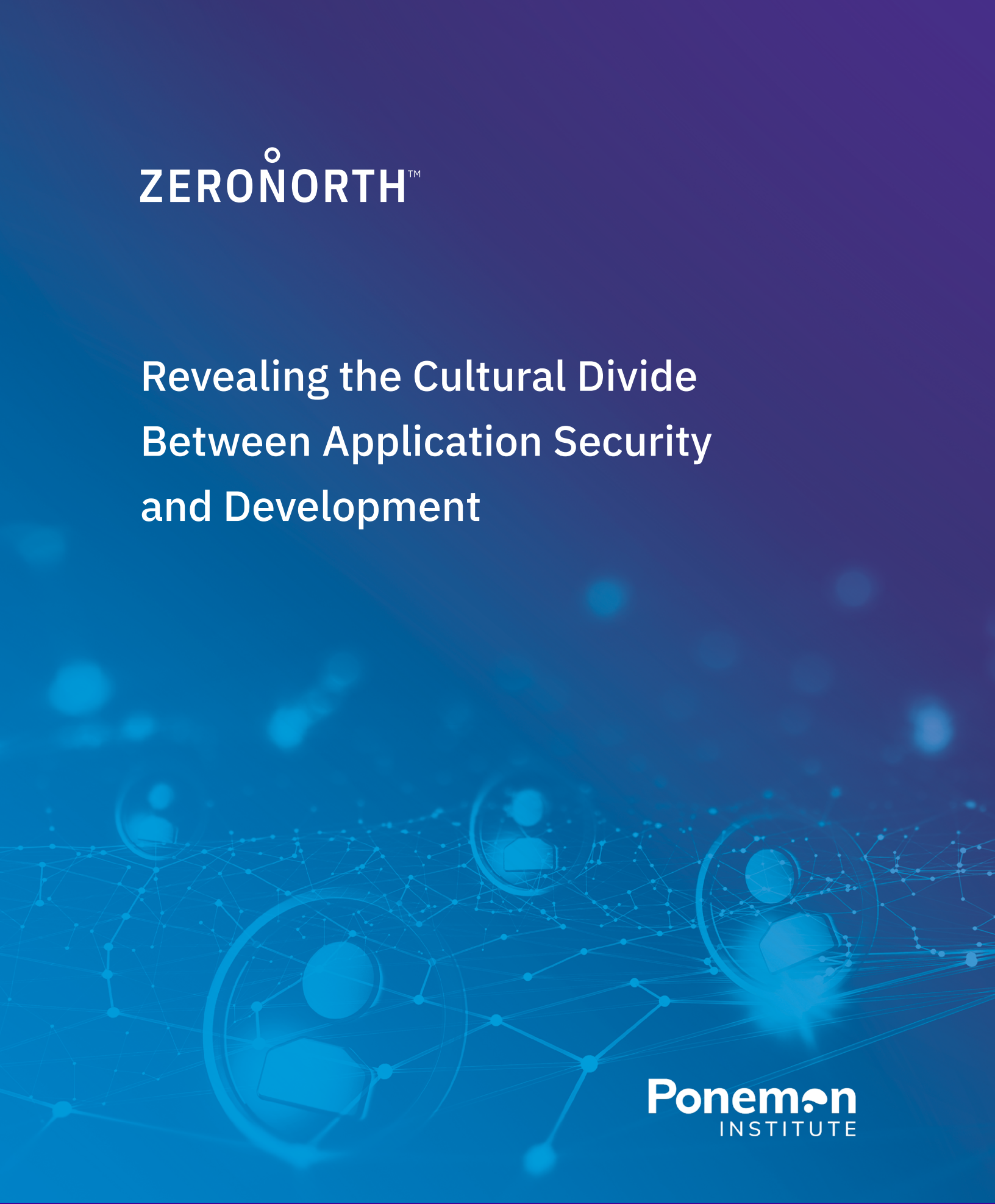
ZERONORTH™

Revealing the Cultural Divide Between Application Security and Development



Ponemon INSTITUTE

A Ponemon Institute© Research Report | Sponsored by ZeroNorth | September 2020

Revealing the Cultural Divide Between Application Security and Development

Prepared by Ponemon Institute, September 2020

Part 1. Introduction

Organizations are at risk when application security (AppSec) and development don't have a common vision for delivering software capabilities required by the business — securely. In short, there must be a fundamental agreement that security is integrated throughout the application development process. As business and product teams push developers to build and deliver code on a continual basis — and at an increasingly rapid rate — the perception of security as a hindrance raises its head. In this research, we refer to the lack of a common vision and the inability to work as a team as the cultural divide.

To determine the extent of the cultural divide in organizations, we surveyed 581 security practitioners who are involved in and knowledgeable about their organization's application security activities and 549 who are involved in and knowledgeable about their organization's software application development process.

Conducted by Ponemon Institute with sponsorship from ZeroNorth,® this research reveals the serious impact the cultural divide can have on organizations. Seventy-seven percent of developer respondents say the cultural divide affects their ability to meet deadlines and 70% of AppSec respondents say it is putting the security of applications at risk, which means people are holding up technology.

As shown in this research, technology alone cannot bridge the cultural divide. Rather, senior leadership must create an environment that encourages teamwork, collaboration and accountability. Currently, most organizations are not actively taking steps to encourage AppSec and development to work more effectively as a team.

AppSec respondents are far more likely to recognize the cultural divide exists. As shown in Figure 1, while 75 percent of AppSec respondents believe a cultural divide exists in their organizations, slightly less than half of developer respondents (49 percent) believe it exists. A hindrance to bridging the divide is that only 36 percent of security respondents and 45 percent of developer respondents believe their organizations' senior leadership is aware of this problem. This lack of awareness can have a serious impact on the security of their applications.

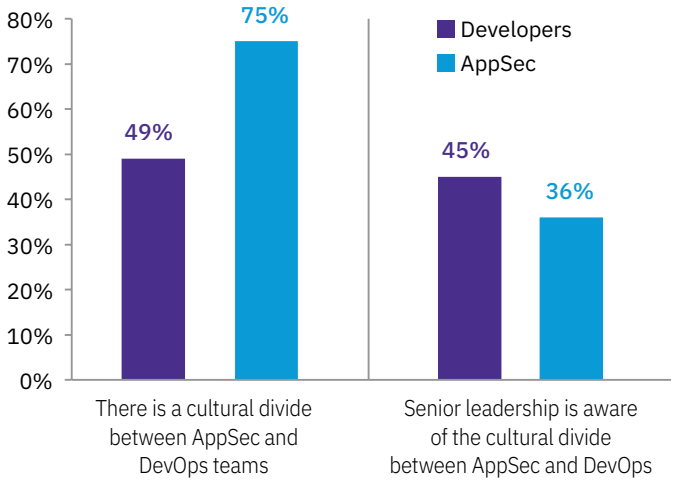


Figure 1. ***Do you believe there is a cultural divide between AppSec and development?*** (Yes responses presented)

Findings That Reveal Why the Cultural Divide Exists and Its Effect on the Security of Applications

Who is responsible for the security of applications? Developer and AppSec respondents don't agree on which function is ultimately responsible for the security of applications. Only 39% of developer respondents say the security team is ultimately responsible for application security. In contrast, 67% of AppSec say their teams are responsible. This lack of alignment demonstrates the potential for security to simply fall through the cracks if ownership is not clearly understood.

AppSec and developer respondents admit working together is difficult. AppSec respondents say it's because the developers publish code with known vulnerabilities. They also believe developers will accept flaws if they think the application will be a big seller. Developers say security does not understand the pressure they have to meet their deadlines. Developers also believe working with the AppSec team stifles their ability to innovate. It's clear that today, priorities, goals and objectives across these two teams are not aligned and this disconnect drives a wedge between the functions.

AppSec and development need to work as a team, now more than ever. Digital transformation is putting pressure on organizations to develop applications at increasing speeds, potentially putting their security at risk. Sixty-five percent of developer respondents say they feel the pressure to develop applications faster than before digital transformation. Fifty percent of AppSec respondents agree.

