Application Security in the DevOps Environment

Research sponsored by HCL Software

Independently Conducted by Ponemon Institute LLC

September 2020

Part 1. Introduction

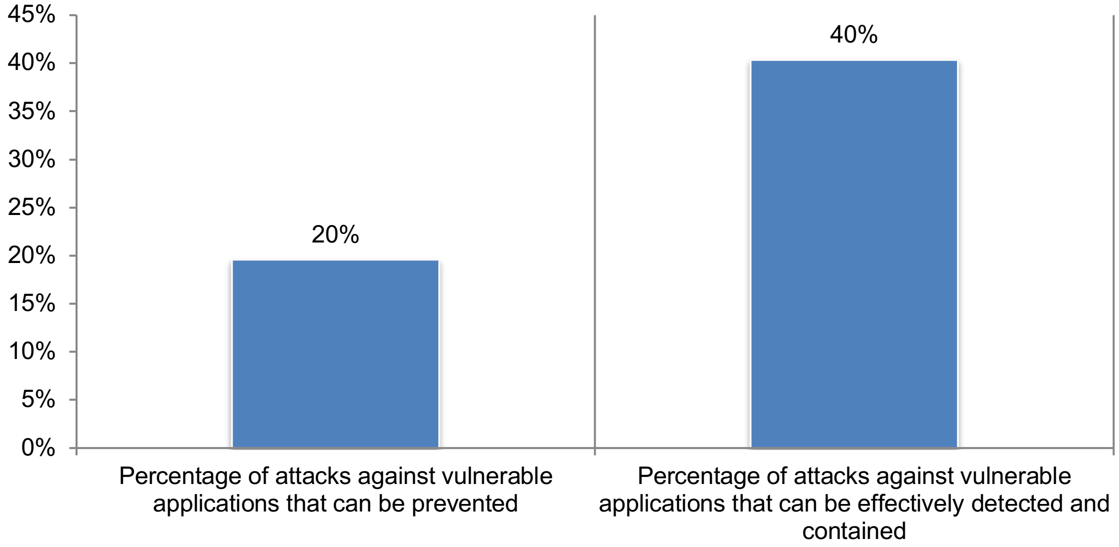
The consequences of attacks against unsecured applications are costly and increase the likelihood of data breaches that involve customer and employee information. According to our research findings, 84 percent of participants in this research rate the threat from insecure applications as significant. As organizations struggle to address these threats, they estimate the total economic loss they have incurred in the past 12 months as a result of attacks against vulnerable applications averaged $12 million.

The purpose of the *Application Security in the DevOps Environment* study, sponsored by HCL Software, is to better understand the state of organizations' ability to quickly prioritize and repair vulnerabilities in their applications. In the context of this research, DevOps (short for development and operations) is an approach that's based on lean and agile principles, in which business owners and the development, operations and quality assurance departments collaborate to deliver software in a continuous manner that enables the business to more quickly seize market opportunities and reduce the time to incorporate stakeholder feedback.

Ponemon Institute surveyed 626 individuals in IT security, quality assurance or development. All respondents work in organizations that use a DevOps approach which includes application security testing. That approach encompasses multiple measures that are taken to improve the security of an application by finding, fixing and preventing security vulnerabilities in order to reduce overall risk.

Why application security risk is significant. Sixty-seven percent of respondents say it is very likely or likely that their organizations will experience a cyber incident within the next year. Furthermore, as shown in Figure 1, once a vulnerable application makes its way into production, respondents believe an average of only 20 percent of all attacks against vulnerable applications can be prevented and only an average of 40 percent of attacks can be effectively detected and contained.

Figure 1. Percentage of attacks that can be prevented, detected and contained
Extrapolated values presented



Following are the most salient findings regarding application security risk in the DevOps environment:

Application security risk in organizations

- The DevOps software delivery culture prioritizes speed, automation and continuous delivery over addressing potential security risks, according to 65 percent of respondents. In fact, 60 percent of respondents say their organizations are very effective in creating innovative applications or services, but only slightly more than half (51 percent) of respondents say their organizations are very effective in creating secure applications or services.

- On average, 31 percent of applications are considered business-critical, yet an average of 67 percent of those business-critical applications are not continuously tested for vulnerabilities.

- Outdated or insufficient technologies and staffing shortages are making it difficult to prevent attacks against vulnerable applications, according to 63 percent of respondents.

- According to 70 percent of respondents, faster release cycles put applications at risk because there is less time for testing and more opportunity for vulnerabilities to make their way into production. Only slightly more than half (51 percent) of respondents integrate development and testing activities to ensure security is built in as early in the software development life cycle as possible.

- Only 17 percent of respondents test their applications continuously (10 percent) or daily (7 percent). Slightly more than half (56 percent) of respondents test vulnerabilities throughout the application development life cycle. However, 20 percent of respondents say their organizations do not test for vulnerabilities.

- Fifty-six percent of organizations require secure coding to reduce application security risk. However, less than half (47 percent) of respondents say their organizations ensure developers receive training on how to secure the coding process. This is despite the fact that 49 percent of respondents say their organizations empower developers to identify vulnerabilities during the coding process.

- Application security risk is difficult to reduce because DevOps security practices lack visibility and consistency, according to 71 percent of respondents. As a result, customer and employee data are at risk. In addition, a lack of visibility is caused by a decentralized approach, according to 45 percent of respondents.

Consequences of application security risk

- Sixty-seven percent of respondents say it is very likely or likely that their organizations will experience a cyber incident within the next year. Furthermore, as depicted in Figure 1, once a vulnerable application is released into production, respondents believe an average of only 20 percent of all attacks against their vulnerable applications can be prevented and an average of only 40 percent of attacks can be effectively detected and contained.

- It can take more than a year to identify and recover from an attack against a vulnerable application. On average, it can take nearly 8 months to identify an attack and 6 months to recover from an attack.

- Attacks against vulnerable applications are costly. In the past 12 months, organizations represented in this research incurred an average cost of $12 million as a result of attacks against vulnerable applications. Some of the organizations surveyed in this study incurred astonishing total economic losses that exceeded $100 million as a result of attacks against their vulnerable applications.

Steps to achieving a stronger application security posture

- Visibility into the state of application security is the most important control activity for ensuring a strong application security program. Seventy-seven percent of respondents say obtaining visibility into the state of application security across the enterprise help ensures a strong application security program. Sixty-nine percent of respondents say setting priorities for scanning and repairing vulnerable applications is critical to improving the state of application security.

- More than half (52 percent) of respondents say it is essential or very important to have the ability to automate vulnerability scanning at every stage of the software development life cycle. And, 56 percent of respondents say the ability to fix identified vulnerabilities quickly using automated tools is essential or very important.

- Organizations require the staffing and technologies to deal with the increasing number of application security vulnerabilities. Fifty-four percent of respondents say keeping up the growth in application security vulnerabilities is the biggest challenge in having an effective application security program.

- To shed further light on one of our earlier findings, 84 percent of respondents rate the threat from insecure applications to their organizations as very significant (54 percent of respondents) or significant (30 percent of respondents).

Part 2. Key findings

In this section we present an analysis of the findings. The complete audited findings are presented in the Appendix, at the end of this report. We have organized the report according to the following topics.

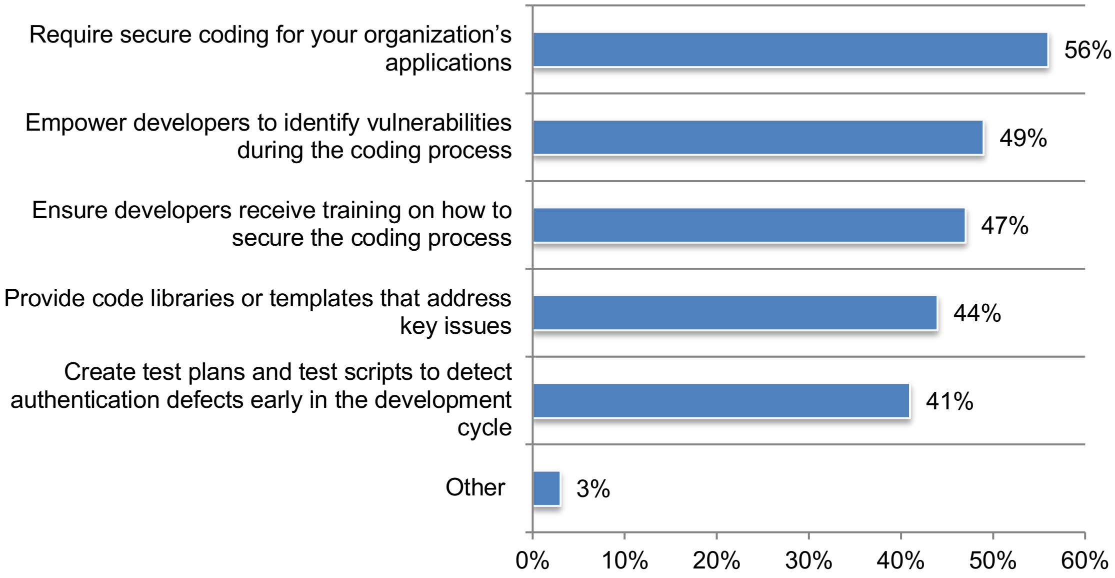
- Application security risk
- Why conventional testing practices are not mitigating application security risk
- The security/innovation balance
- Critical success factors in application security
- Budget and investment in application security

Application security risk

The majority of organizations require secure coding to reduce application security risk, but fewer than half of respondents say their organization empowers developers to identify vulnerabilities during the coding process. As discussed above, 84 percent of respondents rate the threat from insecure applications to their organizations as significant. However, are organizations taking the appropriate steps to reduce the threat?

