Ponemon INSTITUTE

The Increasing Risk to Enterprise Applications

Sponsored by Prevoty

Independently conducted by Ponemon Institute LLC

Publication Date: November 2015

The Increasing Risk to Enterprise Applications

Ponemon Institute, November 2015

Part 1. Introduction

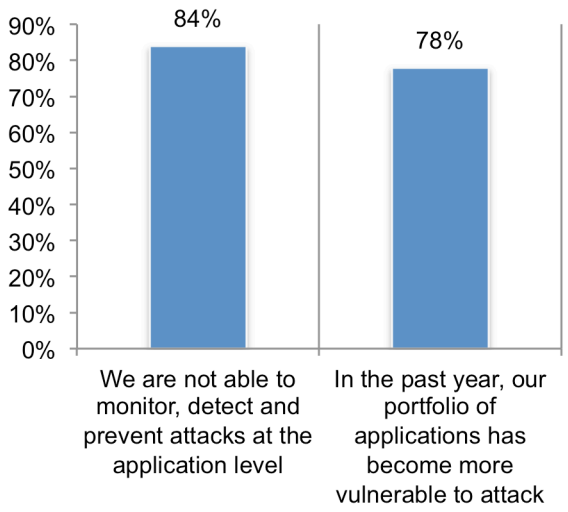
Today's typical organization has thousands of applications supporting their business operations and hundreds of these are considered business critical. *The Increasing Risk to Enterprise Applications* study examines the reasons why the highest level of security risk is considered by many to be in the application layer. Yet, many companies are not making the necessary investment in security measures to mitigate the risk to their business critical applications.

Ponemon Institute, with sponsorship from Prevoty, surveyed 618 IT and IT security practitioners who are familiar with their organizations' approach to securing applications. As part of their responsibilities, most (74 percent of respondents) are engaged in resolving vulnerabilities followed by securing applications and data (69 percent of respondents).

For purposes of this study, enterprise application security refers to the protection of applications from external attacks, privilege abuse and data theft. According to the study, application security is difficult because current solutions are often difficult to implement, too costly and overly complex.

As shown in Figure 1, 78 percent of respondents say just in the past year their organizations' portfolio of applications has become more vulnerable to attack. The most common gateway attack is through SQL injections followed by cross-site scripting. According to 84 percent of respondents, it is difficult to deal with these attacks because their organizations are not able to monitor, detect and prevent attacks at the application level.

Figure 1. Why applications are more at risk
Strongly agree and agree responses combined



Why the risk to application security is increasing. In addition to admitting their organizations are unable to keep up with attacks at the application level, the majority of respondents say they are not able to accomplish the following:

- Stop or curtail attacks to applications by quickly detecting vulnerabilities and threats.
- Manage security of applications across the enterprise and have up-to-date visibility into what is happening in the application environment.
- Ensure the protection of applications is a top security objective with an appropriate level of investment.
- Respond quickly to hacker attacks against applications.
- Quickly perform patches on applications in production.

In addition, applications are at risk due to the movement of application delivery platforms to the cloud that has resulted in the loss of control and visibility over business critical application and because web application firewalls are not considered sufficient to protect internally developed web applications.

Part 2. Key findings

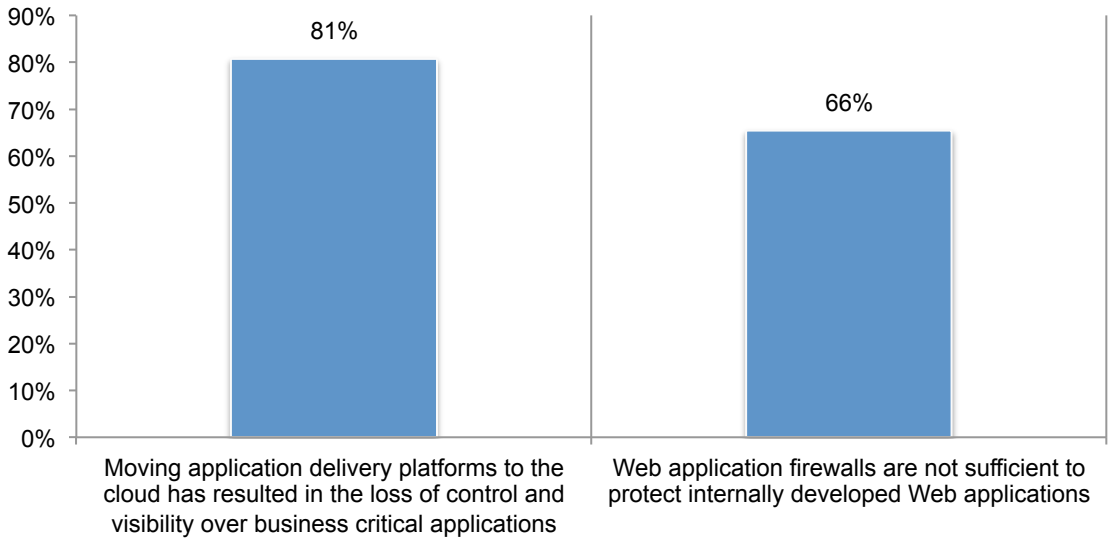
In this section, we discuss the detailed findings. The complete audited findings are presented in the appendix of this report. The research is organized into the following topics:

- **Why applications are more vulnerable to attack**
- **How companies are addressing vulnerabilities in enterprise applications**

Hundreds of deployed applications are considered business critical and at risk. At any one point in time, an average of 2,562 business applications are deployed within the organizations represented in this research and 30 percent of these applications are considered business critical.

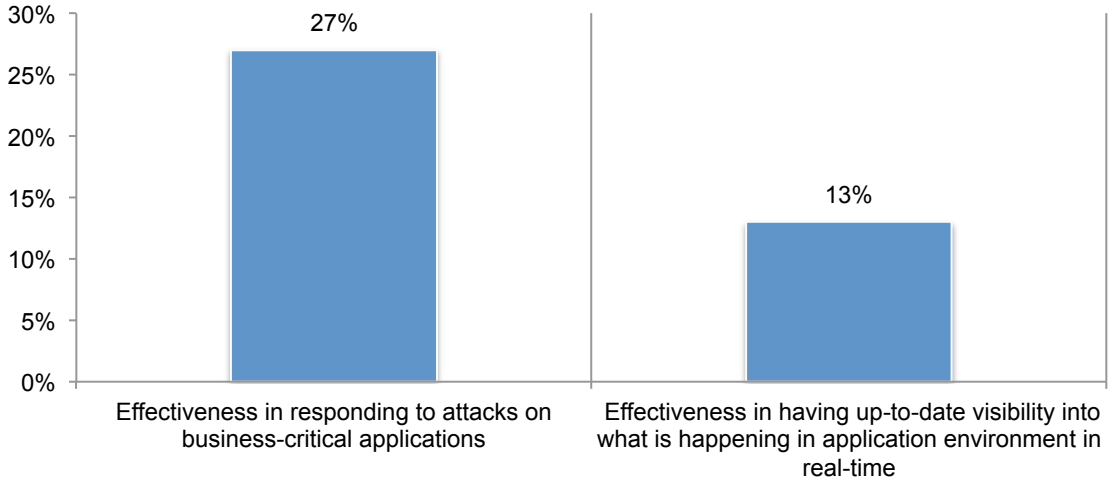
In addition to the inability to monitor, detect and prevent attacks, the cloud is putting applications at risk. As shown in Figure 2, the movement of application delivery platforms to the cloud has resulted in the loss of control and visibility over business critical applications (81 percent of respondents). Further, web application firewalls are not considered sufficient to protect internally developed web applications (66 percent of respondents).

