Ponemon INSTITUTE

Reducing Enterprise Application Security Risks: More Work Needs to Be Done

Sponsored by WhiteSource Software

Independently conducted by Ponemon Institute LLC

Publication Date: February 2021

Ponemon INSTITUTE

Reducing Enterprise Application Security Risks: More Work Needs to Be Done

Ponemon Institute, February 2021

Part 1. Introduction

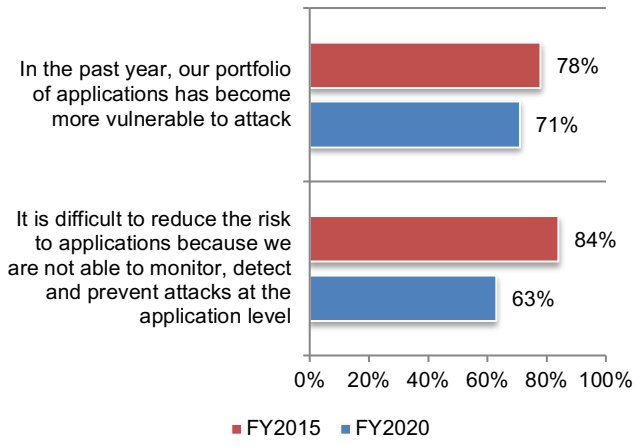
Reducing Enterprise Application Security Risks: More Work Needs to Be Done examines the reasons why the highest level of security risk is considered by many to be in the application layer. In 2015, we conducted a similar study on application security risks.[1] As shown in this research, since the previous study more organizations are concerned about hacks to insecure applications.

Ponemon Institute, with sponsorship from WhiteSource Software surveyed 634 IT and IT security practitioners who are familiar with their organizations' approach to securing applications. More than half (58 percent) of respondents are in organizations with a headcount greater than 5,000. As part of their responsibilities, most (45 percent of respondents) are engaged in testing applications and securing applications and data (41 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 don't enable a quick remediation of vulnerable applications and a high false positive rate.

Most organizations, according to Figure 1, still find it difficult to monitor, detect and prevent attacks at the application level and 71 percent of respondents say just in the past year their organizations' portfolio of applications has become more vulnerable to attack.

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



Based on the research, following are the reasons why business-critical applications continue to be at risk and why more work needs to be done.

- There is an inability to quickly perform patches on applications in production. Fifty-eight respondents say it takes days, weeks and months to shore up an application in production mode after detection of a vulnerability.
- There is an inability to quickly detect vulnerabilities and threats, according to 57 percent of respondents.
- There is limited or no collaboration between the application development and security teams, according to 65 percent of respondents.
- Security is not adequately emphasized during the development of new applications, according to 50 percent of respondents.

[1] *The Increasing Risk to Enterprise Application Security*, conducted by Ponemon Institute, November 2015.

- Despite a lower level of risk, more funds are allocated to protect networks. Thirty-eight percent of respondents say the level of risk in the application layer is high but only 17 percent of the IT security is allocated to application security.

- Since 2015, fewer organizations are building security features into applications under development. In 2020 only 21 percent of respondents say their organizations build security features into applications, a significant decrease from 32 percent of respondents in 2015.

- Since 2015, most organizations still do not emphasize security in the development of new applications. Only 43 percent of respondents say their organizations are making it a point to ensure security is emphasized in the development of new applications. This is a very slight increase from 39 percent of respondents five years ago.

Part 2. Key findings

In this section, we discuss the detailed findings. The complete audited findings are presented in the appendix of this report. Whenever possible the comparison between the 2015 and 2020 results will be presented. The research is organized into the following topics:

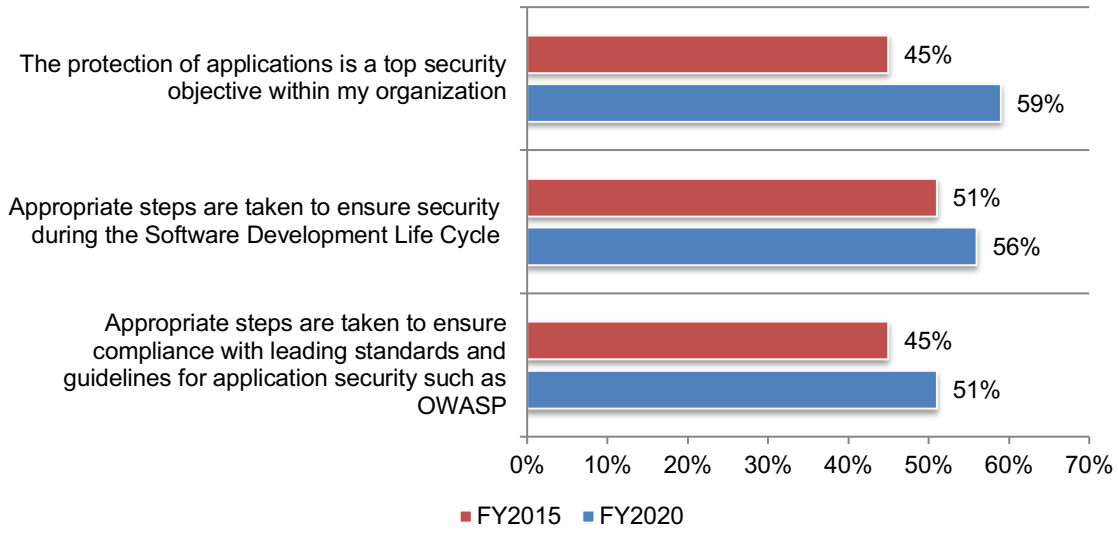
- Why applications are more vulnerable to attack than other areas of vulnerabilities
- Addressing vulnerabilities in enterprise applications
- Best practices of high performing organizations in reducing the application security risk

Why applications are more vulnerable to attack than other areas of vulnerabilities

Hundreds of deployed applications are considered business critical and at risk. At any one point in time, an average of 2,672 business applications are deployed within the organizations represented in this research and 30 percent of these applications are considered business critical.

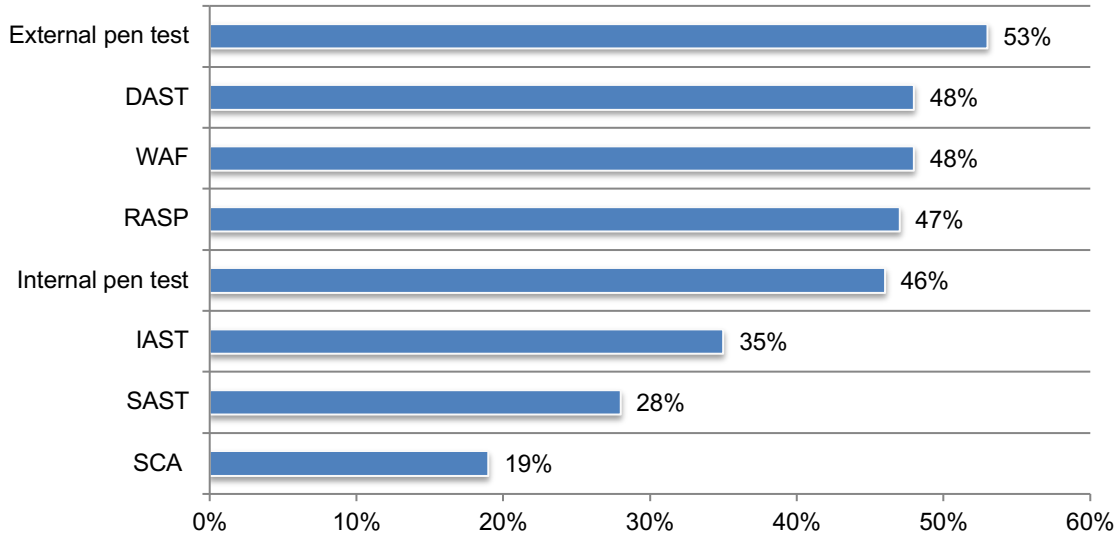
On a positive note, more organizations are making the protection of applications a top security objective. As shown in Figure 2, there was an increase from 45 percent of respondents in 2015 to 59 percent of respondents in 2020 who agree that the protection of applications is a priority. Further, more respondents believe their organizations are taking appropriate steps to ensure security during the Secure Software Development Life Cycle (SSDLC) and achieving compliance with leading standards and guidelines for application security such as OWASP.

