APPLICATION SECURITY IN THE CHANGING RISK LANDSCAPE

Ponemon INSTITUTE

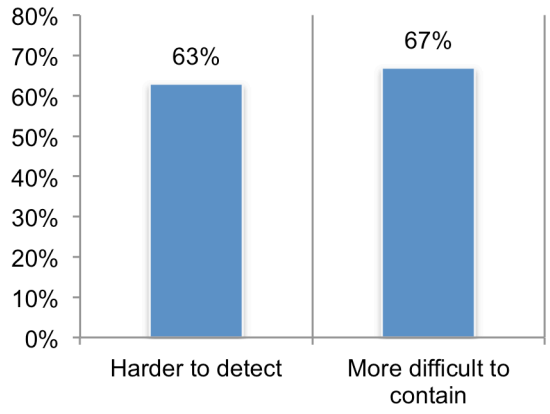
RESEARCH SPONSORED BY F5
INDEPENDENTLY CONDUCTED BY
PONEMON INSTITUTE LLC, JULY 2016

Part 1. Introduction

Ponemon Institute is pleased to present the results of *Application Security in the Changing Risk Landscape* sponsored by F5. The purpose of this study is to understand how today's security risks are affecting application security. We surveyed 605 IT and IT security practitioners in the United States who are involved in their organization's application security activities.

The majority of respondents (57 percent) say it is the lack of visibility in the application layer that is preventing a strong application security. In fact, as shown in Figure 1, 63 percent of respondents say attacks at the application layer are harder to detect than at the network layer and 67 percent of respondents say these attacks are more difficult to contain than at the network layer.

Figure 1. Why attacks at the application layer are worse than those at the network layer
Strongly agree and agree responses combined



Following are key takeaways from this research.

Lack of visibility in the application layer is the main barrier to achieving a strong application security posture. Other significant barriers are created by migration to the cloud (47 percent of respondents), lack of skilled or expert personnel (45 percent of respondents) and proliferation of mobile devices (43 percent of respondents).

The frequency and severity of attacks on the application layer is considered greater than at the network layer. Fifty percent of respondents (29 percent + 21 percent) say the application is attacked more and 58 percent of respondents (33 percent + 21 percent) say attacks are more severe than at the network layer. In the past 12 months, the most common security incidents due to insecure applications were: SQL injections (29 percent), DDoS (25 percent) and Web fraud (21 percent).

Network security is better funded than application security. On average, 18 percent of the IT security budget is dedicated to application security. More than double that amount (an average of 39 percent) is allocated to network security. As a consequence, only 35 percent of respondents say their organizations have ample resources to detect vulnerabilities in applications, and 30 percent of respondents say they have enough resources to remediate vulnerabilities in applications.

Accountability for the security of applications is in a state of flux. Fifty-six percent of respondents believe accountability for application security is shifting from IT to the end user or application owner. However, at this time responsibility for ensuring the security of applications is dispersed throughout the organization. While 21 percent of respondents say the CIO or CTO is accountable, another 20 percent of respondents say no one person or department is responsible. Twenty percent of respondents say business units are accountable and 19 percent of respondents say the head of application development is accountable.

Shadow IT affects the security of applications. Respondents estimate that on average their organizations have 1,175 applications and an average of 33 percent are considered mission critical. Sixty-six percent of respondents are only somewhat confident (23 percent) or have no confidence (43 percent) they know all the applications in their organizations. Accordingly, 68 percent of respondents (34 percent + 34 percent) say their IT function does not have visibility into all the applications deployed in their organizations and 65 percent of respondents (32 percent + 33 percent) agree that Shadow IT is a problem.

Mobile and business applications in the cloud are proliferating. An average of 31 percent of business applications are mobile apps and this will increase to 38 percent in the next 12 months. Today, 37 percent of business applications are in the cloud and this will increase to an average of 46 percent.

The growth in mobile and cloud-based applications is seen as significantly affecting application security risk. Sixty percent of respondents say mobile apps increase risk (25 percent) or increase risk significantly (35 percent). Fifty-one percent of respondents say cloud-based applications increase risk (25 percent) or increase risk significantly (26 percent).

Hiring and retaining skilled and qualified application developers will improve an organization's security posture. Sixty-nine percent of respondents believe the shortage of skilled and qualified application developers puts their applications at risk. Moreover, 67 percent of respondents say the "rush to release" causes application developers in their organization to neglect secure coding procedures and processes.

Ensuring developers understand secure coding practices can reduce application security risk. The two main reasons why applications contain vulnerable code are developers not understanding secure coding practices or their poor coding.

More testing of applications is needed. Almost half of respondents say their organization does not test applications for threats and vulnerabilities (25 percent) or testing is not pre-scheduled (23 percent). Only 14 percent of respondents say applications are tested every time the code changes.

Currently, respondents have little confidence that application developers in their organization practice secure design, development and testing of applications. Seventy-four percent of respondents say in application development they are only somewhat confident (27 percent) or have no confidence (47 percent) that such practices as input/output validation, defensive programming and appropriate compiler/linker security options are conducted.

Devops or continuous integration is believed to improve application security. Thirty-five percent of respondents say their organizations have adopted devops or continuous integration practices into the application development lifecycle. Of these respondents, 71 percent say it improves application security and enables them to respond quickly to security issues and vulnerabilities (56 percent of respondents).

Web application firewalls (WAF) are the primary means of securing applications. Thirty percent of respondents say their organizations use WAFs to secure applications. Twenty-one percent of respondents say they use application scanning and 19 percent of respondents say they use penetration testing to secure applications.

Thirty-nine percent of respondents say their organization uses micro-segmentation to enhance the security posture of their applications and 37 percent use Linux or Windows containers. Thirty-one percent of respondents say their organizations use managed, cloud-based application

Cyber security threats will weaken application security programs, but new IT security and privacy compliance requirements will strengthen these programs. Eighty-eight percent of respondents are concerned that new and emerging cyber security threats will affect the security of applications. In contrast, 54 percent of respondents say new and emerging IT security and privacy compliance requirements will help their security programs. According to respondents, there are more trends expected to weaken application security than will strengthen security.

The responsibility for securing applications will move closer to the application developer. Sixty percent of respondents anticipate the applications developer will assume more responsibility for the security of applications. Testing for vulnerabilities should take place in the design and development phase of the system development life cycle (SDLC). Today, most applications are tested in the launch or post-launch phase (61 percent). In the future, the goal is to perform more testing in the design and development phase (63 percent).

Do secure coding practices affect the application delivery cycle? Fifty percent of respondents say secure coding practices, such as penetration testing, slow down the application delivery cycle within their organizations significantly (12 percent of respondents) or some slowdown (38 percent of respondents). However, 44 percent of respondents say there is no slowdown.

How secure coding practices will change. The secure coding practices most often performed today are: run applications in a safe environment (67 percent of respondents), use automated scanning tools to test applications for vulnerabilities (49 percent of respondents) and perform penetration testing procedures (47 percent of respondents).

In the next 24 months, the following practices will most likely be performed: run applications in a safe environment (80 percent of respondents), monitor the runtime behavior of applications to determine if tampering has occurred (65 percent of respondents) and perform penetration testing procedures (63 percent of respondents).

Part 2. Key findings

In this section, we provide a deeper analysis of the research. The complete audited findings are presented in the Appendix of the report. We have organized the analysis of the findings according to the following topics.

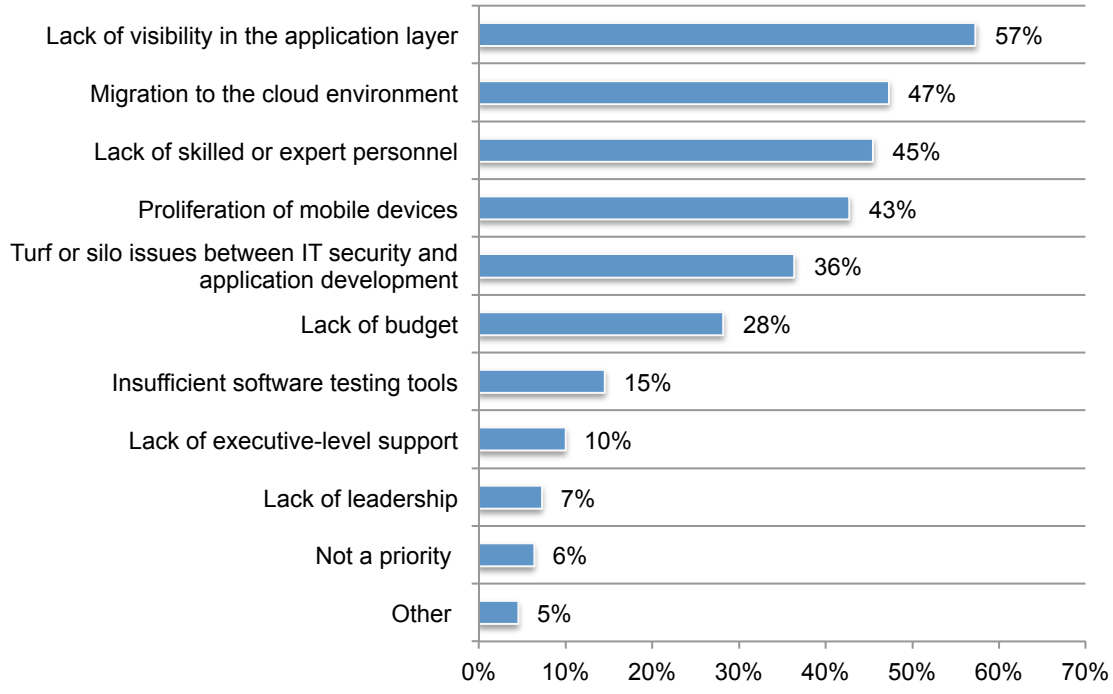
- Risks and challenges in achieving a strong application security posture
- The proliferation of applications in the workplace
- The role of application developers in mitigating risk
- How organizations are addressing application security risk
- The future state of application security programs

Risks and challenges in achieving a strong application security posture

Lack of visibility in the application layer is the main barrier to achieving a strong application security posture. According to Figure 2, the majority of respondents (57 percent) say it is the lack of visibility in the application layer that is preventing strong application security. As discussed previously, 63 percent of respondents say attacks at the application layer are harder to detect than at the network layer and 67 percent of respondents say these attacks are more difficult to contain than at the network layer.