Figure 2. Perceptions about the increasing risk to enterprise applications
Strongly agree and agree responses combined



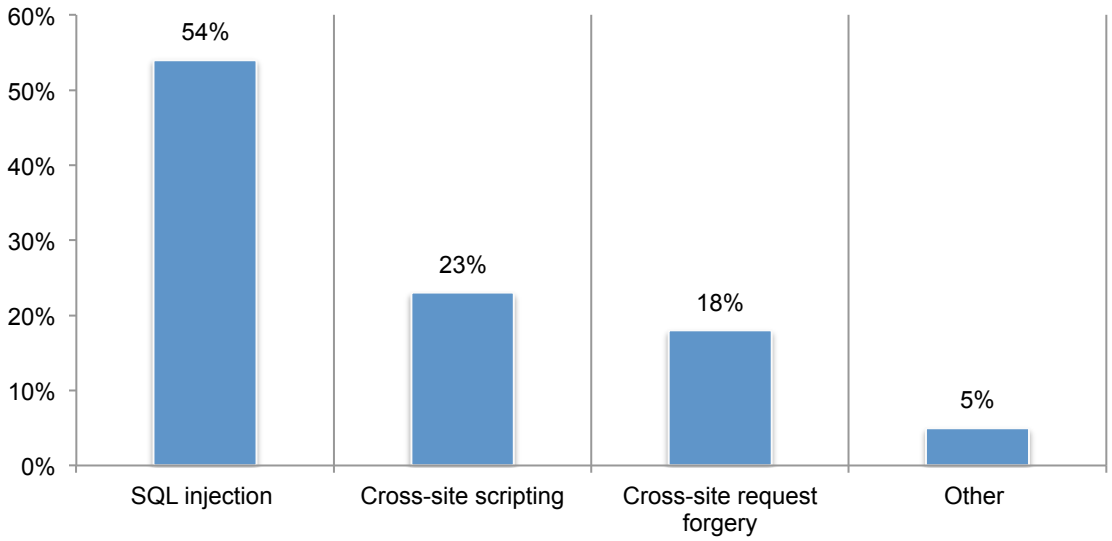
In fact, according to Figure 3, only 13 percent of respondents rate having up-to-date visibility into what is happening in its application environment as highly effective and only 27 percent of respondents rate their ability to respond to attacks on business-critical applications as highly effective.

Figure 3. How effective is your organization in responding to attacks and do you have up-to-date visibility of the application environment?
1 = low effectiveness to 10 = high effectiveness, 7+responses reported



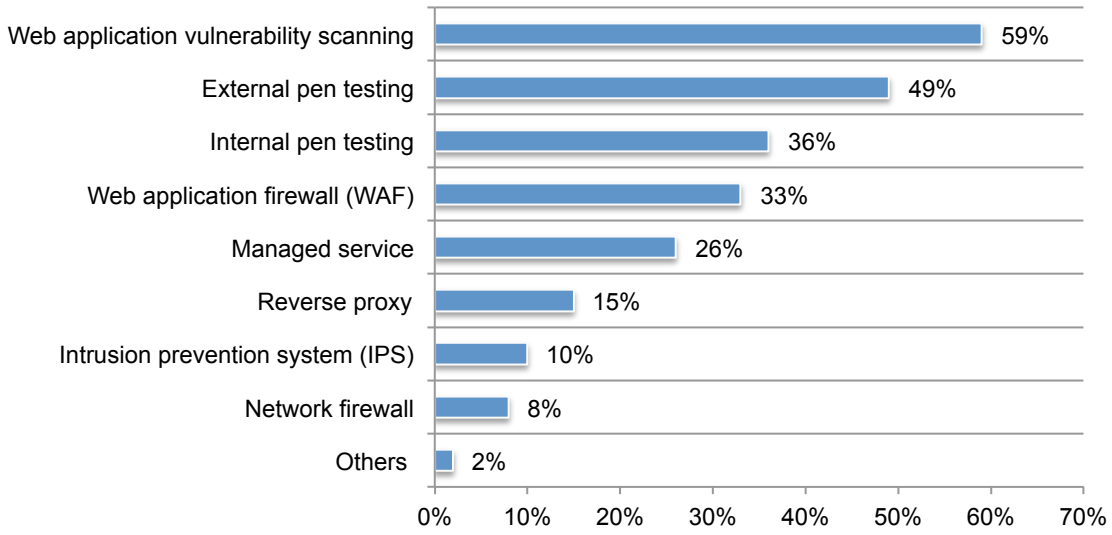
Applications today are exploitable in many ways. As shown in Figure 4, 54 percent of respondents say the most common gateway attack experienced by their organization over the past 12 months is an SQL injection followed by cross-site scripting (23 percent of respondents) and cross-site request forgery (18 percent of respondent).

Figure 4. What is the most common gateway attack experienced by your organization over the past 12 months?



