobile apps and devices will increase. Sixty-one percent of respondents say their organizations will need to address the growing risk of malware-infected mobile apps. However, only 29 percent of respondents say their organization has ample resources to prevent the use of vulnerable or malware-infected mobile apps.
4. Not enough is spent on mobile app security. While an average of \$34 million is spent annually on mobile app development, only 5.5 percent, or \$2 million, is allocated to mobile app security.
5. There is a dearth of trained and expert security professionals. Only 41 percent of respondents say their organization has sufficient mobile application security expertise.
6. Organizations lack policies that provide guidance on employees' use of mobile apps. The findings reveal most employees' are "heavy users of apps", but 55 percent of respondents say their organization does not have a policy that defines the acceptable use of mobile apps in the workplace.

## Part 2. Key findings

In this section, we provide a detailed analysis of the findings of this study. We have organized the report according to the following themes:

- Why mobile application security eludes many organizations.
- The difficulty in controlling employees' risky behaviors.
- Are organizations taking the right steps to secure mobile apps?

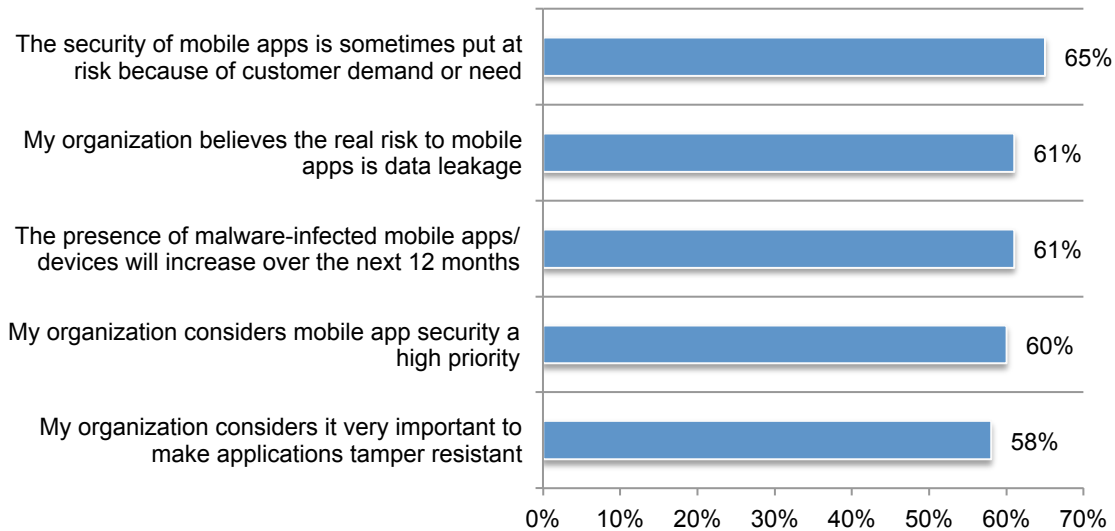
### Why mobile application security eludes many organizations.

**Customer needs and demand often affect mobile application security.** Figure 2 reveals the perceptions respondents have about the state of mobile application security in their organizations. Sixty-five percent strongly agree or agree that the security of mobile apps is sometimes put at risk because of customer demand or need. The “rush to release” phenomenon challenges an organization’s ability to stop the risks of data leakage and malware.

The presence of malware-infected mobile apps/devices will increase over the next 12 months (61 percent) and a similar percentage believes the real risk to mobile apps is data leakage. Because of these concerns, 60 percent say their organization considers mobile app security a high priority. Further, 58 percent say their organizations consider it very important to make applications tamper resistant.

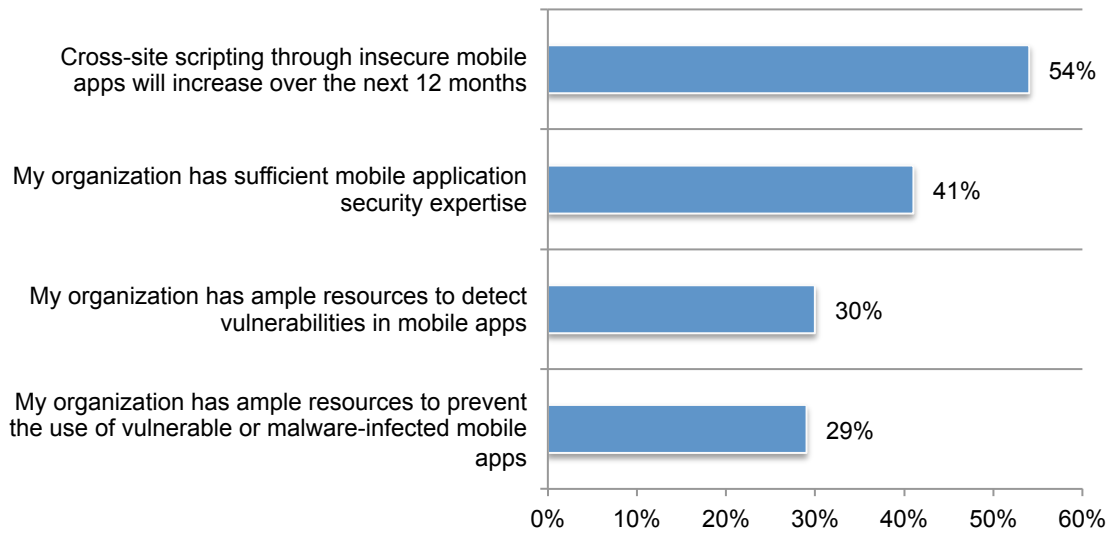
**Figure 2. Reasons why mobile application security is difficult to achieve**

Strongly agree and agree responses combined



**Expertise and budget are needed to reduce mobile app security risks.** According to Figure 3, 54 percent of respondents are concerned that cross-site scripting through insecure mobile apps will increase over the next 12 months. However, only 41 percent believe their organization has sufficient mobile application security expertise. Moreover, only 30 percent believe their organization has ample resources to detect vulnerabilities in mobile apps and 29 percent say resources are available to prevent the use of vulnerable or malware-infected mobile apps.

**Figure 3. Why mobile apps are at risk**  
Strongly agree and agree responses combined



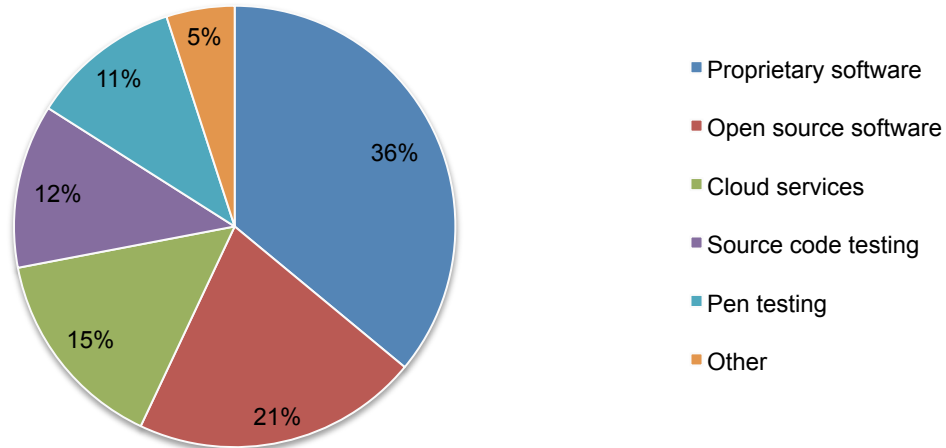
**Are enough resources available to deal with mobile app security?** In this study, we asked respondents how much their organizations spend on mobile app development each year in terms of technologies, personnel, managed or outsourced services and other cash outlays. As shown in Table 1, an average of \$34 million is spent on mobile app development.

We also asked what percent of the budget for mobile app development is dedicated to mobile app security. The dollar amount falls dramatically to only \$2 million for mobile app security or only an average of 5.5 percent of the total budget for mobile app development.

<b>Table 1. Annual mobile app development &amp; security budget</b> Extrapolated Average	
Annual budget for mobile app development	\$33,812,500
Average percentage of annual budget spent on mobile app security	5.5%
Estimated average spent on mobile app security	\$1,859,688

Most spending is allocated to reducing vulnerabilities and threats from proprietary software (36 percent) followed by open source software (21 percent), as shown in Figure 4. Only 11 percent is spent on pen testing to reduce threats from insecure mobile apps.