AppSec respondents see serious problems with application security practices in their organization. Seventy-one percent of AppSec respondents say the state of security is undermined by developers who don't care about the need to secure applications early in the SDLC. Sixty-nine percent of AppSec respondents say developers do not have visibility into the overall state of application security. As evidence of the tension between security and developers, 53% of AppSec respondents say developers view security as a hindrance to releasing new applications. Here again, competing priorities—speed for developers, security for AppSec—are often at odds.

Security respondents and developers disagree on whether the application security risk is increasing. Only 35% of developer respondents say application security risk in the organization is significantly increasing or increasing. In contrast, 60% of AppSec respondents say application security risk is increasing. This raises a question: which teams have clear visibility into the security posture of an application throughout its life cycle?

COVID-19 and the Cultural Divide

Teleworking as a result of the COVID-19 pandemic is stressful for both security and development. Sixty-six percent of developers and 72% of AppSec respondents say teleworking is very stressful. In addition, there is a lack of confidence that teleworkers are complying with their organizations' security and privacy requirements. Only 29% of developer respondents are very confident, and 38% of security respondents are very confident that teleworkers are complying with their organizations' security and privacy requirements.

The COVID-19 pandemic has significantly diminished the security of software applications. Seventy-four percent of AppSec and 47% of developer respondents say their organizations were highly effective in stopping or curtailing security compromises or exploits in software applications before the COVID-19 pandemic. After the pandemic started, only one-third of both respondents say their effectiveness is high.

Part 2. Key Findings

This section contains an analysis of the report's findings. The complete research results are found in the Appendix. The report is organized according to the following themes:

- Understanding the cultural divide
- How application security practices are affected by the cultural divide
- The impact of COVID-19 and teleworking on the cultural divide
- Bridging the cultural divide

Understanding the Cultural Divide

Who is ultimately responsible for the security of applications? According to Figure 2, only 39% of developer respondents say the AppSec team is ultimately responsible for application security. In contrast, 67% of AppSec respondents say their team is responsible. Such a significant gap in agreement could result in a lack of accountability that would affect application security.

Possible explanations for this gap are that the developers view security as a hindrance to innovation and would like more control over what they consider reasonable security practices. From the AppSec perspective, they are concerned they will be blamed for security mishaps to business-critical applications and believe AppSec teams should have control and accountability for the security of applications. Seventy percent of AppSec respondents vs. 60% of developer respondents say the existence of software vulnerabilities impacts the quality of applications.

As digital transformation takes hold, AppSec and developers need to work together as a team. Digital transformation is putting pressure on organizations to develop applications at increasing speeds, potentially putting their security at risk. Sixty-five percent of developer respondents say they feel the pressure to develop applications faster than before digital transformation. Fifty percent of AppSec respondents agree.

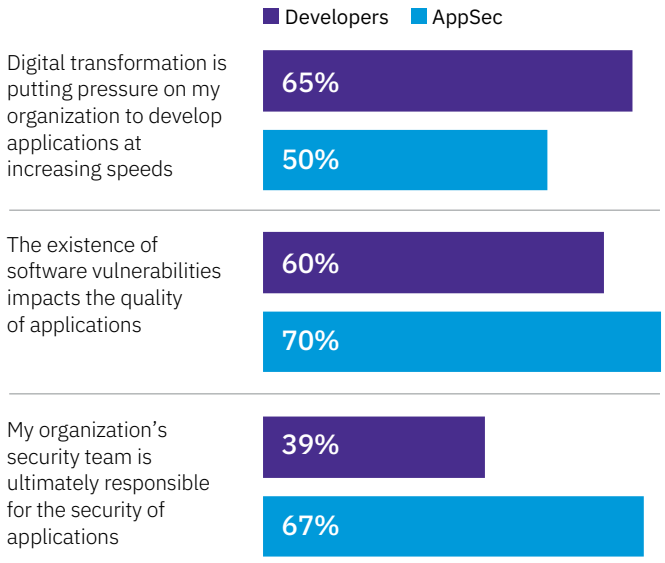


Figure 2. ***The cultural divide and the security of applications.*** *(*Strongly agree and Agree responses combined)

Both AppSec and developers admit working together is difficult. When asked to rate the difficulty in working together on a scale of 1 = not difficult to 10 = very difficult, 69% of developer respondents and 66% of AppSec respondents say it is very difficult.

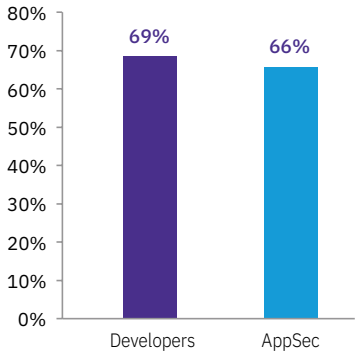


Figure 3. ***How difficult is it to work with AppSec and development?*** (Responses 7+ on the scale of 1 to 10)

AppSec respondents say it is very difficult to work with developers because they publish code with known vulnerabilities. According to Figure 4, 65% of AppSec respondents say developers publish code with known vulnerabilities. Fifty-five percent of AppSec respondents say it is difficult to work with developers because they accept flaws if they believe the application will be a big seller.

Figure 4. ***Why is it difficult to work with developers?*** (More than one response required)

Developers say the pressure to meet deadlines is not understood by AppSec. As shown in Figure 5, 65% of developers say the AppSec team does not understand the pressure to meet their deadlines, and 56% say AppSec stifles their ability to innovate.

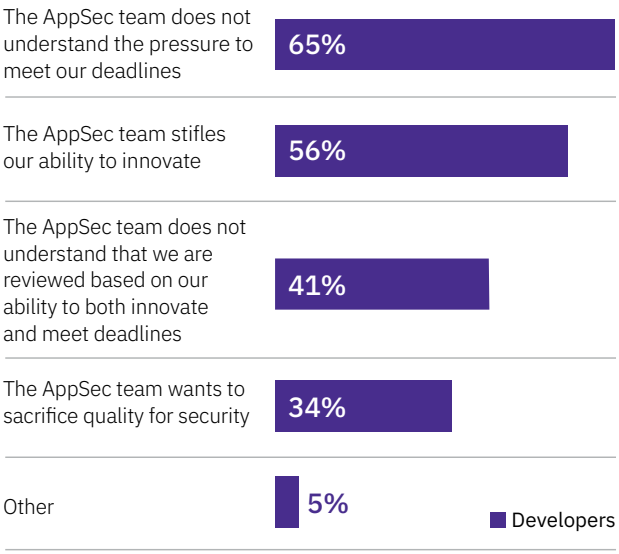


Figure 5. ***Why is it difficult to work with AppSec?*** (More than one response required)

The cultural divide affects the ability to meet deadlines and the security of applications. Respondents were asked to rate the impact of the cultural divide on developers' ability to meet deadlines and AppSec's ability to ensure the security of applications on a scale of 1 = no impact to 10 = severe impact. As shown in Figure 6, 77% of developer respondents say it has a serious impact on meeting deadlines, and 70% of security respondents say the cultural divide is putting the security of applications at risk.

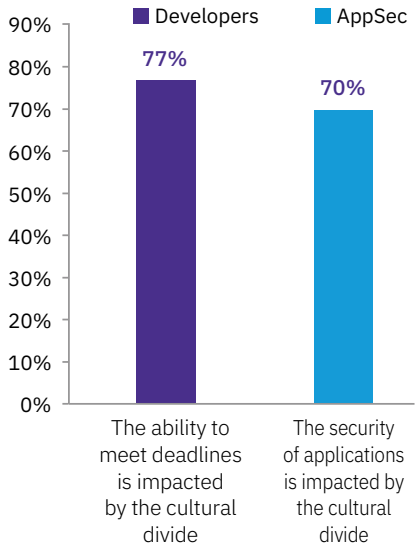


Figure 6. ***The impact on the ability to meet deadlines and security of applications.*** (On a scale from 1 = No impact to 10 = Severe impact, 7+ responses combined)

AppSec respondents do not believe senior management is interested in helping both functions work more effectively as a team. According to Figure 7, less than one-third of AppSec respondents say their organizations are actively helping security and development work more effectively as a team. Whereas, almost half (48%) of developer respondents say their organizations are trying to improve teamwork. Only 28% of AppSec respondents and 33% of developer respondents say senior leadership favors a DevSecOps approach to application security.