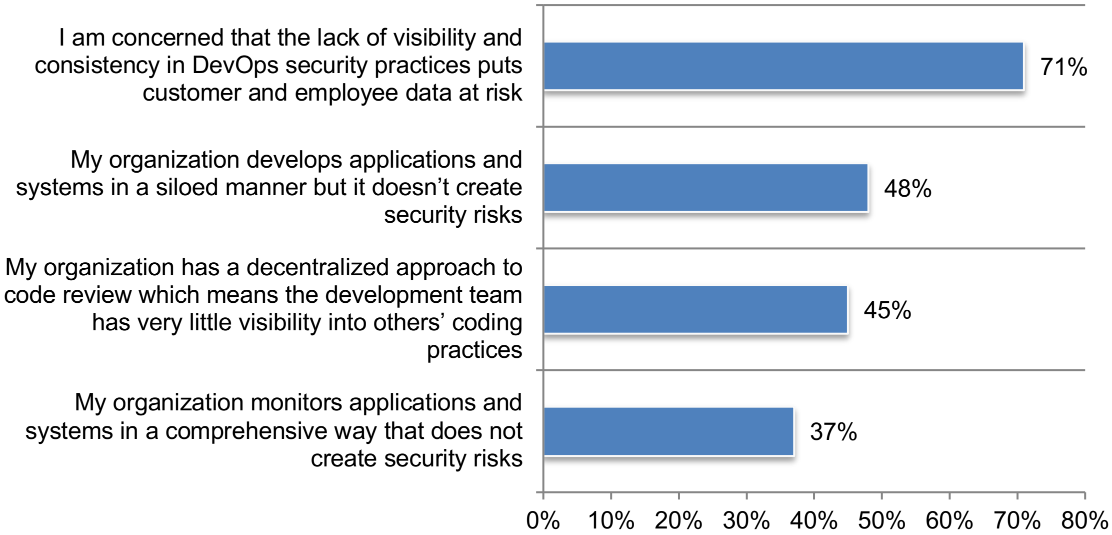
Figure 2 presents the steps organizations take to remediate risks associated with vulnerable applications. As shown, 56 percent of respondents say their organizations require secure coding for their applications, but only 47 percent of respondents say their organizations ensure developers receive training on how to secure the coding process.

Figure 2. What steps does your organization take to remediate the risks associated with vulnerable applications?
More than one response permitted



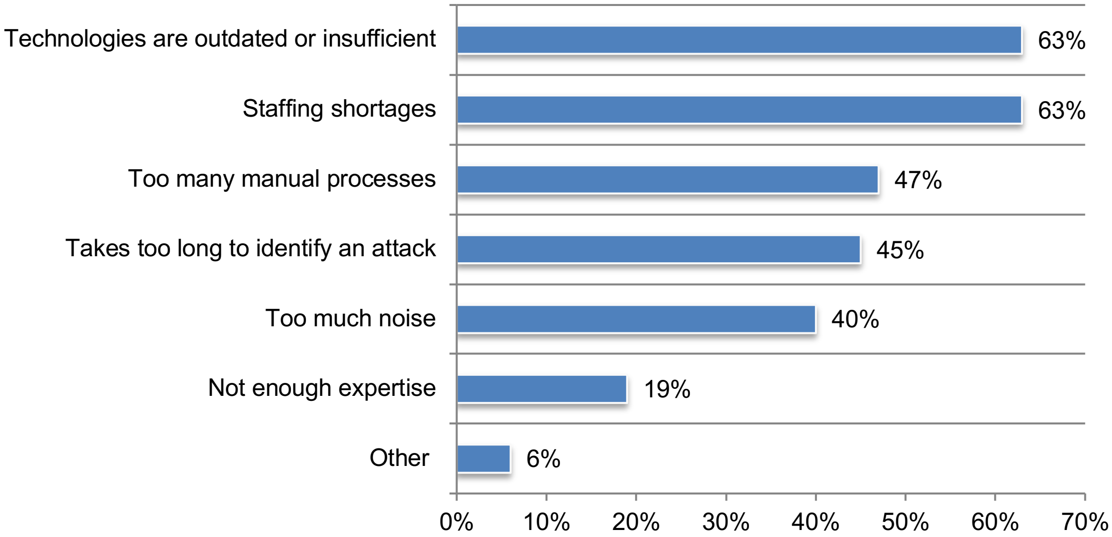
Application security risk is difficult to reduce because DevOps security practices lack visibility and consistency. According to Figure 3, 71 percent of respondents say they are concerned that customer and employee data is at risk because of the lack of visibility and consistency in DevOps security practices. Further, 45 percent of respondents say their organizations have a decentralized approach to code review which means the development team has very little visibility into others' coding practices. Another impact on application security risk is that only 37 percent of respondents agree that they have a comprehensive approach for monitoring applications and systems that does not create security risks.

Figure 3. Perceptions about application security risk
Strongly agree and Agree responses combined



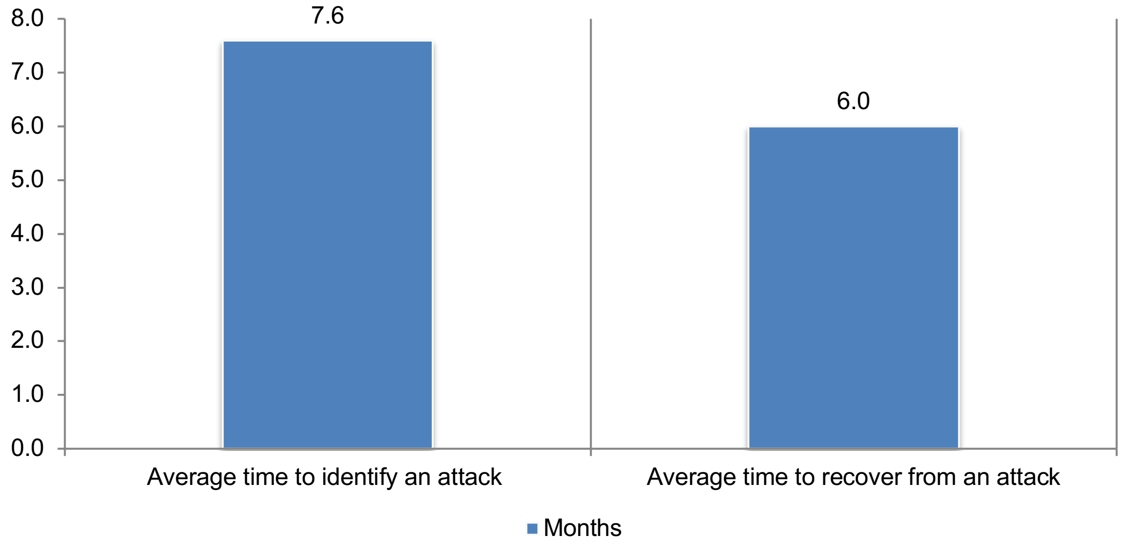
Insufficient or outdated technologies and staffing shortages are the primary barriers to preventing attacks against vulnerable applications, as shown in Figure 4.

Figure 4. What are the barriers to preventing attacks against vulnerable applications?
More than one response permitted



It can take more than a year to identify and recover from an attack against a vulnerable application. As discussed previously, 63 percent of respondents say insufficient technologies and staffing shortages are the biggest barriers to preventing an attack. As a consequence, according to Figure 5, It can take an average of nearly eight months to identify an attack and another 6 months to recover from an attack against a vulnerable application.

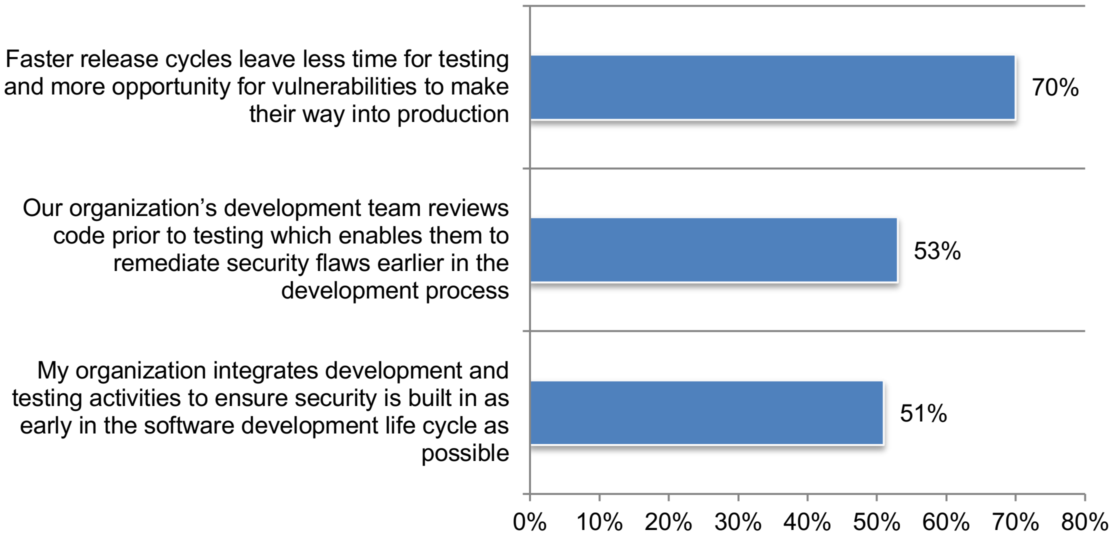
Figure 5. The average time to identify and recover from an attack against a vulnerable application



Why conventional testing practices are not reducing application security risk

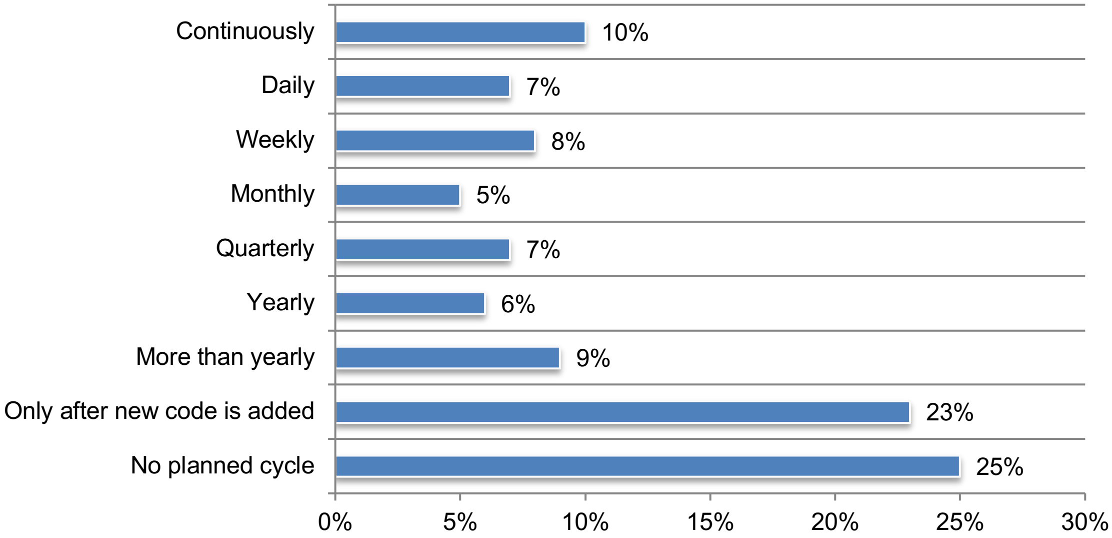
Applications are at risk because of faster release cycles. According to Figure 6, 70 percent of respondents say faster release cycles leave less time for testing and more opportunity for vulnerabilities to make their way into production. It is encouraging to see that slightly more than half of respondents (51 percent) say their organizations integrate development and testing activities to ensure that security is built in as early in the software development life cycle as possible. However, only 53 percent of respondents say their organization's development team reviews code prior to testing, which would normally have enabled them to remediate security flaws earlier in the development process.