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



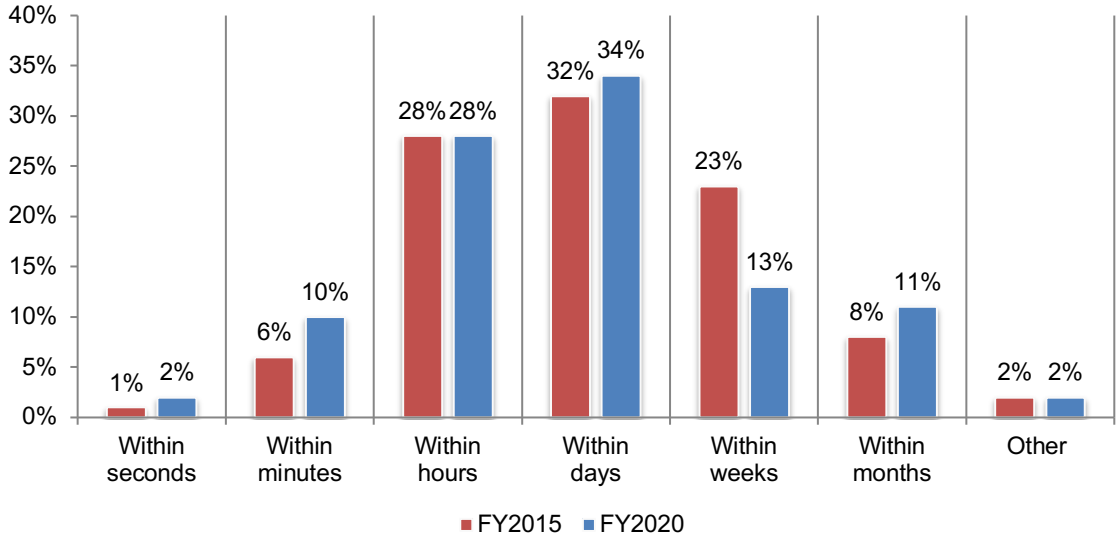
How organizations keep applications secure. As shown in Figure 3, the primary means of securing applications are an external pen test (53 percent of respondents) followed by DAST and WAF (both 48 percent of respondents).

Figure 3. How does your organization secure applications?
More than one response permitted



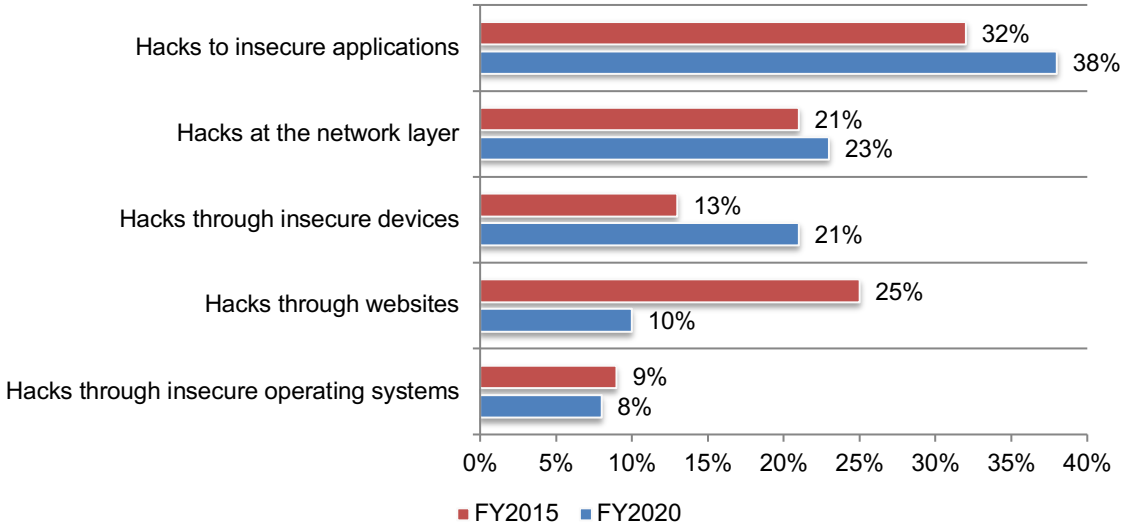
It takes too long to shore up an application in production mode after detection of a vulnerability. As shown in Figure 4, 58 percent of respondents say it can take days, weeks or months to shore up an application in production mode after the detection of a vulnerability. This is a slight decrease from 2015 (63 percent of respondents).

Figure 4. How long does it take to shore up an application in production mode after detection of a vulnerability?



Since 2015, more organizations are concerned about hacks to insecure applications. As shown in Figure 5, the kinds of attacks that create the greatest worry are hacks to insecure applications (38 percent of respondents). Only 23 percent say they worry about hacks at the network layer.

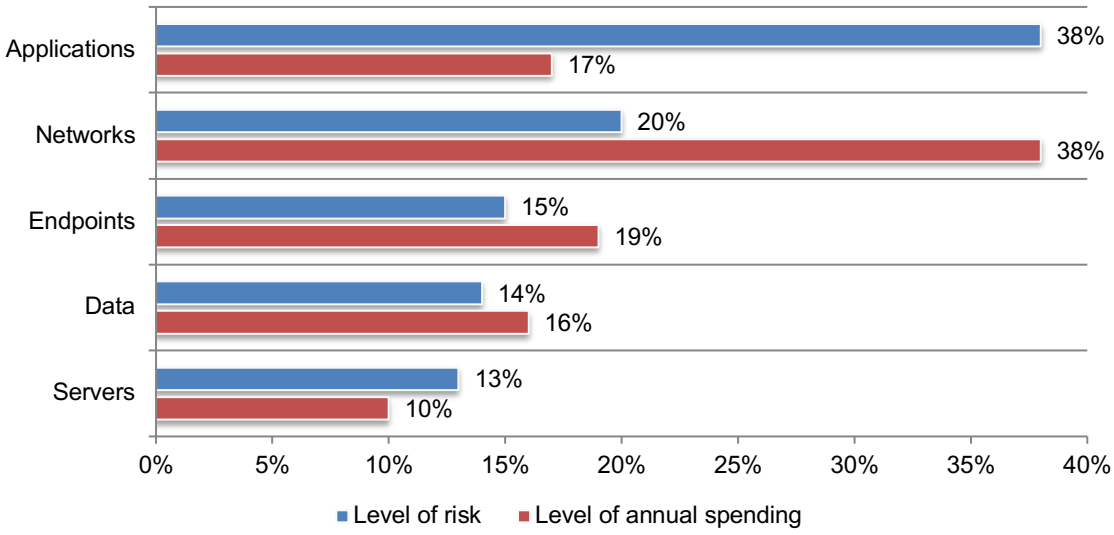
Figure 5. What kinds of attacks concern your organization most?



Despite a lower level of risk, more funds are allocated to protect networks. An average of 32 percent of the overall IT budget is dedicated to data protection and security. Figure 6 shows the level of risk and the level of annual spending for each of the following five layers: applications, endpoints, networks, data and servers and the level of annual spending (investment) in IT security to these same areas.

As shown in Figure 6, 38 percent of respondents say the level of risk is high but only 17 percent of the data protection and security budget is allocated to application security. In contrast, only 20 percent of respondents rate network risk as high but 38 percent of the budget is designated for network security.