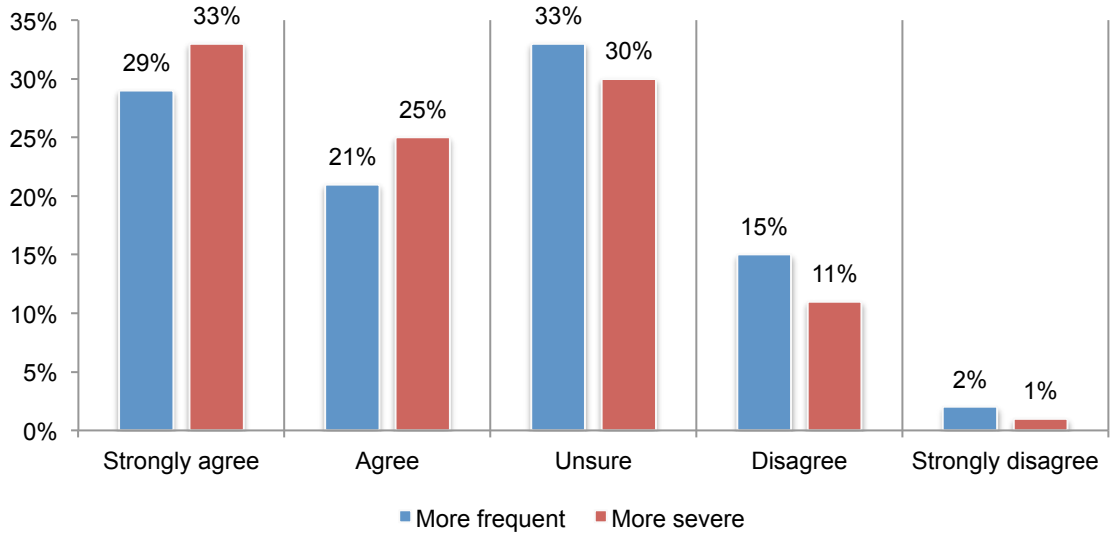
Other significant barriers are created by migration to the cloud (47 percent of respondents), lack of skilled or expert personnel (45 percent of respondents) and proliferation of mobile devices (43 percent of respondents).

Figure 2. What do you see as the main barriers to achieving a strong application security posture?
More than one choice permitted



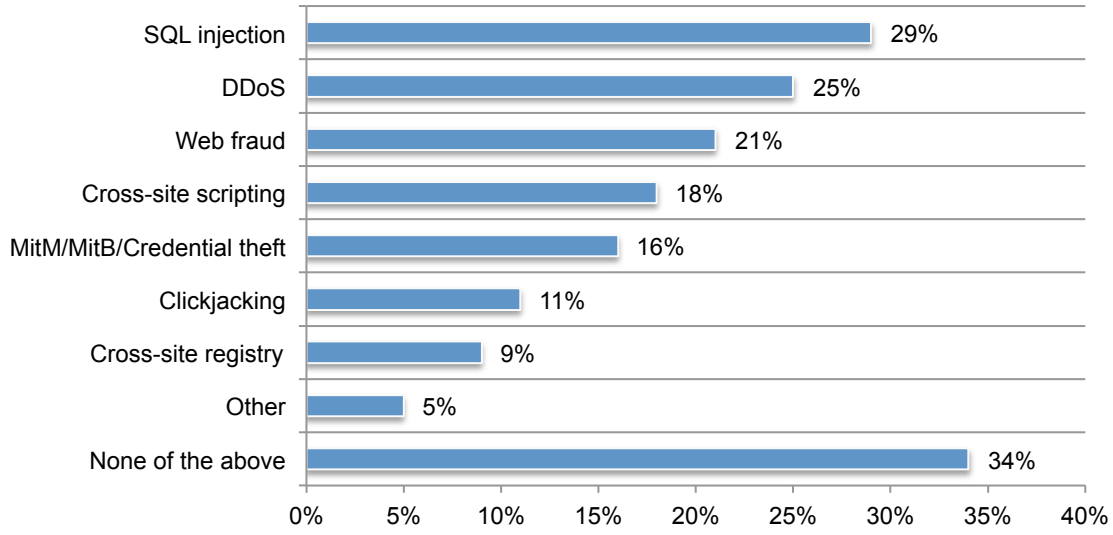
The frequency and severity of attacks on the application layer is considered greater than at the network layer. As shown in Figure 3, 50 percent of respondents (29 percent + 21 percent) say the application is attacked more and 58 percent of respondents (33 percent + 21 percent) say attacks are more severe than at the network layer.

Figure 3. Application layer attacks are more frequent and severe than at the network layer



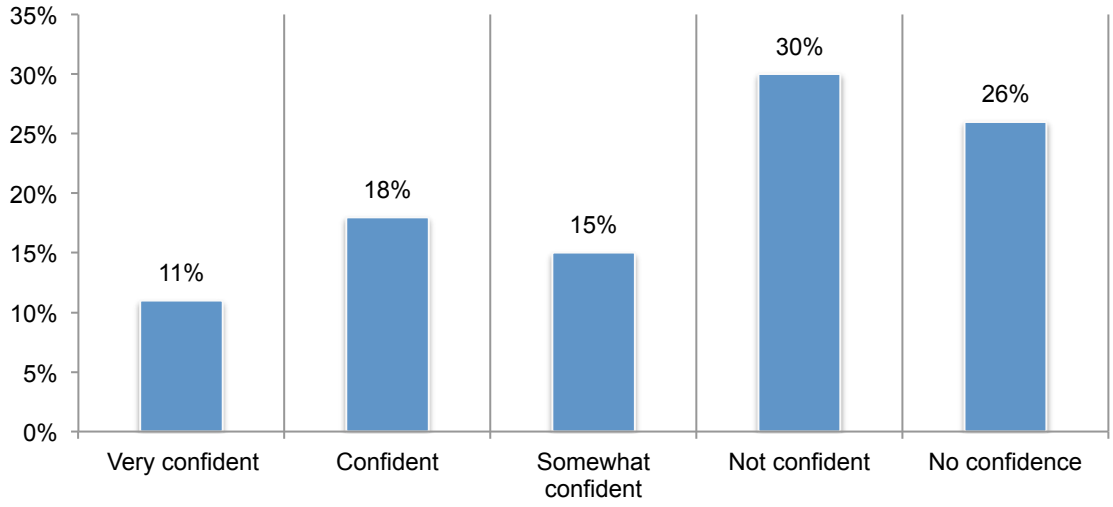
In the past 12 months, as presented in Figure 4, the most common security incidents due to insecure applications were: SQL injections (29 percent), DDoS (25 percent) and Web fraud (21 percent). Thirty-four percent of respondents say none of these occurred.

Figure 4. Which of the following types of incidents or compromises has your organization experienced over the past 12 months because of insecure applications?
More than one choice permitted



Only 29 percent of respondents (11 percent + 18 percent) are confident that their organization's SSL-encrypted traffic is being inspected to ensure that there is no malware.

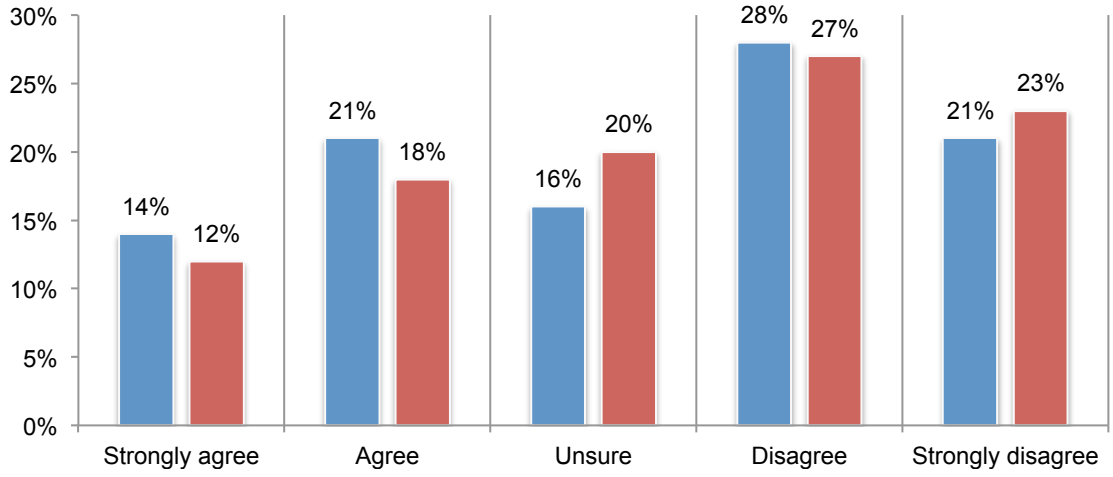
Figure 5. How confident are you that your organization's SSL-encrypted traffic is being inspected?



Network security is better funded than application security. While respondents believe attacks against the application layer are more severe and frequent than attacks against the network layer, application security is not allocated the same or a greater percentage of the IT security budget.