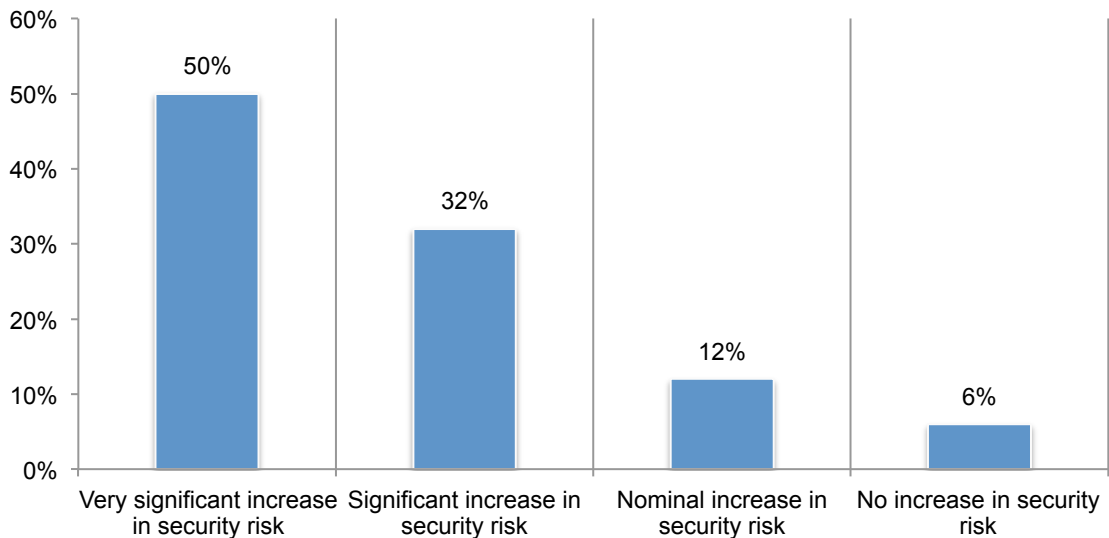
**Figure 4. Allocation of spending for application security categories**



**The difficulty in controlling employees’ risky behaviors**

**If an organization wants to reduce security risks, then control employees’ use of mobile apps.** As shown in Figure 5, 82 percent of respondents say mobile apps in the workplace has very significantly (50 percent) or significantly (32 percent) increased security risks.

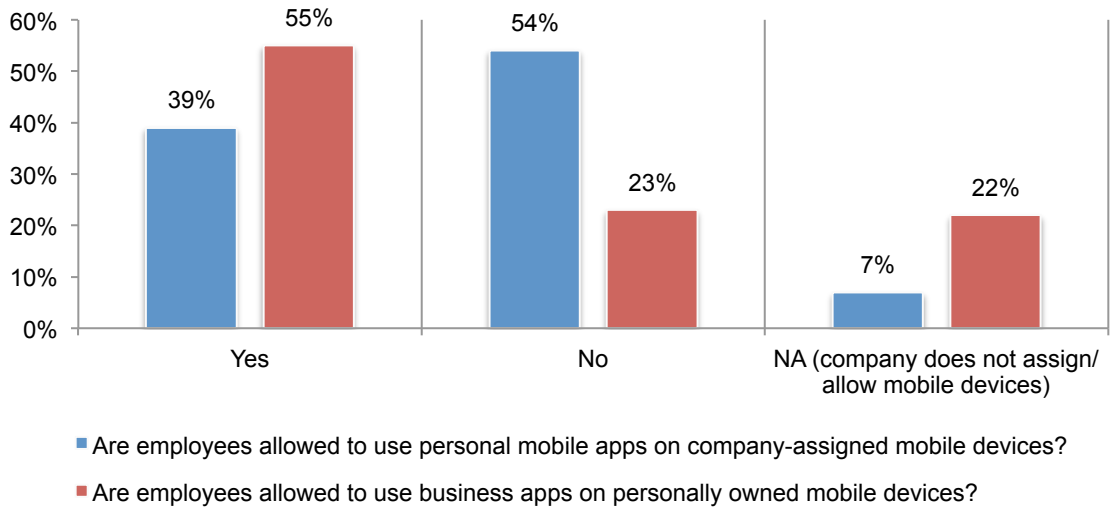
**Figure 5. How has the use of mobile apps by employees affected your organization’s security posture?**



**More organizations need to have a policy on the acceptable use of mobile apps.** Most respondents say employees' use of mobile apps is very heavy (32 percent of respondents) or heavy (34 percent). However, more than half of respondents (55 percent) say their organization does not have a policy that defines the acceptable use of mobile apps in the workplace.

According to Figure 6, 39 percent of respondents say they are allowing employees to use their personal mobile apps on company-assigned mobile devices such as smartphones and tablets and 55 percent say employees are permitted to use and download business apps on their personally owned devices (BYOD).

**Figure 6. Does your organization permit personal mobile apps on company assigned mobile devices and the use of business apps on personal devices?**

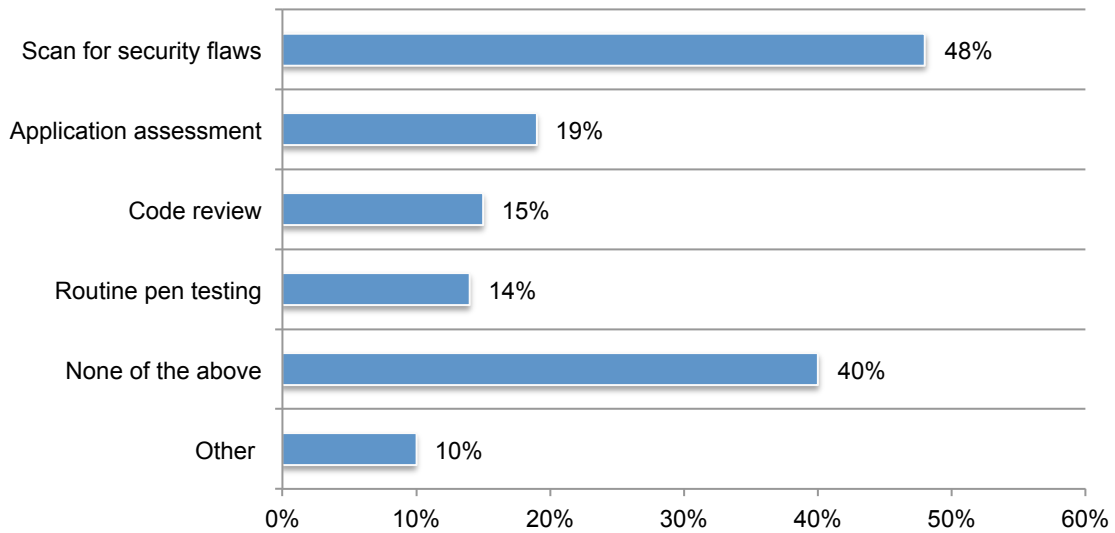


**Can an organization’s app store reduce the use of unsecured mobile apps?** Only 30 percent of respondents say their organization has an app store. Sixty-seven percent of respondents admit that even if they have an app store, employees can use mobile apps from other sources. Fifty-one percent say employees are permitted to download apps from the organizations’ app store onto personally owned mobile devices.

When asked what techniques are used to vet mobile apps for security in the app store, 48 percent of respondents say they scan for security flaws. However, 40 percent are not taking any of the precautions shown in Figure 7.