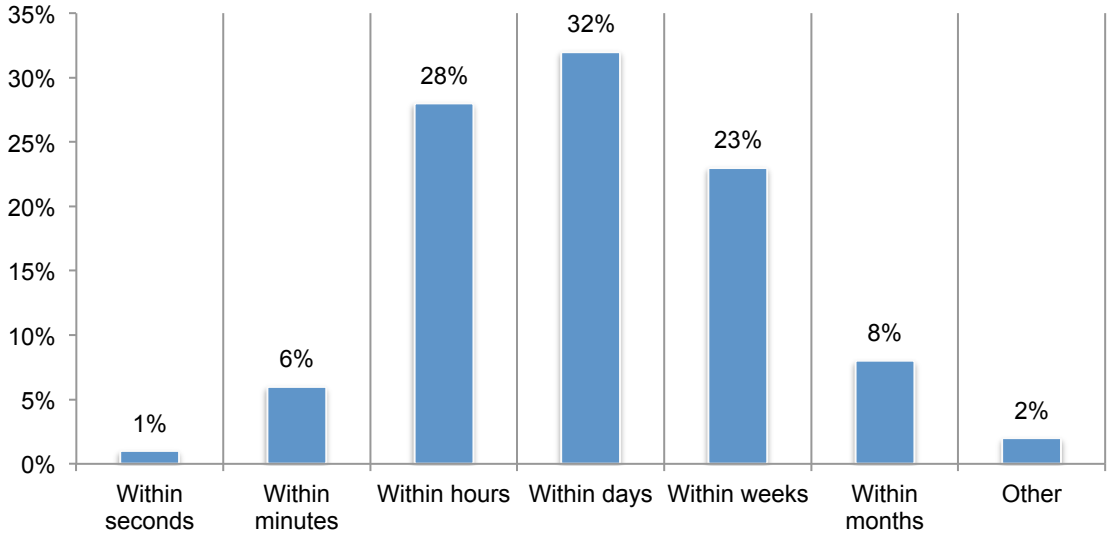
How organizations keep applications secure. As shown in Figure 5, the primary means of securing applications are web application vulnerability scanning (59 percent of respondents) followed by external pen testing (49 percent of respondents) and internal pen testing (36 percent of respondents).

Figure 5. What are your primary means of securing applications?
More than one response permitted



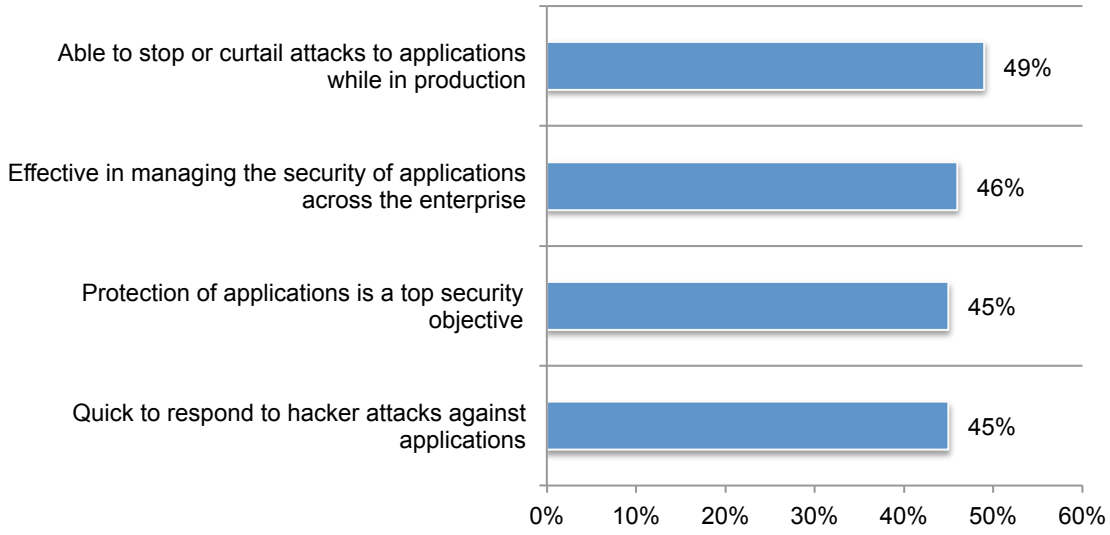
Applications while in production are vulnerable. However, less than half of respondents (49 percent) say their organizations' are able to stop or curtail attacks to applications while in production. As shown in Figure 6, 31 percent of respondents say it can take weeks (23 percent of respondents) or months (8 percent of respondents) to shore up an application in production mode after the detection of a vulnerability.

Figure 6. How long does it take to shore up an application in production mode after detection of a vulnerability?



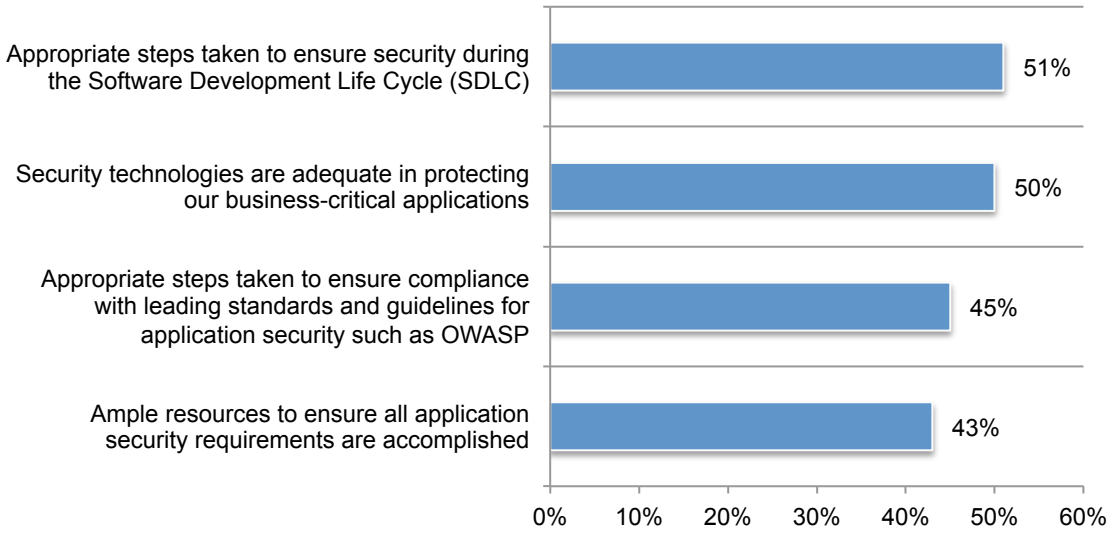
The majority of respondents admit to weaknesses in their application security practices. Fewer respondents are confident that their organization is effective in managing the security of applications across the enterprise (46 percent of respondents) and 45 percent say their organization is quick in responding to hacker attacks against applications, as shown in Figure 7.

