2012 Application Security Gap Study: A Survey of IT Security & Developers

Research sponsored by Security Innovation

Independently Conducted by Ponemon Institute LLC

March 2012

2012 Application Security Gap Study:
A Survey of IT Security & Developers
March 2012

Part 1. Introduction

Ponemon Institute is pleased to present the results of *2012 Application Security Gap Study: A Survey of IT Security & Developers* sponsored by Security Innovation. The research focuses on understanding the perceptions both security and development practitioners have about application security maturity.

The purpose of the research is to measure the tolerance to risk across the established phases of application security, and define what works and what hasn't worked, how industries are organizing themselves and what gaps exist. The research reveals a significant divide between the IT Security and Development organizations that is caused by a major skills shortage and a fundamental misunderstanding of how an application security process should be developed. This lack of alignment seems to hurt their business based on not prioritizing secure software, but also not understanding what to do about it.

In this study, we surveyed 567 IT security practitioners who have an average of 9 years of experience and 256 developers who have an average of 8 years experience. Most of the participants work in organizations with a headcount greater than 500. The following are the key topics covered in the research:

- Application security processes considered most effective
- Adoption and use of technologies that are affecting the state of application security
- Gaps between people, process and technology and the affect they have on the enterprise
- Different perceptions security and development practitioners have about application maturity, readiness and accountability
- Threats to the application layer, including emerging platforms
- Application-layer links to data breaches

In general, the findings reveal that IT security practitioners are more positive than developers that their organization is making application security a top priority. Further they are more positive about the adequacy of security technologies to protect information assets and IT infrastructure and the existence of security and data protection policies that are well defined and fully understood by employees. In contrast, the majority of developers are not confident about the maturity of IT security activities.

We believe the importance of this research is to create greater awareness around application security. What emerged in this study was that companies do not seem to be looking at the root causes of data breaches, and they aren't moving very fast to bridge the existing gaps to fix the myriad of problems. The threat landscape has grown substantially in scope, most notably respondents say that Web 2.0 and mobile attacks are the targets of the next wave of threats beyond just Web applications.

Some of the most interesting findings from the research include:

- Only 12 percent of security personnel responded that all of their organization's applications meet regulations for privacy, data protection and information security. And 15 percent of developers feel the same way.

- Forty-four percent of the developers surveyed stated there is absolutely no collaboration between their development organization and the security organization when it comes to application security.

- Seventy-one percent of developers feel security is not adequately addressed during the software development life cycle. And half (51 percent) of the security respondents feel the same way.

- Fifty-one percent of developers and the same percentage of security personnel say their organizations do not have a training program on application security.

- Sixty percent of security respondents and 65 percent of developers stated that they do not test mobile applications in the production, development or Q/A processes.