**Figure 7. What security techniques are used to vet mobile apps in an organization’s app store for security?**

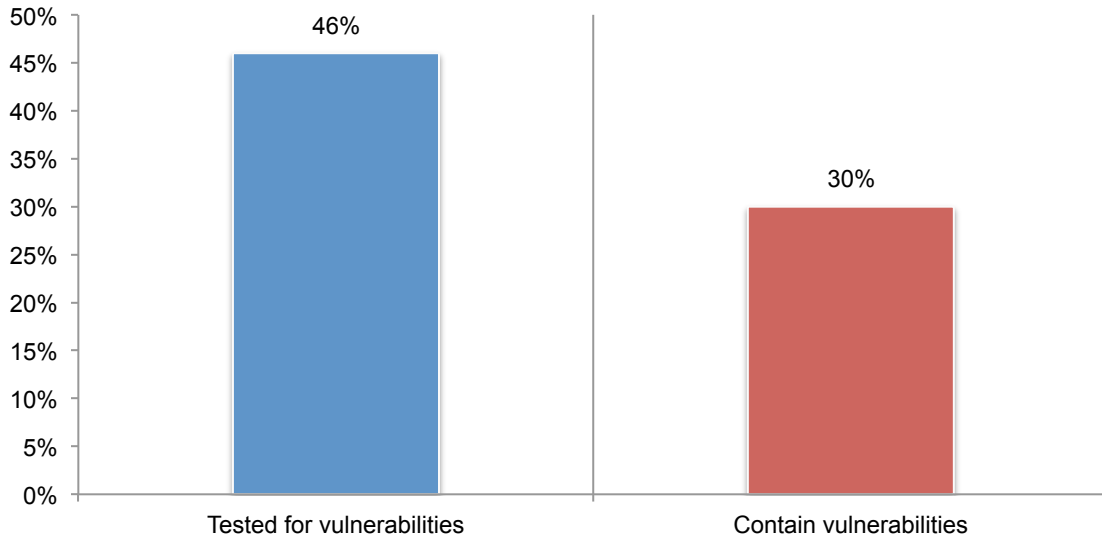
More than one response permitted



**Are organizations taking the right steps to secure mobile apps?**

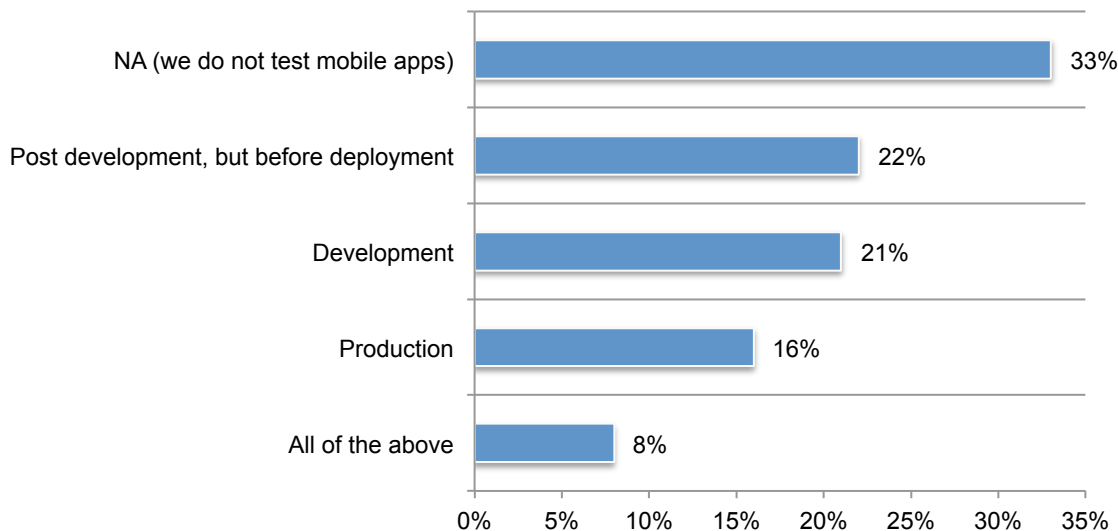
**More mobile apps need testing.** As shown in Figure 8, on average an organization tests less than half of their mobile apps. But of those tested, 30 percent contain vulnerabilities. The obvious implication is that more testing would reduce risks and prevent the use of unsecured mobile apps in the workplace.

**Figure 8. Extrapolated average of mobile apps tested for vulnerabilities & percentage with vulnerabilities**



**Mobile apps often tested too late.** On average, respondents say their organizations have about 105 mobile apps in use today and an average of only 36 percent are mission critical. This means many apps are not needed by employees to do their work. As shown in Figure 9, 33 percent of respondents say their organizations do not test mobile apps at all. Rarely are they tested during production. Most often they are tested in the deployment (22 percent) or in development (21 percent) stage.

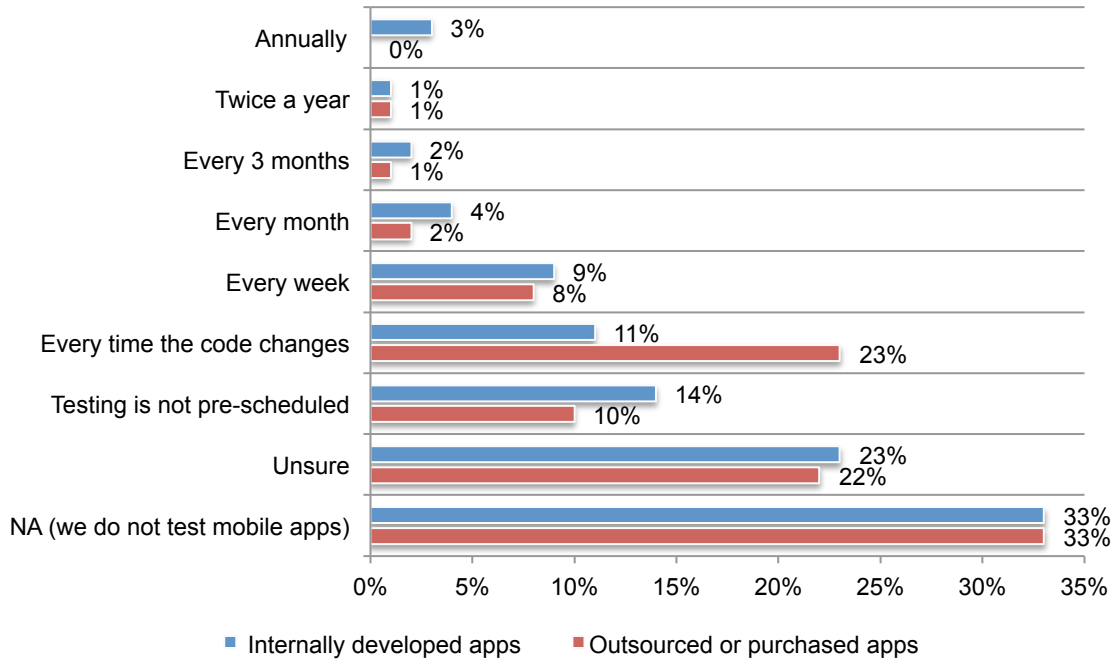
**Figure 9. At what stage are mobile apps tested?**





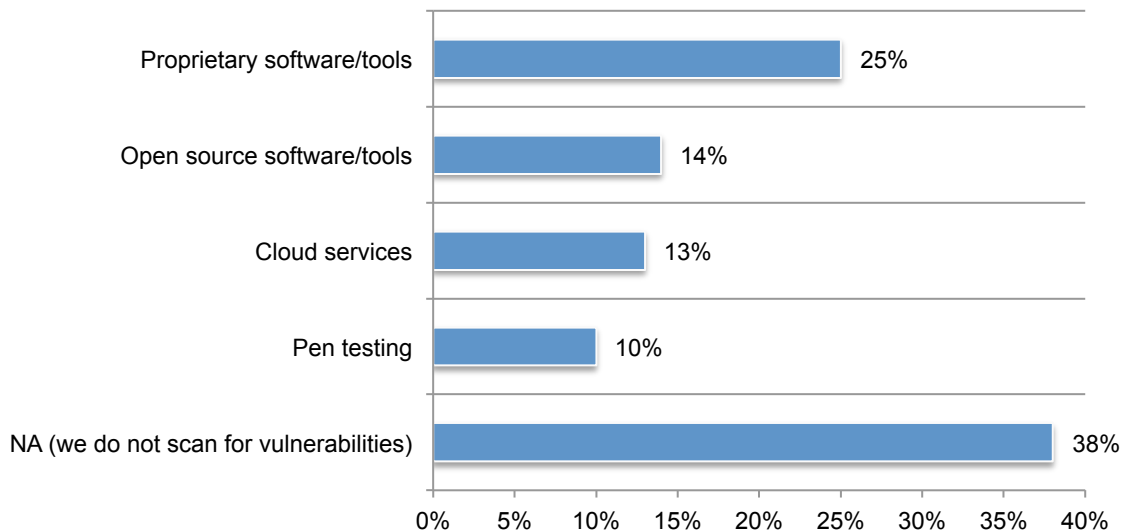
**How frequent does testing of apps occur?** Most respondents say their organization does not test internally developed apps or outsourced or purchased apps, as shown in Figure 10. Even if they do test, respondents are not certain when testing occurs (23 percent for internally developed apps) followed by no pre-scheduled testing (14 percent). In the case of purchased or outsourced apps, most testing takes place every time the code changes (23 percent). However, 22 percent of respondents are unsure when testing takes place.