Figure 7. More perceptions about application security
Strongly agree and agree responses combined



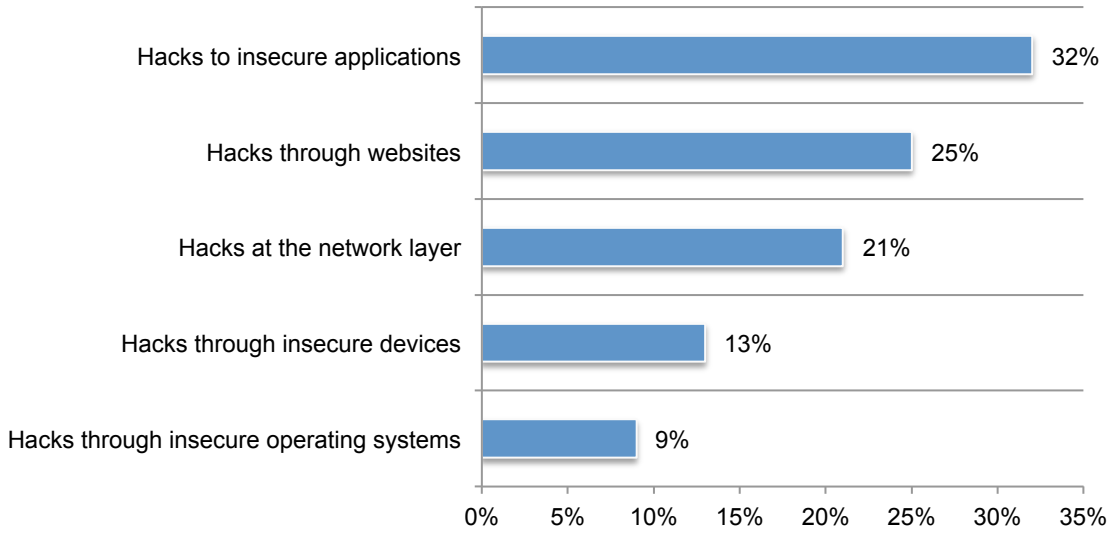
How organizations practice application security. According to Figure 8, 50 percent of respondents say their security technologies are adequate in protecting their business-critical applications. However, only 43 percent of respondents say their organization has ample resources to ensure all application security requirements are accomplished. Moreover, only 45 percent of respondents say they take appropriate steps to ensure compliance with leading standards and guidelines for application security such as OWASP.

Figure 8. Perceptions about resources and practices to secure applications
Strongly agree and agree responses combined



The highest level of security risk and vulnerability is in the application layer. Applications are considered to pose the highest security risk for organizations but networks receive the highest level of annual spending in the IT security. As shown in Figure 9, the kinds of attacks that create the greatest worry are hacks to insecure applications (32 percent of respondents) and hacks through websites (25 percent of respondents). Only 21 percent say they worry about hacks at the network layer.

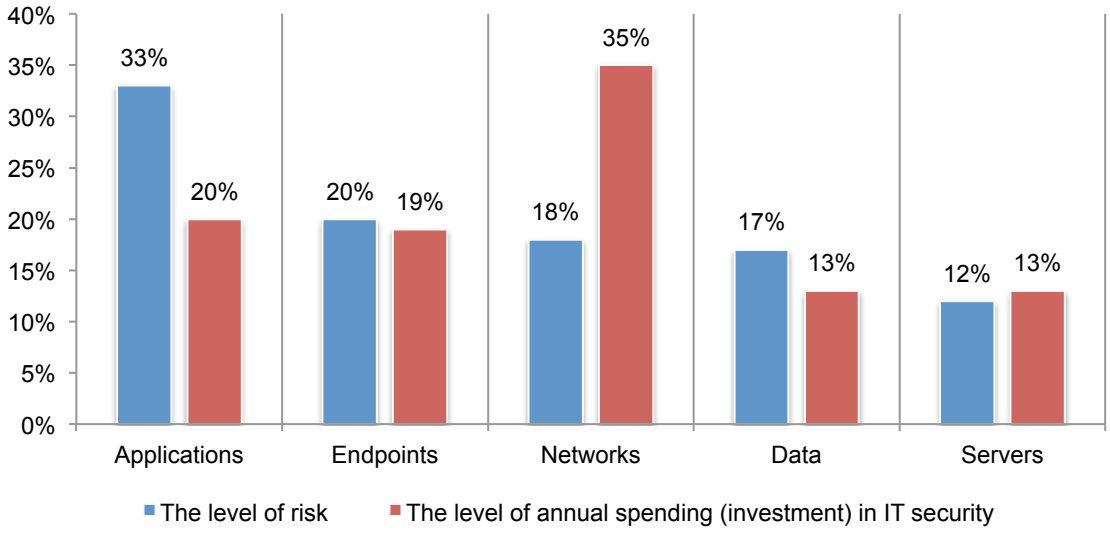
Figure 9. What kinds of attacks concern your organization most?



Investment in application security is not commensurate with the risk. An average of 16 percent of the overall IT budget is dedicated to data protection and security. Figure 10, reveals how respondents allocated the level of risk to the following five areas: applications, endpoints, networks, data and servers and the level of annual spending (investment) in IT security to these same areas.

There is a significant gap between the level of application risk (33 percent of total risk) and what companies are spending to protect their applications (20 percent of annual spending in IT security). However, the level of risk to networks is much lower (18 percent) than the investment in network security (35 percent).

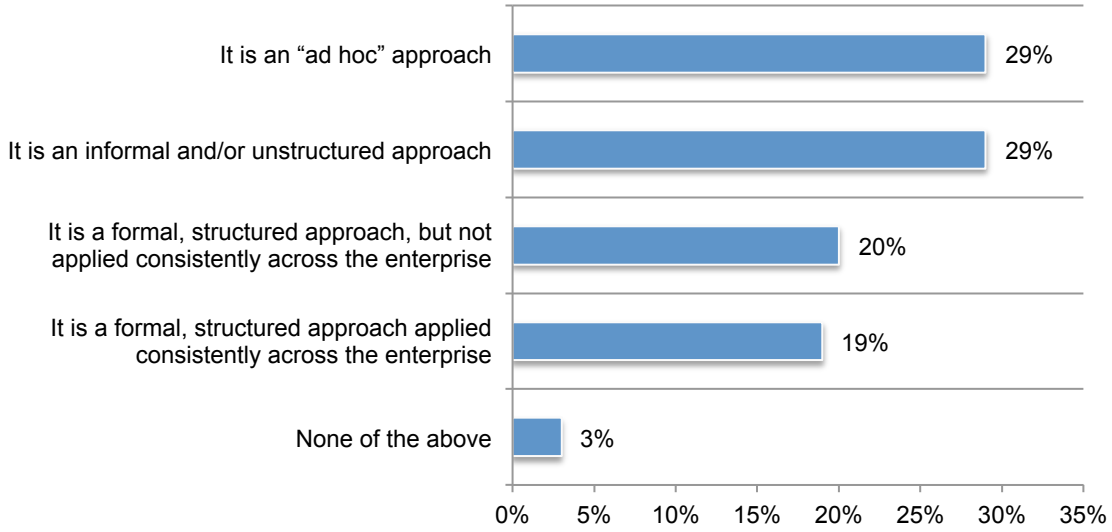
Figure 10. Gaps in security risks and the allocation of spending



Addressing vulnerabilities in enterprise applications

Majority of organizations represented in this research (51 percent of respondents) take steps to ensure security in the SSDLC[1]. According to Figure 11, 58 percent of respondents say the approach is informal or ad hoc.