On average, 18 percent of the IT security budget is dedicated to application security. More than double that amount (an average of 39 percent) is allocated to network security. According to Figure 6, only 35 percent of respondents (14 percent + 21 percent) say their organizations have ample resources to detect vulnerabilities in applications and 30 percent of respondents (12 percent + 18 percent) say they have enough resources to remediate vulnerabilities in applications.

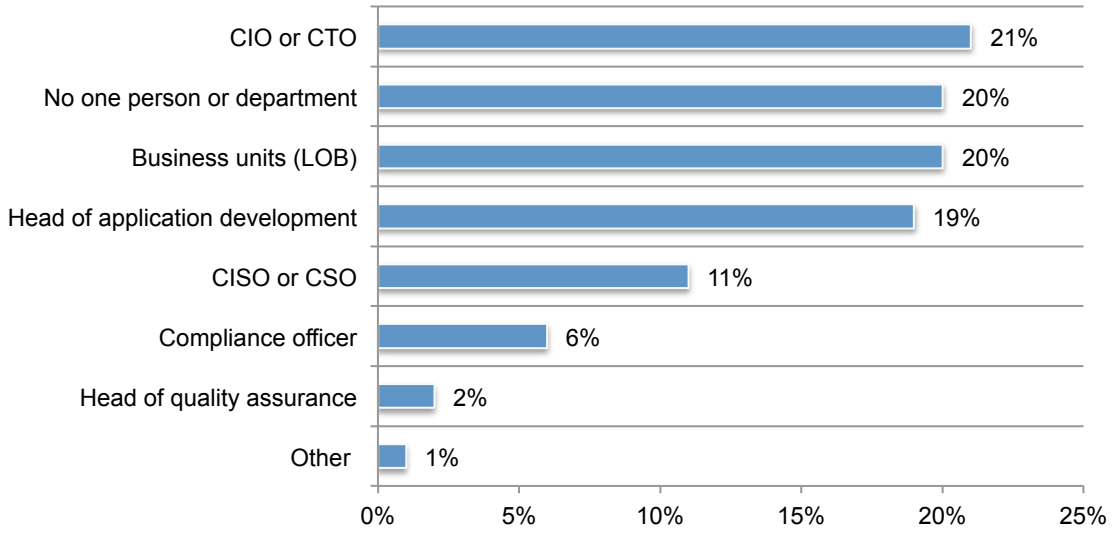
Figure 6. My organization has ample resources to detect and remediate vulnerabilities in applications



Accountability for the security of applications is in a state of flux. Fifty-six percent of respondents believe accountability for application security is shifting from IT to the end user or application owner.

However, at this time responsibility for ensuring the security of applications is dispersed throughout the organization, as shown in Figure 7. While 21 percent of respondents say the CIO or CTO is accountable, another 20 percent of respondents say no one person or department is responsible. Twenty percent of respondents say business units are accountable and 19 percent of respondents say the head of application development is accountable.

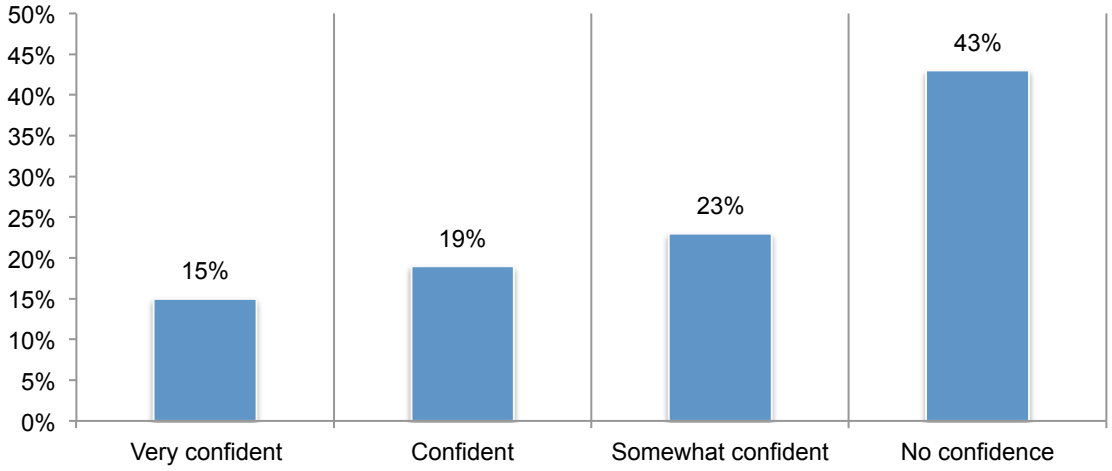
Figure 7. Who owns your organization's application security risk management process?



The proliferation of applications in the workplace

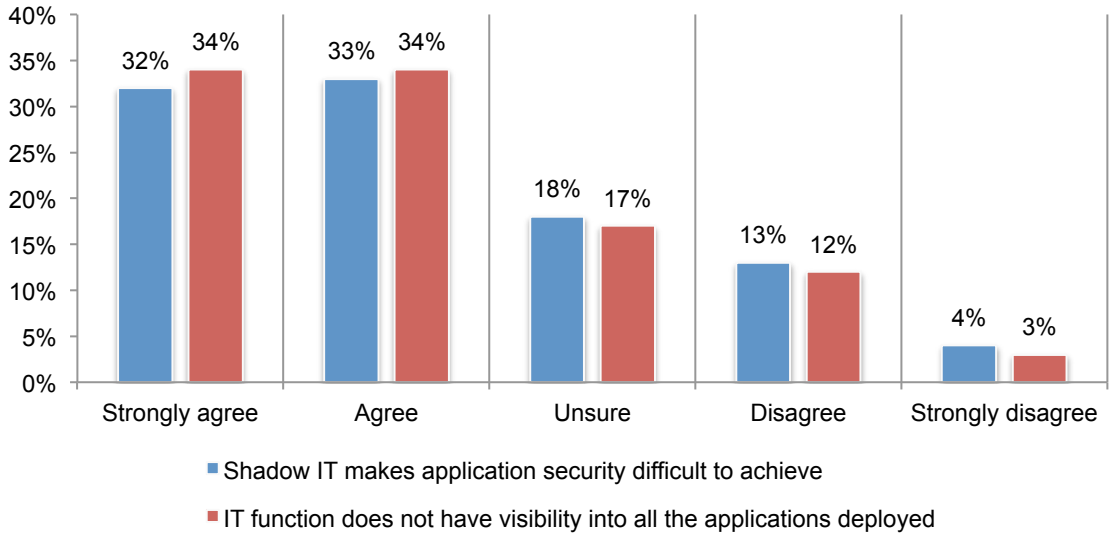
Shadow IT affects the security of applications. Respondents estimate that on average their organizations have 1,175 applications and an average of 33 percent are considered mission critical. According to Figure 8, 66 percent of respondents are only somewhat confident (23 percent) or have no confidence (43 percent) they know all the applications in their organizations.

Figure 8. How confident are you that you know all the applications in your organization today?



Accordingly, 68 percent of respondents (34 percent + 34 percent) say their IT function does not have visibility into all the applications deployed in their organizations and 65 percent of respondents (32 percent + 33 percent) agree that Shadow IT is a problem, as shown in Figure 9.

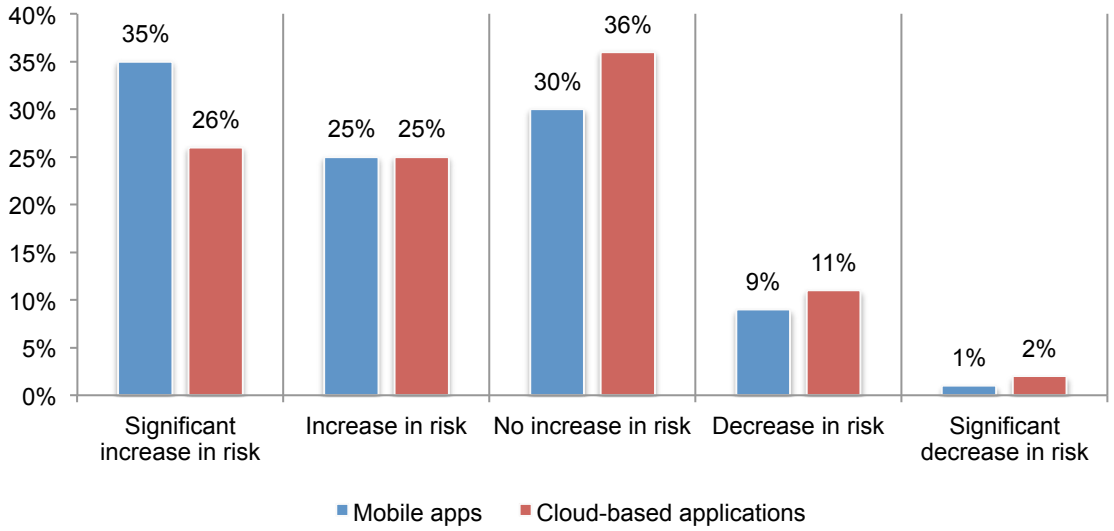
Figure 9. Perceptions about Shadow IT and visibility into all applications deployed



Mobile and business applications in the cloud are proliferating. An average of 31 percent of business applications are mobile apps and this will increase to 38 percent in the next 12 months. Today, 37 percent of business applications are in the cloud and this will increase to an average of 46 percent.

The growth in mobile and cloud-based applications is seen as significantly affecting application security risk. According to Figure 10, 60 percent of respondents say mobile apps increase risk (25 percent) or increase risk significant significantly (35 percent). Fifty-one percent of respondents say cloud-based applications increase risk (25 percent) or increase risk significantly (26 percent).