Figure 6. Gaps in security risks and the allocation of spending

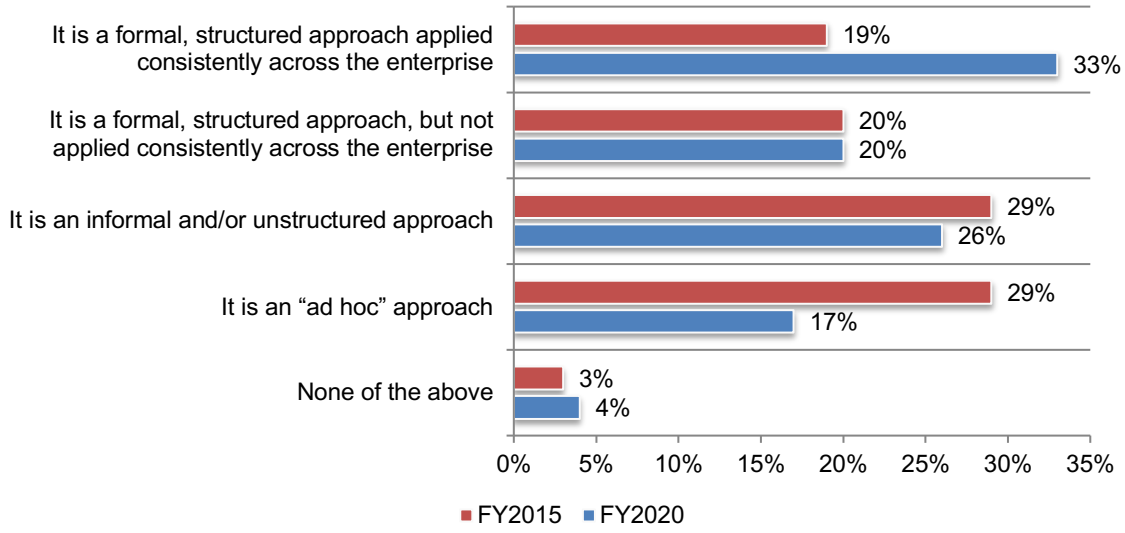


Addressing vulnerabilities in enterprise applications

More organizations need to establish a formal structured approach to their SSDLC. As discussed previously, the majority of organizations represented in this research (51 percent of respondents) take steps to ensure security in the SSDLC[2]. However, more work needs to be done to formalize organizations' approach to their SSDLC to improve application security.

While 33 percent of respondents say their organizations have a formal structured approach applied consistently across the enterprise, an increase from 19 percent in 2015. However, according to Figure 7, almost half (47 percent) of respondents only have an informal, ad hoc approach or no approach to the SSDLC.

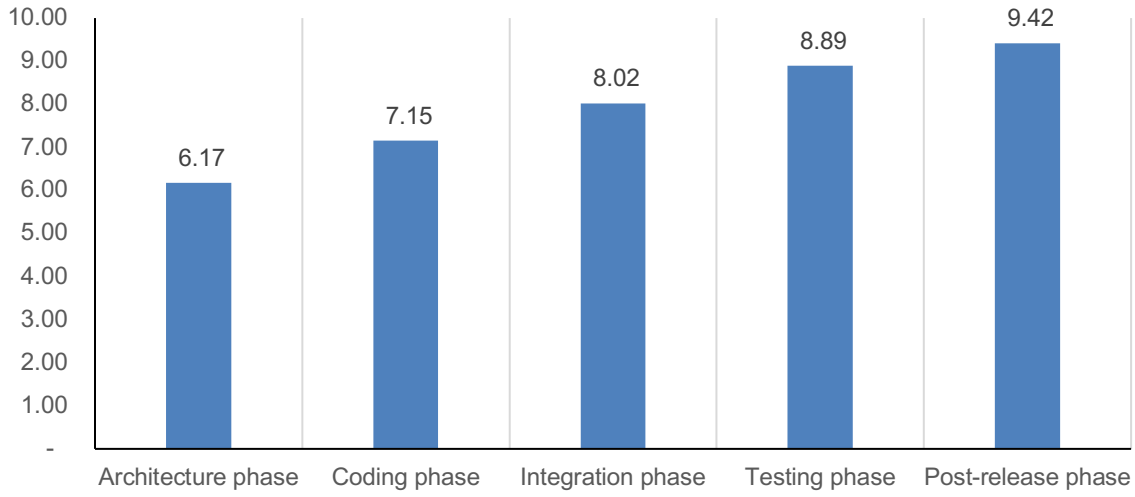
Figure 7. What best describes the SSDLC in your organization?



[2] **Secure Software Development Life Cycle** (or SSDLC) is the process, which is designed 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.

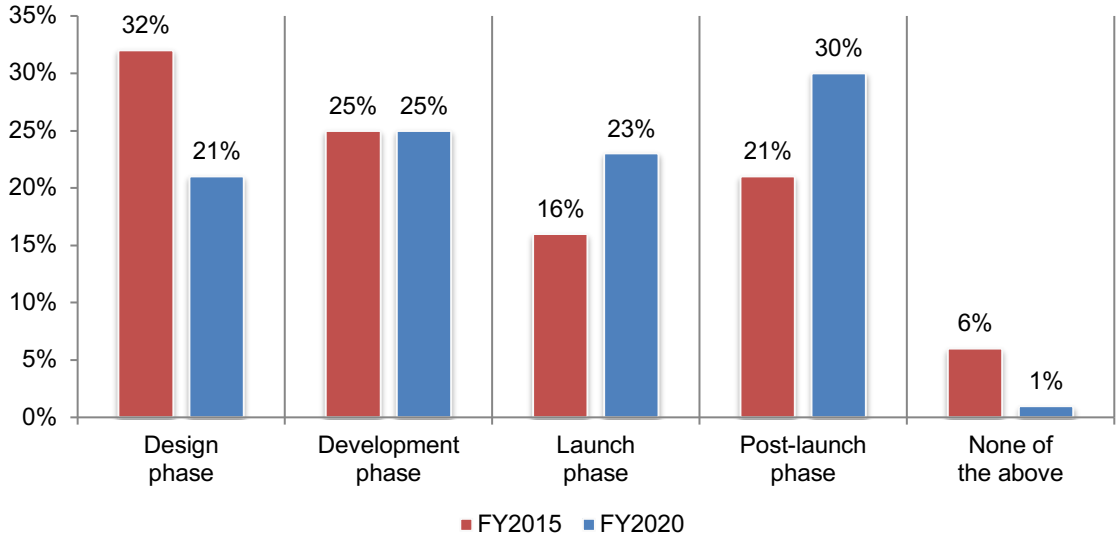
Figure 8 presents the five phases in the application development process. Respondents were asked to estimate the average number of hours it takes to remediate a vulnerability once it is detected in each of the five phases. As shown, the average number of hours steadily increases the later in the process the vulnerability is detected from 6.17 hours in the architecture phase to 9.42 hours once the application is released.

Figure 8. Average hours remediating a vulnerability once it is detected



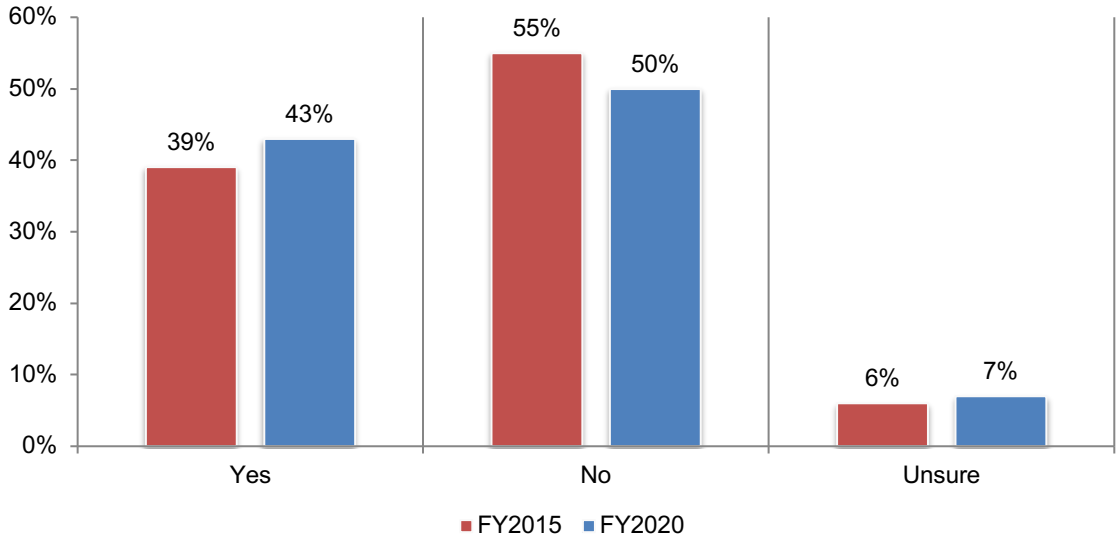
Fewer organizations are building security features into the application design phase. As shown in Figure 9, in 2020 only 21 percent of respondents say their organizations build security features into applications, a significant decrease from 32 percent of respondents in 2015.