Figure 11. What best describes the SSDLC in your organization?

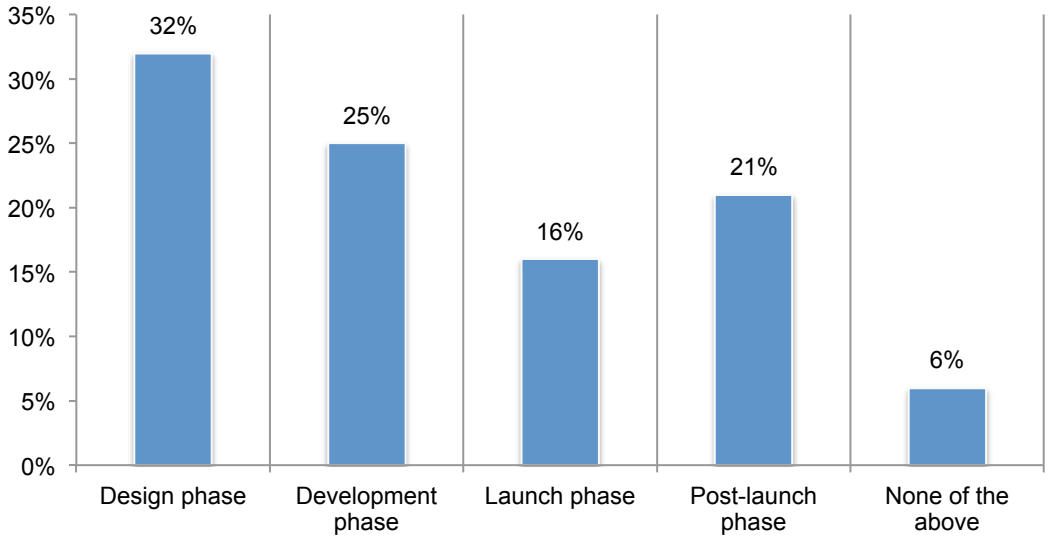


[1] **Secure Software Development Life Cycle** (or SSDLC) is the process, which is followed to develop a software product safely and securely. It is a structured way of building software applications with security as a top of mind consideration.

Further analysis of the findings, reveals only 30 percent of respondents rate the level of maturity of their organizations' SSDLC as mature (7+ on a scale of 1 = immature to 10 = mature). Fifty-five percent of respondents say security is not adequately emphasized during the development of new applications and only 25 percent say security features are built into applications under development.

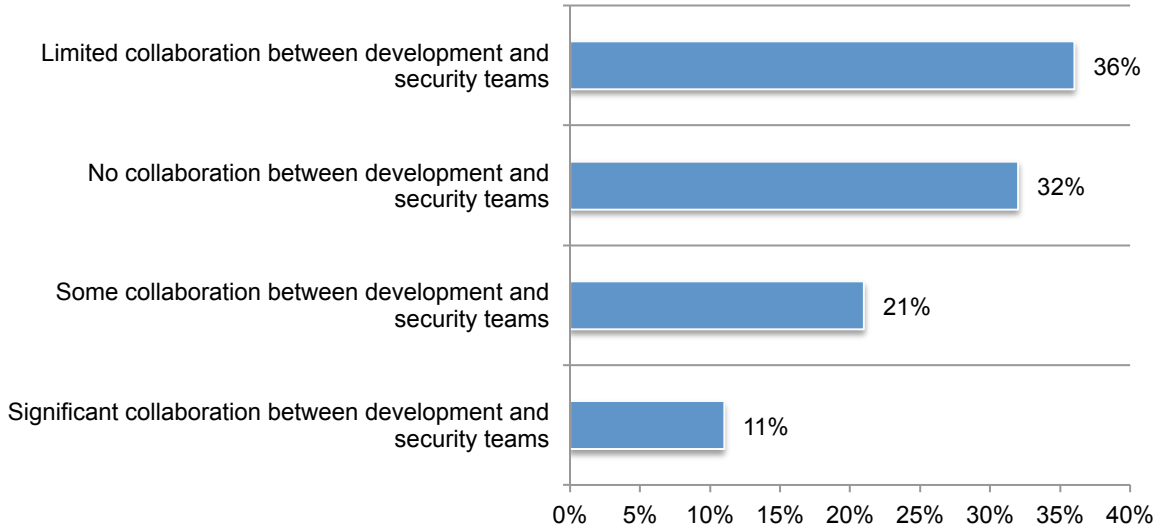
As shown in Figure 12, 32 percent of respondents say their organizations build security features into applications under development in the design phase. Twenty-five percent of respondents say security is built into the development phase, 16 percent responded the launch phase and 21 percent responded the post-launch phase of applications under development.

Figure 12. Where in the SSDLC does your organization build security features into applications under development?



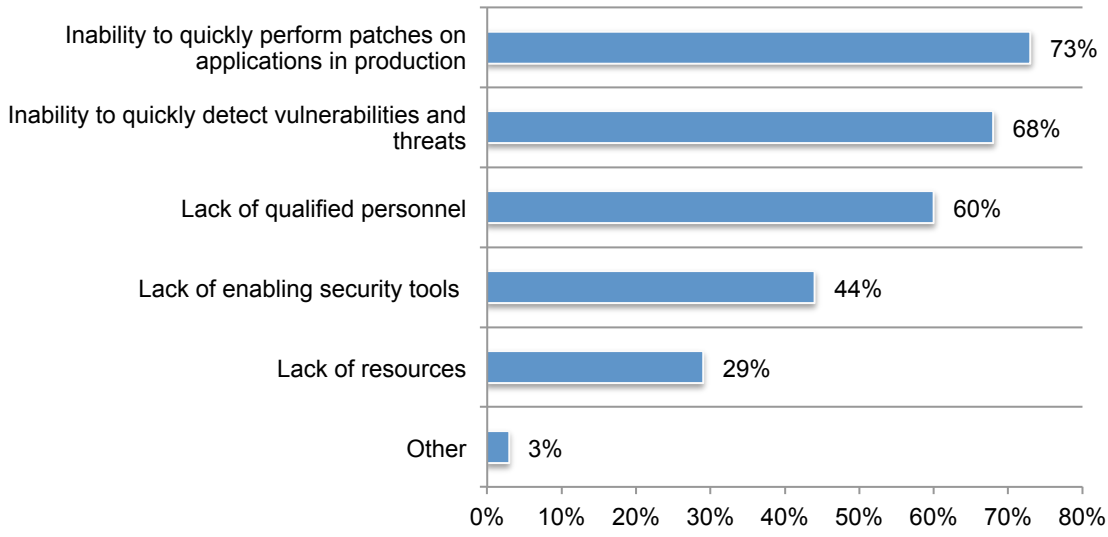
The reason for the lack of maturity and the failure to address security in the development of new applications is caused by poor collaboration between the application development and security teams. According to Figure 13, 68 percent of respondents say such collaboration is limited (36 percent) or non-existent (32 percent).