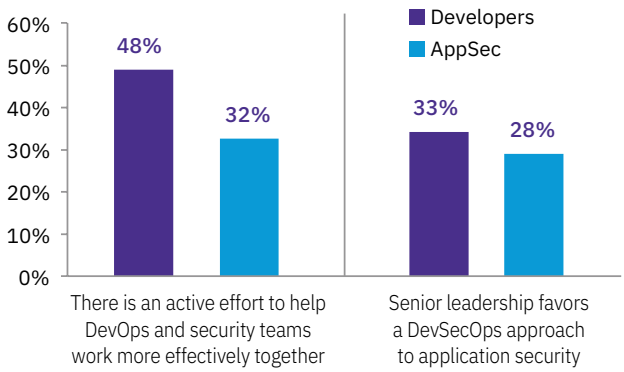


Figure 7. ***Perceptions about senior leadership's involvement in application security.*** (Strongly agree and Agree responses combined)

As discussed previously, only 36% of AppSec respondents and 45% of developer respondents say their senior leadership is aware of the cultural divide. However, if they are aware, senior leadership is taking steps to emphasize the necessity for both security and developers to work closely (43% of developer respondents and 44% of AppSec). Only 19% of both groups of respondents say senior leadership is helping to find a balance between application quality and security that is acceptable for both groups.

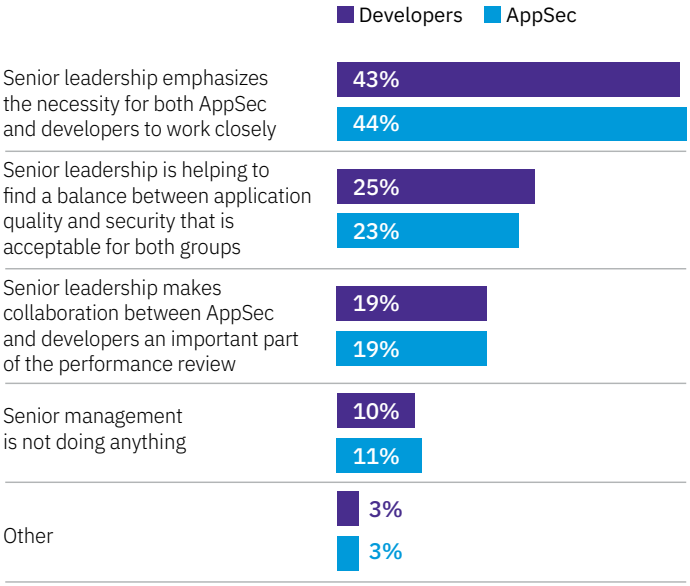


Figure 8. ***What is the one most important effort being made to help developers and AppSec teams work more effectively together?*** (Only one response permitted)

Both development and AppSec agree that not enough resources are allocated to application security. According to Figure 9, both developers and AppSec respondents agree that not having enough resources to ensure applications are secured in the development phase of the SDLC is the biggest challenge.

Less than half (48%) of developer respondents and 45% of AppSec respondents say developers have the knowledge and skill to address critical vulnerabilities in the application production life cycle. Very few respondents in both groups agree that application security practices are consistently applied across the enterprise (36% of developers and 34% of AppSec respondents).

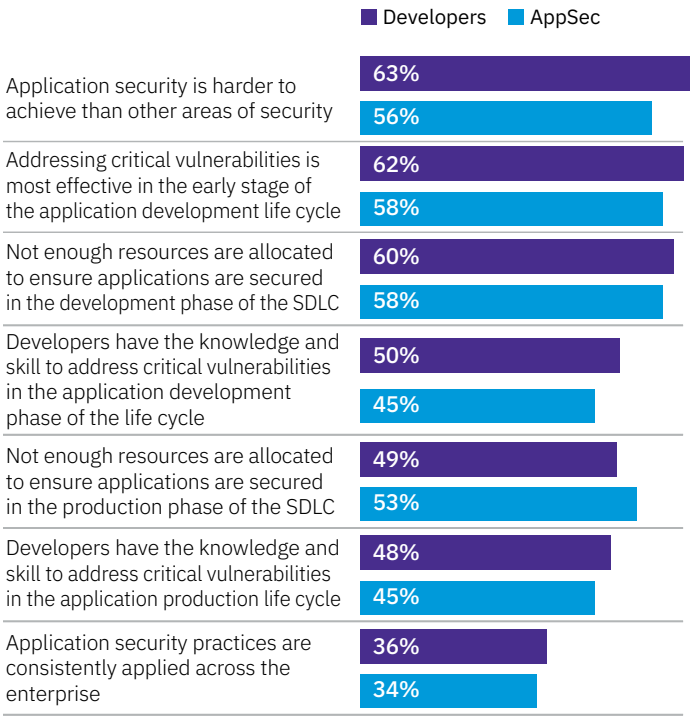


Figure 9. ***The challenges AppSec and development do agree upon.*** (Strongly agree and Agree responses combined)

Application security practices

AppSec respondents see serious problems with application security practices in their organization. As shown in Figure 10, 71% of AppSec respondents say the state of security is undermined by developers who don't care about the need to secure applications early in the SDLC. Sixty-nine percent of security respondents say the IT function does not have visibility into the overall state of application security. As evidence of the tension between AppSec and development, 53% of AppSec respondents say developers view security as a hindrance to releasing new applications.

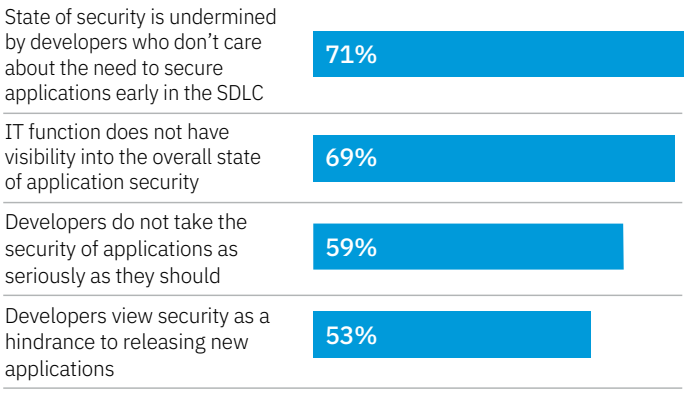


Figure 10. ***Perceptions of problems with application security practices according to AppSec.*** (Strongly agree and Agree responses combined)

Developers recognize the pressure to release applications is a security risk. As shown in Figure 11, only 43% of developer respondents do not view the pressure to release applications as a security risk, which means 57% of developers say the pressure to release is a security risk.

That said, most developers (63%) believe they do take quality of applications seriously. This is not surprising given development teams are focused on delivering high quality software products. However, based on this data, it appears developers may not correlate delivering secure software with delivering quality software.

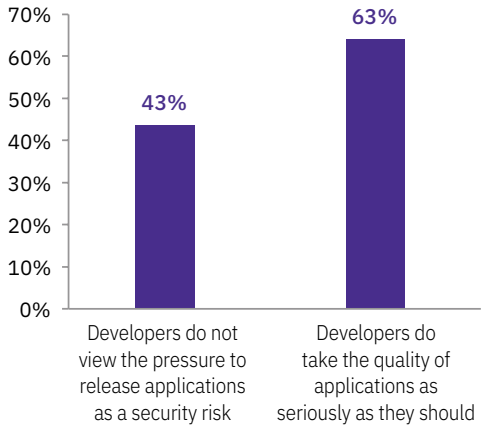


Figure 11. ***Developers' perception of application security practices.*** (Strongly agree and Agree responses combined)

Developers and AppSec agree on what challenges keep their application security posture from being fully effective. As shown in Figure 12, when security scanning increases, the number of vulnerabilities discovered grows. Both functions agree that the growth in application security vulnerabilities is the biggest deterrent to achieving a stronger application security posture. As security scanning increases, so does the number of found vulnerabilities. Often, these may be duplicative, and the net result is developers face an unending series of remediation tickets.

The second challenge—tightly related to the topic above—is the pressure to release new applications. Clearly, vulnerability overload and a focus on application delivery speeds are making stronger application security hard to achieve.

Figure 12. ***What challenges keep your organization's application security posture from being fully effective.*** (Two responses permitted)

The significant difference in perceptions about the increasing application security risk is evidence of the cultural divide. According to Figure 13, 60% of AppSec respondents say application security risk is significantly increasing. In contrast, only 35% of developer respondents say it is increasing.