Figure 6. Perceptions about application testing
Strongly agree and Agree responses combined



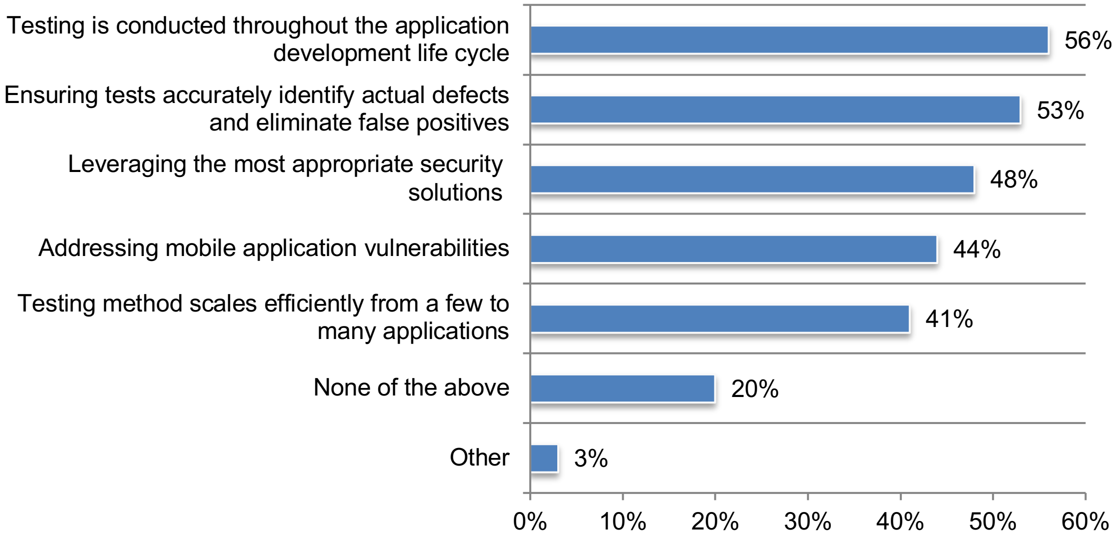
The lack of frequent application testing is putting customer and employee data at risk. As shown in Figure 7, nearly half of all respondents describe their testing cycles as quarterly or even less frequently, with some organizations (6 percent) reporting that at least a year passes between testing cycles. Another 25 percent of respondents report that they have no planned testing cycle.

Figure 7. What best describes your organization's application testing cycle?



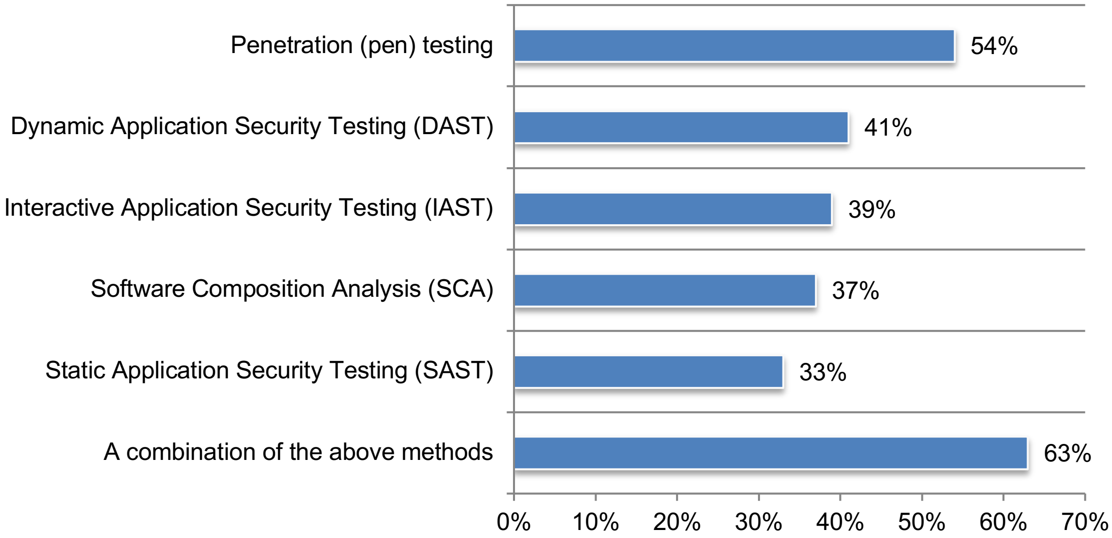
Slightly more than half of organizations test for vulnerabilities throughout the application development life cycle. However, 20 percent of organizations are not testing for vulnerabilities. As shown in Figure 8, 56 percent of respondents say testing is conducted throughout the application development life cycle and slightly more than half (53 percent) of respondents say their organizations ensure tests accurately identify actual defects and eliminate false positives. Nearly half (48 percent) of respondents leverage the most appropriate security solutions.

Figure 8. What steps are being taken to test for vulnerabilities in applications?
More than one response permitted



Most organizations use a combination of methods to scan and test for vulnerabilities. Figure 9 presents the various methods used to scan and test for vulnerabilities in applications. Fifty-four percent of respondents say they use penetration testing. And, 63 percent of respondents say they use a combination of application security testing methodologies.

Figure 9. What does your organization use to scan and test for vulnerabilities in applications?
More than one response permitted



Rarely are business-critical applications continuously tested for vulnerabilities. As shown in Figure 10a, respondents estimate that an average of 31 percent of applications are considered business-critical. An average of 67 percent of those business-critical applications are not continuously tested for vulnerabilities, as shown in Figure 10b.

Figure 10a. Percentage of applications considered business-critical
Extrapolated value presented

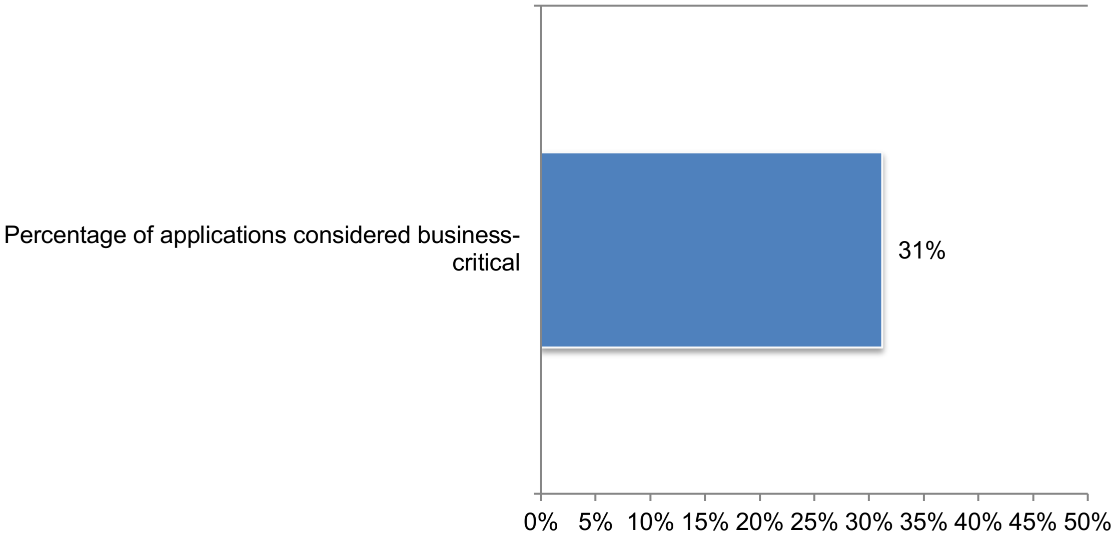
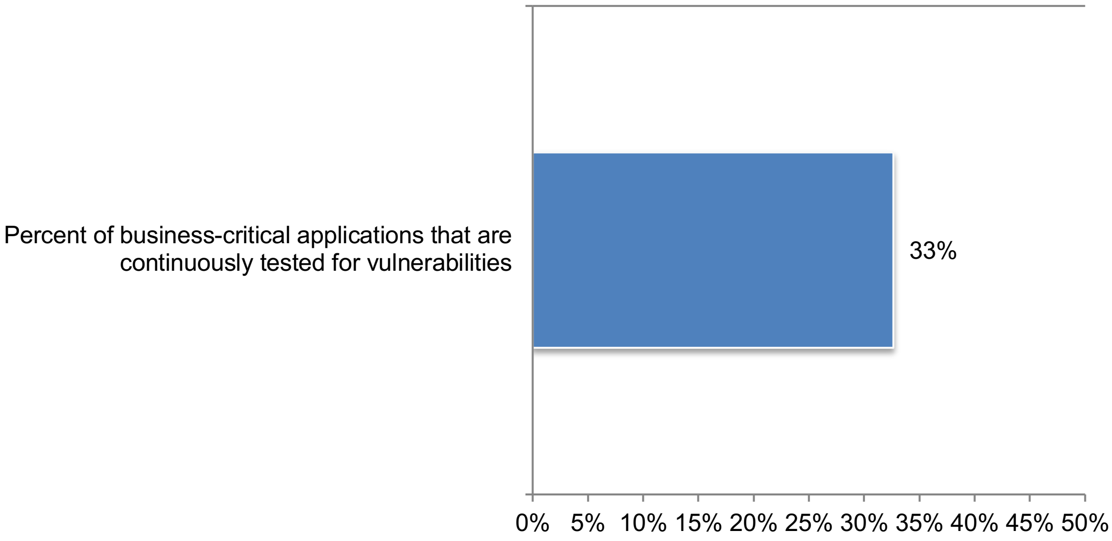
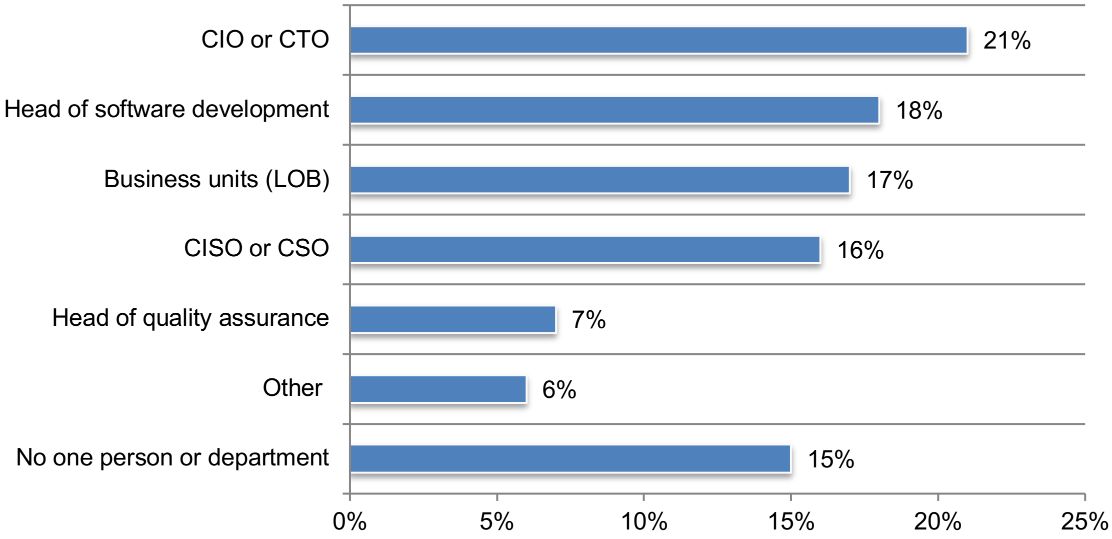