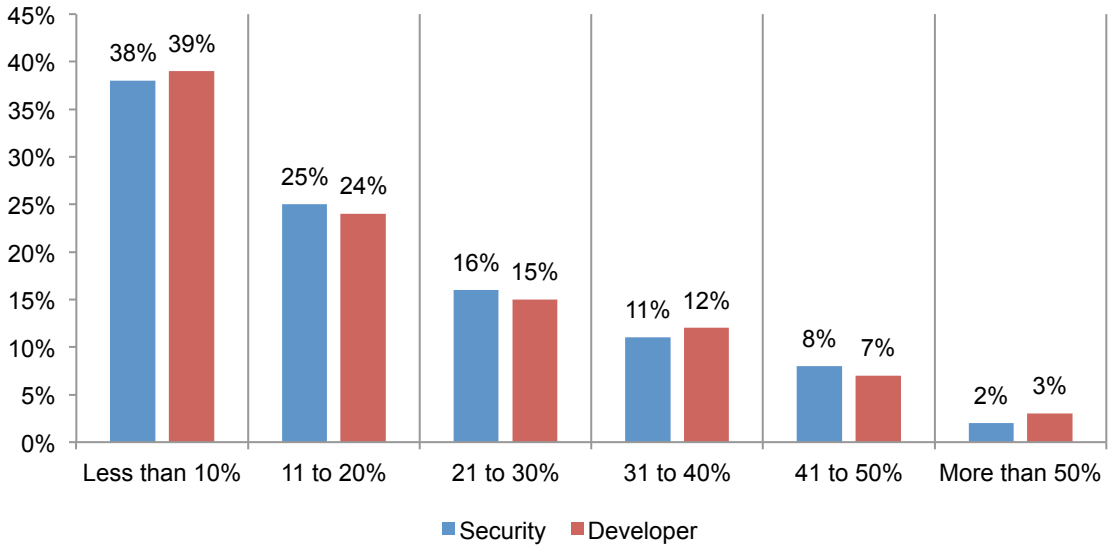
Part 2. Key Findings

Based on the research findings, we have organized the key findings according to the following five themes:

- Application security is often not a priority
- There is uncertainty about how to fix vulnerable code in critical applications
- A lack of knowledge about application security is resulting in a high rate of data breaches
- Developers and security practitioners have different perceptions about accountability and collaboration to improve application security
- Mobile technology and social media platforms are putting organizations at risk

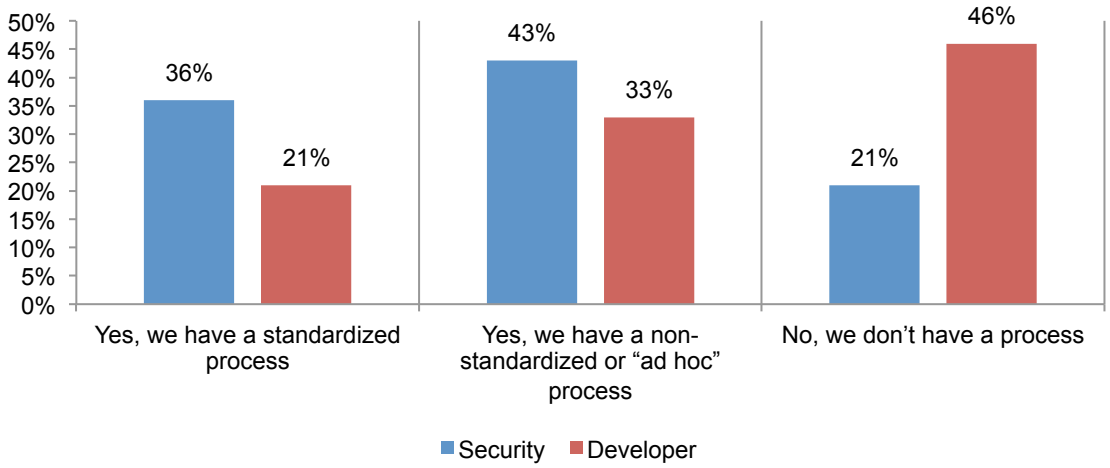
Application security is not a priority. The one area both security and developers agree upon is the lack of resources for application security. As evidence that application security is not a priority, Bar Chart 1 reveals that the same percentage of security professionals and developers (63 percent) state that application security consumes 20 percent or less of their overall IT security budget.

Bar Chart 1. The percentage of IT security budget dedicated to application security