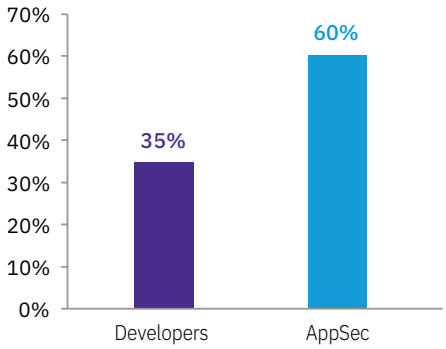


Figure 13. ***Is application security risk with your organization increasing?*** (Significantly increasing and Increasing responses combined)

AppSec and developers differ about what steps are taken to test for vulnerabilities in applications. Fifty-six percent of AppSec respondents vs. 45% of developer respondents say the primary step taken to test for vulnerabilities is to ensure tests accurately identify actual defects and eliminate false positives, as shown in Figure 14.

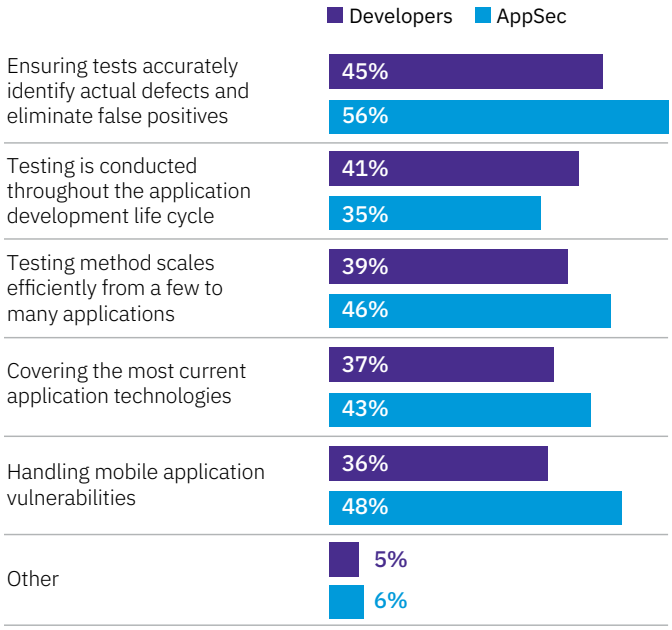


Figure 14. ***Steps taken to test for vulnerabilities in applications.*** (More than one response permitted)

Developers and AppSec also differ on the steps taken to remediate the risks associated with vulnerable applications. According to Figure 15, 68% of developer respondents say the primary step taken is to ensure developers receive training to support their coding process is secure vs. 57% of AppSec security respondents. Seventy-two percent of AppSec respondents say the primary step is to create test plans and test scripts to detect authentication defects early in the development cycle.

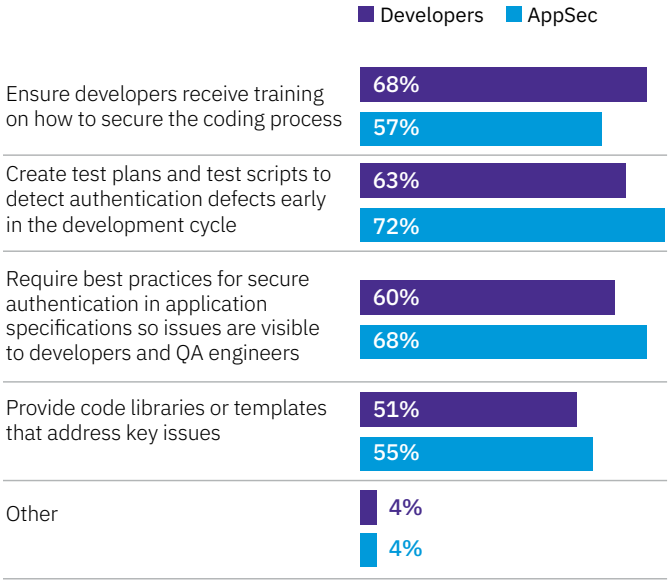


Figure 15. ***What steps does your organization take to remediate the risks associated with vulnerable applications?*** (More than one response permitted)

The impact of the COVID-19 pandemic and teleworking on the cultural divide

Teleworking is not feasible for security and development teams. As shown in Figure 16, 53% of AppSec respondents and 48% of developers do not believe teleworking will become the new norm even when the COVID-19 pandemic is over.

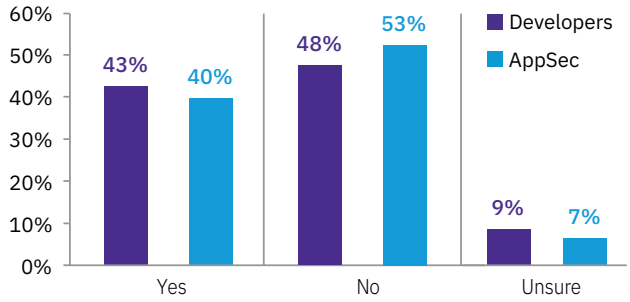


Figure 16. ***Do you think teleworking will become the new norm even when the coronavirus pandemic is over?***

Teleworking is stressful and explains why the majority of respondents say it will not be the new norm. When asked to rate their level of stress when teleworking on a scale of 1 = not stressful to 10 = very stressful, 66% of developer respondents and 72% of AppSec respondents say teleworking is stressful. (7+ responses)

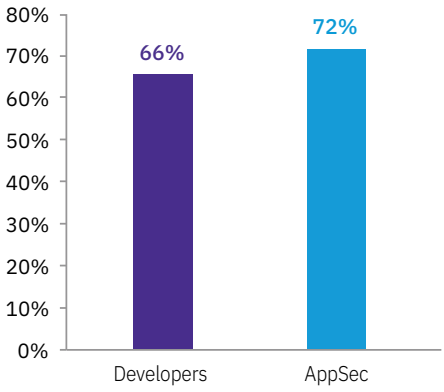


Figure 17. ***How stressful is teleworking?*** (From 1 = not stressful to 10 = very stressful, 7+ responses presented)

There is a lack of confidence that teleworkers are complying with security and privacy requirements. Respondents were asked to rate their confidence that teleworkers in their organizations are complying with their organizations' security and privacy requirements on a scale of 1 = not confident to 10 = very confident. As shown in Figure 18, only 29% of developer respondents and 38% of AppSec respondents say their organizations are confident their teleworkers are complying with security and privacy requirements.

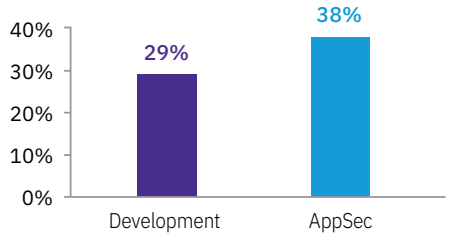


Figure 18. ***How confident are you that teleworkers are complying with your organization's security and privacy requirements?*** (From 1 = not confident to 10 = very confident, 7+ responses presented)

The COVID-19 pandemic has significantly diminished the security of software applications. Respondents were asked to rate the effectiveness of their organizations in stopping or curtailing security compromises or exploits in software applications before and after the COVID-19 pandemic on a scale of 1 = not effective to 10 = very effective.

According to Figure 19, before the COVID-19 pandemic, 74% of AppSec respondents and 47% of developer respondents say the ability to stop or curtail security compromises or exploits in software applications was very effective.

The pandemic has had a significant impact on organizations' effectiveness to stop security compromises or exploits in software applications. Only one-third of both respondents say their effectiveness is very high.