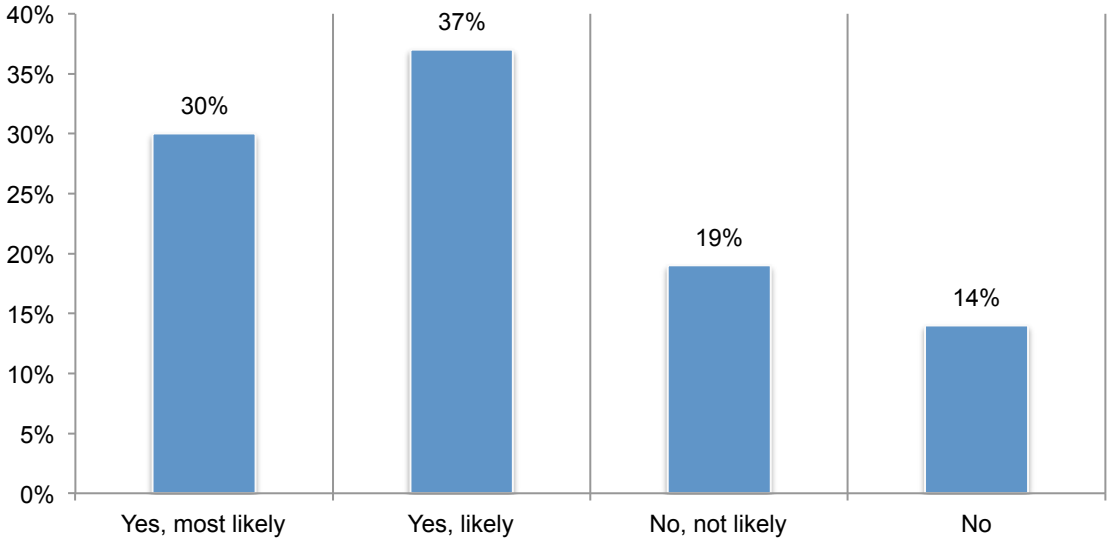
Figure 10. Do you believe mobile apps and cloud-based applications affect your organization's security risk profile?



The role of application developers in mitigating risk

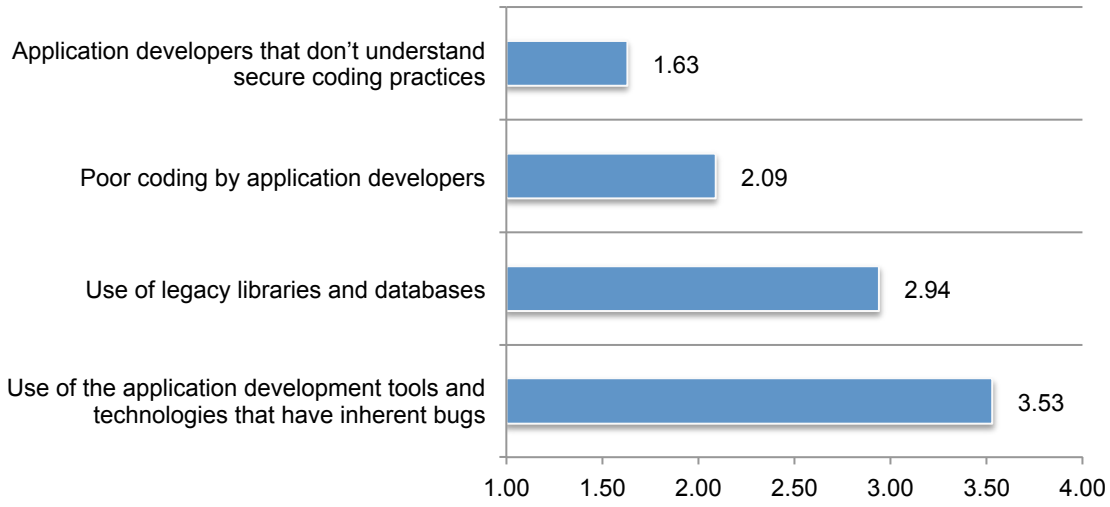
Hiring and retaining skilled and qualified application developers will improve an organization's security posture. Sixty-nine percent of respondents believe the shortage of skilled and qualified application developers puts their applications at risk. Moreover, 67 percent of respondents say the "rush to release" causes application developers in their organization to neglect secure coding procedures and processes, according to Figure 11.

Figure 11. Does the "rush to release" cause application developers in your organization to neglect secure coding procedures and processes?



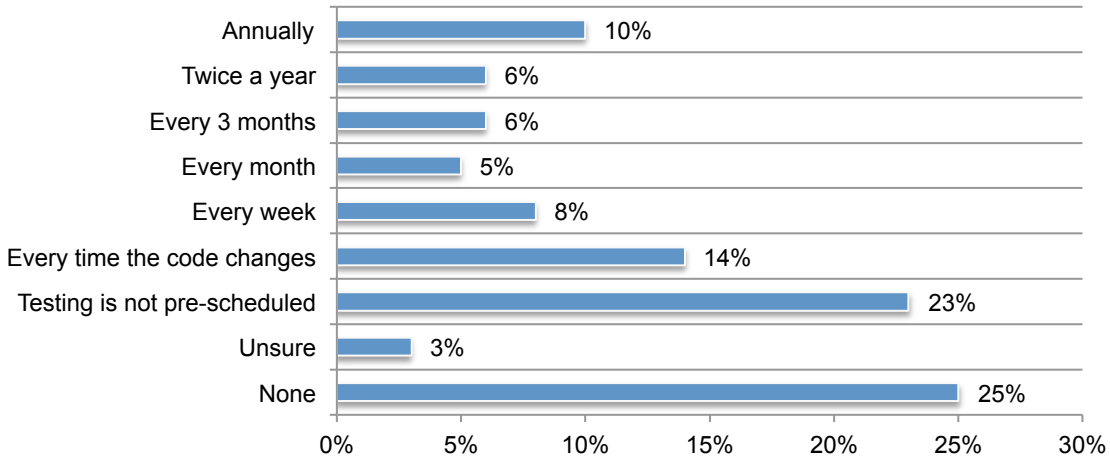
Ensuring developers understand secure coding practices can reduce application security risk. The two main reasons why applications contain vulnerable code are developers not understanding secure coding practices or their poor coding, as shown in Figure 12.

Figure 12. Why does your organization's applications contain vulnerable code?
1 = most important reason to 4 = least important reason



More testing of applications is needed. As presented in Figure 13, almost half of respondents say their organization does not test applications for threats and vulnerabilities (25 percent) or testing is not pre-scheduled (23 percent). Only 14 percent of respondents say applications are tested every time the code changes.

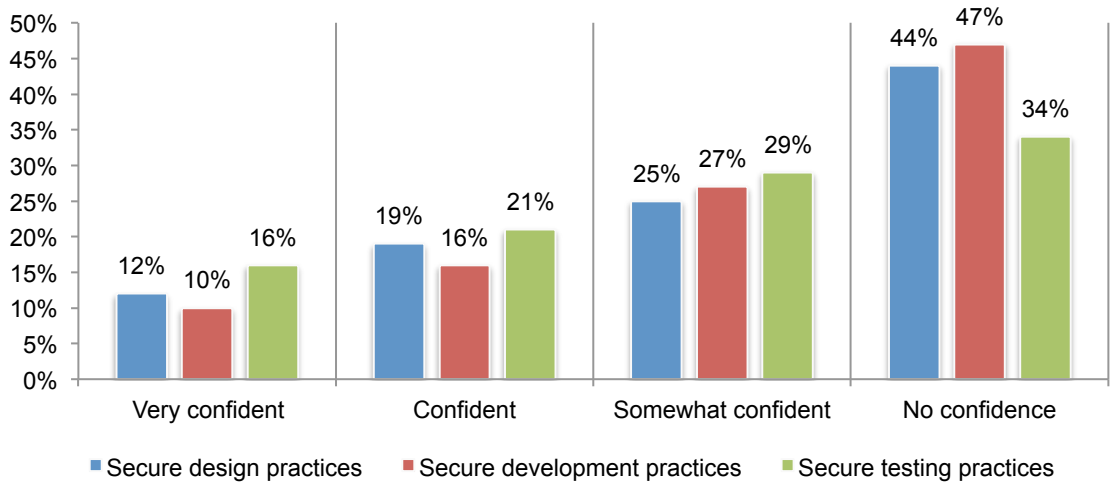
Figure 13. How often does your organization test applications for threats and vulnerabilities?



Currently, respondents have little confidence that application developers in their organization practice secure design, development and testing of applications. According to Figure 14, 74 percent of respondents say in application development they are only somewhat confident (27 percent) or have no confidence (47 percent) that such secure development practices as input/output validation, defensive programming and appropriate compiler/linker security options are conducted.

Sixty-nine percent of respondents are only somewhat confident (25 percent) or have no confidence (44 percent) developers follow such secure design practices as threat modeling and architectural risk analysis. Sixty-three percent of respondents are somewhat confident (29 percent) or have no confidence (34 percent) that application developers follow such secure testing practices as manually analyzing code for security issues, using static code analysis tools, analyzing software security requirements and creating security test plans and cases.

Figure 14. How confident are you that developers practice secure application design, development and testing?