Figure 10b. Percentage of applications continuously tested for vulnerabilities
Extrapolated value presented



Development and quality assurance teams have significant ownership of application security risk testing programs. As shown in Figure 11, most respondents reported ownership of their application security testing programs by development or quality assurance teams (25 percent of respondents) or organizational business units (17 percent of respondents) Only 16 percent of respondents reported that their application security risk testing programs were owned by traditional security teams, such as the CISO and CSO.

Figure 11. Who owns your organization's application security risk testing program?

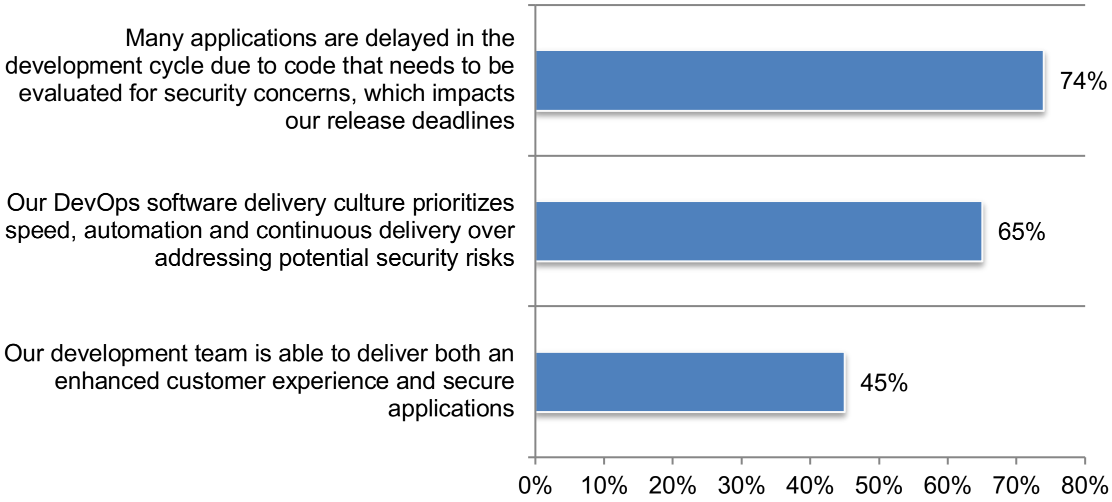


The security/innovation balance

Organizations struggle to provide an enhanced customer experience that's combined with secure applications. According to Figure 12, the DevOps software delivery culture prioritizes speed, automation and continuous delivery over addressing potential security risks, according to 65 percent of respondents.

As a consequence, 74 percent of respondents say many applications are delayed in the development cycle due to code that needs to be evaluated for security concerns, which impacts their release deadlines. And, only 45 percent of respondents say their development team is able to deliver both an enhanced customer experience and secure applications.

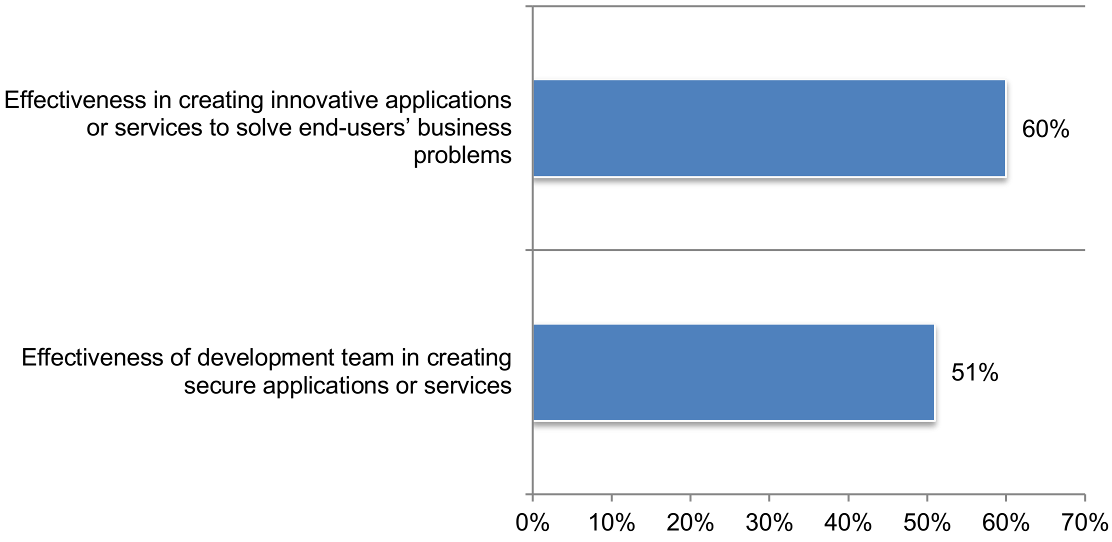
Figure 12. Perceptions about the security innovation balance
Strongly agree and Agree responses combined



Organizations are more effective in creating innovative applications than creating secure applications. Respondents were asked to rate their organizations' effectiveness in creating innovative and secure applications or services on a scale of 1 = not effective to 10 = very effective.

As shown in Figure 13, 60 percent of respondents rated their organizations as very effective in creating innovative applications or services to solve end-users' business problems. Similarly, slightly more than half (51 percent) of respondents rated the development team's effectiveness in creating secure applications or services as very effective.

Figure 13. Effectiveness in creating innovative and secure applications
On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



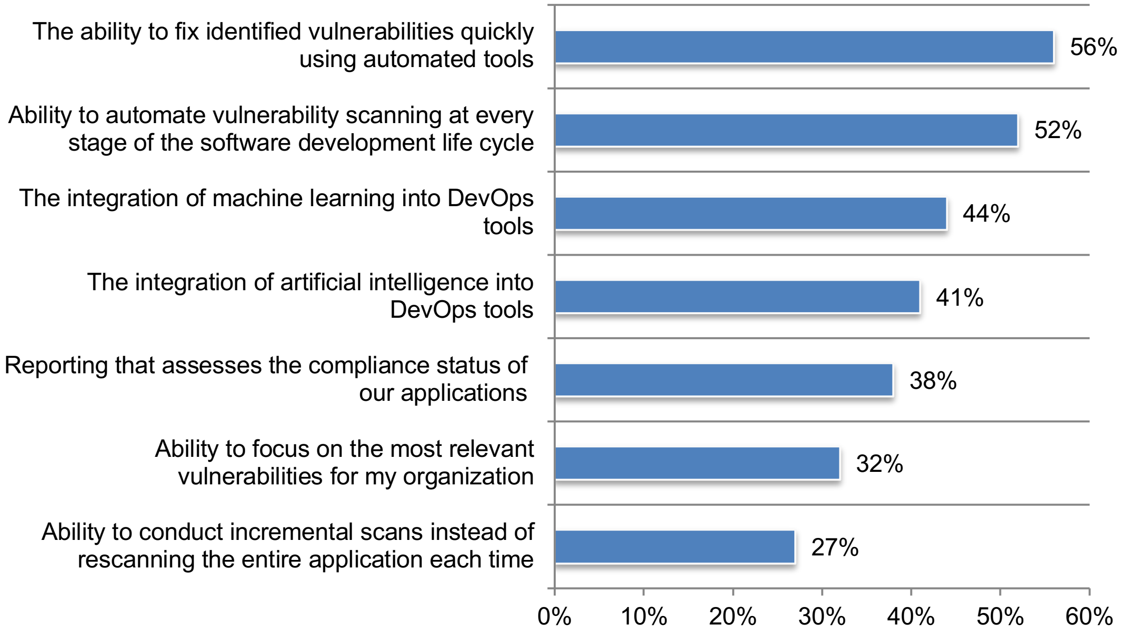
Critical success factors in application security

Automation is critical to reducing application security risk. Figure 14 presents a list of features that are considered essential or very important in creating secure applications or services.

The top two features are the ability to fix identified vulnerabilities quickly using automated tools (56 percent of respondents) and the ability to automate vulnerability scanning at every stage of the software development life cycle (52 percent of respondents). The least important factors are the ability to focus on the most relevant vulnerabilities for their organization (32 percent of respondents) and the ability to conduct incremental scans instead of rescanning the entire application each time (27 percent of respondents).