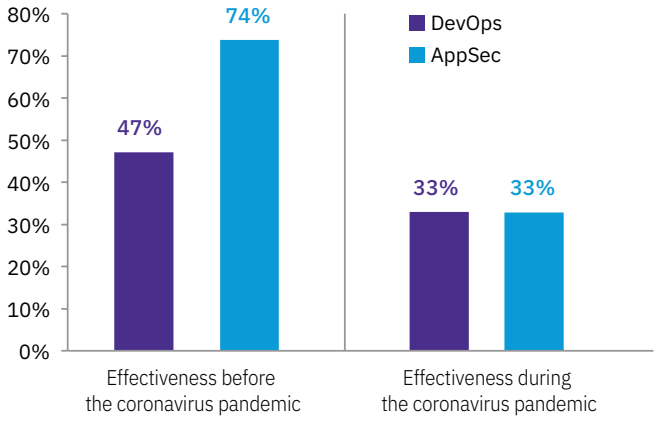


Figure 19. ***The effectiveness of the of their organizations in stopping or curtailing security compromises or exploits in software applications before and after the COVID-19 pandemic.*** (From 1 = not effective to 10 = very effective, 7+ responses combined)

Bridging the cultural divide

Technology alone will not reduce the security risks caused by the cultural divide. Senior leadership needs to understand how these admissions by security and development on the difficulty of working together can put business-critical applications at risk.

To bridge the cultural divide, senior leadership must address the following concerns of both security and development.

AppSec concerns

- Sixty-six percent of AppSec respondents say it is very difficult to work with developers because they publish code with known vulnerabilities, will accept flaws if they believe the application will be a big seller, do not demonstrate sufficient security practices and are not incentivized to have sufficient security practices in place.
- Seventy percent of AppSec respondents say the cultural divide is putting the security of applications at risk.
- Fifty-six percent of AppSec respondents say application security is harder to achieve than other areas of security.

Developer concerns

- Sixty-nine percent of developers say it is very difficult to work with security because they don't understand development's need to remain innovative while meeting pressurized deadlines or how their performance is reviewed based on the ability to stay productive in these areas without sacrificing quality for security.
- Seventy-seven percent of developer respondents say the cultural divide has a serious impact on meeting deadlines.
- Sixty-three percent of respondents say application security is harder to achieve than other areas of security

Recommendations on improving application security

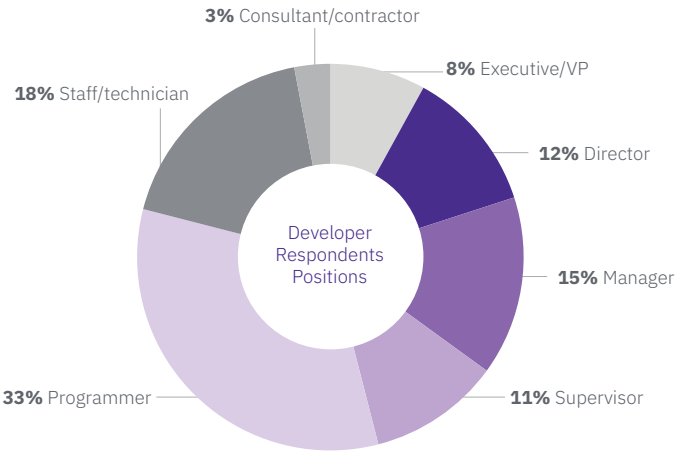
- Ensure sufficient resources are allocated to safeguard applications in the development and production phase of the SDLC.
- Apply application security practices consistently across the enterprise.
- Ensure developers have the knowledge and skill to address critical vulnerabilities in the application development and production life cycle.
- Conduct testing throughout the application development life cycle.
- Make sure testing methods scale efficiently from a few to many applications.

Part 3. Methods

A sampling frame of 16,008 AppSec professionals who are involved in and knowledgeable about their organization's application security activities and 15,665 developers who are involved in and knowledgeable about their organization's software application development process were selected as participants in this survey. Table 1 shows 605 development total returns and 641 AppSec total returns. Screening and reliability checks required the removal of 56 development surveys and 60 AppSec surveys. The final sample consisted of 549 development surveys, or a 3.5% response rate and 581 AppSec surveys, or a 3.6% response rate.

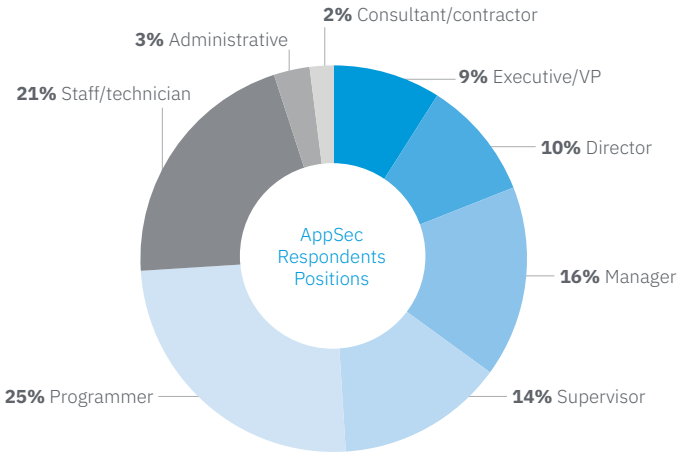
Table 1. Sample response	Developers	AppSec
Sampling frame	15,665	16,008
Total returns	605	641
Rejected or screened surveys	56	60
Final sample	549	581
Response rate	3.5%	3.6%

The following pie chart summarizes the position level of qualified developer respondents. At 33%, the largest segment contains those who are programmers followed by 18% of respondents who are technicians. The smallest segment (3%) includes consultants/ contractors. Almost half (49%) of respondents are at or above the supervisory level.



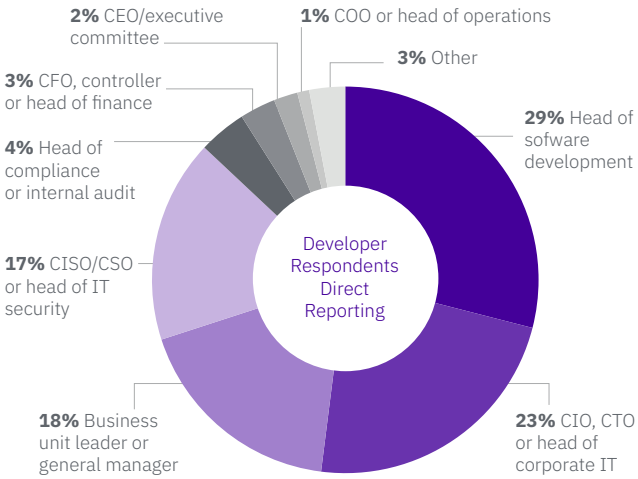
Pie Chart 1. ***Position level of developer respondents***

The following pie chart summarizes the position level of qualified AppSec respondents. At 25%, the largest segment contains those who are programmers followed by 21% of respondents who are staff/ technicians. The smallest segment (2%) includes consultants/contractors. Almost half (49%) of respondents are at or above the supervisory level.



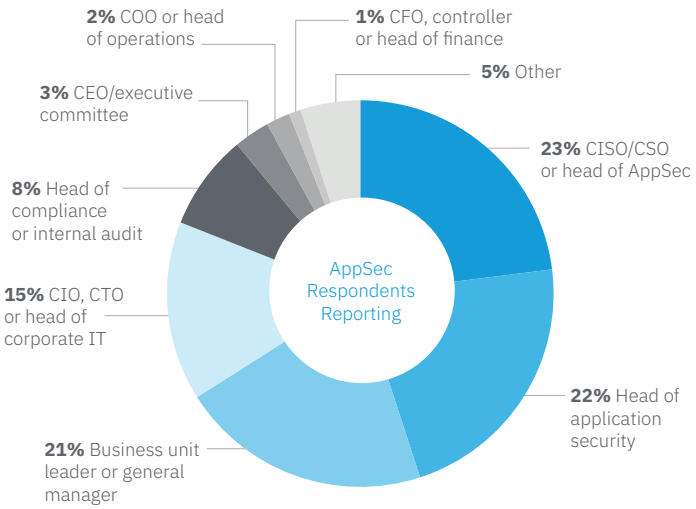
Pie Chart 2. ***Position level of AppSec respondents***

As shown in Pie Chart 3, 29% of developer respondents report directly to the head of software development, 23% of respondents report to the CIO,CTO or head of corporate IT and 18% of respondents report to the business unit leader or general manager.