**Figure 10. How often are internally developed & outsourced or purchased apps tested?**



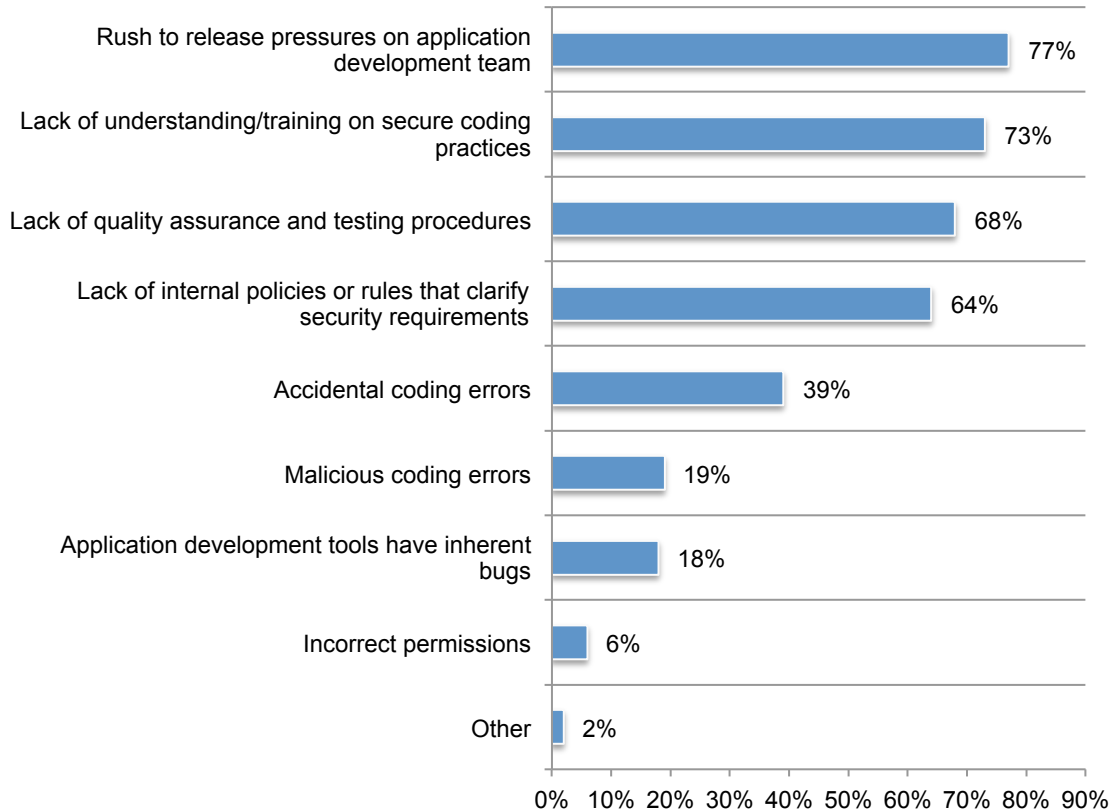
**Many organizations are not scanning for vulnerabilities.** Thirty-eight percent of respondents say their organizations do not scan for vulnerabilities. If they do scan, they mostly use proprietary software or tools (25 percent of respondents) or open source software or tools (14 percent of respondents).

**Figure 11. How does your organization scan code for vulnerabilities?**



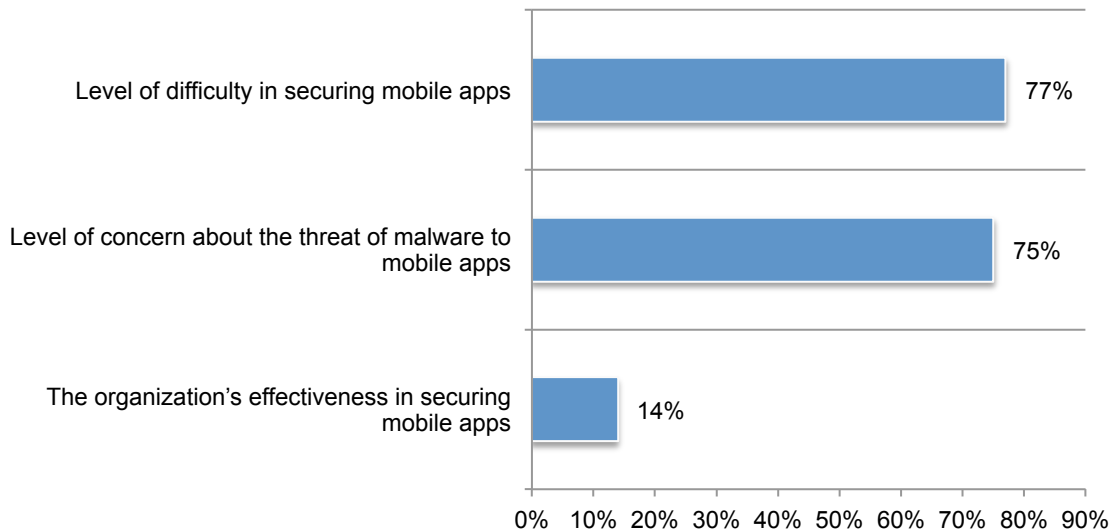
**Rush to release and lack of training makes mobile apps insecure.** The practices and policies of organizations are to blame for mobile apps that contain vulnerable code. Figure 12 reveals 77 percent of respondents say it is the pressure to release apps before testing for vulnerable code followed by 73 percent who lack understanding or training on secure coding practices. A lack of quality assurance and testing procedures (68 percent of respondents) and internal policies or rules that clarify security requirements (64 percent of respondents) are also to blame.

**Figure 12. Why mobile apps contain vulnerable code**



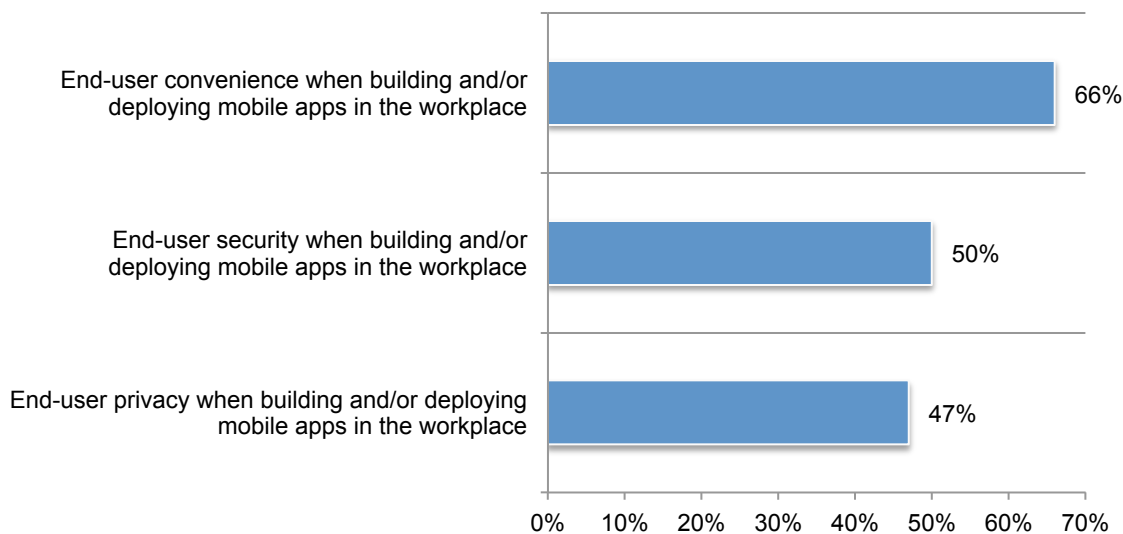
**Effectiveness in securing mobile apps is low.** Respondents rate the level of difficulty in securing mobile apps and concern about the threat of malware to mobile apps as very difficult (77 percent and 75 percent, respectively). However, organizations lack the ability to secure mobile apps and stop malware. Only 14 percent of respondents rate their organizations' effectiveness as high, according to Figure 13.

**Figure 13. Concern about threats is rated high but effectiveness in securing mobile apps is rated low** On a scale of 1 = least difficult, least concern, least effective to 10 = most difficult, most concern and most effective



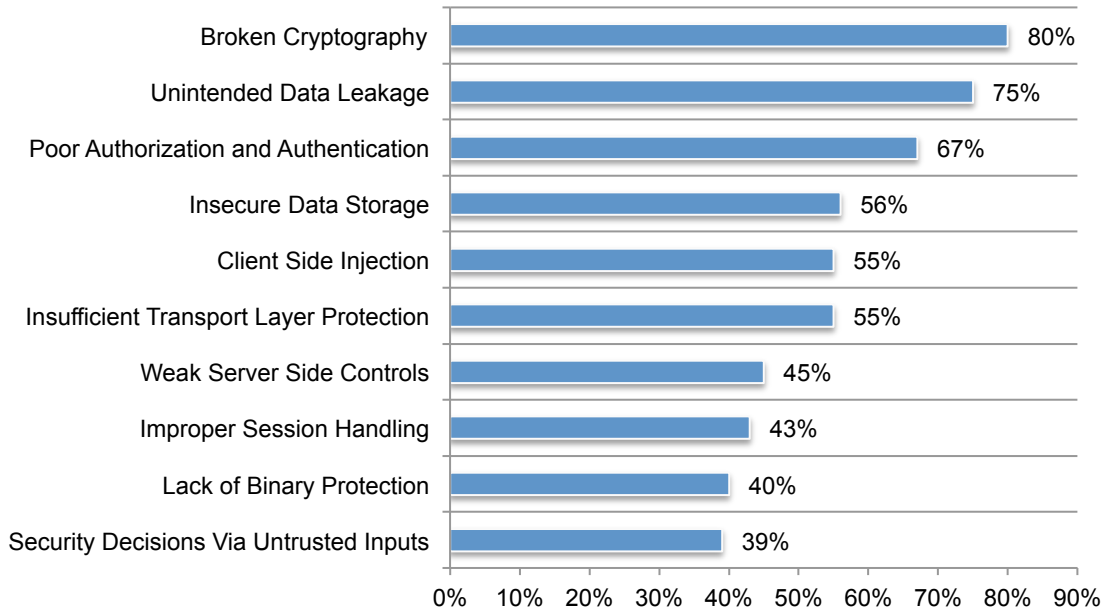
**Keeping the end-user happy is key.** As shown in Figure 14, 66 percent of respondents rate the importance of end-user convenience when building and/or deploying mobile apps as very important and important. Fifty percent of respondents say security is very important and important and less than half (47 percent of respondents) say end-user privacy is very important and important.