Figure 9. Where in the SSDLC does your organization build security features into applications under development?



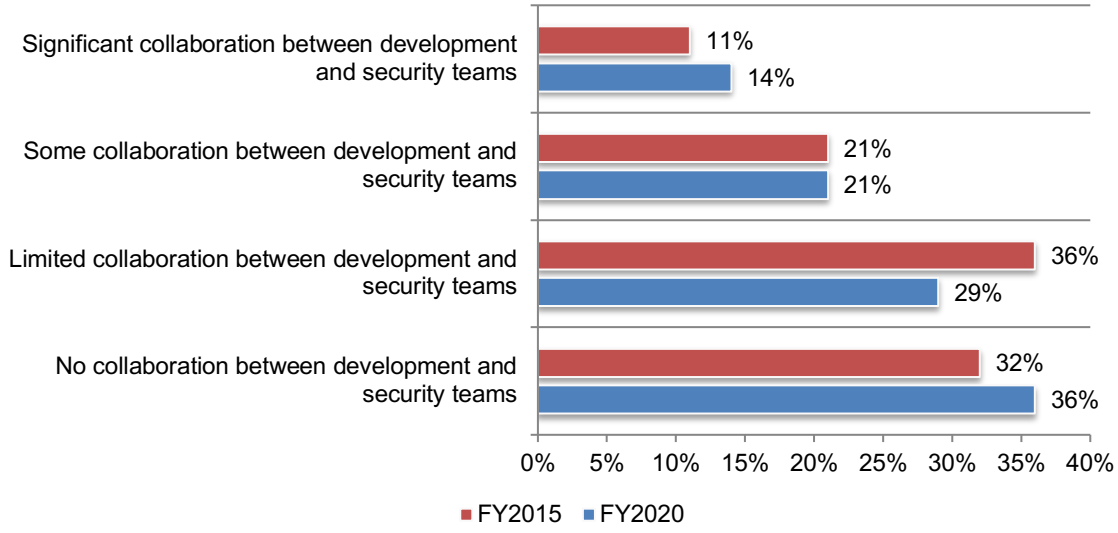
Since 2015, most organizations still do not emphasize security in the development of new applications. According to Figure 10, only 43 percent of respondents say their organizations are making it a point to ensure security is emphasized in the development of new applications. This is a very slight increase from 2015.

Figure 10. Is security adequately emphasized during the development of new applications?



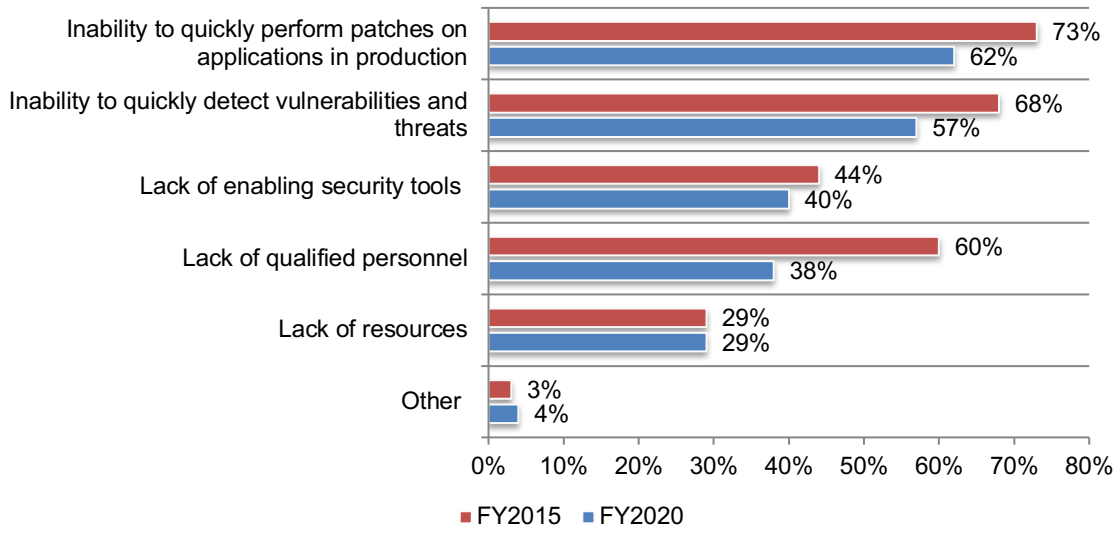
Collaboration between development and security teams remains poor. As a possible reason for the failure to address security in the development of new applications is the poor collaboration between the application development and security teams. According to Figure 11, 65 percent of respondents say such collaboration is limited (29 percent) or non-existent (36 percent). In 2015, 68 percent of respondents say such collaboration is poor.

Figure 11. What best describes the nature of collaboration between your organization's application development and security teams?



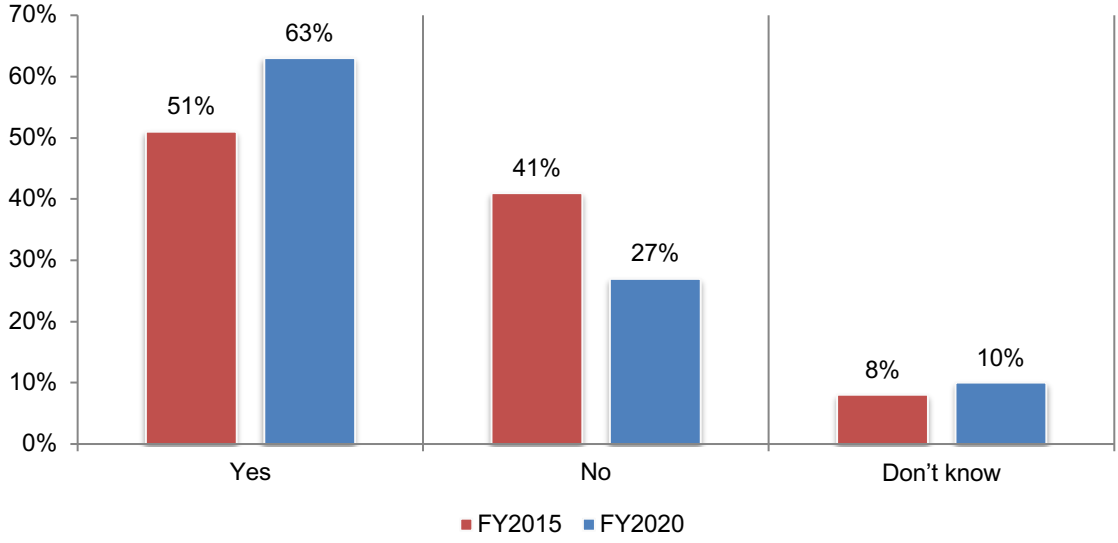
Organizations continue to have difficulties in remediating vulnerabilities in applications. In 2020, 67 percent of respondents say it is very difficult or difficult to remediate vulnerabilities in applications. According to Figure 12**,** In 2015 and 2020, the top two difficulties are the inability to quickly perform patches on applications in production and the inability to quickly detect vulnerabilities and threats. More organizations are confident about the ability to have qualified personnel.