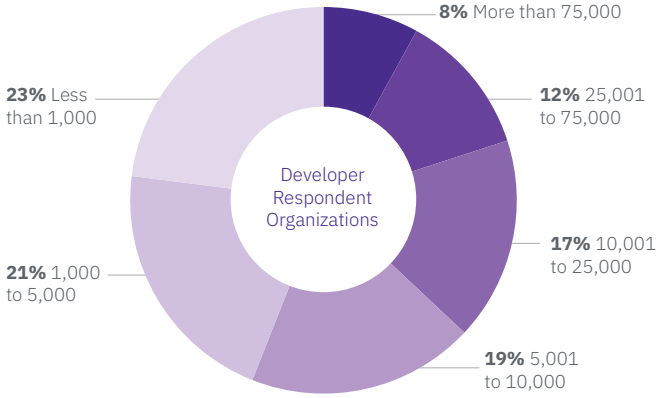
Pie Chart 3. ***Direct reporting channel of developer respondents***

As shown in Pie Chart 4, 23% of AppSec respondents report directly to the CISO/CSO or head of AppSec, 22% of respondents report to the head of application security and 21% of respondents report to the business unit leader or general manager.



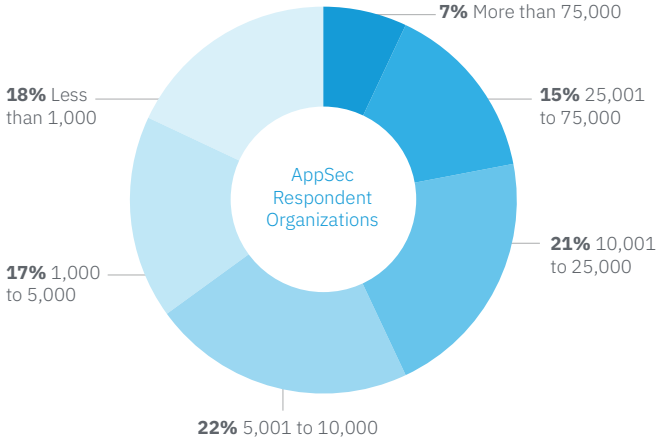
Pie Chart 4. ***The direct reporting channel of AppSec respondents***

Pie Chart 5 summarizes the total worldwide headcount of developer respondents' organizations. More than half (56%) of respondents are from organizations with a worldwide headcount greater than 5,000 employees.



Pie Chart 5. ***Global headcount of developer respondents' organizations***

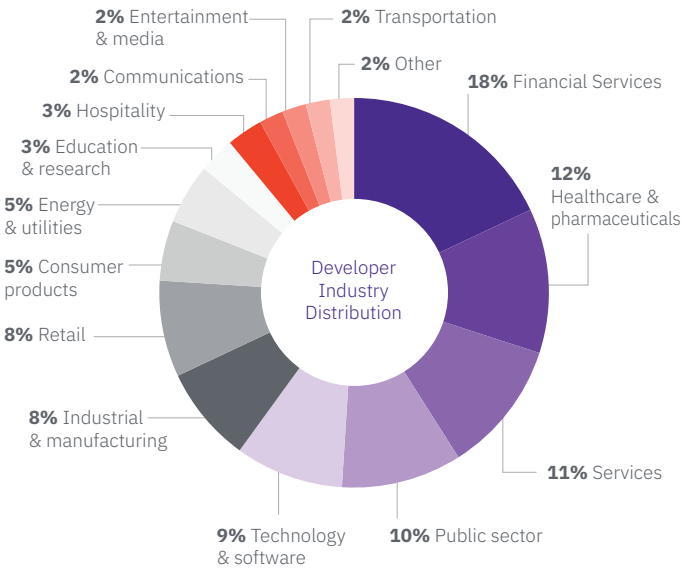
Pie Chart 6 summarizes the total worldwide headcount of AppSec respondents' organizations. More than half (65%) of respondents are from organizations with a worldwide headcount greater than 5,000 employees.



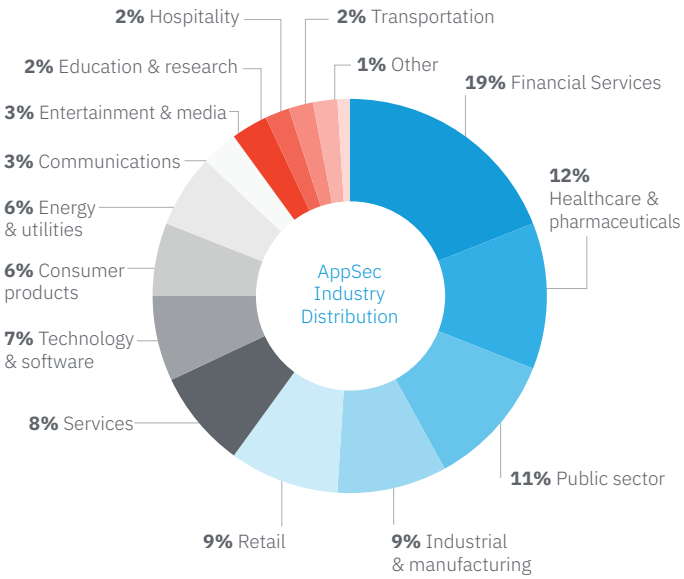
Pie Chart 6. ***Global headcount of AppSec respondents' organizations***

Pie Chart 7 reports the industry segments of developer respondents' organizations. This chart identifies financial services (18% of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceuticals (12% of respondents), services sector (11% of respondents), public sector (10% of respondents) and technology and software (9% of respondents).

Pie Chart 8 reports the industry segments of AppSec respondents' organizations. This chart identifies financial services (19% of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceuticals (12% of respondents), public sector (11% of respondents), industrial and manufacturing (9% of respondents) and retail (9% of respondents).



Pie Chart 7. ***Industry distribution of developer respondents' organizations***



Pie Chart 8. ***Industry distribution of AppSec respondents' organizations***

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. Surveys were send 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 knowledgeable about their organizations' application security activities and software application development processes. 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 from Developers

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between May 18, 2020 to June 5, 2020.

Survey response	Developers	Pct%
Total sampling frame	15,665	100.0%
Total returns	605	3.9%
Rejected surveys	56	0.4%
Final sample	549	3.5%

Screening	Developers
S1. What best defines your **level of involvement** in your organization's software application development process?	
Significant involvement	49%
Some involvement	51%
Minimal or no involvement (stop)	0%
Total	100%
S2. What best defines your **level of knowledge** in your organization's software application development process?	
Significant involvement	53%
Some involvement	47%
Minimal or no involvement (stop)	0%
Total	100%

Part 1. Attributions

Please rate each statement using the scale provided below each item. **Strongly agree and Agree responses combined.**

	Developers
Q1a. Digital transformation is putting pressure on my organization to develop applications at increasing speeds.	65%
Q1b. Developers do take the quality of applications as seriously as they should.	63%
Q1c. The existence of software vulnerabilities impacts the quality of applications.	60%
Q1d. My organization's application security practices are consistently applied across the enterprise	36%
Q1e Developers in my organization have the knowledge and skill to address critical vulnerabilities in the application **development phase** of the life cycle.	50%
Q1f. Developers in my organization have the knowledge and skill to address critical vulnerabilities in the **application production** life cycle.	48%
Q1g. Developers do not view the pressure to release applications as a security risk.	43%

	Developers
Q1h. My organization recognizes that addressing critical vulnerabilities is most effective in the early stage of the application development life cycle.	62%
Q1i. My organization does not allocate enough resources to ensure applications are secured in the **development phase** of the SDLC.	60%
Q1j. My organization does not allocate enough resources to ensure applications are secured in the **production phase** of the SDLC.	49%
Q1k. In my organization, application security is harder to achieve than other areas of security.	63%
Q1l. There is an active effort within my organization to help developers and security teams work more effectively together.	48%
Q1m. Senior leadership favors a DevSecOps approach to application security.	33%
Q1n. My organization's security team is ultimately responsible for the security of applications.	39%

Part 2. Coronavirus & teleworking

	Developers
Q2a. Do you telework?	
Yes	40%
No	60%
Total	100%
Q2b. If yes, how long have you been teleworking because of the coronavirus pandemic?	
Less than four weeks	24%
Four to eight weeks	44%
More than eight weeks	32%
Total	100%
Q3. Will teleworking become the new norm even when the coronavirus pandemic is over?	
Yes	43%
No	48%
Unsure	9%
Total	100%
Q4. How stressful is teleworking? From 1 = not stressful to 10 = very stressful.	
1 or 2	3%
3 or 4	8%
5 or 6	23%
7 or 8	34%
9 or 10	32%
Total	100%
Extrapolated value	7.18