Figure 13. What best describes the nature of collaboration between your organization's application development and security teams?



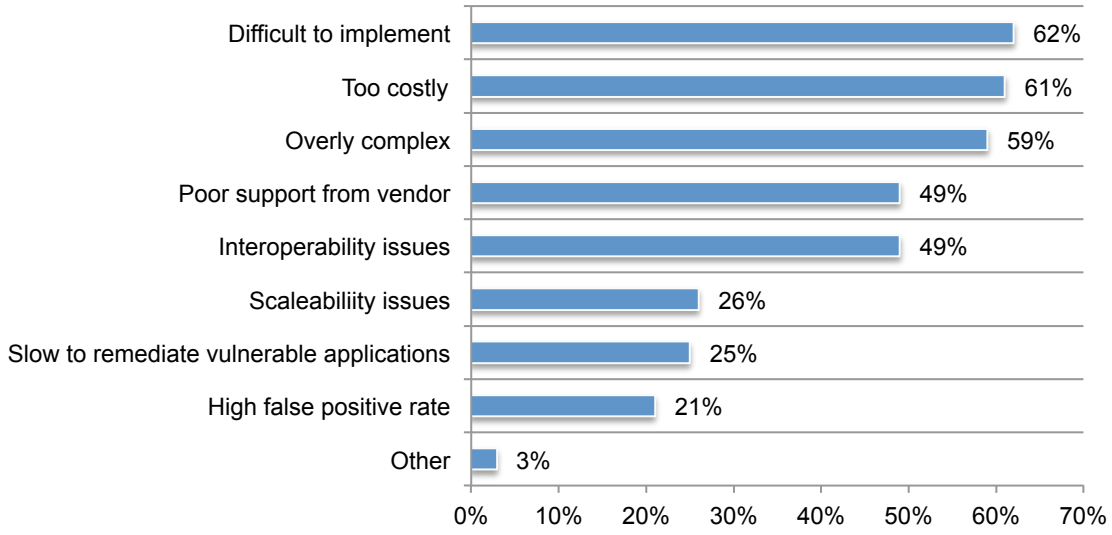
The remediation of vulnerabilities in applications is considered very difficult. Sixty-four percent of respondents say it is either very difficult or difficult to remediate vulnerabilities in applications. Figure 14 reveals that this difficulty is mainly due to the inability to quickly perform patches on applications in production (73 percent of respondents), the inability to quickly detect vulnerabilities and threats (68 percent of respondents) and lack of qualified personnel (60 percent of respondents).

Figure 14. Why is it very difficult or difficult to remediate vulnerabilities in applications?
More than one response permitted



Fifty-one percent of respondents say their organizations have a vulnerability backlog of applications that have been identified as vulnerable but not remediated and an average of 45 percent of vulnerable applications have not been remediated. According to Figure 15, reasons for the problems with remediation are difficulty in implementation, too costly and overly complex.

Figure 15. What is wrong with current solutions to remediate vulnerabilities in applications?
More than one response permitted



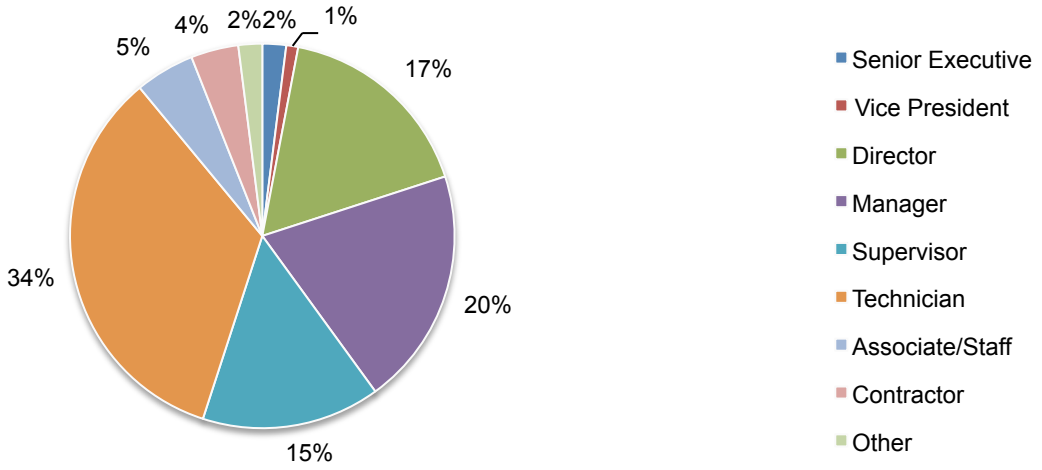
Part 3. Methods

A sampling frame of 16,889 IT security practitioners in the U.S. who are familiar with their organizations' approach to securing applications were selected as participants to this survey. Table 1 shows 701 total returns. Screening and reliability checks required the removal of 83 surveys. Our final sample consisted of 618 surveys or a 3.7 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,889	100.0%
Total returns	701	4.2%
Rejected or screened surveys	83	0.5%
Final sample	618	3.7%

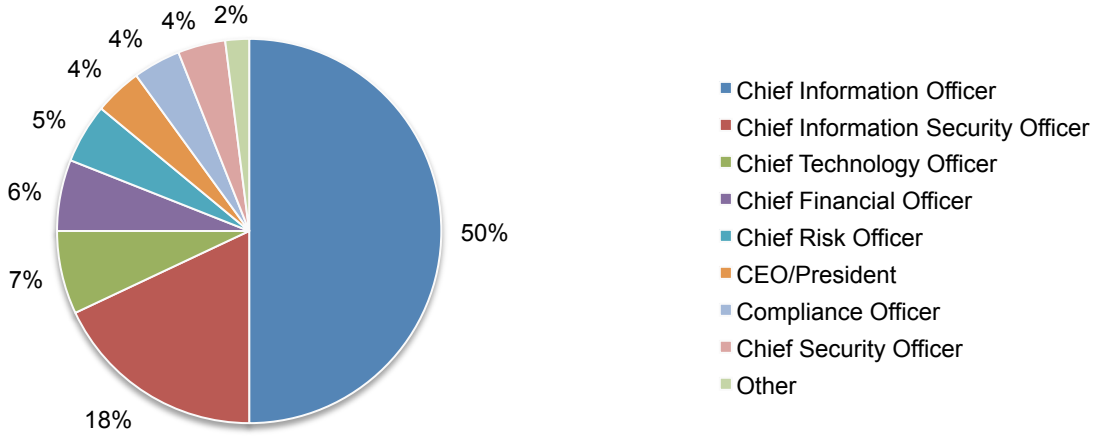
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of respondents (55 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