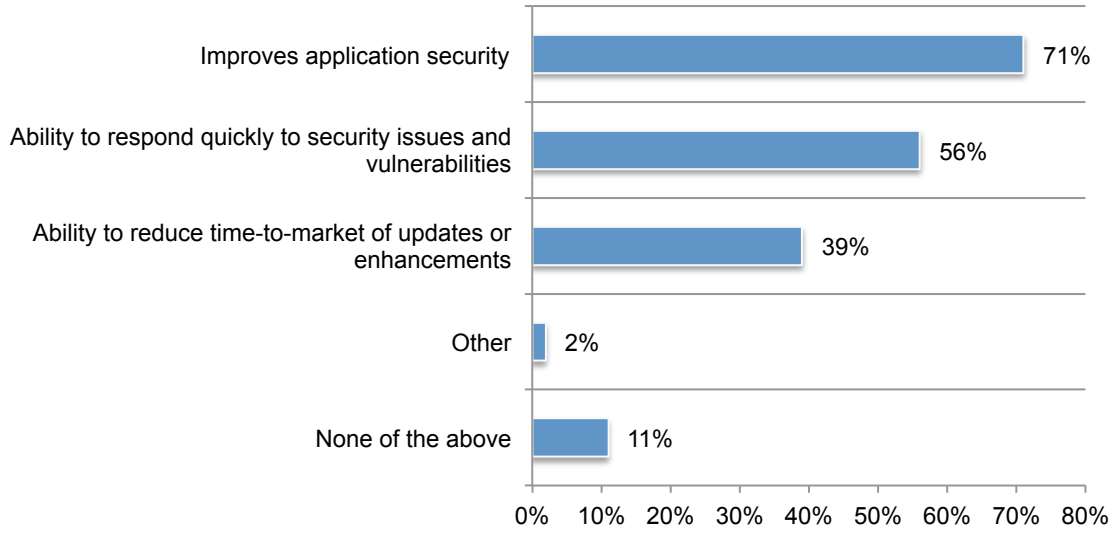


How organizations are addressing application security risk

Devops or continuous integration is believed to improve application security. Thirty-five percent of respondents say their organizations have adopted devops or continuous integration practices into the application development lifecycle. Only 27 percent of respondents say their organizations have evaluated and implemented tenant isolation methods or models for segregating application traffic and data.

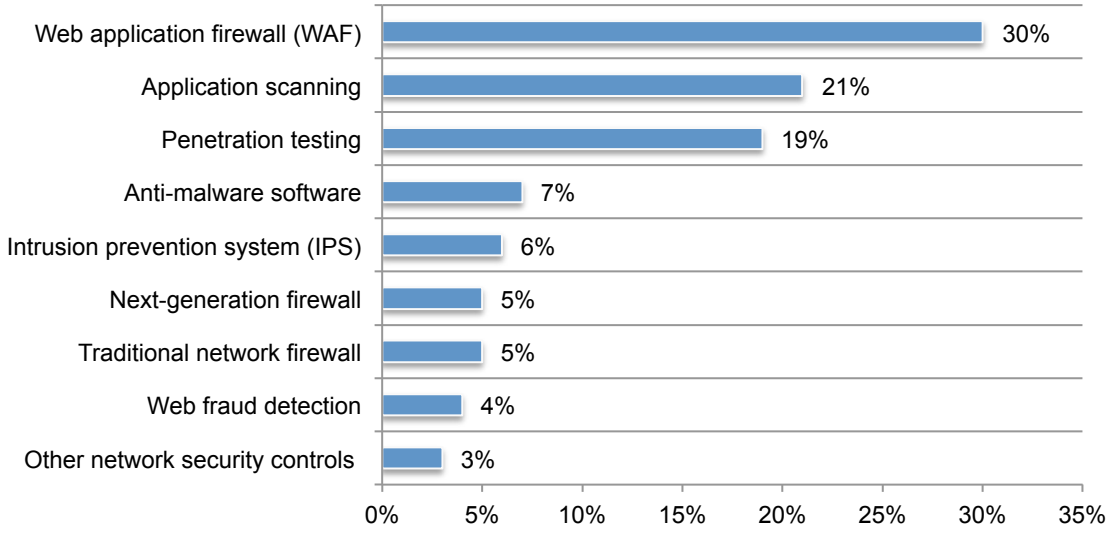
According to Figure 15, of those respondents who say their organizations have adopted devops or continuous integration practices, 71 percent say it improves application security and enables them to respond quickly to security issues and vulnerabilities (56 percent of respondents).

Figure 15. Why organizations adopted devops or continuous integration practices into their application development lifecycle
More than one choice permitted



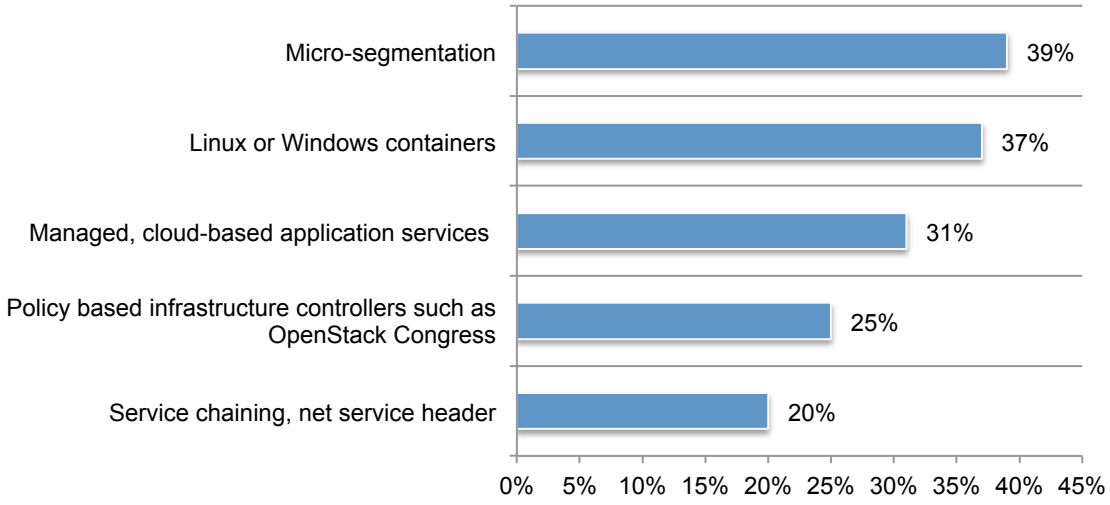
Web application firewalls (WAF) are the primary means of securing applications. Thirty percent of respondents say their organizations use WAFs to secure applications. Twenty-one percent of respondents say they use application scanning and 19 percent of respondents say they use penetration testing to secure applications, as shown in Figure 16.

Figure 16. What is your organization's primary means of securing applications?



According to Figure 17, 39 percent of respondents say their organization use micro-segmentation to enhance the security posture of their applications and 37 percent use Linux or Windows containers. Thirty-one percent of respondents say their organizations use managed, cloud-based application services.

Figure 17. Does your organization use any of the following technologies to enhance its security posture?

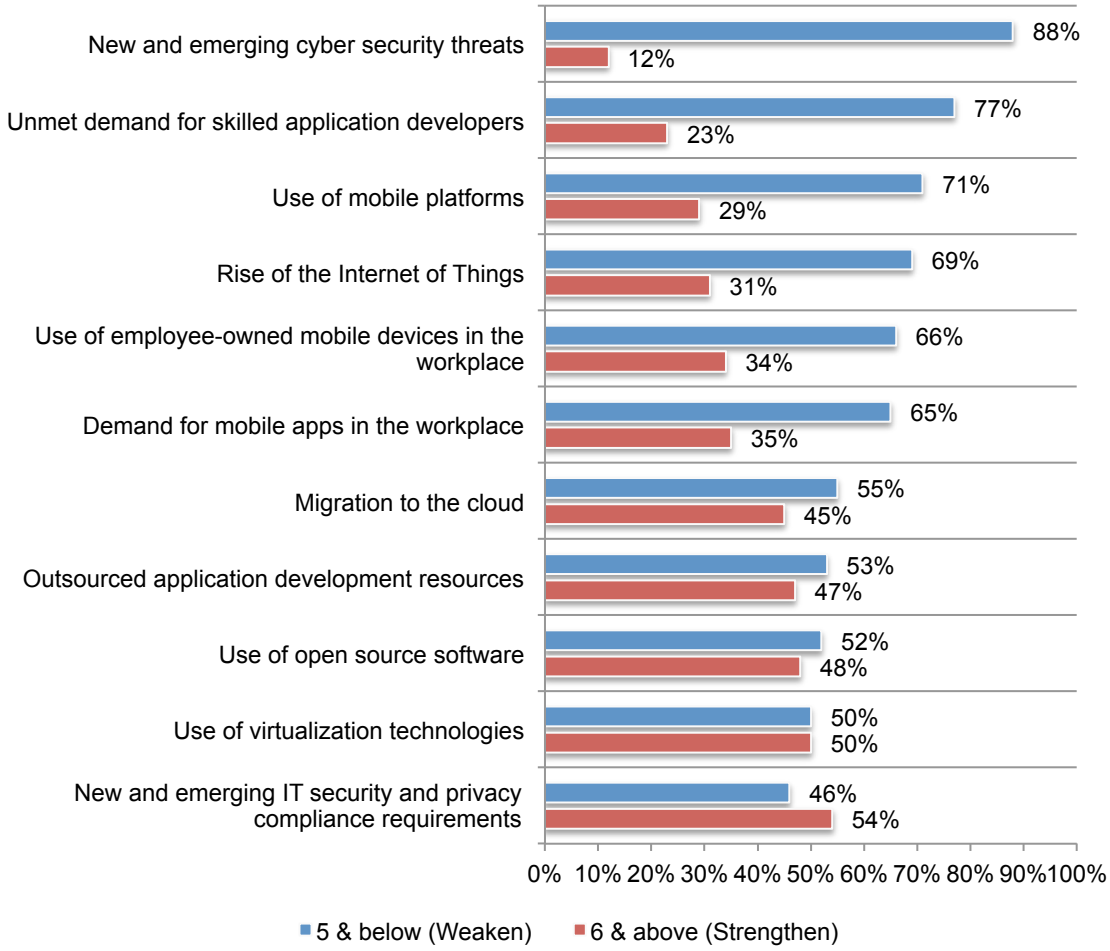


Future state of application security programs

Cyber security threats will weaken application security programs, but new IT security and privacy compliance requirements will strengthen these programs. As shown in Figure 18, 88 percent of respondents are concerned that new and emerging cyber security threats will affect the security of applications. In contrast, 54 percent of respondents say new and emerging IT security and privacy compliance requirements will help their security programs. According to respondents, there are more trends expected to weaken application security than will strengthen security.