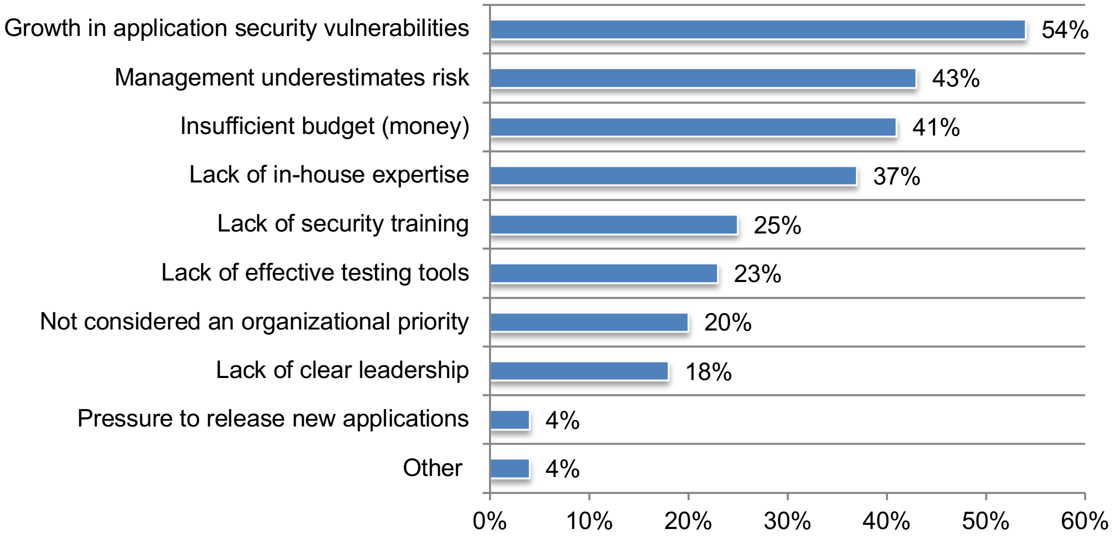
Figure 14. Essential and very important features in creating secure applications or services

Essential and Very important response combined



Growth in application security vulnerabilities is the biggest challenge to having a fully effective application security program. As shown in Figure 15, 54 percent of respondents say keeping up with the growth in application security vulnerabilities is making it difficult for organizations to reduce application security risk. This is followed by management underestimating the risk (43 percent of respondents) and insufficient budget (41 percent of respondents).

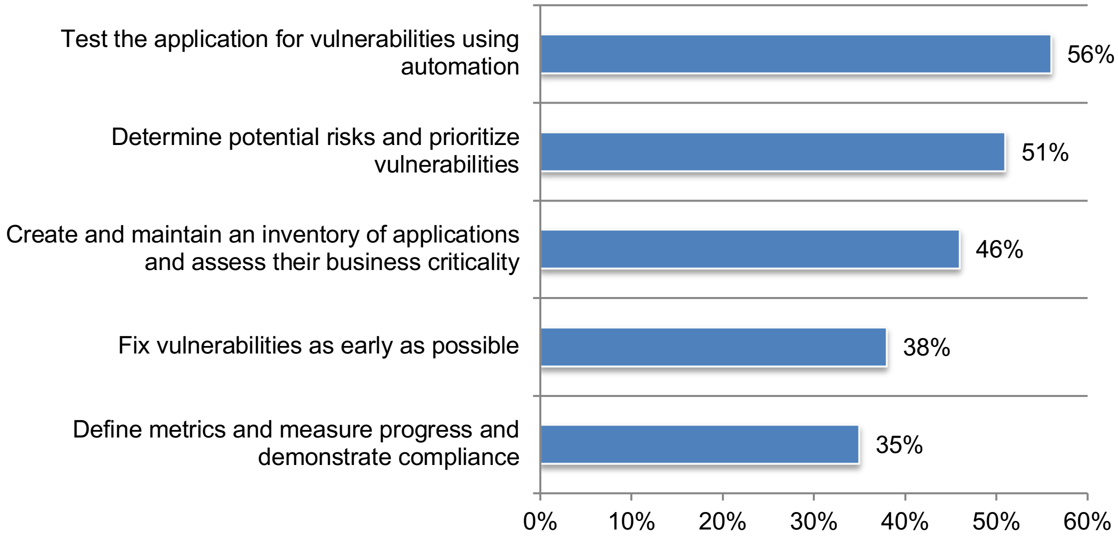
Figure 15. Challenges keeping the application security program from being fully effective
Three responses permitted



Automation is most often implemented in organizations. There are five strategically important steps for managing application security. Respondents were asked to report at what stage their organizations were implementing these steps using the following categories: not implemented, planning to implement, partially implemented and fully implemented.

Figure 16 shows the fully and partially implemented responses combined together. Fifty-six percent of respondents say their organizations have fully or partially implemented testing applications for vulnerabilities using automation, followed by 51 percent of respondents who say that activities to determine potential risks and prioritize vulnerabilities have been implemented to some extent. But, automation alone is not enough. Only 38 percent of organizations fix their vulnerabilities as early as possible and only 35 percent have defined metrics and measure their progress and demonstrate compliance.

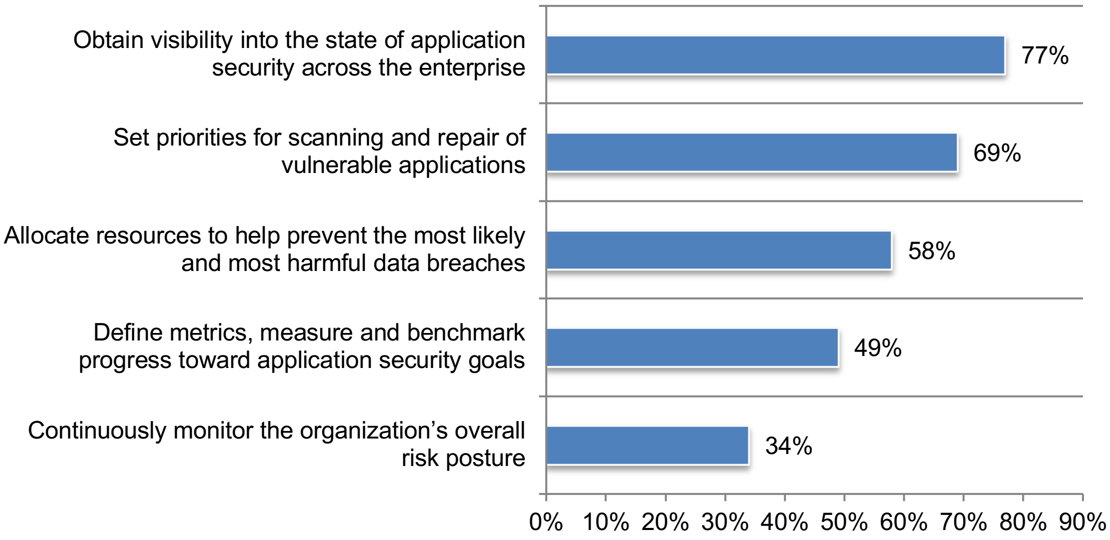
Figure 16. The implementation of five strategically important steps for managing application security risk
Fully and Partially implemented responses combined



Visibility into the state of application security is the most important control activity to ensure a strong application security posture. There are five critical control activities that facilitate a strong application security posture. Respondents were asked to rate each control activity as not important, important, very important or essential.

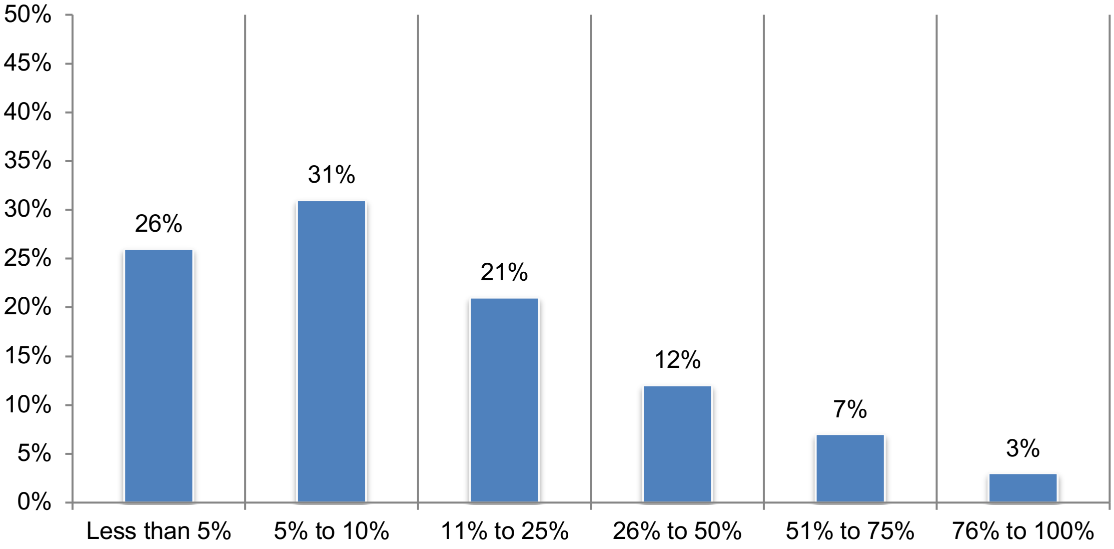
Figure 17 shows the essential and very important responses combined together. Seventy-seven percent of respondents say obtaining visibility into the state of application security across the enterprise is important and 69 percent of respondents say setting priorities for scanning and repairing of vulnerable applications is essential or very important.

Figure 17. Five control activities critical to establishment of a strong application security posture
Essential and Very important response combined



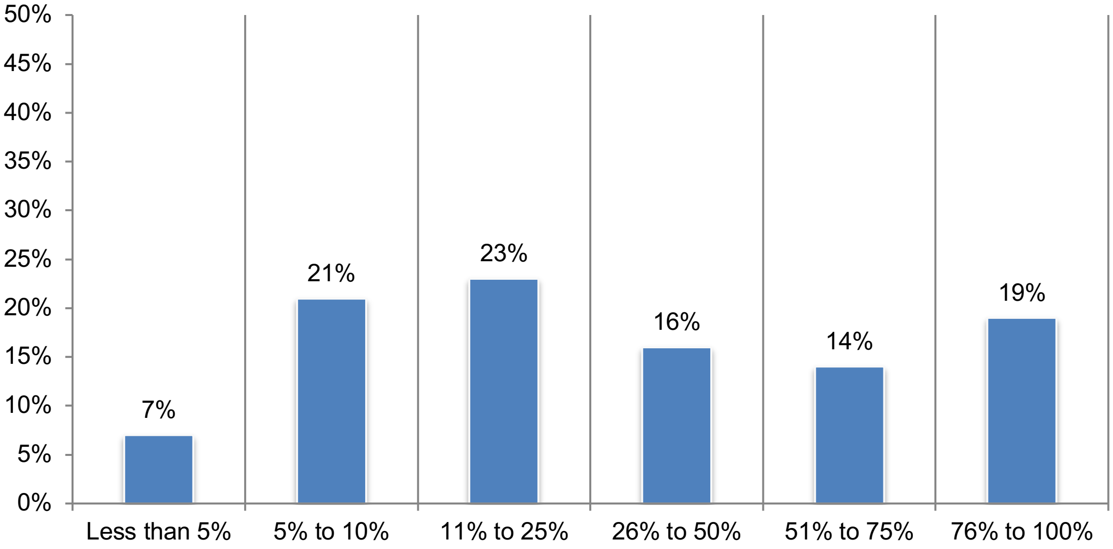
Most attacks against vulnerable applications are not prevented. Fifty-seven percent of respondents say that fewer than 10 percent of attacks against their vulnerable applications are prevented, as depicted in Figure 18a below.