**Figure 14. End-user convenience is most important**  
Very important and important responses combined



**To reduce mobile app risks, do organizations follow guidance from the Open Web Application Security Project (OWASP)?** Forty percent of respondents say their organizations do follow the top 10 mobile app security risks. Figure 15 shows the difficulty in minimizing the top 10 mobile app security risks. The most difficult risk to minimize, according to 80 percent of respondents is broken cryptography followed by unintended data leakage (75 percent) and poor authorization and authentication (67 percent). The least difficult is security decisions via untrusted inputs.

**Figure 15. How difficult is it to minimize the OWASP top 10 mobile app security risks?**  
Difficult and very difficult responses combined



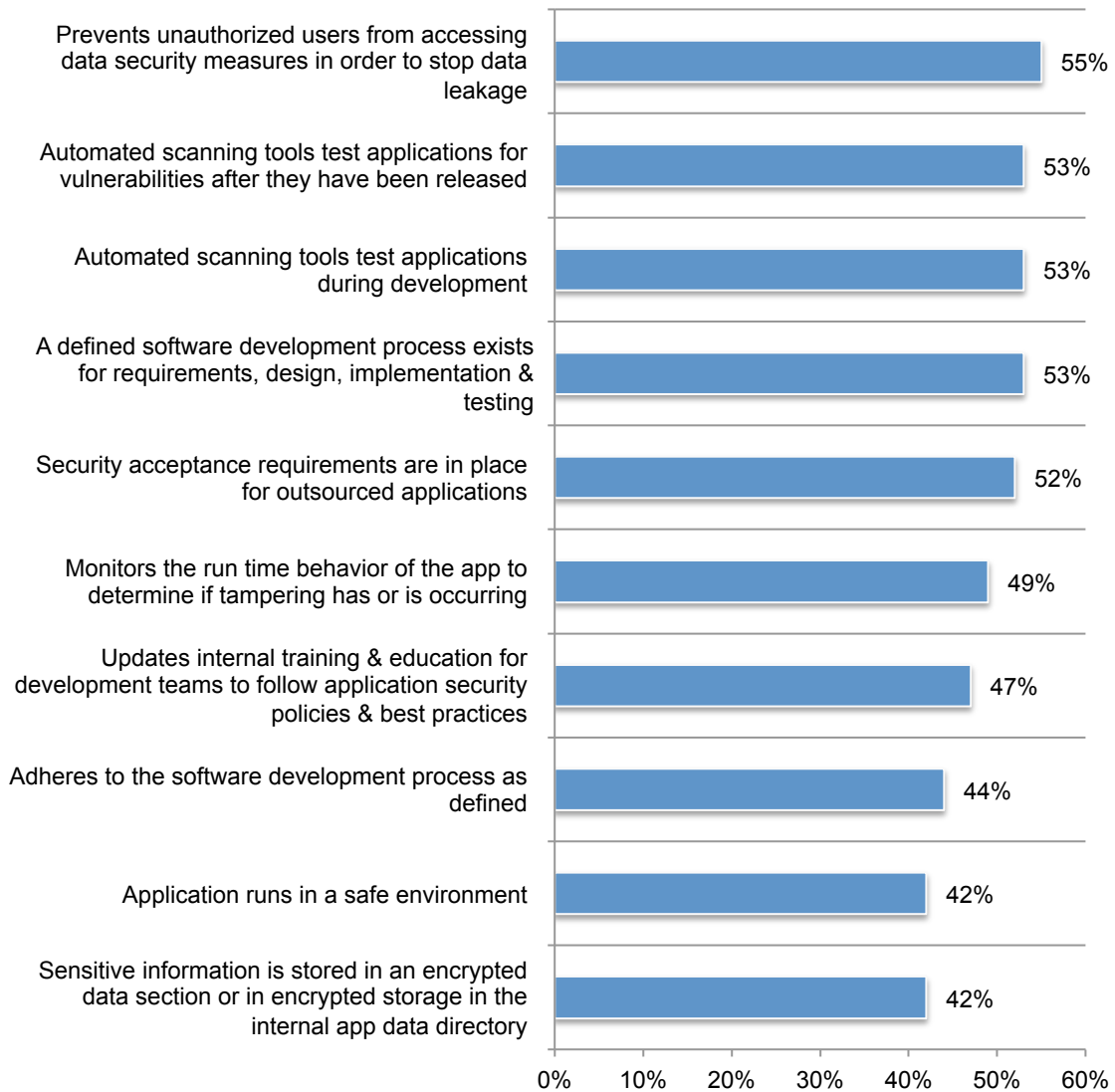
**The most frequent practices for securing the application development process.**

Respondents were asked to rate the practices they most often follow in standards and compliance, secure coding and testing and assessment.

Figure 16 presents the top ten practices from these areas. Because data leakage has been identified as a significant risk to mobile app security, 55 percent of respondents say a priority is to prevent unauthorized users from accessing data security measures to stop data leakage. A similar percentage of respondents (53 percent) say their organizations use automated scanning tools to test applications for vulnerabilities during development and after they have been released.

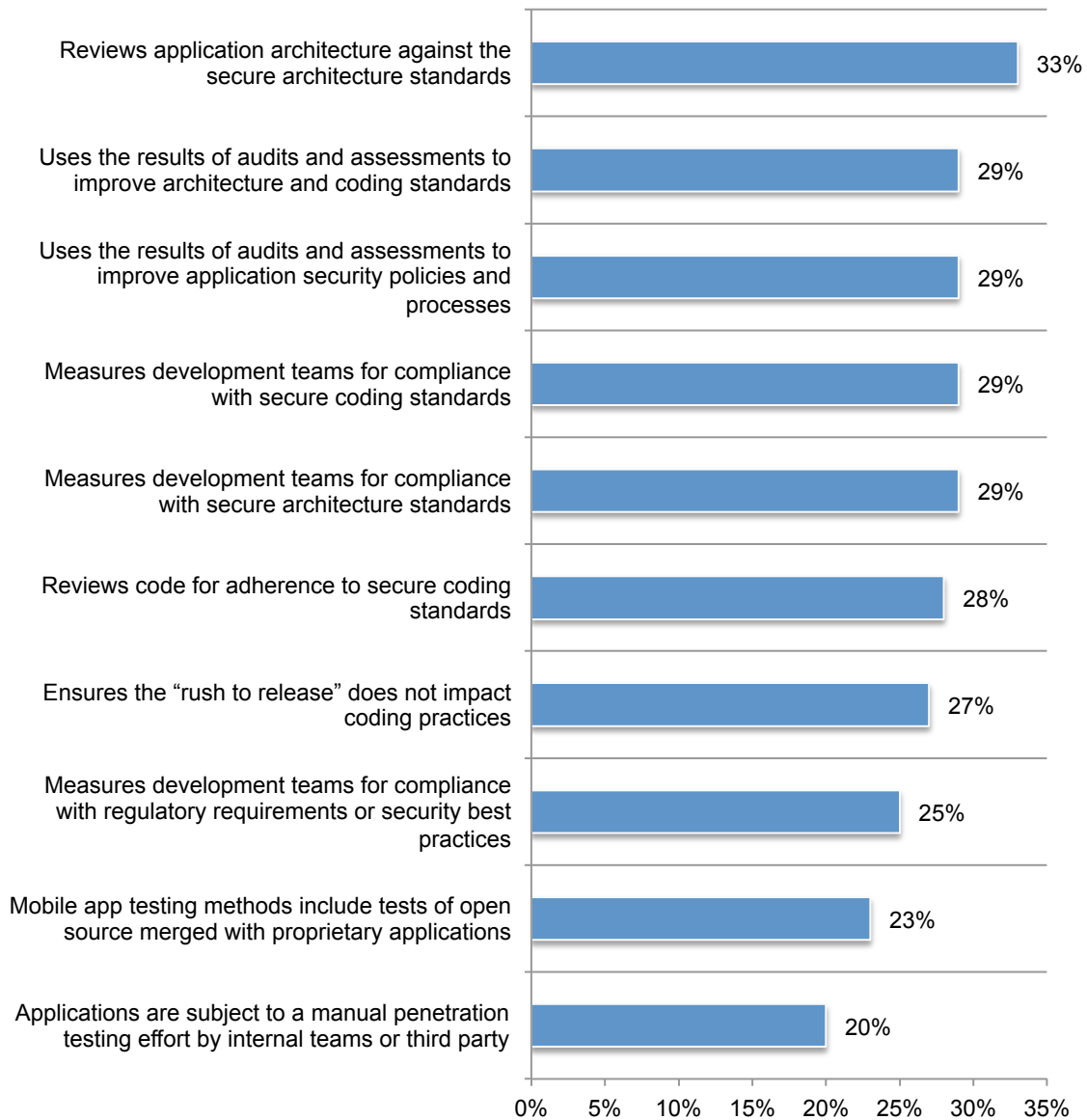
**Figure 16. The 10 most frequently used practices to secure mobile apps**

More than one response permitted



**Practices not often followed for securing the application development process.** While the previous figure revealed the practices most favored by respondents, Figure 17 lists the practices not often followed. Based on the risks to mobile app security certain practices should be at the top of the list. Specifically, only 27 percent say their organization ensures the “rush to release” does not impact coding practices and 29 percent say development teams are not often measured against secure coding and architecture standards.