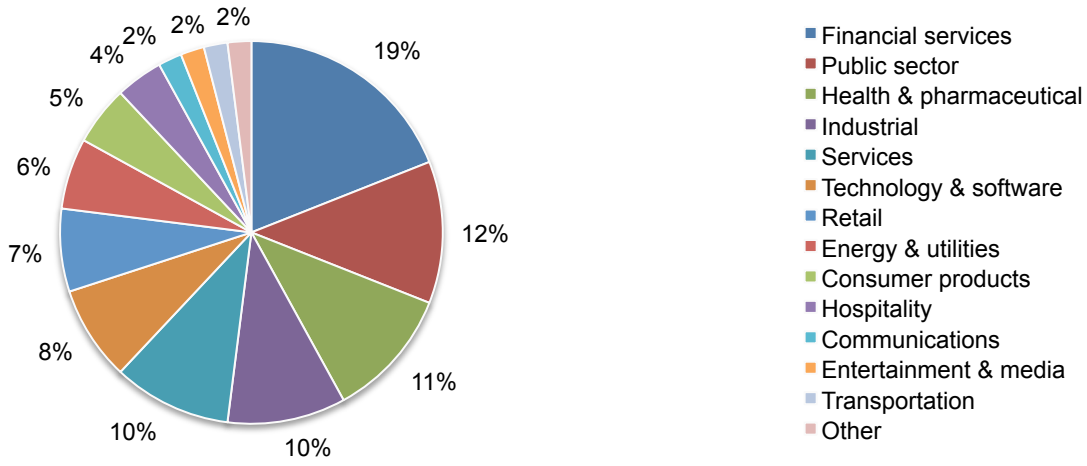
As shown in Pie Chart 2, half of the respondents indicated they report directly to the CIO and another 18 percent report to the CISO.

Pie Chart 2. Primary Person you or your supervisor reports to



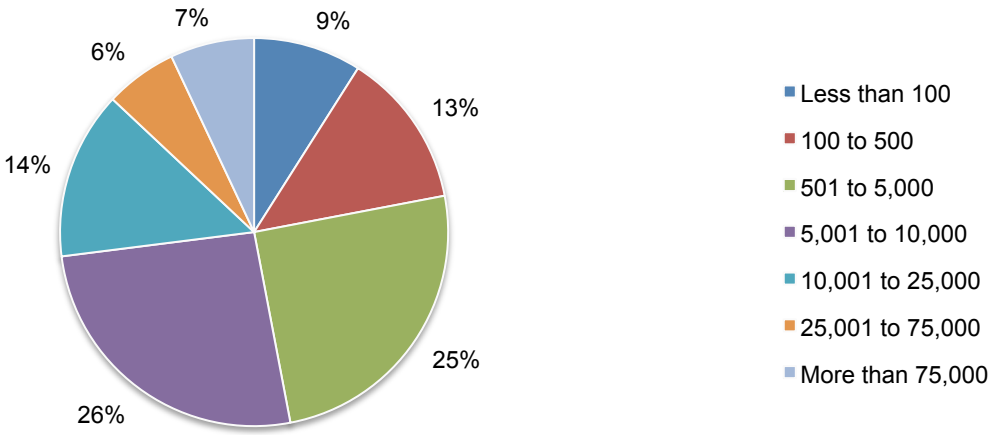
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (12 percent) and health & pharmaceutical (11 percent).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 4, 53 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 4. Global employee headcount



Part 4. Caveats to this study

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

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

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

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in September 2015.

Sample response	Freq.	Pct%
Total sampling frame	16889	100.0%
Total returns	701	4.2%
Rejected or screened surveys	83	0.5%
Final sample	618	3.7%

Part 1. Screening

S1. Which of the following best describes your role in the secure software development life cycle	Pct%
Writing secure code	50%
Implementing security technologies	51%
Testing applications	29%
Ensuring compliance	59%
Resolving vulnerabilities	74%
Securing applications and data	69%
None of the above (Stop)	0%
Total	332%

S2. How familiar are you with your organization's approach to securing applications?	Pct%
Very familiar	38%
Familiar	43%
Somewhat familiar	19%
No knowledge (Stop)	0%
Total	100%

Part 2. Attributions: Following are attributions about your organization's application security. Strongly agree and Agree responses.	SA%	A%
Q1. My organization's security technologies are adequate in protecting our business-critical applications.	23%	27%
Q2. My organization takes appropriate steps to ensure security during the Software Development Life Cycle (SDLC).	20%	31%
Q3. My organization takes appropriate steps to ensure compliance with leading standards and guidelines for application security such as OWASP.	18%	27%
Q4. My organization has ample resources to ensure all application security requirements are accomplished.	18%	25%
Q5. My organization is quick in responding to hacker attacks against applications.	21%	24%
Q6. My organization is effective in managing the security of applications across the enterprise.	20%	26%
Q7. The protection of applications is a top security objective within my organization.	17%	28%
Q8. My organization is able to stop or curtail attacks to applications while in production.	18%	31%
Q9. It is difficult to reduce the risk to applications because we are not able to monitor, detect and prevent attacks at the application level.	40%	44%
Q10. Web application firewalls are not sufficient to protect internally developed Web applications.	26%	40%
Q11. Moving application delivery platforms to the cloud has resulted in the loss of control and visibility over business critical applications.	41%	40%
Q12. In the past year, our organization's portfolio of applications has become more vulnerable to attack.	35%	43%

Part 3. Background

Q13. What best describes the SSDLC in your organization?	Pct%
It is a formal, structured approach applied consistently across the enterprise	19%
It is a formal, structured approach, but not applied consistently across the enterprise	20%
It is an informal and/or unstructured approach	29%
It is an "ad hoc" approach	29%
None of the above	3%
Total	100%

Q14. Using the following 10-point scale, please rate the level of maturity of your organization's SSDLC.	Pct%
1 or 2 (immature)	20%
3 or 4	19%
5 or 6	31%
7 or 8	20%
9 or 10 (mature)	10%
Total	100%
Extrapolated value	5.12