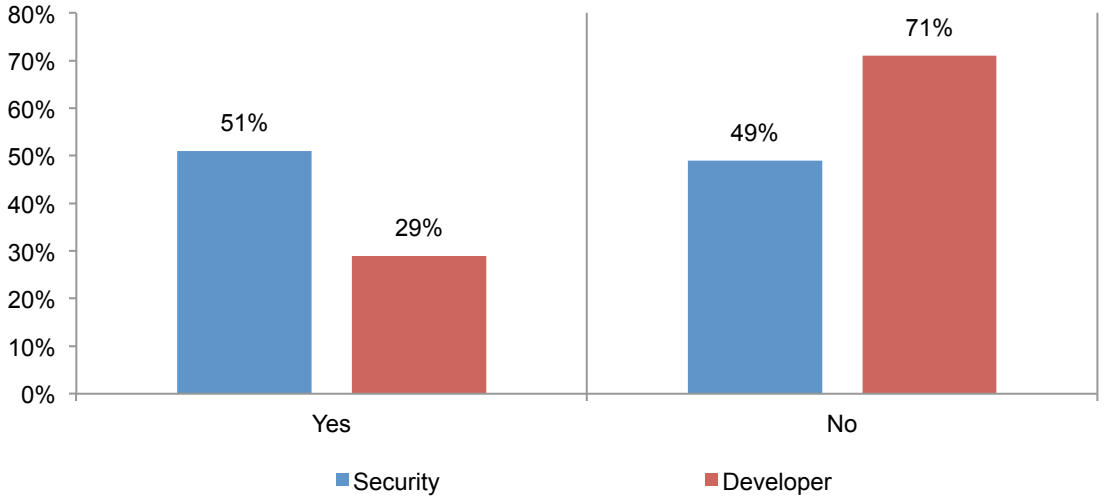
As additional proof that application security is not a priority, Bar Chart 2 reveals that 64 percent of security practitioners state they either have no process, such as systems development life cycle (SDLC) at all, or an inefficient ad-hoc process for building security into their applications. A larger percentage (79 percent) of developers say they either have no process or an inefficient, ad-hoc process for building security into their applications.

Bar Chart 2. Is there a process for ensuring that security is built into new applications?



Further, the majority of developers (71 percent) believe security is not adequately addressed during the software development life cycle. Fifty-one percent of the security respondents agree. In many cases, security is built in during the post-launch phase of the software development cycle and bugs are fixed during the launch phase.

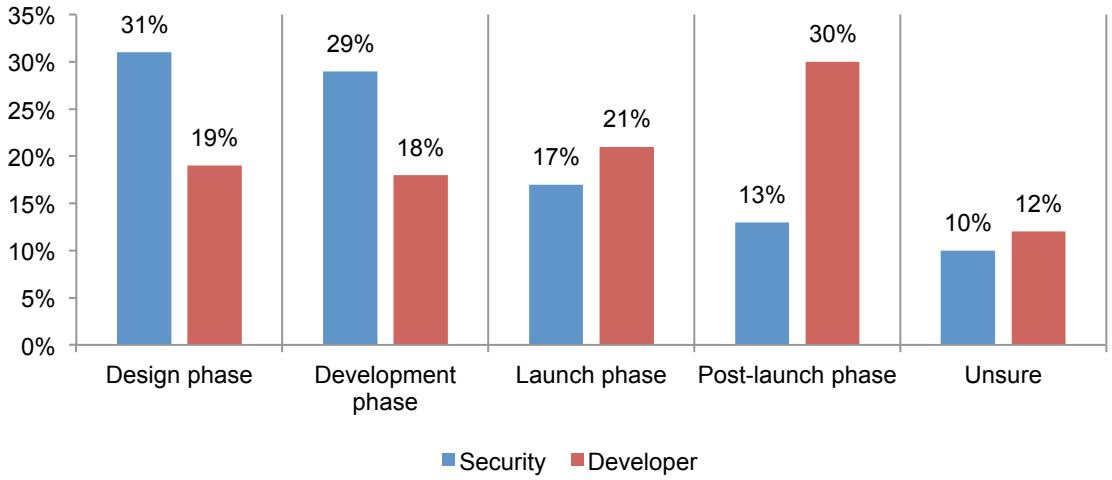
Bar Chart 3. Do you believe security is adequately emphasized during the application development lifecycle?



.