Figure 12. Why is it very difficult or difficult to remediate vulnerabilities in applications?
More than one response permitted



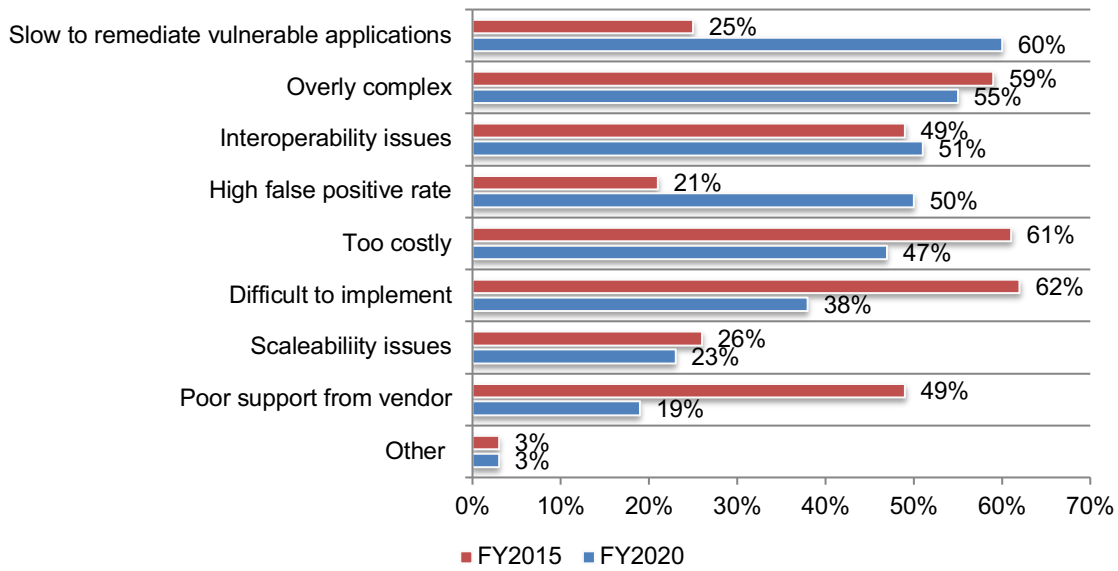
Vulnerability backlogs have increased significantly, and current solutions are slow to remediate vulnerable applications. As shown in Figure 13, 63 percent of respondents say their organizations have a vulnerability backlog of applications that have been identified as vulnerable but not remediated, a significant increase from 51 percent in 2015. An average of 51 percent of vulnerable applications have not been remediated, an increase from an average of 45 percent in 2015.

Figure 13. Did your organization have a vulnerability backlog in the past 12 months?



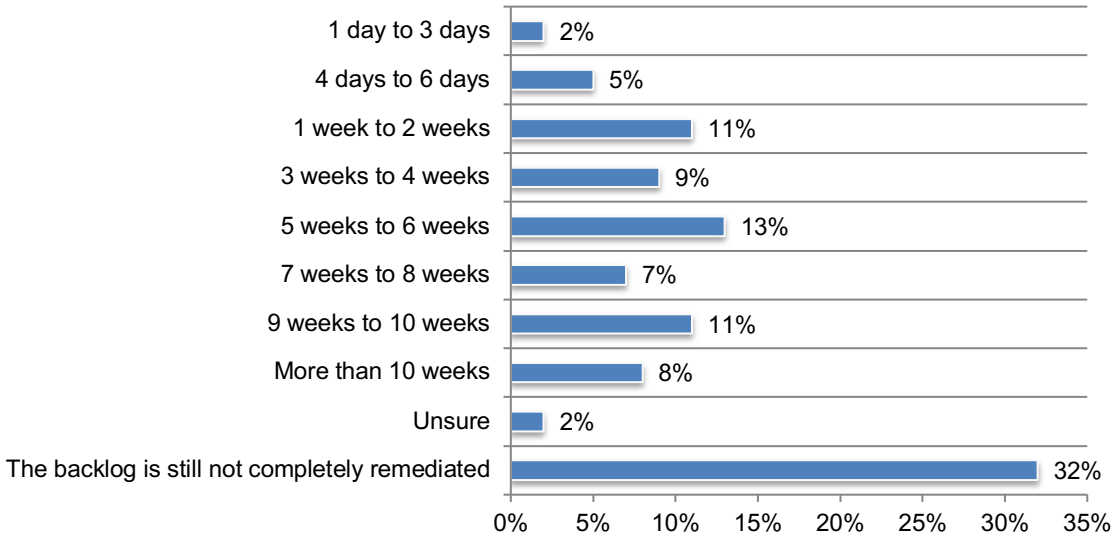
According to Figure 14, two problems that have grown in significance since 2015 are that solutions are slow to remediate vulnerable applications and the high false positive rate. Problems with cost and difficulty in implementation have decreased in the past five years.

Figure 14. What is wrong with current solutions to remediate vulnerabilities in applications?
More than one response permitted



Organizations are at risk because of the number of vulnerabilities that are not remediated. As discussed previously, on average, more than half (51 percent) of vulnerabilities were not remediated in the past 12 months. As shown in Figure 15, almost one-third of respondents say all vulnerabilities in the backlog are not completely remediated. Only 7 percent of respondents say the backlog is remediated within a week.

Figure 15. In the past 12 months, how long did it take to remediate this backlog?



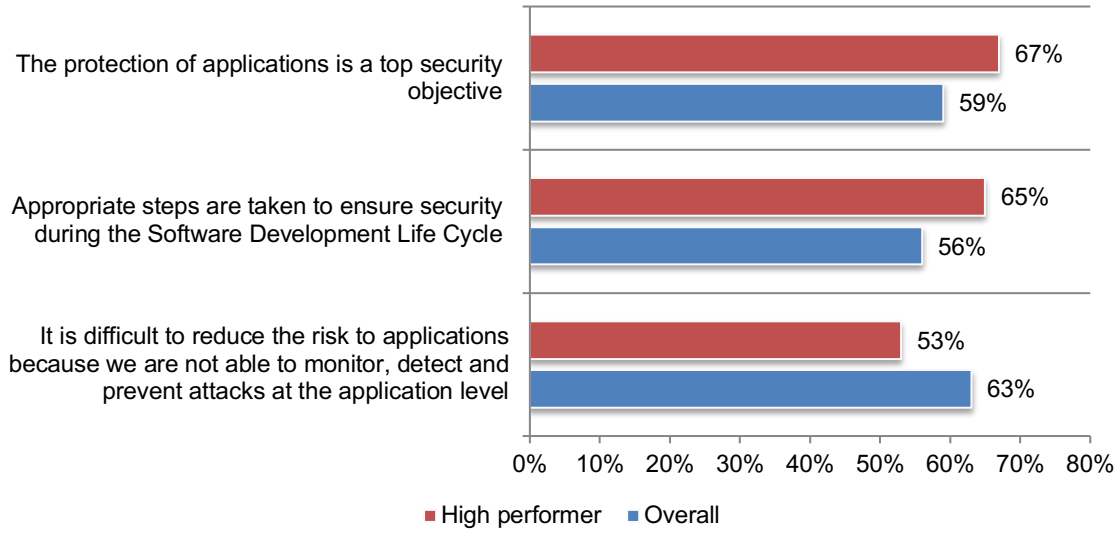
Best practices of high performing organizations in reducing application security risk

In this section, we compare the findings of organizations with characteristics that indicate they are more effective than the overall sample of respondents in reducing application security risks. We refer to these organizations as high performers. These organizations take the following steps.

- Establish a formal structured approach to the SSDLC that is applied consistently across the enterprise.
- Ensure the SSDLC builds security features in the design and development phase.
- The development and security teams collaborate to ensure the mitigation of application security risk.

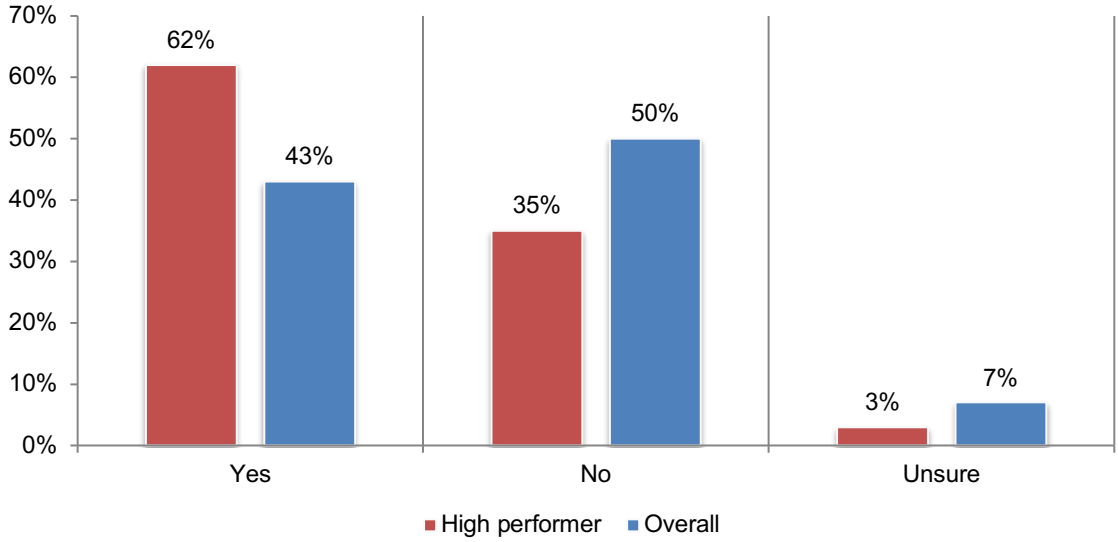
High performers are more likely to make the protection of applications a priority. As shown in Figure 16, high performers are less likely to consider it difficult to monitor, detect and prevent attacks at the application level. Possible reasons are that high performing organizations make application security a priority and action is taken to ensure security during the Secure Software Development Life Cycle (SSDLC).