Q15. Where in the SSDLC does your organization build in security features into applications under development?	Pct%
Design phase	32%
Development phase	25%
Launch phase	16%
Post-launch phase	21%
None of the above	6%
Total	100%

Q16. In your opinion, is security adequately emphasized during the development of new applications?	Pct%
Yes	39%
No	55%
Unsure	6%
Total	100%

Q17. Approximately, how many business applications are deployed within your organization (at any point in time)?	Pct%
Less than 100	5%
100 to 500	9%
501 to 1,000	11%
1,001 to 2,500	34%
2,501 to 5,000	23%
More than 5,000	18%
Total	100%
Extrapolated value	2,562

Q18. What percentage of all deployed applications are considered business-critical?	Pct%
Less than 5%	5%
5 to 10%	17%
11 to 25%	36%
26 to 50%	22%
51 to 75%	13%
76 to 100%	7%
Total	100%
Extrapolated value	30%

Q19. How long does it take to shore up an application in production mode after a vulnerability is detected?	Pct%
Within seconds	1%
Within minutes	6%
Within hours	28%
Within days	32%
Within weeks	23%
Within months	8%
Other (please specify)	2%
Total	100%

Q20. Applications today are exploitable in many ways. What is the most common gateway attack experienced by your organization over the past 12 months?	Pct%
Cross-site scripting	23%
SQL injection	54%
Cross-site request forgery	18%
Other (please specify)	5%
Total	100%

Q21a. How difficult is it to remediate vulnerabilities in applications?	Pct%
Very difficult	31%
Difficult	33%
Somewhat difficult	24%
Not difficult	7%
Easy	5%
Total	100%

Q21b. [If difficult or very difficult] Why is it difficult to remediate vulnerabilities in applications?	Pct%
Inability to quickly detect vulnerabilities and threats	68%
Inability to quickly perform patches on applications in production	73%
Lack of enabling security tools	44%
Lack of qualified personnel	60%
Lack of resources	29%
Other (please specify)	3%
Total	277%

Q22a. Does your organization have a vulnerability backlog (i.e. applications that have been identified as vulnerable but have not been remediated)?	Pct%
Yes	51%
No	41%
Don’t know	8%
Total	100%

Q22b. If yes, what percentage of vulnerable applications have not been remediated?	Pct%
Less than 5%	5%
5 to 10%	7%
11 to 25%	13%
26 to 50%	35%
51 to 75%	26%
76 to 100%	14%
Total	100%
Extrapolated value	45%

Q23. What is wrong with current solutions to remediate vulnerabilities in applications?	Pct%
Too costly	61%
Overly complex	59%
Difficult to implement	62%
Interoperability issues	49%
Scaleabiliity issues	26%
Poor support from vendor	49%
High false positive rate	21%
Slow to remediate vulnerable applications	25%
Other (please specify)	3%
Total	355%

Q24. The following table lists five areas of potential security risks and vulnerabilities for your organization. Please allocate 100 points to denote the level of risk presented by each area.	Total points
Networks	18
Servers	12
Endpoints	20
Applications	33
Data	17
Total	100

Q25. The following table lists five areas of potential security risks and vulnerabilities. Please allocate 100 points to denote the level of annual spending (investment) in IT security.	Total points
Networks	35
Servers	13
Endpoints	19
Applications	20
Data	13
Total	100

Q26. How much of the present year's overall IT budget is dedicated to data protection/security?	Pct%
Less than 5%	13%
6% to 10%	28%
11% to 20%	32%
21% to 30%	15%
31% to 40%	9%
41% to 50%	2%
More than 50%	1%
Total	100%
Extrapolated value	16%

Q27. How much of the data security budget is invested in application security?	Pct%
Less than 5%	4%
6% to 10%	26%
11% to 20%	29%
21% to 30%	19%
31% to 40%	15%
41% to 50%	7%
More than 50%	0%
Total	100%
Extrapolated value	20%

Q28. What best describes the nature of collaboration between your organization's application development and security teams.	Pct%
Significant collaboration between development and security teams	11%
Some collaboration between development and security teams	21%
Limited collaboration between development and security teams	36%
No collaboration between development and security teams	32%
Total	100%

Q29. What kind of attacks concerns your organization the most?	Pct%
Hacks at the network layer	21%
Hacks through insecure devices	13%
Hacks through websites	25%
Hacks through insecure operating systems	9%
Hacks to insecure applications	32%
Total	100%

Q30. What is your primary means of securing applications? Please select all that apply.	Pct%
Intrusion prevention system (IPS)	10%
Web application firewall (WAF)	33%
Network firewall	8%
Reverse proxy	15%
Web application vulnerability scanning	59%
Managed service	26%
External pen testing	49%
Internal pen testing	36%
Others (please specify)	2%
Total	238%

Q31. To the best of your knowledge, are your organization's applications compliant with all regulations for data protection and information security?	Pct%
Yes, for all applications	9%
Yes, for most applications	25%
Yes, but only for some applications	25%
No	38%
Unsure	3%
Total	100%

Q32. How effective is your organization in having up-to-date visibility into what is happening in its application environment in real-time? Please use the following 10-point scale from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	32%
3 or 4	30%
5 or 6	25%
7 or 8	12%
9 or 10	1%
Total	100%
Extrapolated value	3.90

Q33. How effective is your organization's ability to respond to attacks on business-critical applications? Please use the following 10-point scale from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	15%
3 or 4	23%
5 or 6	35%
7 or 8	19%
9 or 10	8%
Total	100%
Extrapolated value	5.14

Part 4. Organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	1%
Director	17%
Manager	20%
Supervisor	15%
Technician	34%
Associate/Staff	5%
Contractor	4%
Other (please specify)	2%
Total	100%

D2. Check the Primary Person you or your supervisor reports to within your organization.	Pct%
CEO/President	4%
Chief Financial Officer	6%
Chief Information Officer	50%
Chief Information Security Officer	18%
Compliance Officer	4%
Chief Privacy Officer	0%
Director of Internal Audit	1%
General Counsel	1%
Chief Technology Officer	7%
Human Resources VP	0%
Chief Security Officer	4%
Chief Risk Officer	5%
Other (please specify)	0%
Total	100%

D3. What industry best describes your organization's industry concentration or focus?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Energy & utilities	6%
Entertainment & media	2%
Financial services	19%
Health & pharmaceutical	11%
Hospitality	4%
Industrial	10%
Public sector	12%
Retail	7%
Services	10%
Technology & software	8%
Transportation	2%
Other (please specify)	0%
Total	100%

D8. What is the worldwide headcount of your organization?	Pct%
Less than 100	9%
100 to 500	13%
501 to 5,000	25%
5,001 to 10,000	26%
10,001 to 25,000	14%
25,001 to 75,000	6%
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 confidentiality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.