	Developers
Q5. How confident are you that teleworkers are complying with your organization's security and privacy requirements? From 1 = not confident to 10 = very confident.	
1 or 2	16%
3 or 4	32%
5 or 6	23%
7 or 8	19%
9 or 10	10%
Total	100%
Extrapolated value	5.00
Q6. Before the coronavirus pandemic, please rate the effectiveness of your organization's efforts to stop or curtail security compromises or exploits in software applications. From 1 = not effective to 10 = very effective.	
1 or 2	8%
3 or 4	15%
5 or 6	30%
7 or 8	23%
9 or 10	24%
Total	100%
Extrapolated value	6.30
Q7. During the coronavirus pandemic, please rate the effectiveness of your organization's efforts to stop or curtail security compromises or exploits in software applications. From 1 = not effective to 10 = very effective.	
1 or 2	16%
3 or 4	25%
5 or 6	26%
7 or 8	19%
9 or 10	14%
Total	100%
Extrapolated value	5.30

Part 3. The cultural divide

In the context of this research, ***the cultural divide*** *occurs when AppSec and development do not have a common vision on how to both secure and meet the business goals for the development and production of software applications.*

	Developers
Q8a. Please rate the difficulty in working with AppSec From 1 = not difficult to 10 = very difficult.	
1 or 2	5%
3 or 4	11%
5 or 6	15%
7 or 8	34%
9 or 10	35%
Total	100%
Extrapolated value	7.16
Q8b. Why is it very difficult to work with AppSec? (7+ responses on the 10-point scale) Please select all that apply.	
The AppSec team stifles our ability to innovate	56%
The AppSec team wants to sacrifice quality for security	34%
The AppSec team does not understand the pressure to meet our deadlines	65%
The AppSec team does not understand that we are reviewed based on our ability to both innovate and meet deadlines	41%
Other (please specify)	5%
Total	201%
Q9a. Within your organization, do you believe there is a cultural divide between AppSec and development teams?	
Yes	49%
No	51%
Total	100%
Q9b. If yes, is senior leadership aware of the cultural divide between AppSec and development?	
Yes	45%
No	51%
Unsure	4%
Total	100%

	Developers
Q9c. If yes, how is the ability to meet deadlines impacted by the cultural divide? 1=no impact to 10=severe impact	
1 or 2	3%
3 or 4	8%
5 or 6	12%
7 or 8	34%
9 or 10	43%
Total	100%
Extrapolated value	7.62
Q9d. If yes, what is the one most important effort being made to help AppSec and development work more effectively as a team? Please select one choice only.	
Senior leadership is helping to find a balance between app quality and security that is acceptable for both groups	25%
Senior leadership emphasizes the necessity for both AppSec and development to work closely	43%
Senior leadership makes collaboration between AppSec and development an important part of the performance review	19%
Senior management is not doing anything	10%
Other (please specify)	3%
Total	100%

Part 3. Application security practices

	Developers
Q10. Who owns your organization's application security process of function? Please select one person/department.	
CIO or CTO	23%
CISO or CSO	18%
Head of software development	21%
Head of quality assurance	7%
Business units (LOB)	12%
Other (please specify)	0%
No one person or department	19%
Total	100%
Q11. What challenges keep your organization's application security posture from being fully effective? Please select your top two challenges.	
Insufficient budget (money)	31%
Growth in application security vulnerabilities	51%
Lack of in-house expertise	15%
Lack of clear leadership	12%
Lack of effective testing tools	25%
Management underestimates risk	3%
Pressure to release new applications	47%
Not considered an organizational priority	16%
Total	200%
Q12. In your opinion, is application security risk within your organization increasing, decreasing or staying at about the same level?	
Significantly increasing	12%
Increasing	23%
Staying the same	28%
Decreasing	20%
Significantly decreasing	12%
Cannot determine	5%
Total	100%

	Developers
Q13. How frequently do developers publish/deploy code with known vulnerabilities?	
Very frequently	14%
Frequently	13%
Not frequently	27%
Rarely	25%
Never	21%
Total	100%
Q14. What best describes your organization's application testing cycle?	
Continuously	14%
Daily	8%
Weekly	9%
Monthly	9%
Quarterly	8%
Yearly	14%
More than yearly	12%
Only after new code is added	11%
No planned cycle	15%
Total	100%
Q15. Please check all the steps taken to test for vulnerabilities in applications.	
Testing is conducted throughout the application development life cycle	41%
Testing method scales efficiently from a few to many applications	39%
Ensuring tests accurately identify actual defects and eliminate false positives	45%
Covering the most current application technologies	37%
Handling mobile application vulnerabilities	36%
Other (please specify)	5%
Total	203%

Part 3. Application security practices *(continued)*

	Developers
Q16. What steps does your organization take to remediate the risks associated with vulnerable applications? Please select all that apply.	
Ensure developers receive training on how to secure the coding process	68%
Provide code libraries or templates that address key issues	51%
Create test plans and test scripts to detect authentication defects early in the development cycle	63%
Require best practices for secure authentication in application specifications so issues are visible to developers and QA engineers	60%
Other (please specify)	4%
Total	246%

Part 4. Organization and respondents' demographics

	Developers
D1. What best describes your position level within the organization?	
Executive/VP	8%
Director	12%
Manager	15%
Supervisor	11%
Programmer	33%
Staff/technician	18%
Administrative	0%
Consultant/contractor	3%
Other	0%
Total	100%
D2. What best describes your direct reporting channel?	
CEO/executive committee	2%
COO or head of operations	1%
CFO, controller or head of finance	3%
CIO, CTO or head of corporate IT	23%
Head of software development	29%
Business unit leader or general manager	18%
Head of compliance or internal audit	4%
CISO/CSO or head of AppSec	17%
Other	3%
Total	100%
D3. What range best describes the full-time headcount of your global organization?	
Less than 1,000	23%
1,000 than 5,000	21%
5,001 to 10,000	19%
10,001 to 25,000	17%
25,001 to 75,000	12%
More than 75,000	8%
Total	100%

	Developers
D4. What best describes your organization's primary industry classification?	
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Healthcare & pharmaceuticals	12%
Hospitality	3%
Industrial & manufacturing	8%
Public sector	10%
Retail	8%
Services	11%
Technology & software	9%
Transportation	2%
Other	0%
Total	100%

Detailed Survey Results from AppSec

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between May 18, 2020 to June 5, 2020.

Survey response	AppSec	Pct%
Total sampling frame	16,008	100.0%
Total returns	641	4.0%
Rejected surveys	60	0.4%
Final sample	581	3.6%

Screening	AppSec
S1a. What best defines your **level of involvement** in your organization's application security activities within the AppSec function?	
Significant involvement	45%
Some involvement	55%
Minimal or no involvement (stop)	0%
Total	100%
S1b. What best defines your **level of knowledge** about your organization's application security activities?	
Significant involvement	51%
Some involvement	49%
Minimal or no involvement (stop)	0%
Total	100%

Part 1. Attributions

Please rate each statement using the scale provided below each item. **Strongly Agree and Agree responses combined.**

	AppSec
Q1a. Digital transformation is putting pressure on my organization to develop applications at increasing speeds.	50%
Q1b. Developers do not take the security of applications as seriously as they should.	59%
Q1c. The existence of software vulnerabilities impacts the quality of applications.	70%
Q1d. In my organization, the creation of quality applications is considered more important than having a strong security posture.	36%
Q1e. My organization's IT function does not have visibility into the overall state of application security.	69%
Q1f. My organization's application security practices are consistently applied across the enterprise.	34%
Q1g. Developers in my organization have the knowledge and skill to address critical vulnerabilities in the **application development** phase of the life cycle.	45%
Q1h. Developers in my organization have the knowledge and skill to address critical vulnerabilities in the application **production phase** of the life cycle.	45%
Q1i. Developers in my organization view security as a hindrance to releasing new applications.	53%
Q1j. My organization recognizes that addressing critical vulnerabilities is most effective in the early stage of the application development life cycle.	58%
Q1k My organization does not allocate enough resources to ensure applications are secured in the **development phase** of the SDLC.	58%