Figure 16. Differences in characteristics of organizations' approach to application security
Strongly agree and Agree responses combined



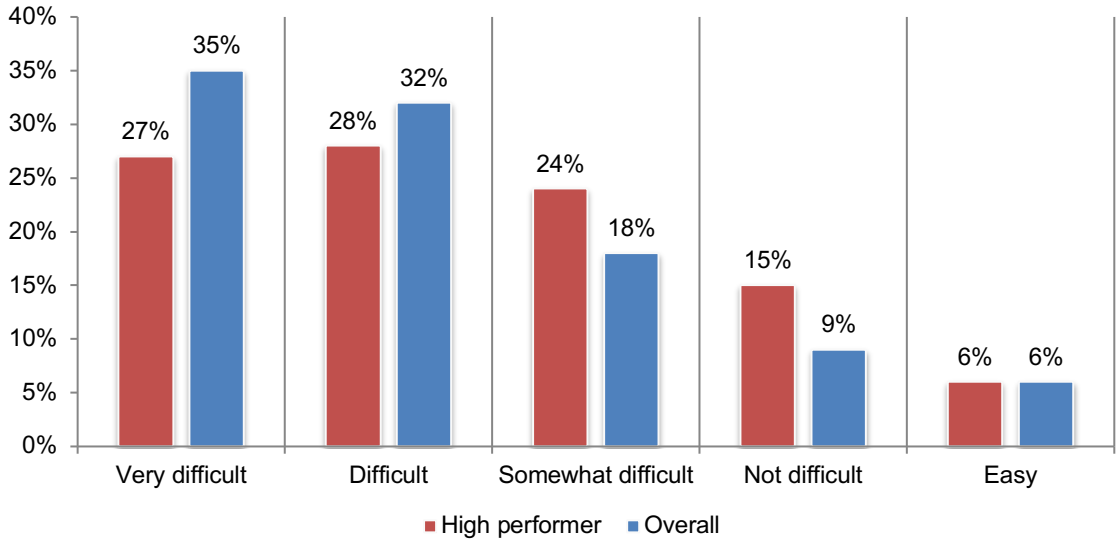
High performers make security in the development of new applications a priority. According to Figure 17, 62 percent of high performing organizations vs. 43 percent of the overall sample say security is adequately emphasized during the development of new applications.

Figure 17. Is security adequately emphasized during the development of new applications?



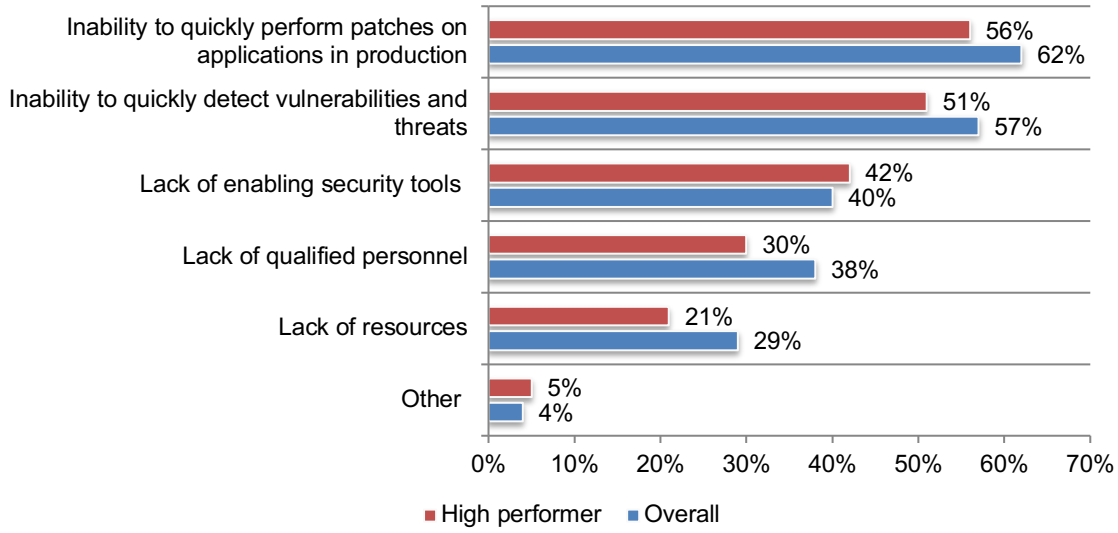
High performers are more likely to say that it is only somewhat difficult, not difficult or easy (45 percent of respondents vs. 33 percent in the overall sample) to remediate vulnerabilities in applications, as shown in Figure 18.

Figure 18. How difficult is it to remediate vulnerabilities in applications?



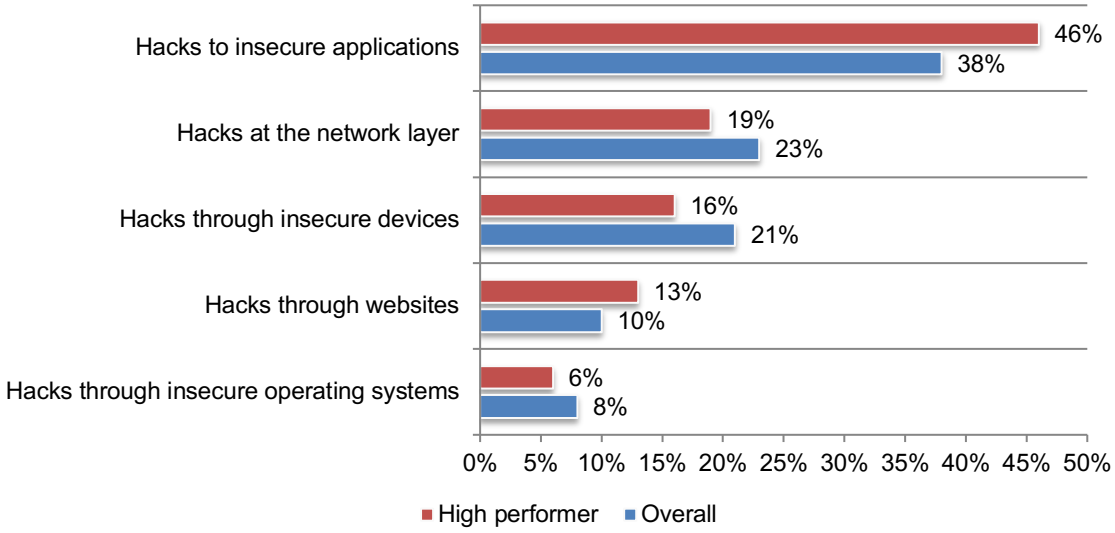
The top two challenges in remediating vulnerabilities in applications are the inability to quickly perform patches on applications in production and quickly detect vulnerabilities. Sixty-two percent of respondents in the overall sample and 56 percent of high performer respondents agree that these are the reasons for the difficulty in remediating applications, as shown in Figure 19.

Figure 19. Why is it difficult to remediate vulnerabilities in applications?
More than one response permitted



High performers are more concerned about hacks to insecure applications. As discussed previously, more high performing organizations than the overall sample make application security a priority. According to Figure 20, almost half (46 percent) of respondents in high performing organizations vs. 38 percent of respondents in the overall sample worry about hacks to insecure applications.