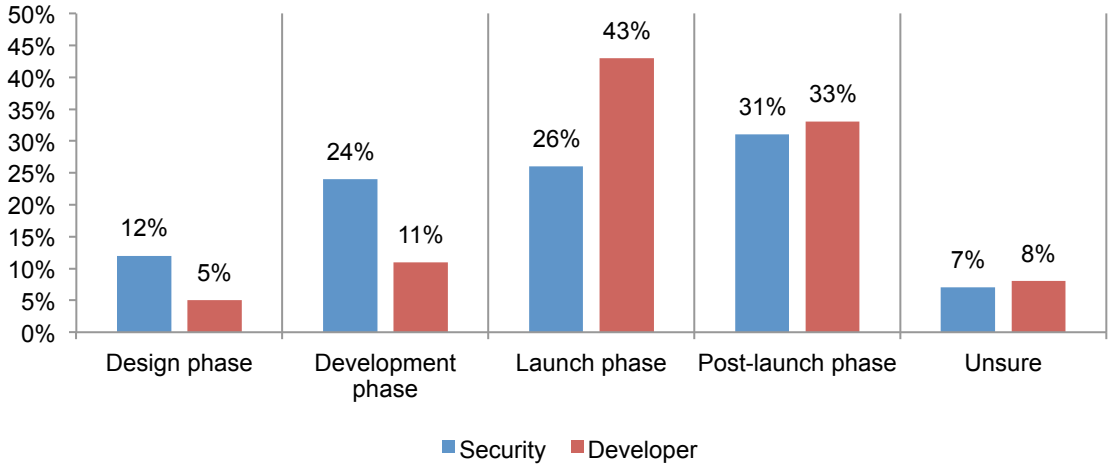
Security and development do not seem to be in agreement as to when security should be addressed in the development lifecycle. Bar Chart 4 shows that 60 percent of security practitioners say it is addressed in the design and development phase. Fifty-one percent of developers say it is addressed in the launch and post-launch phase.

Bar Chart 4. Where is security addressed in the application development lifecycle?



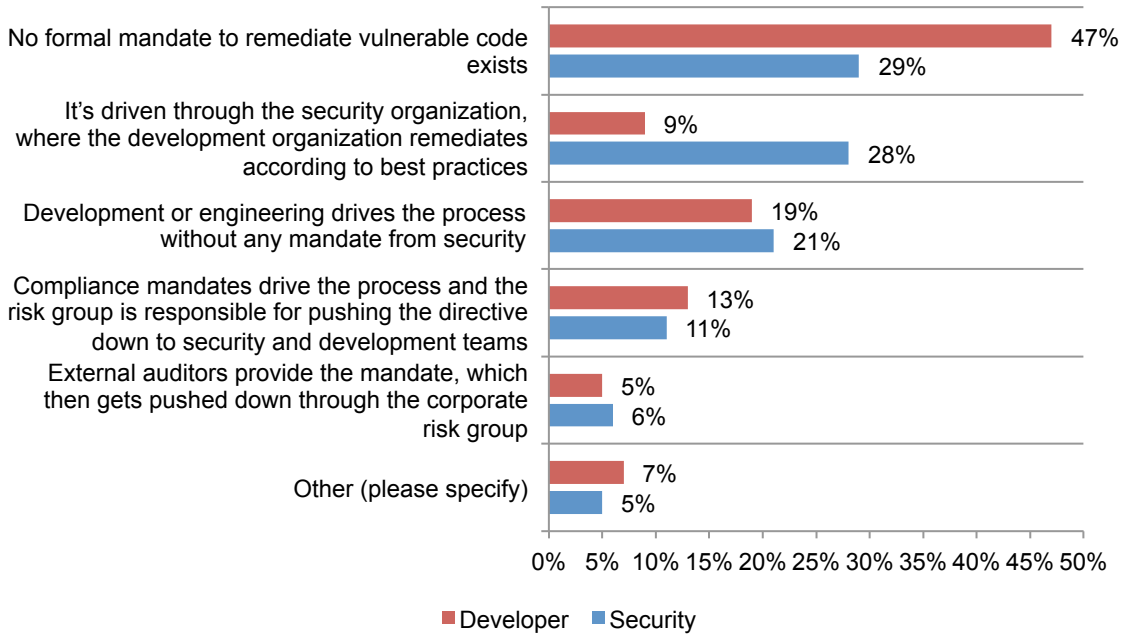
As shown in Bar Chart 5, 57 percent of security practitioners and 76 percent of developers believe the launch phase and the post-launch phase is when patching and fixing bugs becomes the most costly and time consuming.