**Figure 17. The 10 least used practices for securing mobile apps**  
More than one response permitted



### **Part 3. Conclusion**

For a variety of reasons, companies find it difficult to improve the security of their mobile applications. This study reveals the vulnerabilities and areas of greatest risk. Following are some recommendations to improve your organization's state of mobile application insecurity.

- Testing of mobile apps should be conducted frequently. The findings reveal many organizations are not testing apps. They are rarely tested in production.
- Ensure the “rush to release” does not impact coding practices.
- Conduct internal training and education programs for development teams to follow application security policies and best practices.
- Increase the budget for mobile application security. The average budget is insufficient to have the technologies and expertise necessary to secure mobile apps.
- Create policies and procedures to control employees' risky behaviors. Most employees in the companies represented in this study are “heavy users of apps” but very often there are no policies that define the acceptable use of mobile apps in the workplace.

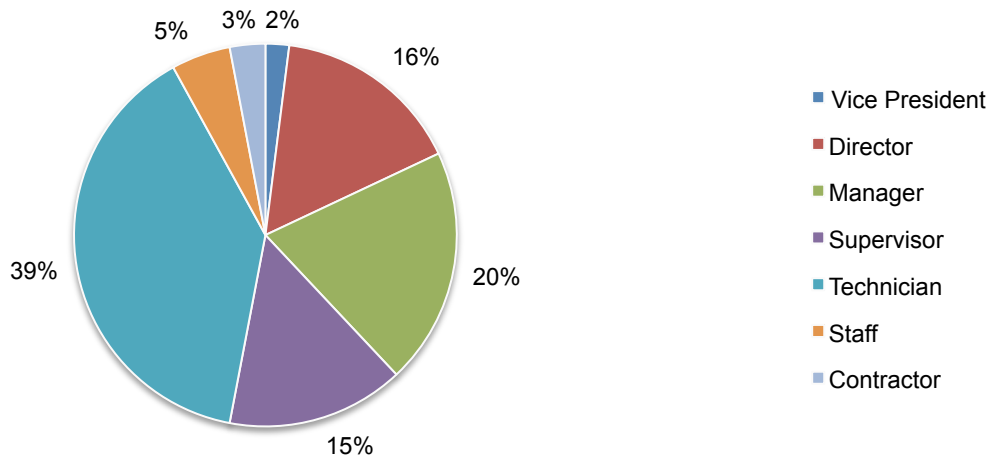
## Part 4. Methods

A sampling frame composed of 19,890 IT and IT security practitioners located in the United States and involved in their company’s application development and security process were selected for participation in this survey. As shown in the Table 1, 707 respondents completed the survey. Screening removed 67 surveys. The final sample was 640 surveys (or a 3.2 percent response rate).

<b>Table 1. Sample response</b>	<b>Freq</b>	<b>Pct%</b>
Total sampling frame	19,890	100.0%
Total returns	707	3.6%
Rejected and screened surveys	67	0.3%
Final sample	640	3.2%

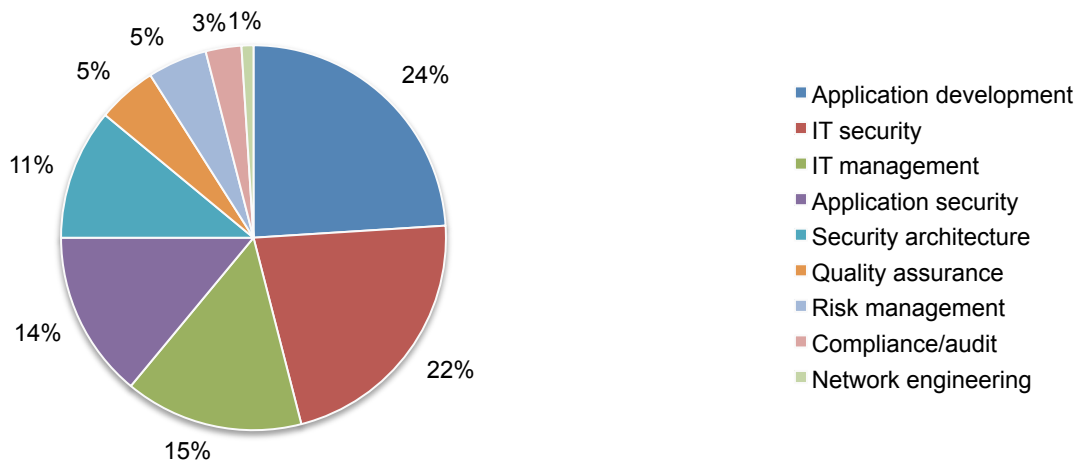
Pie chart 1 reports the current position or organizational level of respondents. By design, 53 percent of respondents reported their current position is at or above the supervisory level.

**Pie Chart 1. Current position or organizational level**



According to Pie Chart 2, 24 percent of the respondents identified application development as their primary role, 22 percent responded IT security and 15 percent responded IT management.

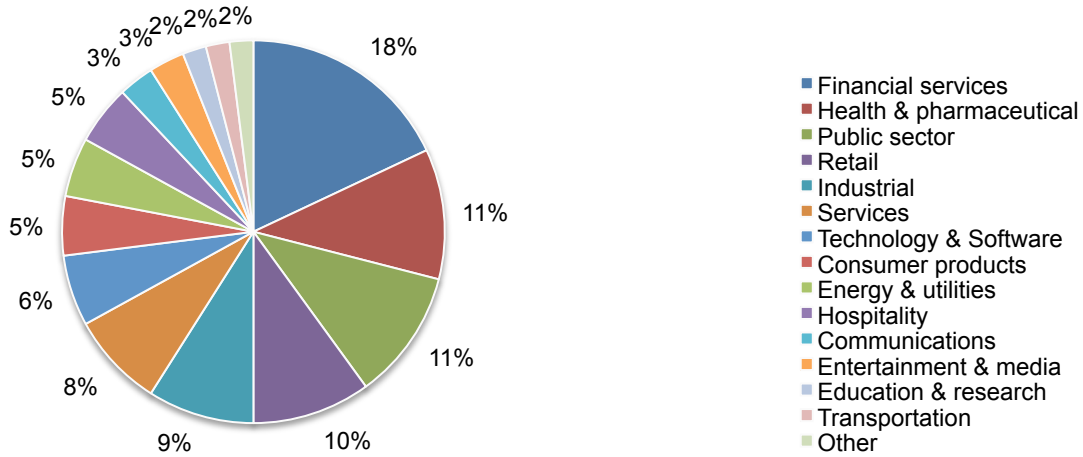
**Pie Chart 2. Primary role in the organization**





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

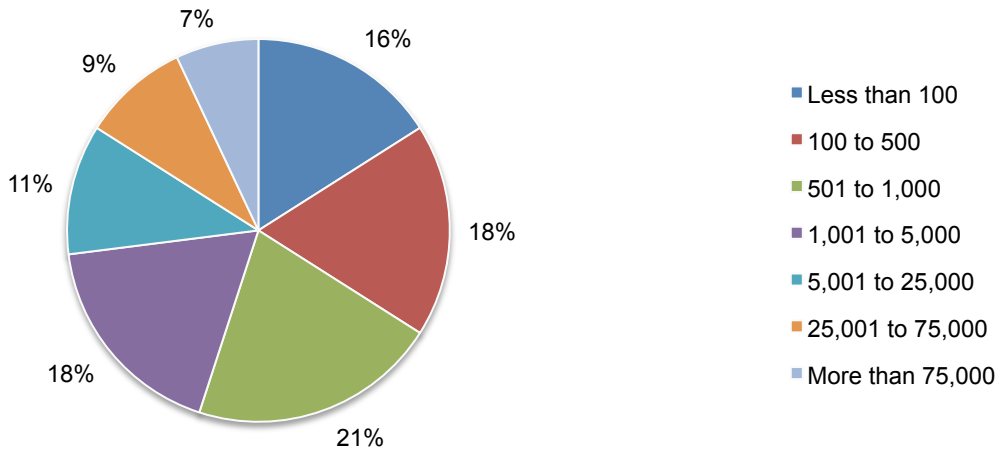
**Pie Chart 3. Primary industry focus**



According to Pie Chart 4, 45 percent of the respondents are from organizations with a global headcount of over 1,000 employees.