	AppSec
Q1l. My organization does not allocate enough resources to ensure applications are secured in the **production phase** of the SDLC.	53%
Q1m. In my organization, application security is harder to achieve than other areas of security.	56%
Q1n There is an active effort within my organization to help developers and security teams work more effectively together.	32%
Q1o. Senior leadership favors a DevSecOps approach to application security.	28%
Q1p. My organization's security team is ultimately responsible for the security of applications.	67%
Q1q. My organization's state of security is undermined by developers who don't care about the need to secure applications early in the SDLC.	71%

Part 2. Coronavirus & teleworking

	AppSec
Q2a. Do you telework?	
Yes	35%
No	65%
Total	100%
Q2b. If yes, how long have you been teleworking because of the coronavirus pandemic?	
Less than four weeks	29%
Four to eight weeks	51%
More than eight weeks	20%
Total	100%
Q3. Do you think teleworking will become the new norm even when the coronavirus pandemic is over?	
Yes	40%
No	53%
Unsure	7%
Total	100%
Q4. How stressful is teleworking? From 1 = not stressful to 10 = very stressful.	
1 or 2	2%
3 or 4	9%
5 or 6	17%
7 or 8	30%
9 or 10	42%
Total	100%
Extrapolated value	7.52
Q5. How confident are you that teleworkers are complying with your organization's security and privacy requirements? From 1 = not confident to 10 = very confident.	
1 or 2	12%
3 or 4	19%
5 or 6	31%
7 or 8	23%
9 or 10	15%
Total	100%
Extrapolated value	5.70

	AppSec
Q6. **Before** the coronavirus pandemic, please rate the effectiveness of your organization's efforts to stop or curtail security compromises or exploits in software applications. From 1 = not effective to 10 = very effective.	
1 or 2	2%
3 or 4	5%
5 or 6	19%
7 or 8	39%
9 or 10	35%
Total	100%
Extrapolated value	7.50
Q7. **During** the coronavirus pandemic, please rate the effectiveness of your organization's efforts to stop or curtail security compromises or exploits in software applications. From 1 = not effective to 10 = very effective.	
1 or 2	13%
3 or 4	21%
5 or 6	33%
7 or 8	18%
9 or 10	15%
Total	100%
Extrapolated value	5.52

Part 3. The cultural divide

In the context of this research, the cultural divide occurs when AppSec and development do not have a common vision on how to both secure and meet the business goals for the development and production of software applications.

	AppSec
Q8a. Please rate the difficulty in working with your organization's developers team From 1 = not difficult to 10 = very difficult.	
1 or 2	3%
3 or 4	5%
5 or 6	26%
7 or 8	29%
9 or 10	37%
Total	100%
Extrapolated value	7.34
Q8b. Why is it very difficult to work with developers? (7+ responses on the 10-point scale) Please select all that apply.	
The development team does not demonstrate sufficient security practices	46%
The development team will accept flaws if they believe the app will be a big seller	55%
The development team is not incentivized to have sufficient security practices in place	39%
The development team publishes code with known vulnerabilities	65%
Other (please specify)	3%
Total	208%
Q9a. Within your organization, do you believe there is a cultural divide between AppSec and development teams?	
Yes	75%
No	25%
Total	100%

	AppSec
Q9b. If yes, is senior leadership aware of the cultural divide between AppSec and development?	
Yes	36%
No	57%
Unsure	7%
Total	100%
Q9c. How is the security of applications impacted by the cultural divide? 1= no impact to 10 = severe impact.	
1 or 2	0%
3 or 4	6%
5 or 6	24%
7 or 8	29%
9 or 10	41%
Total	100%
Extrapolated value	7.60
Q9d. If yes, what is the one most important effort being made to help AppSec and development work more effectively as a team? Please select one choice only.	
Senior leadership is helping to find a balance between app quality and security that is acceptable for both groups	23%
Senior leadership emphasizes the necessity for both AppSec and development to work closely	44%
Senior leadership makes collaboration between AppSec and development an important part of the performance review	19%
Senior management is not doing anything	11%
Other (please specify)	3%
Total	100%

Part 4. Application security practices

	AppSec
Q10. Who owns your organization's application security process of function? Please select one person/department.	
CIO or CTO	30%
CISO or CSO	25%
Head of software development	16%
Head of quality assurance	4%
Business units (LOB)	7%
No one person or department	16%
Other (please specify)	2%
Total	100%
Q11. What challenges keep your organization's application security posture from being fully effective? Please select your top two challenges.	
Insufficient budget (money)	40%
Growth in application security vulnerabilities	52%
Lack of in-house expertise	14%
Lack of clear leadership	9%
Lack of effective testing tools	24%
Management underestimates risk	4%
Pressure to release new applications	44%
Not considered an organizational priority	13%
Total	200%

	AppSec
Q12. In your opinion, is application security risk within your organization increasing, decreasing or staying at about the same level?	
Significantly increasing	35%
Increasing	25%
Staying the same	20%
Decreasing	10%
Significantly decreasing	6%
Cannot determine	4%
Total	100%
Q13. How frequently do developers publish/ deploy code with known vulnerabilities?	
Very frequently	31%
Frequently	26%
Not frequently	22%
Rarely	12%
Never	9%
Total	100%
Q14. What best describes your organization's application testing cycle?	
Continuously	8%
Daily	5%
Weekly	8%
Monthly	7%
Quarterly	15%
Yearly	11%
More than yearly	14%
Only after new code is added	12%
No planned cycle	20%
Total	100%

	AppSec
Q15. Please check all the steps taken to test for vulnerabilities in applications.	
Testing is conducted throughout the application development life cycle	35%
Testing method scales efficiently from a few to many applications	46%
Ensuring tests accurately identify actual defects and eliminate false positives	56%
Covering the most current application technologies	43%
Handling mobile application vulnerabilities	48%
Other (please specify)	6%
Total	234%
Q16. What steps does your organization take to remediate the risks associated with vulnerable applications? Please select all that apply.	
Ensure developers receive training on how to secure the coding process	57%
Provide code libraries or templates that address key issues	55%
Create test plans and test scripts to detect authentication defects early in the development cycle	72%
Require best practices for secure authentication in application specifications so issues are visible to developers and QA engineers	68%
Other (please specify)	4%
Total	256%

	AppSec
Q17. Within your organization, how much responsibility do you feel development has for application security?	
Significant responsibility	34%
Some responsibility	47%
Minimal responsibility	11%
No responsibility	8%
Total	100%

Part 5. Organization and respondents' demographics

	AppSec
D1. What best describes your position level within the organization?	
Executive/VP	9%
Director	10%
Manager	16%
Supervisor	14%
IT/Cyber Security analyst	25%
Staff/technician	21%
Administrative	3%
Consultant/contractor	2%
Other	0%
Total	100%

	AppSec
D2. What best describes your direct reporting channel?	
CEO/executive committee	3%
COO or head of operations	2%
CFO, controller or head of finance	1%
CIO, CTO or head of corporate IT	15%
Head of application security	22%
Business unit leader or general manager	21%
Head of compliance or internal audit	8%
CISO/CSO or head of AppSec	23%
Other	5%
Total	100%

	AppSec
D3. What range best describes the full-time headcount of your global organization?	
Less than 1,000	18%
1,000 than 5,000	17%
5,001 to 10,000	22%
10,001 to 25,000	21%
25,001 to 75,000	15%
More than 75,000	7%
Total	100%

	AppSec
D4. What best describes your organization's primary industry classification?	
Agriculture & food services	0%
Communications	3%
Consumer products	6%
Defense aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	3%
Financial services	19%
Healthcare & pharmaceuticals	12%
Hospitality	2%
Industrial & manufacturing	9%
Public sector	11%
Retail	9%
Services	8%
Technology & software	7%
Transportation	2%
Other	0%
Total	100%

Ponemon Institute – *Advancing Responsible Information Management*

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.

ZERONORTH™ ZeroNorth brings security, DevOps and the business together to improve application security performance and reduce organizational risk. The company's application security automation and orchestration platform unites enterprises to rapidly identify, prioritize and remove the vulnerabilities standing in the way of software excellence. In an age where the security of applications needs to be everyone's responsibility, ZeroNorth is where organizations come together for the good of software. For more information, follow ZeroNorth on Twitter (@ ZeroNorthSec), or LinkedIn—or visit www.zeronorth.io

ZERONORTH™

202006#2