Bar Chart 5. Which phase is most costly to patching and fixing bugs in the application development lifecycle?



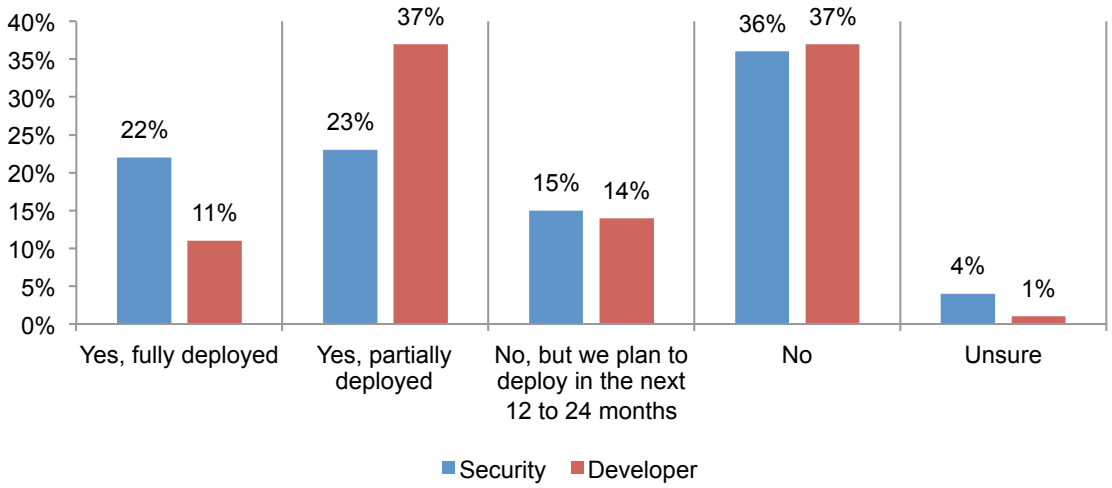
There is uncertainty about how to fix vulnerable code in critical applications. As shown in Bar Chart 6, 47 percent of developers and 29 percent of security practitioners say their organization has no mandate to remediate vulnerable code. Only 9 percent of developers say it is driven through the security organization, where the development of organization remediates according to best practices. However, more of the security practitioners believe this to be the case.

Bar Chart 6. How does your organization mandate the remediation of vulnerable code?