Other future threats to application security are: the unmet demand for skilled application developers (77 percent of respondents), use of mobile platforms (71 percent of respondents), rise of the Internet of Things (69 percent of respondents) and use of employee-owned mobile devices in the workplace (66 percent of respondents). Trends that are expected to support application security are: use of virtualization technologies (50 percent of respondents) and use of open source software (48 percent of respondents).

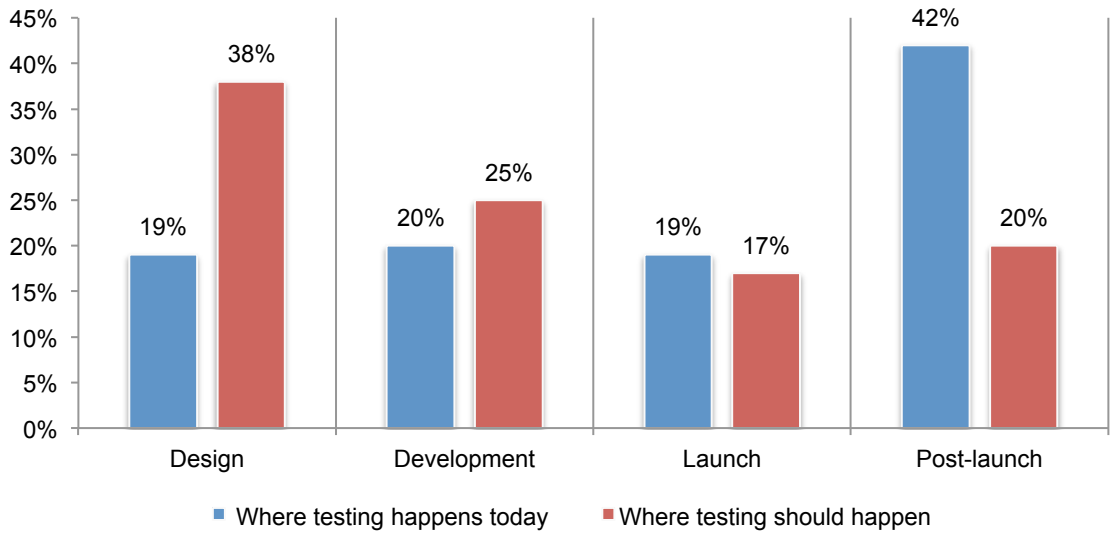
Figure 18. What are the trends that weaken or strengthen the state of application security in the future?
1 = Weaken to 10 = Strengthen



The responsibility for securing applications will move closer to the application developer. Sixty percent of respondents anticipate the applications developer will assume more responsibility for the security of applications.

As shown in Figure 19, testing for vulnerabilities should take place in the design and development phase of the system development life cycle (SDLC). Today, most applications are tested in the launch or post-launch phase (61 percent). In the future, the goal is to perform more testing in the design and development phase (63 percent).

Figure 19. Where testing happens and where testing should take place

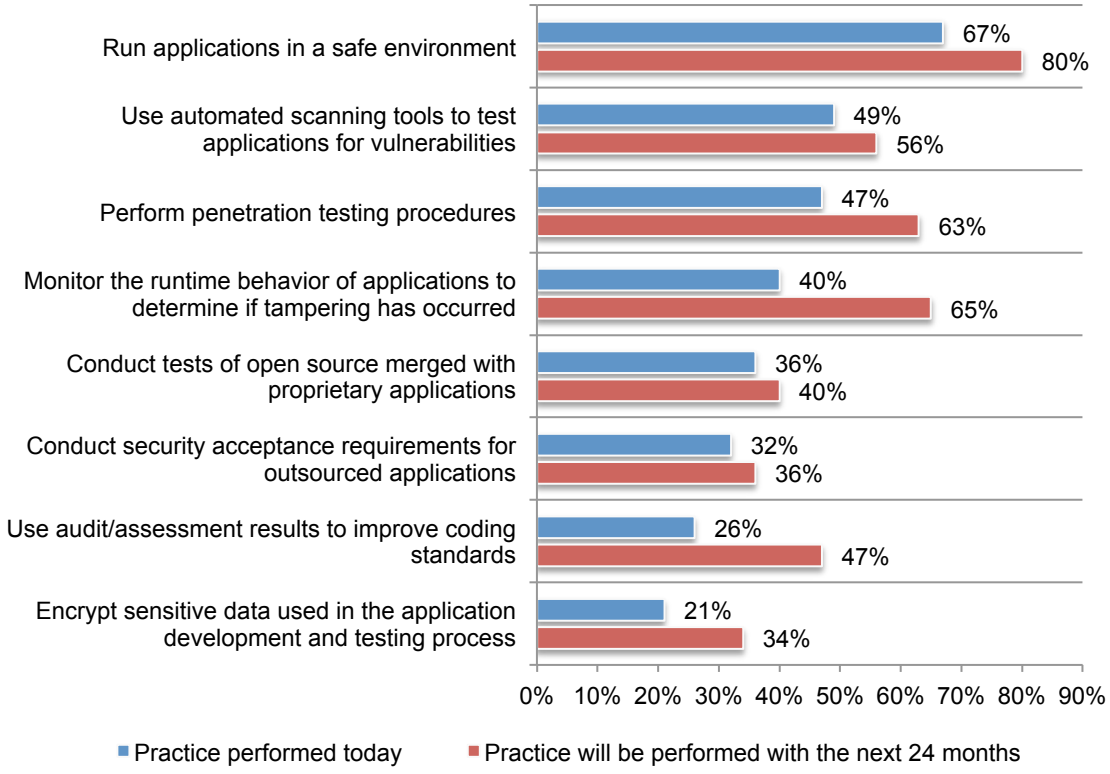


Do secure coding practices affect the application delivery cycle? Fifty percent of respondents say secure coding practices, such as penetration testing, slow down the application delivery cycle within their organizations significantly (12 percent of respondents) or some slowdown (38 percent of respondents). However, 44 percent of respondents say there is no slowdown.

As shown in Figure 20, the secure coding practices most often performed today are: run applications in a safe environment (67 percent of respondents), use automated scanning tools to test applications for vulnerabilities (49 percent of respondents) and perform penetration testing procedures (47 percent of respondents).

In the next 24 months, the following practices will most likely be performed: run applications in a safe environment (80 percent of respondents), monitor the runtime behavior of applications to determine if tampering has occurred (65 percent of respondents) and perform penetration testing procedures (63 percent of respondents).

Figure 20. Secure coding practices today and performed in the next two years
More than one choice permitted



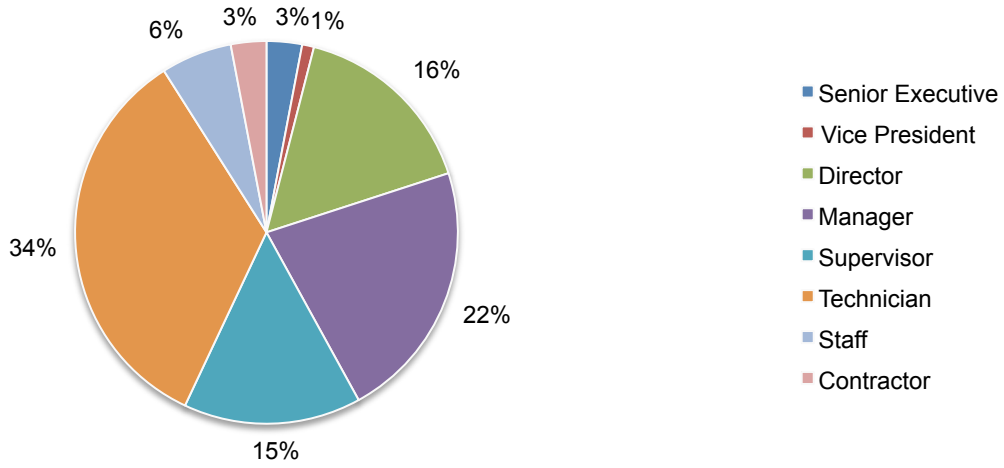
Part 3. Methods

A sampling frame of 16,401 IT and IT security practitioners in the United States who are involved in their organization's application security activities were selected as participants in the research. Table 1 shows 647 total returns. Screening and reliability checks required the removal of 42 surveys. Our final sample consisted of 605 surveys or a 3.7 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,442	100.0%
Total returns	647	3.9%
Rejected or screened surveys	42	0.3%
Final sample	605	3.7%

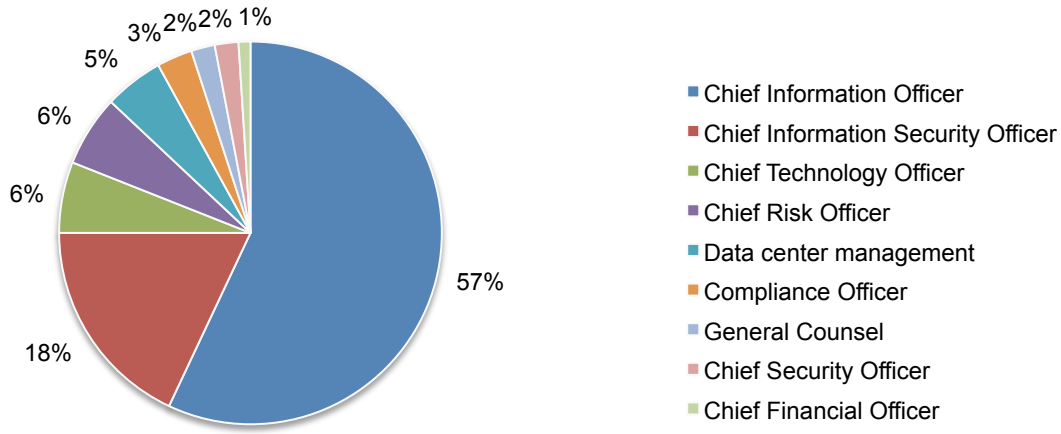
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of the respondents (57 percent) are at or above the supervisory levels.