**Pie Chart 4. Worldwide headcount of the organization**

Extrapolated value = 12,516



#### **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 located in the United States, 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. 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 accurate response.

## Appendix: Detailed Survey Results

The following tables provide the percentage frequency of responses to all survey questions on a consolidated (global) basis across four regional clusters. All survey responses were captured in January 2015.

Survey response	Freq
Total sampling frame	19,890
Total returns	707
Screened or rejected surveys	67
Final sample	640
Response rate	3.2%

### Part 1. Screening

S1. What best describes your involvement in the application development process within the organization?	Pct%
Very significant	29%
Significant	33%
Moderate	24%
Minimal	14%
None (stop)	0%
Total	100%

S2. What best describes your involvement in the application security process within the organization?	Pct%
Very significant	23%
Significant	25%
Moderate	31%
Minimal	21%
None (stop)	0%
Total	100%

### Part 2. General questions

Q1. What describes your organization's process for developing applications?	Pct%
In-house	30%
Outsourced	41%
Combination of in-house and outsourced	29%
Total	100%

Q2. Does your organization use the following products?	Pct%
Mobile device management (MDM)	22%
Mobile application management (MAM)	18%
Both products, but separately	11%
Both, in one single product	14%
None of the above	35%
Total	100%

Q3. What best describes your organization's use of mobile apps by employees in the workplace today?	Pct%
Very heavy use	32%
Heavy use	34%
Moderate use	20%
Light use	14%
Total	100%

Q4. In your opinion, how will the use of mobile apps by employees change over the next 12 months?	Pct%
Significant increase	32%
Increase	39%
No change	28%
Decrease	1%
Significant decrease	0%
Total	100%

Q5. How does the use of mobile apps by employees affect your organization's security risk posture?	Pct%
Very significant increase in security risk	50%
Significant increase in security risk	32%
Nominal increase in security risk	12%
No increase in security risk	6%
Total	100%

Q6. Does your organization have a policy that defines the acceptable use of mobile apps in the workplace?	Pct%
Yes	45%
No	55%
Total	100%

Q7. Does your organization allow employees to use their personal mobile apps on company-assigned mobile devices such as smartphones and tablets?	Pct%
Yes	39%
No	54%
NA (company does not assign mobile devices)	7%
Total	100%

Q8. Does your organization allow employees to use/download business apps on their personally owned mobile devices (BYOD)?	Pct%
Yes	55%
No	23%
NA (company does not allow BYOD)	22%
Total	100%

Q9. What best describes the types of mobile platforms supported by your organization today for accessing business apps. Please select all that apply.	Pct%
iOS	62%
Android	65%
Windows	60%
Blackberry	54%
Other (please specify)	10%
Total	251%

Q10. Please select all the tasks (type of mobile apps) that your organization's employees use on their smart phone or tablet.	Pct%
Business email	99%
Calendar	87%
Contact lists	84%
Data storage	73%
Document collaboration	65%
Manage information on smartphone	13%
Mobile payments	8%
Sales management tools (CRM)	19%
Other (please specify)	13%
Total	461%

Q11a. Does your organization have an app store?	Pct%
Yes	30%
No	70%
Total	100%

Q11b. If yes, what techniques are used to vet mobile apps for security?	Pct%
Routine pen testing	14%
Application assessment	19%
Scan for security flaws	48%
Code review	15%
None of the above	40%
Other (please specify)	10%
Total	146%

Q11c if yes [to Q11a], are employees permitted to only use mobile apps from the organization's app store?	Pct%
Yes	33%
No	67%
Total	100%

Q11d. If yes [to Q11a], are employees permitted to download mobile apps from the organization's app store onto personally owned mobile devices (BYOD)?	Pct%
Yes	51%
No	29%
NA (company does not allow BYOD)	20%
Total	100%

Q12. Does your organization follow guidance from the Open Web Application Security Project (OWASP) to mitigate or reduce mobile app security risks?	Pct%
Yes	40%
No	48%
Unsure	12%
Total	100%

Q13. Following are the OWASP top 10 mobile app security risks. Please rate each one based on difficulty to minimize each risk using the following scale: 1 = Very difficult, 2 = Difficult, 3 = Moderately difficult, 4 = Not difficult, 5 = Cannot determine.	1+2 High Difficulty
M1: Weak Server Side Controls	45%
M2: Insecure Data Storage	56%
M3: Insufficient Transport Layer Protection	55%
M4: Unintended Data Leakage	75%
M5: Poor Authorization and Authentication	67%
M6: Broken Cryptography	80%
M7: Client Side Injection	55%
M8: Security Decisions Via Untrusted Inputs	39%
M9: Improper Session Handling	43%
M10. Lack of Binary Protection	40%
Average	56%

Q14. What is your organization's primary means for securing mobile apps? Please select all that apply.	Pct%
Intrusion prevention system (IPS)	23%
Application scanning	36%
Mobile application management (MAM)	31%
Anti-malware software	38%
Network firewall	25%
Other network security controls	17%
Mobile device management (MDM)	34%
Other (please specify)	6%
Total	210%

Q15. How does your organization scan code for vulnerabilities?	Pct%
Pen testing	10%
Proprietary software/tools	25%
Open source software/tools	14%
Cloud services	13%
NA (we do not scan for vulnerabilities)	38%
Other (please specify)	0%
Total	100%

Q16. Please rate the level of difficulty in securing mobile apps.	Pct%
1 or 2	3%
3 or 4	4%
5 or 6	16%
7 or 8	29%
9 or 10	48%
Total	100%
Extrapolated average	7.8

Q17. Please rate your organization's level of concern about the threat of malware to mobile apps.	Pct%
1 or 2	4%
3 or 4	4%
5 or 6	17%
7 or 8	32%
9 or 10	43%
Total	100%
Extrapolated average	7.6

Q18. Please rate your organization's effectiveness in securing mobile apps.	Pct%
1 or 2	36%
3 or 4	30%
5 or 6	20%
7 or 8	9%
9 or 10	5%
Total	100%
Extrapolated average	3.8

Q19. Please rate the importance of end-user convenience when building and/or deploying mobile apps in the workplace.	Pct%
1 or 2	6%
3 or 4	9%
5 or 6	19%
7 or 8	17%
9 or 10	49%
Total	100%
Extrapolated average	7.4

Q20. Please rate the importance of end-user security when building and/or deploying mobile apps in the workplace.	Pct%
1 or 2	7%
3 or 4	10%
5 or 6	33%
7 or 8	25%
9 or 10	25%
Total	100%
Extrapolated average	6.5

Q21. Please rate the importance of end-user privacy when building and/or deploying mobile apps in the workplace.	Pct%
1 or 2	12%
3 or 4	20%
5 or 6	21%
7 or 8	28%
9 or 10	19%
Total	100%
Extrapolated average	5.9

Q22. Approximately, how many mobile apps does your organization have in use today? Your best guess is welcome.	Pct%
Less than 50	50%
51 to 100	8%
101 to 500	3%
501 to 1,000	3%
More than 1,000	1%
Do not know	35%
Total	100%
Extrapolated average	105.4

Q23. Approximately, what percentage of these mobile apps are mission critical to your organization?	Pct%
None	0%
1 to 10%	5%
11 to 20%	13%
21 to 30%	34%
31 to 40%	17%
41 to 50%	14%
51 to 75%	8%
76 to 100%	9%
Total	100%
Extrapolated average	36%

Q24. Where do you test mobile apps? Please check all that apply.	Pct%
Production	16%
Development	21%
Post development, but before deployment	22%
All of the above	8%
NA (we do not test mobile apps)	33%
Total	100%

Q25. How often does your organization test mobile apps?	Pct%
Q25a. Internally developed apps	
Annual	3%
Twice a year	1%
Every 3 months	2%
Every month	4%
Every week	9%
Every time the code changes	11%
Testing is not pre-scheduled	14%
Unsure	23%
NA (we do not test mobile apps)	33%
Total	100%

Q25b. Outsourced or purchased apps	Pct%
Annual	0%
Twice a year	1%
Every 3 months	1%
Every month	2%
Every week	8%
Every time the code changes	23%
Testing is not pre-scheduled	10%
Unsure	22%
NA (we do not test mobile apps)	33%
Total	100%