Figure 18a. Percentage of all attacks against vulnerable applications that were prevented
Extrapolated value is 18 percent



One-third of respondents say that more than 50 percent of all attacks that impacted their organizations were not detected until the attacks resulted in damage to their infrastructure, as shown in Figure 18b below.

Figure 18b. Percentage of all attacks that impacted your organization but were not detected until they resulted in damage to the infrastructure
Extrapolated value is 37 percent



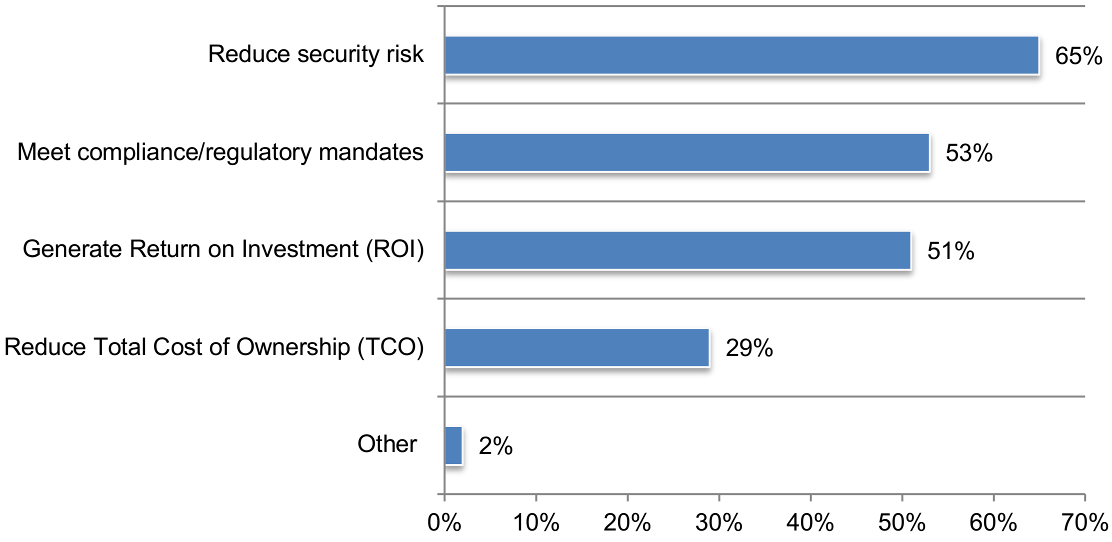
Application security and DevOps budget

Attacks against vulnerable applications are costly. In the past 12 months, organizations represented in this research incurred an average cost of $12 million as a result of attacks against vulnerable applications. On average, organizations represented in this research have an annual budget of approximately $100 million. Of that budget, a sizeable $25 million is allocated to application security activities and another $20 million is allocated to DevOps security activities, demonstrating organizations' commitment to those focus areas.

Table 1. Average annual budget for application security and DevOps	Budget
Organization's average total IT budget	$99,647,500
Average total budget for application security activities (25% of total IT budget)	$24,911,875
Average total budget for DevOps security activities (20% of total IT budget)	$19,929,500

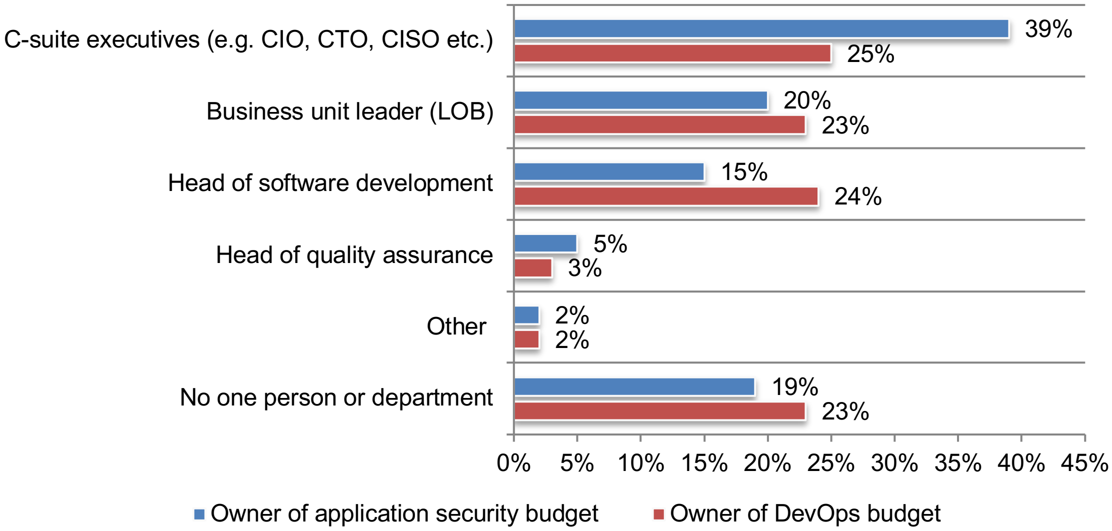
Organizations prioritize the reduction of security risk as the budget and investment priority. According to Figure 19, 65 percent of respondents say the most important driver for their organization is to reduce security risk followed by the need to meet compliance/regulatory mandates (53 percent of respondents).

Figure 19. What are the most important drivers for your organization's security budget and investment decisions?
Two responses permitted



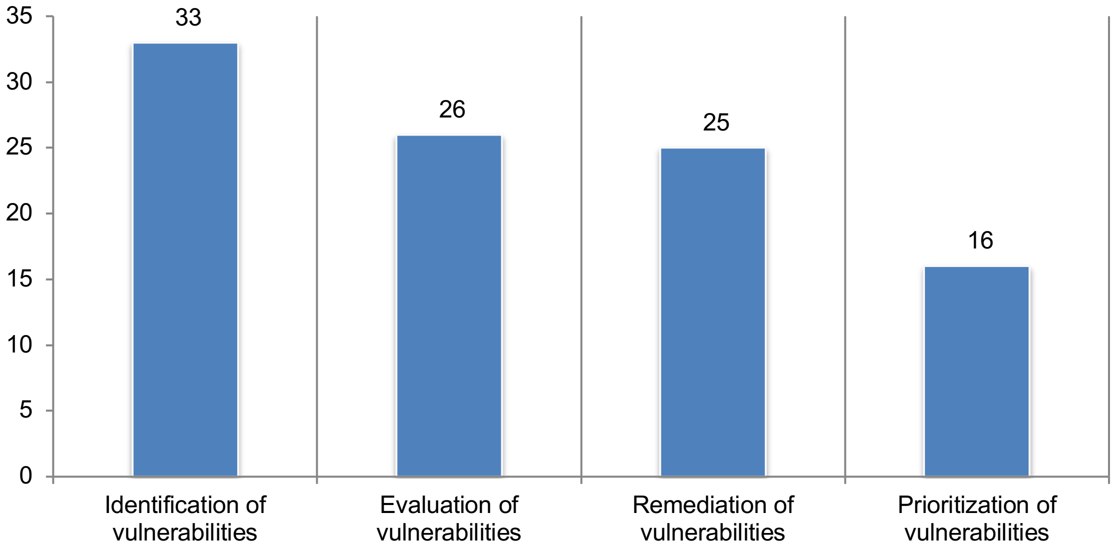
The C-suite owns the application security budget, while the head of software development and business unit leaders are more likely to own the DevOps budget. According to Figure 20, 39 percent of respondents say C-suite executives are more likely to own the application security budget. The DevOps budget is more likely owned by the head of software development (24 percent of respondents) and business unit leaders (23 percent of respondents).

Figure 20. Who owns the application security budget and the DevOps budget?



The largest proportion of the application security budget is allocated for identification of vulnerabilities. Figure 21 shows four phases for securing business-critical applications. Respondents were asked to allocate 100 points to describe how their organization currently spends budgeted resources for each of the four phases. Most of the budget is allocated to the identification of vulnerabilities.

Figure 21. How is the budget for application security budgeted?
Allocation of 100 points



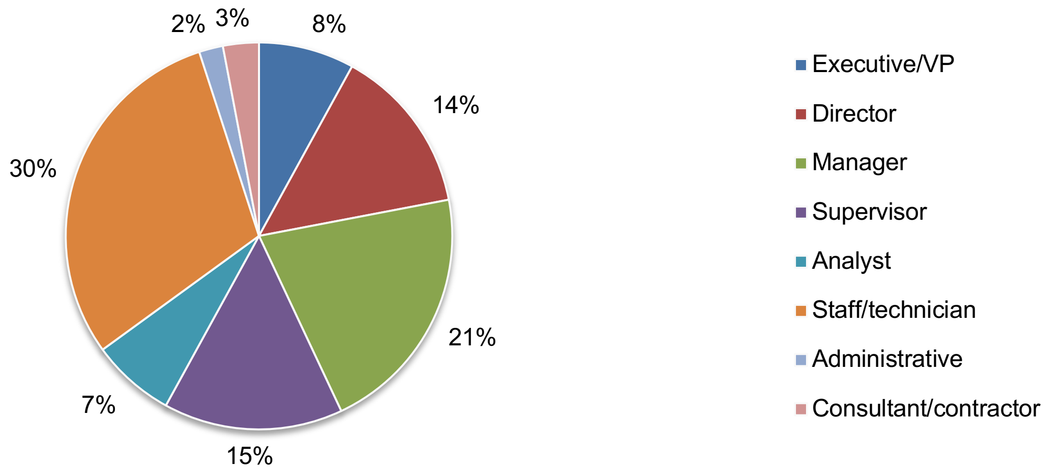
Part 3. Methods

The sampling frame is composed of 16,343 IT and IT security practitioners in organizations that use a DevOps approach. As shown in Table 2, 673 respondents completed the survey. Screening removed 47 surveys. The final sample was 626 surveys resulting in a 3.8 percent response rate.