Pie Chart 1. Current position level within the organization



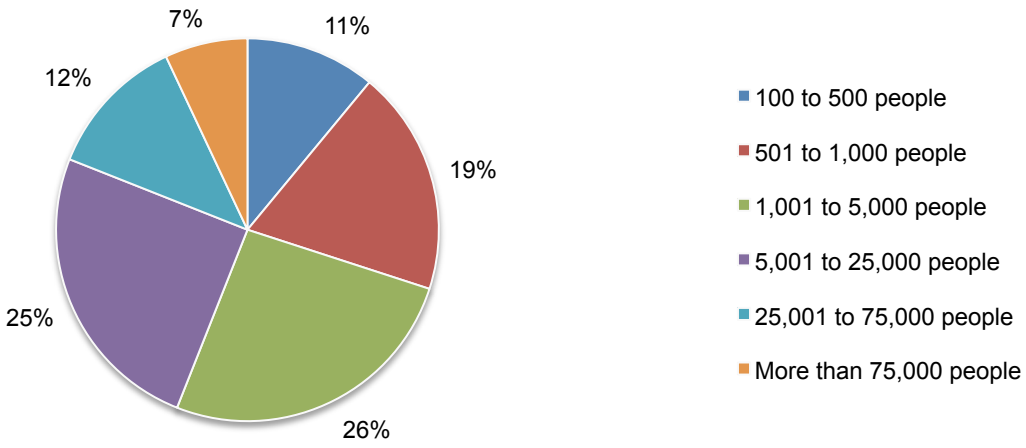
As shown in Pie Chart 2, 57 percent of respondents report directly to the chief information officer and 18 percent report to the chief information security officer.

Pie Chart 2. Direct reporting channel



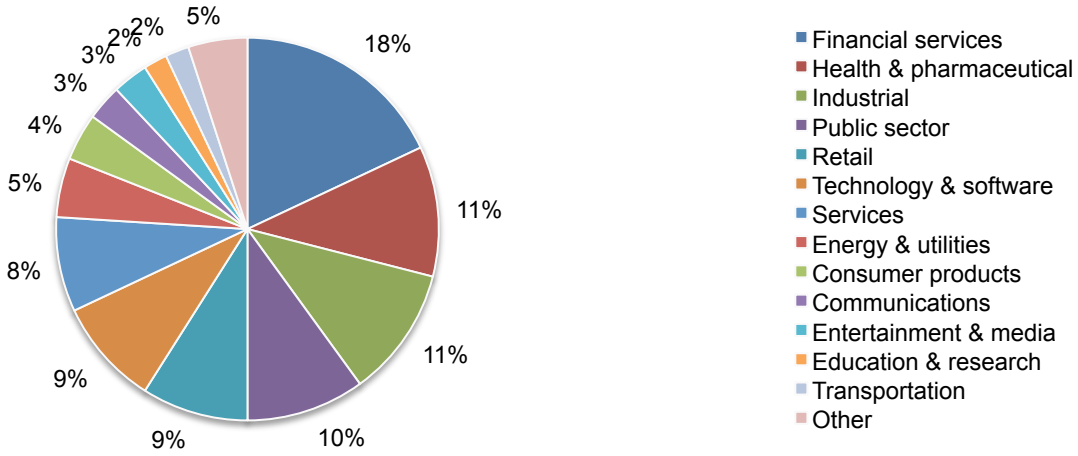
As shown in Pie Chart 3, 70 percent of respondents are from organizations with a global headcount of more than 1,000 employees

Pie Chart 3. Global employee headcount



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

Pie Chart 3. Primary industry focus



Part 4. Caveats to this study

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

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

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from April 25, 2016 through May 9, 2016.

Survey response	Freq	Pct%
Total sampling frame	16,442	100.0%
Total returns	647	3.9%
Screened or rejected surveys	42	0.3%
Final sample	605	3.7%

Part 1. Screening questions

S1. Which of the following best describes your role in the IT security function within your organization? Check all that apply.	Pct%
Setting IT security priorities	48%
Determining IT security strategy	40%
Assessing IT security risks	56%
Developing software applications	29%
Implementing enabling security technologies	50%
Managing IT security spending	37%
Evaluating vendors and contractors	45%
Selecting vendors and contractors	41%
None of the above (stop)	0%
Total	346%

S2. What best defines your level of involvement in your organization's application security activities?	Pct%
Significant involvement	41%
Some involvement	59%
Minimal or no involvement (stop)	0%
Total	100%

Part 2. Background

Q1. Approximately, how many applications does your organization have today?	Pct%
Less than 50	4%
50 to 100	15%
101 to 500	19%
501 to 1,000	29%
1,001 to 2,500	21%
2,501 to 5,000	8%
More than 5,000	4%
Total	100%
Extrapolated value	1,175

Q2. Approximately, what percentage of applications do you consider mission critical?	Pct%
None	0%
1 to 10%	18%
11 to 25%	31%
26 to 50%	29%
51 to 75%	14%
76 to 100%	8%
Total	100%
Extrapolated value	33%

Q3. How confident are you that you know all the applications in your organization today?	Pct%
Very confident	15%
Confident	19%
Somewhat confident	23%
No confidence	43%
Total	100%

Q4. What do you see as the main barriers to achieving a strong application security posture? Please check the top three choices.	Pct%
Lack of visibility in the application layer	57%
Migration to the cloud environment	47%
Lack of skilled or expert personnel	45%
Proliferation of mobile devices	43%
Turf or silo issues between IT security and application development	36%
Lack of budget	28%
Insufficient software testing tools	15%
Lack of executive-level support	10%
Lack of leadership	7%
Not a priority	6%
Other (please specify)	5%
Total	300%

Q5. Who owns your organization's application security risk management process?	Pct%
CIO or CTO	21%
Business units (LOB)	20%
No one person or department	20%
Head of application development	19%
CISO or CSO	11%
Compliance officer	6%
Head of quality assurance	2%
Other (please specify)	1%
Total	100%

Q6. Do you feel your organization's security posture is negatively impacted by a shortage of skilled and/or qualified application developers?	Pct%
Yes	69%
No	31%
Total	100%

Q8. How confident are you that application developers in your organization do the following:	
Q8a. Secure design practices (e.g. secure design principles, threat modeling, architectural risk analysis and so forth)	Pct%
Very confident	12%
Confident	19%
Somewhat confident	25%
No confidence	44%
Total	100%

Q8b. Secure development practices (e.g. input/output validation, defensive programming, using appropriate compiler/linker security options etc.)	Pct%
Very confident	10%
Confident	16%
Somewhat confident	27%
No confidence	47%
Total	100%

Q8c. Secure testing practices (e.g. manually analyzing code for security issues, using static code analysis tools, analyzing software security requirements, creating security test plans/test cases)	Pct%
Very confident	16%
Confident	21%
Somewhat confident	29%
No confidence	34%
Total	100%

Q9. Does the "rush to release" cause application developers in your organization to neglect secure coding procedures and processes?	Pct%
Yes, most likely	30%
Yes, likely	37%
No, not likely	19%
No	14%
Total	100%

Part 3. Changing technology & threat landscape

Q10. Please rate each one of the following two statements using the scale provided below each item.	
Q10a. My organization has ample resources to detect vulnerabilities in applications.	Pct%
Strongly agree	14%
Agree	21%
Unsure	16%
Disagree	28%
Strongly disagree	21%
Total	100%

Q10b. My organization has ample resources to remediate vulnerabilities in applications.	Pct%
Strongly agree	12%
Agree	18%
Unsure	20%
Disagree	27%
Strongly disagree	23%
Total	100%

Q11. Does your organization have a risk-based approach for prioritizing which applications need to be free of insecure code?	Pct%
Yes, formal risk assessment process	18%
Yes, informal risk assessment process	39%
No	43%
Total	100%

Q12. How often does your organization test applications for threats and vulnerabilities?	Pct%
Annually	10%
Twice a year	6%
Every 3 months	6%
Every month	5%
Every week	8%
Every time the code changes	14%
Testing is not pre-scheduled	23%
Unsure	3%
None	25%
Total	100%

Q13. Why does your organization's applications contain vulnerable code? Please rank the following reasons from 1 = most important reason to 4 = least important reason.	Average rank	Rank order
Poor coding by application developers (programmers)	2.09	2
Application developers (programmers) that don't understand secure coding practices	1.63	1
Use of the application development tools and technologies that have inherent bugs	3.53	4
Use of legacy libraries and databases	2.94	3

Q14. How confident are you that your organization can architect around failures in your detection system?	Pct%
Very confident	11%
Confident	12%
Somewhat confident	32%
No confidence	45%
Total	100%

Q15. Do you use any of the following technologies to enhance the security posture of your applications?	Pct%
Micro-segmentation	39%
Linux or Windows containers	37%
Managed, cloud-based application services (databases, object storage etc.)	31%
Policy based infrastructure controllers such as OpenStack Congress	25%
Service chaining, net service header	20%
Total	152%