Figure 20. What kinds of attacks concerns your organization the most?



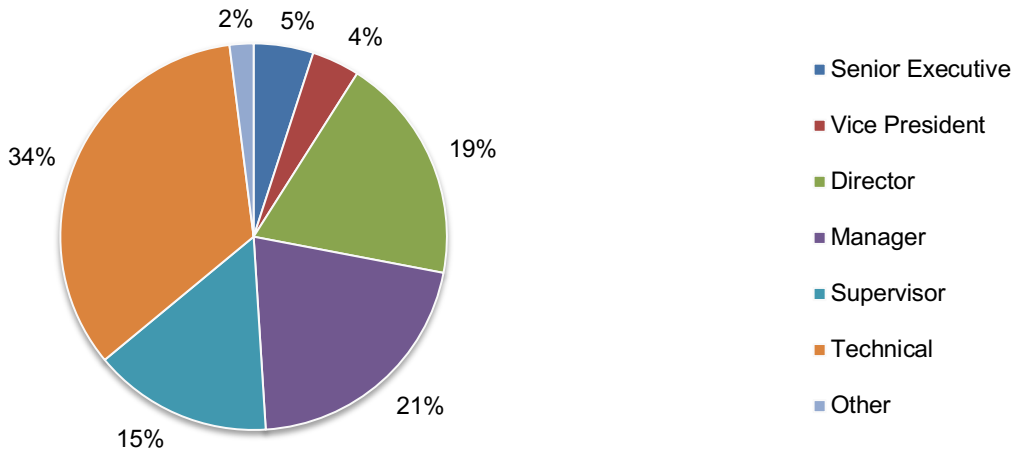
Part 3. Methods

A sampling frame of 16,575 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 704 total returns. Screening and reliability checks required the removal of 70 surveys. Our final sample consisted of 634 surveys or a 3.8 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,575	100.00%
Total returns	704	4.25%
Rejected or screened surveys	70	0.42%
Final sample	634	3.8%

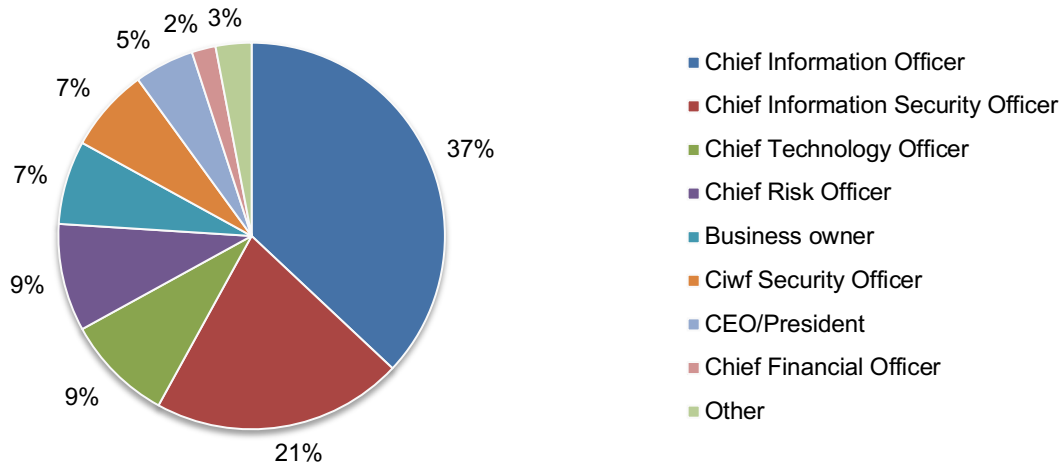
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (64 percent) of respondents are at or above the supervisory levels. The largest category at 34 percent of respondents is technical staff.

Pie Chart 1. Current position within the organization



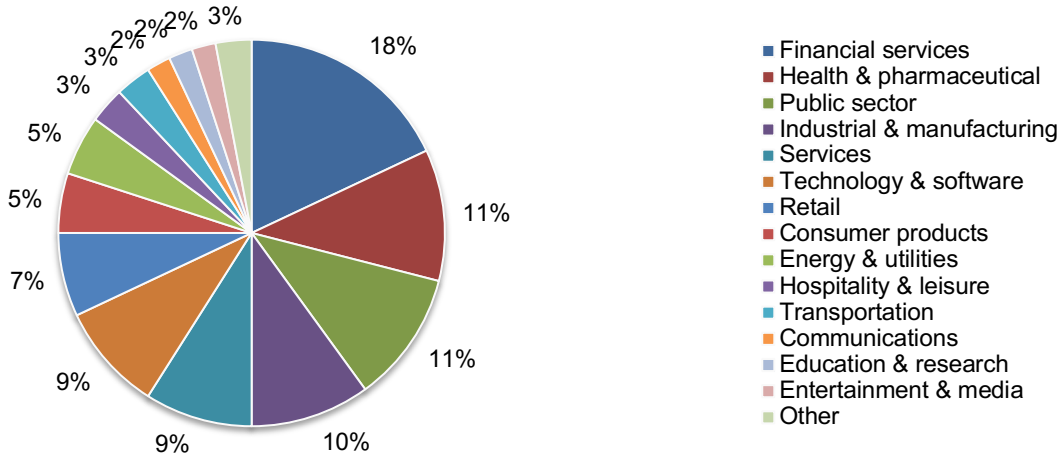
As shown in Pie Chart 2, 37 percent of the respondents indicated they report directly to the CIO and another 21 percent report to the CISO.

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



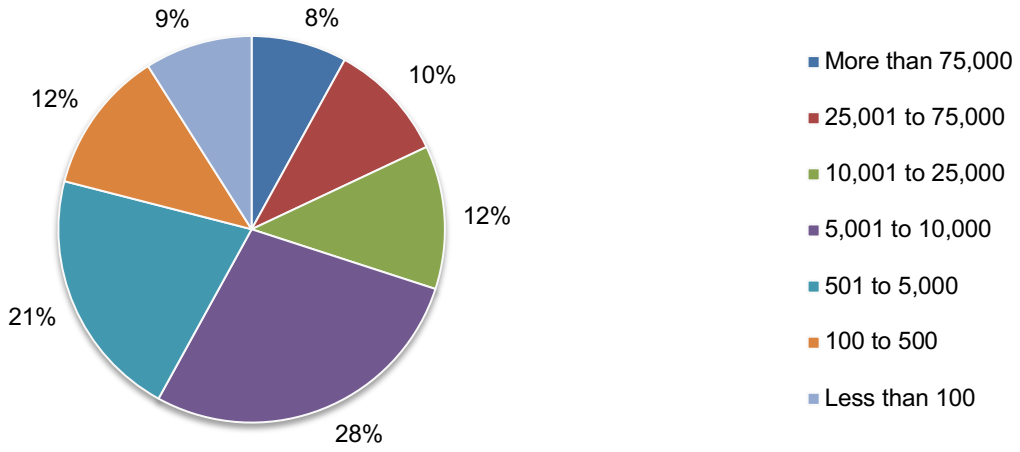
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals (11 percent of respondents), public sector (11 percent of respondents) and industrial and manufacturing (10 percent of respondents).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 4, 58 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 November 2020.