Table 2. Sample response	Freq	Pct%
Total sampling frame	16,343	100.0%
Total returns	673	4.1%
Rejected or screened surveys	47	0.3%
Final sample	626	3.8%

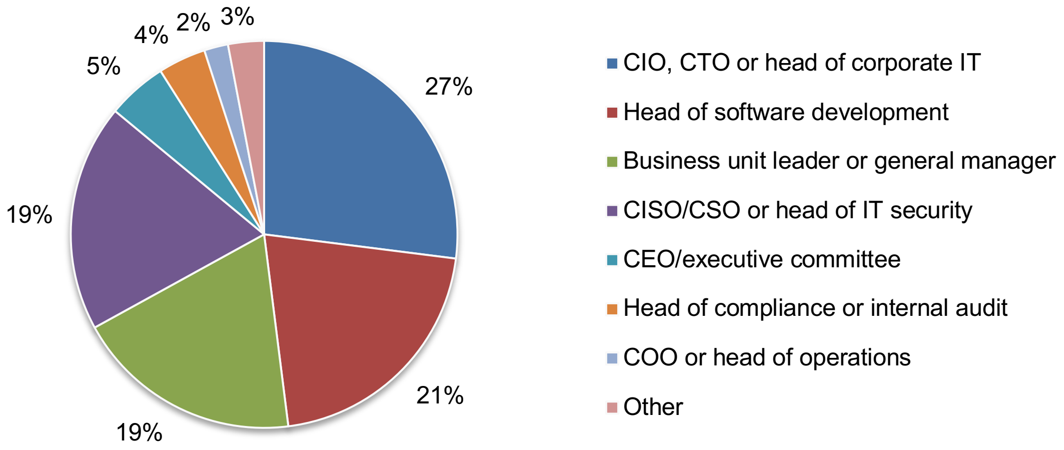
The following pie chart summarizes the position level of qualified respondents. At 30 percent, the largest segment contains those who are rank-and-file level employees (e.g., staff/technicians). More than half (58 percent) of respondents are at or above the supervisory level.

Pie Chart 1. Current position or organizational level



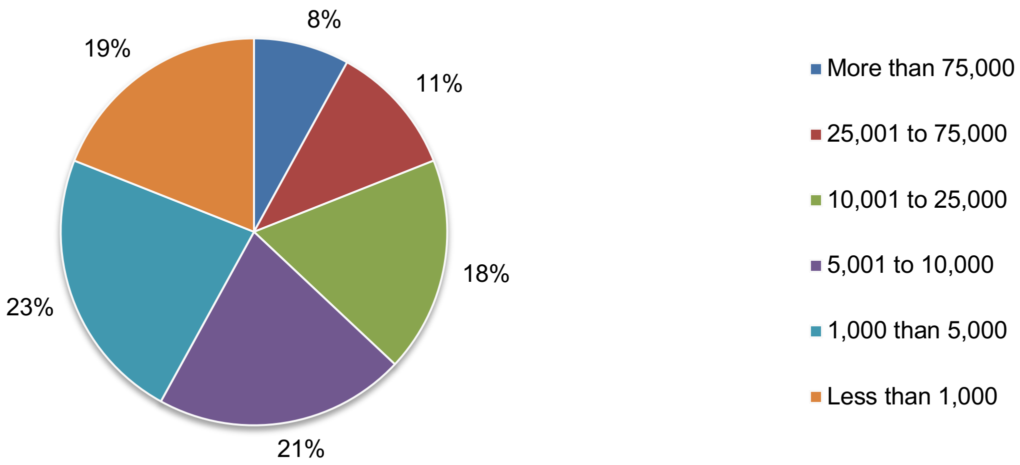
As shown in Pie Chart 2, 27 percent of respondents report to the CIO, CTO or head of corporate IT, 21 percent of respondents report to the head of software development, 19 percent of respondents report to the business unit leader or general manager, and 19 percent of respondents indicated they report to the CISO/CSO/head of IT security.

Pie Chart 2. Direct reporting channel



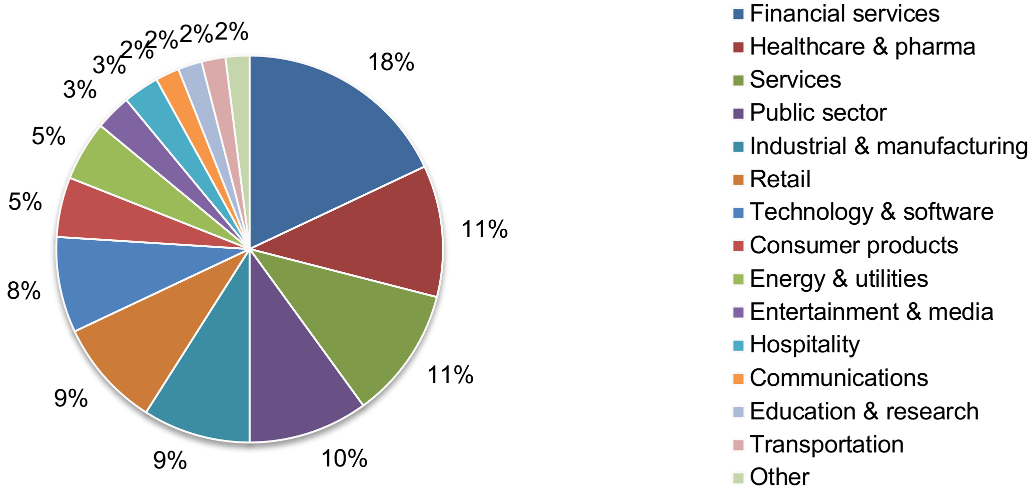
Pie Chart 3 summarizes the total worldwide headcount of respondents' companies. In the context of this study, headcount serves as an indicator of size. At 23 percent, the largest segment contains organizations with 1,000 to 5,000 full-time equivalent employees. The smallest segment (8 percent) includes larger-sized organizations with 75,000 or more employees. More than half (58 percent) of respondents are from organizations with a global headcount greater than 5,000 employees.

Pie Chart 3. Global headcount of respondents' organization



Pie Chart 4 shows the percentage distribution of respondents' companies across 14 industries. Financial services represent the largest industry sector (at 18 percent of respondents), which includes banking, insurance, brokerage, investment management and payment processing. This is followed by healthcare and pharmaceuticals (11 percent of respondents), services (11 percent of respondents), and public sector (10 percent of respondents).

Pie Chart 4. Primary industry focus of respondents' companies



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 professionals. 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, the possibility remains 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 July 2020.

Survey response	Freq
Total sampling frame	16,343
Total returns	673
Rejected survey	47
Final sample	626
Response rate	3.8%

Screening

S1. What best describes your role in the IT security, Quality Assurance or Development function within your organization? Check all that apply.	Pct%
IT security	76%
Quality Assurance	11%
Development	13%
None of the above (stop)	0%
Total	100%

S2. Does your organization use a DevOps approach that includes application security testing?	Pct%
Yes	100%
No (stop)	0%
Total	100%

S3. What best defines your level of knowledge about application security testing as part of DevOps?	Pct%
Very knowledgeable	37%
Knowledgeable	45%
Somewhat knowledgeable	18%
No knowledge (stop)	0%
Total	100%

Part 1. Attributions: Strongly Agree and Agree response.	Pct%
Q1a. Our development team is able to deliver both an enhanced customer experience and secure applications.	45%
Q1b. My organization monitors applications and systems in a comprehensive way that does not create security risks.	37%
Q1c. My organization develops applications and systems in a siloed manner but it doesn't create security risks.	48%
Q1d. My organization integrates development and testing activities to ensure security is built in as early in the software development life cycle as possible.	51%
Q1e. My organization has a decentralized approach to code review which means the development team has very little visibility into others' coding practices.	45%
Q1f. I am concerned that the lack of visibility and consistency in DevOps security practices puts customer and employee data at risk.	71%
Q1g. Our organization's development team reviews code prior to testing which enables them to remediate security flaws earlier in the development process.	53%
Q1h. Many applications are delayed in the development cycle due to code that needs to be evaluated for security concerns, which impacts our release deadlines.	74%
Q1i. Our DevOps software delivery culture prioritizes speed, automation and continuous delivery over addressing potential security risks.	65%
Q1j. Faster release cycles leave less time for testing and more opportunity for vulnerabilities to make their way into production.	70%

Part 2. Background

Q2. Please rank the importance of the following five DevOps benefits from 1 = most important to 5 = least important.	Average Rank
Agility in performance	4.24
Cost minimization	4.69
Security of business-critical applications	3.16
Speed in the release cycle	2.11
Visibility into vulnerable code	1.65

Q3. What does your organization use to scan and test for vulnerabilities in applications? Please check all that apply.	Pct%
Dynamic Application Security Testing (DAST)	41%
Interactive Application Security Testing (IAST)	39%
Penetration (pen) testing	54%
Software Composition Analysis (SCA)	37%
Static Application Security Testing (SAST)	33%
A combination of the above methods	63%
Total	267%

Q4. Using the following 10-point scale, please rate the effectiveness of your organization's development team in creating **innovative applications** or services to solve end-users' business problems. 1 = not effective to 10 = very effective.	Pct%
1 or 2	8%
3 or 4	13%
5 or 6	19%
7 or 8	36%
9 or 10	24%
Total	100%
Extrapolated value	6.60

Q5. Using the following 10-point scale, please rate the effectiveness of your organization's development team in creating **secure applications** or services. 1 = not effective to 10 = very effective.	Pct%
1 or 2	5%
3 or 4	13%
5 or 6	31%
7 or 8	27%
9 or 10	24%
Total	100%
Extrapolated value	6.54

Q6. Approximately, what percentage of your organization's applications are considered business-critical?	Pct%
Less than 5%	12%
5% to 10%	17%
11% to 25%	25%
26% to 50%	23%
51% to 75%	15%
76% to 100%	8%
Total	100%
Extrapolated value	31%

Q7. Approximately, what percent of business-critical applications are continuously tested for vulnerabilities?	Pct%
Less than 5%	17%
5% to 10%	18%
11% to 25%	16%
26% to 50%	23%
51% to 75%	14%
76% to 100%	12%
Total	100%
Extrapolated value	33%

Q8. Who owns your organization's application security risk testing program? Please select only one person/department.	Pct%
Business units (LOB)	17%
CIO or CTO	21%
CISO or CSO	16%
Head of quality assurance	7%
Head of software development	18%
Other (please specify)	6%
No one person or department	15%
Total	100%