Q16. What is your organization's primary means of securing applications? Please select one choice	Pct%
Web application firewall (WAF)	30%
Application scanning	21%
Penetration testing	19%
Anti-malware software	7%
Intrusion prevention system (IPS)	6%
Traditional network firewall	5%
Next-generation firewall	5%
Web fraud detection	4%
Other network security controls (please specify)	3%
Total	100%

Q17. How effective is the Web application firewall (WAF) at mitigating the risk of vulnerable code?	Pct%
Very effective	13%
Effective	23%
Not effective	25%
We don't use one	39%
Don't know	0%
Total	100%

Q18a. Approximately, what percentage of your IT security budget is dedicated to application security?	Pct%
None	6%
1 to 10%	31%
11 to 25%	43%
26 to 50%	13%
51 to 75%	7%
76 to 100%	0%
Total	100%
Extrapolated value	18%

Q18b. Approximately, what percentage of your IT security budget is dedicated to network security?	Pct%
None	2%
1 to 10%	12%
11 to 25%	23%
26 to 50%	31%
51 to 75%	20%
76 to 100%	12%
Total	100%
Extrapolated value	39%

Q19a. Attacks at the application layer are more frequent than at the network layer.	Pct%
Strongly agree	29%
Agree	21%
Unsure	33%
Disagree	15%
Strongly disagree	2%
Total	100%

Q19b. Attacks at the application layer are more severe than at the network layer.	Pct%
Strongly agree	33%
Agree	25%
Unsure	30%
Disagree	11%
Strongly disagree	1%
Total	100%

Q19c. Attacks at the application layer are harder to detect than at the network layer.	Pct%
Strongly agree	35%
Agree	28%
Unsure	27%
Disagree	10%
Strongly disagree	0%
Total	100%

Q19d. Attacks at the application layer are more difficult to contain than at the network layer.	Pct%
Strongly agree	35%
Agree	32%
Unsure	24%
Disagree	9%
Strongly disagree	0%
Total	100%

Q20. Which of the following types of incidents or compromises has your organization experienced over the past 12 months because of insecure applications? Please check all that apply.	Pct%
SQL injection	29%
DDoS	25%
Web fraud	21%
Cross-site scripting	18%
MitM/MitB/Credential theft	16%
Clickjacking	11%
Cross-site registry	9%
Other	5%
None of the above	34%
Total	168%

Q21a. Has your organization adopted devops or continuous integration practices into your application development lifecycle?	Pct%
Yes	35%
No	60%
Do not know	5%
Total	100%

Q21b. If yes, why?	Pct%
Ability to reduce time-to-market of updates or enhancements	39%
Ability to respond quickly to security issues and vulnerabilities	56%
Improves application security	71%
Other	2%
None of the above	11%
Total	179%

Q21c. If yes, has your organization realized any of these benefits? Please check all that apply.	Pct%
Ability to reduce time to market of updates or enhancements	38%
Ability to respond quickly to security issues and vulnerabilities	57%
Improves application security	69%
Total	164%

Q22a. Today, what percentage of your business applications are mobile apps?	Pct%
None	0%
1 to 10%	20%
11 to 25%	26%
26 to 50%	35%
51 to 75%	16%
76 to 100%	3%
Total	100%
Extrapolated value	31%

Q22b. In the next 12 months, what percentage of your business applications will be mobile apps?	Pct%
None	0%
1 to 10%	10%
11 to 25%	25%
26 to 50%	35%
51 to 75%	24%
76 to 100%	6%
Total	100%
Extrapolated value	38%

Q23a. Today, what percentage of your business applications is in the cloud?	Pct%
None	2%
1 to 10%	12%
11 to 25%	28%
26 to 50%	31%
51 to 75%	16%
76 to 100%	11%
Total	100%
Extrapolated value	37%

Q23b. In the next 12 months, what percentage of your business applications will be in the cloud?	Pct%
None	0%
1 to 10%	5%
11 to 25%	19%
26 to 50%	36%
51 to 75%	26%
76 to 100%	14%
Total	100%
Extrapolated value	46%

Q24a. Do you believe mobile apps affect your organization's application security risk profile?	Pct%
Significant increase in risk	35%
Increase in risk	25%
No increase in risk	30%
Decrease in risk	9%
Significant decrease in risk	1%
Total	100%

Q24b. Do you believe cloud-based applications affect your organization's security risk profile?	Pct%
Significant increase in risk	26%
Increase in risk	25%
No increase in risk	36%
Decrease in risk	11%
Significant decrease in risk	2%
Total	100%

Q25. Are new Web application frameworks such as Ruby on Rails, Pylon and Django positively affecting the security of applications?	Pct%
Yes	29%
No	59%
Do not know	12%
Total	100%

Q26. Has your organization evaluated and implemented tenant isolation methods or models for segregating application traffic and data (such as segregated VPCs, and OpenStack projects)?	Pct%
Yes	27%
No	60%
Do not know	13%
Total	100%

Q27. In your opinion, is accountability for application security shifting from IT to the end user (e.g., application owner)?	Pct%
Yes	56%
No	39%
Unsure	5%
Total	100%

Q28a. Shadow IT makes application security difficult to achieve.	Pct%
Strongly agree	32%
Agree	33%
Unsure	18%
Disagree	13%
Strongly disagree	4%
Total	100%

Q28b. My organization's IT function does not have visibility into all the applications deployed.	Pct%
Strongly agree	34%
Agree	34%
Unsure	17%
Disagree	12%
Strongly disagree	3%
Total	100%

Q29. How confident are you that your organization's SSL-encrypted traffic is being inspected (i.e., does not contain malware)?	Pct%
Very confident	11%
Confident	18%
Somewhat confident	15%
Not confident	30%
No confidence	26%
Total	100%

Part 4. Future state of application security programs

Following are trends that might impact the state of application security in the future. Please use the 1-to-10 scale below each item to denote whether or not the trend will strengthen or weaken the state of application security within your organization over the next 24 months.	5 & below (Weaken)	6 & above (Strengthen)
Q30a. Migration to the cloud	55%	45%
Q30b. Use of mobile platforms	71%	29%
Q30c. Use of virtualization technologies	50%	50%
Q30d. Demand for mobile apps in the workplace	65%	35%
Q30e. Outsourced application development resources	53%	47%
Q30f. Unmet demand for skilled application developers	77%	23%
Q30g. Use of employee-owned mobile devices in the workplace (a.k.a. BYOD)	66%	34%
Q30h. Rise of the Internet of Things (a.k.a. IoT)	69%	31%
Q30i. Use of open source software	52%	48%
Q30j. New and emerging IT security and privacy compliance requirements	46%	54%
Q30k. New and emerging cyber security threats	88%	12%

Q31. The following table lists four phases of the system development life cycle (SDLC). Please proportionally allocate all 100 points to show where applications are or should be tested for vulnerabilities within your organization.	
Q31a. Where testing happens today	Points
Design	19
Development	20
Launch	19
Post-launch	42
Total points	100

Q31b. Where testing **should** happen	Points
Design	38
Development	25
Launch	17
Post-launch	20
Total points	100

Q32. Following is a list of eight secure coding practices. Please identify all the practices that are presently performed by application developers within your organization today. Also, please estimate the practices that will be performed 24 months from now within your organization.	
Q32a. Practice performed today	Pct%
Use automated scanning tools to test applications for vulnerabilities	49%
Conduct security acceptance requirements for outsourced applications	32%
Monitor the runtime behavior of applications to determine if tampering has occurred	40%
Run applications in a safe environment	67%
Encrypt sensitive data used in the application development and testing process	21%
Use audit/assessment results to improve coding standards	26%
Conduct tests of open source merged with proprietary applications	36%
Perform penetration testing procedures	47%
Total	318%

Q32b. Practice will be performed with the next 24 months	Pct%
Use automated scanning tools to test applications for vulnerabilities	56%
Conduct security acceptance requirements for outsourced applications	36%
Monitor the runtime behavior of applications to determine if tampering has occurred	65%
Run applications in a safe environment	80%
Encrypt sensitive data used in the application development and testing process	34%
Use audit/assessment results to improve coding standards	47%
Conduct tests of open source merged with proprietary applications	40%
Perform penetration testing procedures	63%
Total	421%

Q33. In your opinion, is the responsibility for securing applications moving closer to the application developer?	Pct%
Yes	60%
No	33%
Unsure	7%
Total	100%

Q34. In your opinion, do secure coding practices (such as penetration testing) slow down the application delivery cycle within your organization today?	Pct%
Yes, significant slowdown	12%
Yes, some slowdown	38%
No slowdown	44%
Unsure	6%
Total	100%

Part 5. Your role

D1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	1%
Director	16%
Manager	22%
Supervisor	15%
Technician	34%
Staff	6%
Contractor	3%
Other	0%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
Chief Financial Officer	1%
General Counsel	2%
Chief Information Officer	57%
Chief Technology Officer	6%
Chief Information Security Officer	18%
Chief Security Officer	2%
Compliance Officer	3%
Data center management	5%
Chief Risk Officer	6%
Other	0%
Total	100%

D3. What is the worldwide headcount of your organization?	Pct%
100 to 500 people	11%
501 to 1,000 people	19%
1,001 to 5,000 people	26%
5,001 to 25,000 people	25%
25,001 to 75,000 people	12%
More than 75,000 people	7%
Total	100%

D4. What industry best describes your organization's focus?	Pct%
Agriculture & food service	1%
Communications	3%
Consumer products	4%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	1%
Industrial	11%
Public sector	10%
Retail	9%
Services	8%
Technology & software	9%
Transportation	2%
Other	2%
Total	100%

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

Ponemon Institute

Advancing Responsible Information Management

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

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.