Survey response	2020	2015
Total sampling frame	16,575	16,889
Total returns	704	701
Rejected surveys	70	83
Final sample	634	618

Part 1. Screening

S1. Which of the following best describes your role in the secure software development life cycle? Please select all that apply.	FY2020	FY2015
Writing secure code	34%	50%
Implementing security technologies	39%	51%
Testing applications	45%	29%
Ensuring compliance	27%	59%
Resolving vulnerabilities	24%	74%
Securing applications and data	41%	69%
None of the above (Stop)	0%	0%
Total	210%	332%

Part 2. Attributions

Following are 5 attributions about your organization's application security. Please rate each statement using the scale provided below each item to express your opinion. **Strongly Agree and Agree response combined.**	FY2020	FY2015
Q1. My organization takes appropriate steps to ensure security during the Software Development Life Cycle (SSDLC).	56%	51%
Q2. My organization takes appropriate steps to ensure compliance with leading standards and guidelines for application security such as OWASP.	51%	45%
Q3. The protection of applications is a top security objective within my organization.	59%	45%
Q4. It is difficult to reduce the risk to applications because we are not able to monitor, detect and prevent attacks at the application level.	63%	84%
Q5. In the past year, our organization's portfolio of applications has become more vulnerable to attack.	71%	78%

Part 3. Background

Q6. What best describes the SSDLC in your organization?	FY2020	FY2015
It is a formal, structured approach applied consistently across the enterprise	33%	19%
It is a formal, structured approach, but not applied consistently across the enterprise	20%	20%
It is an informal and/or unstructured approach	26%	29%
It is an "ad hoc" approach	17%	29%
None of the above	4%	3%
Total	100%	100%

Q7. Where in the SDLC does your organization build in security features into applications under development?	FY2020	FY2015
Design phase	21%	32%
Development phase	25%	25%
Launch phase	23%	16%
Post-launch phase	30%	21%
None of the above	1%	6%
Total	100%	100%

Q8. In your opinion, is security adequately emphasized during the development of new applications?	FY2020	FY2015
Yes	43%	39%
No	50%	55%
Unsure	7%	6%
Total	100%	100%

Q9. Approximately, how many business applications are **deployed** within your organization (at any point in time)?	FY2020	FY2015
Less than 100	4%	5%
100 to 500	9%	9%
501 to 1,000	19%	11%
1,001 to 2,500	25%	34%
2,501 to 5,000	23%	23%
More than 5,000	20%	18%
Total	100%	100%

Q10. What percentage of all deployed applications are considered **business-critical**?	FY2020	FY2015
Less than 5%	9%	5%
5 to 10%	18%	17%
11 to 25%	31%	36%
26 to 50%	22%	22%
51 to 75%	14%	13%
76 to 100%	6%	7%
Total	100%	100%
Extrapolated value	30%	30%

Q11. On average, how long does it take to shore up an application in production mode after a vulnerability is detected?	FY2020	FY2015
Within seconds	2%	1%
Within minutes	10%	6%
Within hours	28%	28%
Within days	34%	32%
Within weeks	13%	23%
Within months	11%	8%
Other (please specify)	2%	2%
Total	100%	100%

Q12a. How difficult is it to remediate vulnerabilities in applications?	FY2020	FY2015
Very difficult	35%	31%
Difficult	32%	33%
Somewhat difficult	18%	24%
Not difficult	9%	7%
Easy	6%	5%
Total	100%	100%

Q12b. [If difficult or very difficult] Why is it difficult to remediate vulnerabilities in applications? Please select all that apply.	FY2020	FY2015
Inability to quickly detect vulnerabilities and threats	57%	68%
Inability to quickly perform patches on applications in production	62%	73%
Lack of enabling security tools	40%	44%
Lack of qualified personnel	38%	60%
Lack of resources	29%	29%
Other (please specify)	4%	3%
Total	230%	277%

Q13a. Did your organization have a vulnerability backlog in the past 12 months (i.e. applications that have been identified as vulnerable but have not been remediated)?	FY2020	FY2015
Yes	63%	51%
No	27%	41%
Don’t know	10%	8%
Total	100%	100%

Q13b. If yes, in the past 12 months what percentage of vulnerable applications were not remediated?	FY2020	FY2015
Less than 5%	5%	5%
5 to 10%	8%	7%
11 to 25%	13%	13%
26 to 50%	19%	35%
51 to 75%	28%	26%
76 to 100%	27%	14%
Total	100%	100%
Extrapolated value	51%	45%

Q13c. If yes, in the past 12 months how long did it take to remediate this backlog?	FY2020
Less than 1 day	0%
1 day to 3 days	2%
4 days to 6 days	5%
1 week to 2 weeks	11%
3 weeks to 4 weeks	9%
5 weeks to 6 weeks	13%
7 weeks to 8 weeks	7%
9 weeks to 10 weeks	11%
More than 10 weeks	8%
Unsure	2%
The backlog is still not completely remediated	32%
Total	100%

Q14. What is wrong with current solutions to remediate vulnerabilities in applications? Please select all that apply.	FY2020	FY2015
Too costly	47%	61%
Overly complex	55%	59%
Difficult to implement	38%	62%
Interoperability issues	51%	49%
Scaleabiliity issues	23%	26%
Poor support from vendor	19%	49%
High false positive rate	50%	21%
Slow to remediate vulnerable applications	60%	25%
Other (please specify)	3%	3%
Total	346%	355%

Q15. 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. Following are five areas for potential security risks and vulnerabilities:	FY2020	FY2015
Networks	20	18
Servers	13	12
Endpoints	15	20
Applications	38	33
Data	14	17
Total=100 points	100	100

Q16. 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. Following are five areas for potential security risks and vulnerabilities:	FY2020	FY2015
Networks	38	35
Servers	10	13
Endpoints	19	19
Applications	17	20
Data	16	13
Total=100 points	100	100

Q17. How much of the present year's overall IT budget is dedicated to data protection/security?	FY2020	FY2015
Less than 5%	7%	13%
6% to 10%	5%	28%
11% to 20%	12%	32%
21% to 30%	23%	15%
31% to 40%	24%	9%
41% to 50%	17%	2%
More than 50%	12%	1%
Total	100%	100%
Extrapolated value	32%	16%

Q18. How much of the data security budget is invested in application security?	FY2020	FY2015
Less than 5%	13%	4%
6% to 10%	18%	26%
11% to 20%	24%	29%
21% to 30%	23%	19%
31% to 40%	15%	15%
41% to 50%	5%	7%
More than 50%	2%	0%
Total	100%	100%
Extrapolated value	20%	20%

Q19. What best describes the nature of collaboration between your organization's application development and security teams.	FY2020	FY2015
Significant collaboration between development and security teams	14%	11%
Some collaboration between development and security teams	21%	21%
Limited collaboration between development and security teams	29%	36%
No collaboration between development and security teams	36%	32%
Total	100%	100%

Q20. What kind of attacks concerns your organization the most?	FY2020	FY2015
Hacks at the network layer	23%	21%
Hacks through insecure devices	21%	13%
Hacks through websites	10%	25%
Hacks through insecure operating systems	8%	9%
Hacks to insecure applications	38%	32%
Total	100%	100%

Q21. What is your primary means of securing applications? Please select all that apply.	FY2020
Internal pen test	46%
External pen test	53%
WAF	48%
SAST	28%
DAST	48%
IAST	35%
SCA	19%
RASP	47%
Total	324%

Part 4. Organizational characteristics

D1. What organizational level best describes your current position?	FY2020	FY2015
Senior Executive	5%	2%
Vice President	4%	1%
Director	19%	17%
Manager	21%	20%
Supervisor	15%	15%
Technical	34%	34%
Other (please specify)	2%	11%
Total	100%	

D2. Check the **Primary Person** you or your supervisor reports to within your organization.	FY2020	FY2015
Business owner	7%	
CEO/President	5%	4%
Chief Financial Officer	2%	6%
Chief Information Officer	37%	50%
Chief Technology Officer	9%	7%
Chief Information Security Officer	21%	18%
Chief Security Officer	7%	4%
Chief Risk Officer	9%	5%
Other (please specify)	3%	6%
Total	100%	100%

D3. What industry best describes your organization's industry concentration or focus?	FY2020	FY2015
Agriculture	1%	1%
Communications	2%	2%
Consumer products	5%	5%
Defense & aerospace	1%	1%
Education & research	2%	
Energy & utilities	5%	6%
Entertainment & media	2%	2%
Financial services	18%	19%
Health & pharmaceutical	11%	11%
Hospitality & leisure	3%	4%
Industrial & manufacturing	10%	10%
Public sector	11%	12%
Retail	7%	7%
Services	9%	10%
Technology & software	9%	8%
Transportation	3%	2%
Other (please specify)	1%	0%
Total	100%	100%

D4. What is the worldwide headcount of your organization?	FY2020	FY2015
Less than 100	9%	9%
100 to 500	12%	13%
501 to 5,000	21%	25%
5,001 to 10,000	28%	26%
10,001 to 25,000	12%	14%
25,001 to 75,000	10%	6%
More than 75,000	8%	7%
Total	100%	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.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.