Q9. Please rate the importance of the following features in creating secure applications or services. Essential and Very important response combined.	Pct%
Q9a. Ability to conduct incremental scans instead of rescanning the entire application each time	27%
Q9b. Ability to focus on the most relevant vulnerabilities for my organization	32%
Q9c. The integration of machine learning into DevOps tools	44%
Q9d. The integration of artificial intelligence into DevOps tools	41%
Q9e. Ability to automate vulnerability scanning at every stage of the software development lifecycle	52%
Q9e. Reporting that assesses the compliance status of our applications	38%
Q9f. The ability to fix identified vulnerabilities quickly using automated tools	56%

Q10. What challenges keep your organization's application security program from being fully effective? Please select your top three challenges.	Pct%
Growth in application security vulnerabilities	54%
Insufficient budget (money)	41%
Lack of clear leadership	18%
Lack of effective testing tools	23%
Lack of in-house expertise	37%
Lack of security training	25%
Management underestimates risk	43%
Not considered an organizational priority	20%
Other (please specify)	4%
Pressure to release new applications	4%
Total	269%

Part 3. Application security risk

Q11. In your opinion, what percentage of all attacks against vulnerable applications can your organization prevent?	Pct%
Zero	5%
< 5%	11%
5% to 10%	9%
11% to 15%	20%
16% to 20%	17%
21% to 30%	13%
31% to 40%	15%
41% to 50%	10%
> 50%	0%
Total	100%
Extrapolated value	20%

Q12. In your opinion, what percentage of all attacks against vulnerable applications can your organization effectively detect and contain?	Pct%
Zero	0%
< 5%	3%
5% to 10%	4%
11% to 15%	8%
16% to 20%	6%
21% to 30%	11%
31% to 40%	15%
41% to 50%	13%
> 50%	40%
Total	100%
Extrapolated value	40%

Q13. In your opinion, how likely is it that your organization will experience a cyber incident within the next year?	Pct%
Very likely	43%
Likely	24%
Somewhat likely	15%
Not likely	18%
Total	100%

Q14. How would you rate the threat from insecure applications to your organization? Please use the following 10-point scale from 1 = low threat to 10 = significant threat.	Pct%
1 or 2	0%
3 or 4	3%
5 or 6	13%
7 or 8	30%
9 or 10	54%
Total	100%
Extrapolated value	8.20

Q15. Following are five strategically important steps for managing application security risk. Please indicate the extent to which your organization is doing each one. Fully and Partially implemented responses.	Pct%
Q15a. Create and maintain an inventory of applications and assess their business criticality.	46%
Q15b. Test the application for vulnerabilities using automation.	56%
Q15c. Determine potential risks and prioritize vulnerabilities.	51%
Q15d. Fix vulnerabilities as early as possible.	38%
Q15e. Define metrics and measure progress and demonstrate compliance.	35%

Q16. Following are five control activities that organizations implement to establish a strong application security posture. Please indicate the level of importance for each control activity presented. Essential and Very important responses combined.	Pct%
Q16a. Obtain visibility into the state of application security across the enterprise.	77%
Q16b. Set priorities for scanning and repair of vulnerable applications.	69%
Q16c. Allocate resources to help prevent the most likely and most harmful data breaches.	58%
Q16d. Define metrics, measure and benchmark progress toward application security goals.	49%
Q16e. Continuously monitor the organization’s overall risk posture.	34%

Q17. What best describes your organization’s application testing cycle?	Pct%
Continuously	10%
Daily	7%
Weekly	8%
Monthly	5%
Quarterly	7%
Yearly	6%
More than yearly	9%
Only after new code is added	23%
No planned cycle	25%
Total	100%

Q18. Please check all the steps your organization takes to test for vulnerabilities in applications.	Pct%
Addressing mobile application vulnerabilities	44%
Ensuring tests accurately identify actual defects and eliminate false positives	53%
Leveraging the most appropriate security solutions	48%
Testing is conducted throughout the application development life cycle	56%
Testing method scales efficiently from a few to many applications	41%
None of the above	20%
Other	3%
Total	265%

Q19. What steps does your organization take to remediate the risks associated with vulnerable applications? Please select all that apply.	Pct%
Create test plans and test scripts to detect authentication defects early in the development cycle	41%
Empower developers to identify vulnerabilities during the coding process	49%
Ensure developers receive training on how to secure the coding process	47%
Provide code libraries or templates that address key issues	44%
Require secure coding for your organization's applications	56%
Other (please specify)	3%
Total	240%

Q20. In your opinion, in the past 12 months what percentage of all attacks against vulnerable applications within your organization were **prevented**?	Pct%
Less than 5%	26%
5% to 10%	31%
11% to 25%	21%
26% to 50%	12%
51% to 75%	7%
76% to 100%	3%
Total	100%
Extrapolated value	18%

Q21. In your opinion, in the past 12 months what percentage of all attacks impacted your organization but were not detected until they resulted in damage to your infrastructure?	Pct%
Less than 5%	7%
5% to 10%	21%
11% to 25%	23%
26% to 50%	16%
51% to 75%	14%
76% to 100%	19%
Total	100%
Extrapolated value	37%

Q22. What are the barriers to **preventing** attacks against vulnerable applications? Please check all that apply.	Pct%
Not enough expertise	19%
Staffing shortages	63%
Takes too long to identify an attack	45%
Technologies are outdated or insufficient	63%
Too many manual processes	47%
Too much noise	40%
Other (please specify)	6%
Total	283%

Q23. What is the average time to **identify** an attack against a vulnerable application?	Pct%
Less than 1 month	5%
1 to 2 months	6%
3 to 4 months	12%
5 to 6 months	16%
7 to 8 months	21%
9 to 10 months	15%
11 to 12 months	13%
More than one year	12%
Total	100%
Extrapolated value (months)	7.6

Q24. What is the average time to **recover** from an attack against a vulnerable application?	Pct%
Less than 1 month	11%
1 to 2 months	10%
3 to 4 months	16%
5 to 6 months	19%
7 to 8 months	23%
9 to 10 months	9%
11 to 12 months	7%
More than one year	5%
Total	100%
Extrapolated value (months)	6.0

Q25. What technology features are important in the prevention of attacks against vulnerable applications? Please select all that apply.	Pct%
Ability to detect vulnerabilities in real-time	33%
Ability to minimize noise	46%
Ability to prevent attacks in real-time	67%
Ability to prioritize based on risk metrics	52%
Cross technology protection	39%
Cross-operating system protection	47%
Other (please specify)	4%
Total	288%

Part 4. Application security and DevOps budget

Q26. What are most important drivers for your organization's security budget and investment decisions? Please select the top two choices.	Pct%
Meet compliance/regulatory mandates	53%
Reduce security risk	65%
Generate Return on Investment (ROI)	51%
Reduce Total Cost of Ownership (TCO)	29%
Other (please specify)	2%
Total	200%

Q27. Who within your organization “owns” the application security budget? Please select one top choice.	Pct%
Business unit leader (LOB)	20%
CIO/CTO	21%
CISO/CSO	18%
Head of quality assurance	5%
Head of software development	15%
Other (please specify)	2%
No one person or department	19%
Total	100%

Q28. Who within your organization “owns” the DevOps budget? Please select one top choice.	Pct%
Business unit leader (LOB)	23%
C-suite executives (e.g. CIO, CTO, CISO, etc.)	25%
Head of quality assurance	3%
Head of software development	24%
Other (please specify)	2%
No one person or department	23%
Total	100%

Q29. What is your organization’s total IT budget?	Pct%
Less than $100,000	0%
$100,000 to $500,000	0%
$500,001 to $1,000,000	5%
$1,000,001 to $5,000,000	7%
$5,000,001 to $10,000,000	10%
$10,000,001 to $50,000,000	23%
$50,000,001 to $100,000,000	25%
$100,000,001 to $250,000,000	22%
$250,000,001 to $500,000,000	6%
More than $500,000,000	2%
Total	100%
Extrapolated value	$ 99,647,500

Q30. Approximately, what percentage of the current year's IT budget will go to application security activities?	Pct%
< 1%	0%
1% to 2%	0%
3% to 5%	2%
6% to 10%	5%
11% to 15%	12%
16% to 20%	11%
21% to 30%	18%
31% to 40%	30%
41% to 50%	13%
> 50%	9%
Total	100%
Extrapolated value	25%

Q31. Approximately, what percentage of the current year's IT budget will go to DevOps activities?	Pct%
< 1%	4%
1% to 2%	3%
3% to 5%	6%
6% to 10%	10%
11% to 15%	15%
16% to 20%	21%
21% to 30%	18%
31% to 40%	16%
41% to 50%	3%
> 50%	4%
Total	100%
Extrapolated value	20%

Q32. The following table lists the four phases for securing business-critical applications. Please allocate all 100 points to describe how your organization currently spends budgeted resources for the four phases.	Points
Identification of vulnerabilities	33
Evaluation of vulnerabilities	26
Prioritization of vulnerabilities	16
Remediation of vulnerabilities	25
Total ((100 points)	100

Q33. Please estimate the total economic loss incurred by your company as a result of attacks against vulnerable applications over the past 12 months.	Pct%
Less than $50,000	2%
$50,000 to $100,000	4%
$100,001 to $500,000	17%
$500,001 to $1,000,000	21%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	16%
$10,000,001 to $50,000,000	7%
$50,000,001 to $100,000,000	5%
More than $100,000,000	3%
Total	100%
Extrapolated value	$ 11,612,000

Part 5. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Pct%
Executive/VP	8%
Director	14%
Manager	21%
Supervisor	15%
Analyst	7%
Staff/technician	30%
Administrative	2%
Consultant/contractor	3%
Other	0%
Total	100%

D2. What best describes your direct reporting channel?	Pct%
CEO/executive committee	5%
COO or head of operations	2%
CFO, controller or head of finance	1%
CIO, CTO or head of corporate IT	27%
Head of software development	21%
Business unit leader or general manager	19%
Head of compliance or internal audit	4%
CISO/CSO or head of IT security	19%
Other	2%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
Less than 1,000	19%
1,000 than 5,000	23%
5,001 to 10,000	21%
10,001 to 25,000	18%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

D4. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense contractor	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	3%
Financial services	18%
Healthcare & pharma	11%
Hospitality	3%
Industrial & manufacturing	9%
Public sector	10%
Retail	9%
Services	11%
Technology & software	8%
Transportation	2%
Other	0%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 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.

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.