Q26a. Approximately, what percent of all mobile apps are outsourced or purchased?	Pct%
None	20%
1 to 10%	4%
11 to 20%	6%
21 to 30%	5%
31 to 40%	5%
41 to 50%	14%
51 to 75%	17%
76 to 100%	29%
Total	100%
Extrapolated average	46%

Q26b. Approximately, what percent of these third parties are located offshore (outside the US)?	Pct%
None	35%
1 to 10%	2%
11 to 20%	3%
21 to 30%	2%
31 to 40%	21%
41 to 50%	11%
51 to 75%	17%
76 to 100%	9%
Total	100%
Extrapolated average	32%

Q27a. On average, what percent of mobile apps are tested for vulnerabilities?	Pct%
None	33%
1 to 10%	0%
11 to 20%	1%
21 to 30%	1%
31 to 40%	5%
41 to 50%	11%
51 to 75%	17%
76 to 100%	32%
Total	100%
Extrapolated average	46%

Q27b. On average, what percent of tested mobile apps contain vulnerabilities?	Pct%
None	0%
1 to 10%	29%
11 to 20%	15%
21 to 30%	13%
31 to 40%	11%
41 to 50%	12%
51 to 75%	14%
76 to 100%	6%
Total	100%
Extrapolated average	30%

Q28. What do you see as the main reason(s) why your organization's mobile apps contain vulnerable code? Please select all that apply.	Pct%
Accidental coding errors	39%
Malicious coding errors	19%
Lack of internal policies or rules that clarify security requirements	64%
Lack of understanding/training on secure coding practices	73%
Rush to release pressures on application development team	77%
Lack of quality assurances and testing procedures	68%
Application development tools have inherent bugs	18%
Incorrect permissions	6%
Other (please specify)	2%
Total	366%

### Part 3. Best practices

Q29. The following 3 tables summarize 30 best practices in securing the application development process. Please check all items that your organization is doing today to secure its development of apps.	
1. Standards & Compliance	Pct%
Your organization has a defined software development process that includes activities for requirements, design, implementation, and testing.	53%
Your organization adheres to the software development process as defined.	44%
Your organization has corporate application security policies defined.	38%
Formal security requirements are defined as part of the development process.	35%
Your organization has defined secure coding standards.	30%
Your organization has defined secure architecture standards.	35%
Development teams are measured for their compliance with regulatory requirements or security best practices.	25%
Development teams are measured for compliance with secure architecture standards.	29%
Development teams are measured for compliance with secure coding standards.	29%

2. Secure Coding	Pct%
Application architecture is reviewed against the secure architecture standards.	33%
Your organization takes security measures to prevent unauthorized users from accessing data security measures and to prevent data leakage.	55%
Your organization creates and uses its own encryption algorithms or protocols.	39%
Your organization uses automated scanning tools to test applications during development.	53%
Your organization uses automated scanning tools to test applications for vulnerabilities after they have been released.	53%
Your organization updates internal training and education to ensure development teams are capable of adhering to application security policies and best practices.	47%
Your organization ensures that sensitive information such as passwords and credit card numbers do not reside directly on a device.	50%
Your organization ensures sensitive information is stored within an encrypted data section or within encrypted storage in the internal app data directory.	42%
In your organization, application security risk is measured and well understood across the application portfolio.	41%
Your organization ensures the "rush to release" does not impact coding practices.	27%
Your organization takes basic steps to protect the application from reverse engineering.	30%
Your organization takes steps to ensure that the environment in which the application runs is safe (e.g., app not running on a jail broken device or in the presence of a debugger).	42%
Your organization takes steps to monitor the run time behavior of the app (e.g., to determine if the app has been or is being tampered with).	49%
Your organization uses risk metrics to guide application security decision-making.	38%

<b>3. Testing &amp; Assessment</b>	Pct%
Applications in your organization are subject to a manual penetration testing effort either by internal teams or by a third party.	20%
Your organization reviews code for adherence to secure coding standards.	28%
A threat model or other high-level risk assessment process is followed during the development process.	35%
Your organization uses the results of audits and assessments to improve application security policies and processes.	29%
Your organization uses the results of audits and assessments to improve architecture and coding standards.	29%
Your organization has security acceptance requirements for outsourced applications.	52%
Your organization's mobile app testing methods include tests of open source merged with proprietary applications.	23%

**Part 4. Attributions:** Please rate each one of the following three statements using the scale provided below each item.

Q30a. My organization has ample resources to detect vulnerabilities in mobile apps.	Pct%
Strongly agree	13%
Agree	17%
Unsure	22%
Disagree	24%
Strongly disagree	24%
Total	100%

Q30b. My organization has ample resources to prevent the use of vulnerable or malware-infected mobile apps.	Pct%
Strongly agree	13%
Agree	16%
Unsure	23%
Disagree	25%
Strongly disagree	23%
Total	100%

Q30c. My organization considers mobile app security a high priority.	Pct%
Strongly agree	23%
Agree	37%
Unsure	18%
Disagree	15%
Strongly disagree	7%
Total	100%

Q30d. The security of mobile apps is sometimes put at risk because of customer demand or need.	Pct%
Strongly agree	33%
Agree	32%
Unsure	16%
Disagree	13%
Strongly disagree	6%
Total	100%

Q30e. The presence of malware-infected mobile apps/devices will increase over the next 12 months.	Pct%
Strongly agree	30%
Agree	31%
Unsure	26%
Disagree	11%
Strongly disagree	2%
Total	100%

Q30f. Cross-site scripting through insecure mobile apps will increase over the next 12 months.	Pct%
Strongly agree	28%
Agree	26%
Unsure	30%
Disagree	13%
Strongly disagree	3%
Total	100%

Q30g. My organization considers it very important to make applications tamper resistant.	Pct%
Strongly agree	26%
Agree	32%
Unsure	23%
Disagree	15%
Strongly disagree	4%
Total	100%

Q30h. My organization has sufficient mobile application security expertise.	Pct%
Strongly agree	21%
Agree	20%
Unsure	26%
Disagree	23%
Strongly disagree	10%
Total	100%

Q30i. My organization believes the real risk to mobile apps is data leakage.	Pct%
Strongly agree	30%
Agree	31%
Unsure	18%
Disagree	11%
Strongly disagree	10%
Total	100%

**Part 5. Budget & Spending**

Q31a. Approximately, how much does your organization spend on mobile app development each year? Please choose the range that best approximates the total investment in terms of technologies, personnel, managed or outsourced services and other cash outlays.	Pct%
None	0%
\$1 to \$500,000	5%
\$501,001 to \$1,000,000	6%
\$1,000,001 to \$5,000,000	6%
\$5,000,001 to \$10,000,000	11%
\$10,000,001 to \$25,000,000	23%
\$25,000,001 to \$50,000,000	31%
\$50,000,001 to \$100,000,000	10%
More than \$100,000,000	8%
Total	100%
Extrapolated average	33,812,500

Q31b. Approximately, what percent of the spending/budget for mobile app development is dedicated to mobile app security?	Pct%
None	50%
1 to 5%	15%
6 to 10%	14%
11 to 15%	10%
16 to 20%	6%
21 to 30%	3%
31 to 50%	2%
More than 50%	0%
Total	100%
Extrapolated average	5.5%
Extrapolated value	1,859,688

Q32. Please allocate the level or proportion of spending incurred by your organization for each one of the following categories to lessen or mitigate vulnerabilities and threats resulting from insecure mobile apps. Note that the sum of your allocation must equal 100 points.	Points
Pen testing	11
Proprietary software	36
Open source software	21
Cloud services	15
Source code testing	12
Other (please specify)	5
Total points	100

**Part 5. Your Role**

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	2%
Director	16%
Manager	20%
Supervisor	15%
Technician	39%
Staff	5%
Contractor	2%
Other	0%
Total	100%

D2. What best describes your primary role in the organization?	Pct%
Application development	24%
Application security	14%
Security architecture	11%
IT management	15%
IT security	22%
Quality assurance	5%
Compliance/audit	3%
Risk management	5%
Network engineering	1%
Other	0%
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%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	5%
Industrial	9%
Public sector	11%
Retail	10%
Services	8%
Technology & Software	6%
Transportation	2%
Other	0%
Total	100%

D5. Where are your employees located? (check all that apply):	Pct%
United States	100%
Canada	73%
Europe	67%
Middle East & Africa	26%
Asia-Pacific	61%
Latin America (including Mexico)	58%

D6. What is the worldwide headcount of your organization?	Pct%
Less than 100	16%
100 to 500	18%
501 to 1,000	21%
1,001 to 5,000	18%
5,001 to 25,000	11%
25,001 to 75,000	9%
More than 75,000	7%
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.