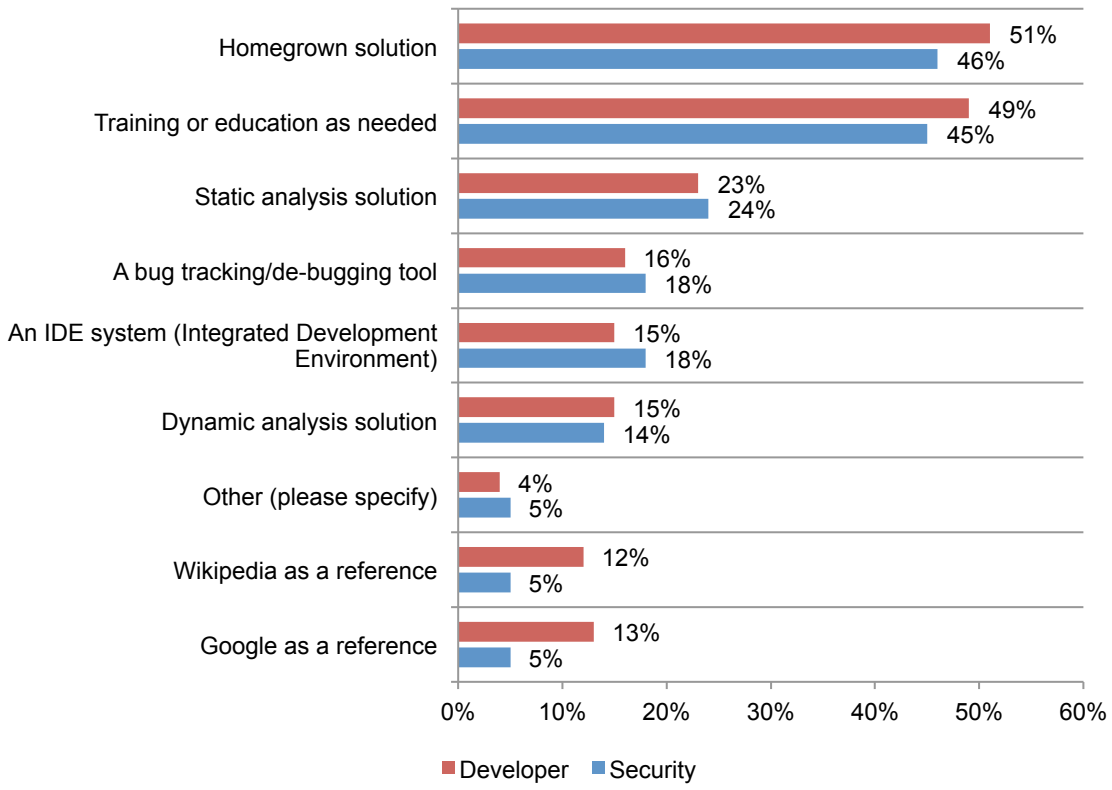
According to Bar Chart 7, a key reason for the uncertainty about how to fix vulnerable code in critical applications is that 51 percent of both developers and security practitioners say their organizations do not have training in application security. A larger percentage of security practitioners than developers say their organization have a fully deployed program (22 percent vs. 11 percent)

Bar Chart 7. Does your organization have an application security training program?



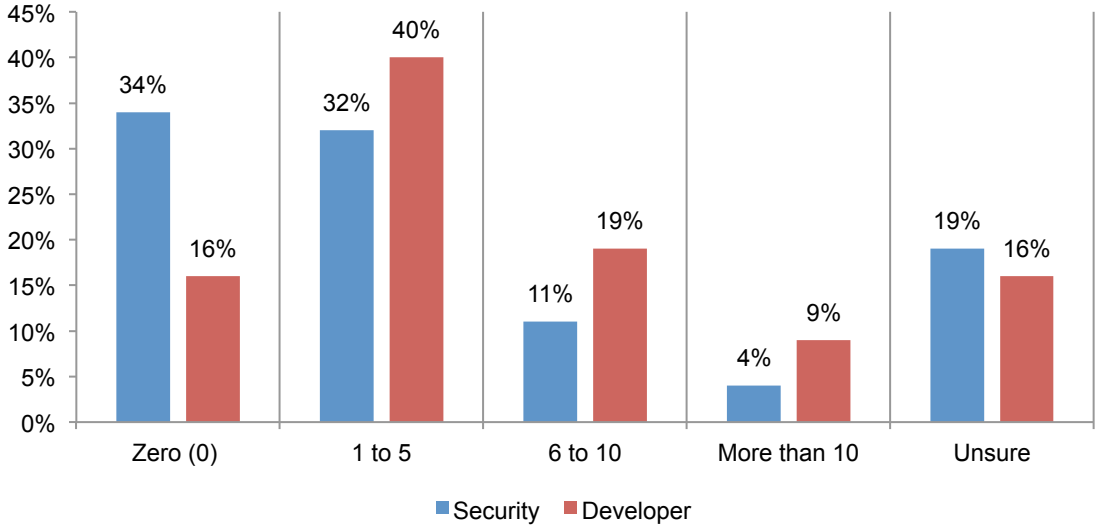
When asked what the development team uses to ensure they are successful in remediating potentially vulnerable code or fixing bugs, Bar Chart 8 shows that 46 percent of security respondents and just over half of developers (51 percent) say they predominantly use homegrown solutions to remediate vulnerable code. Less than half of both security and developers cite the successful use of other methods.

Bar Chart 8. Successful methods used to remediate potentially vulnerable code or bugs
More than one choice permitted



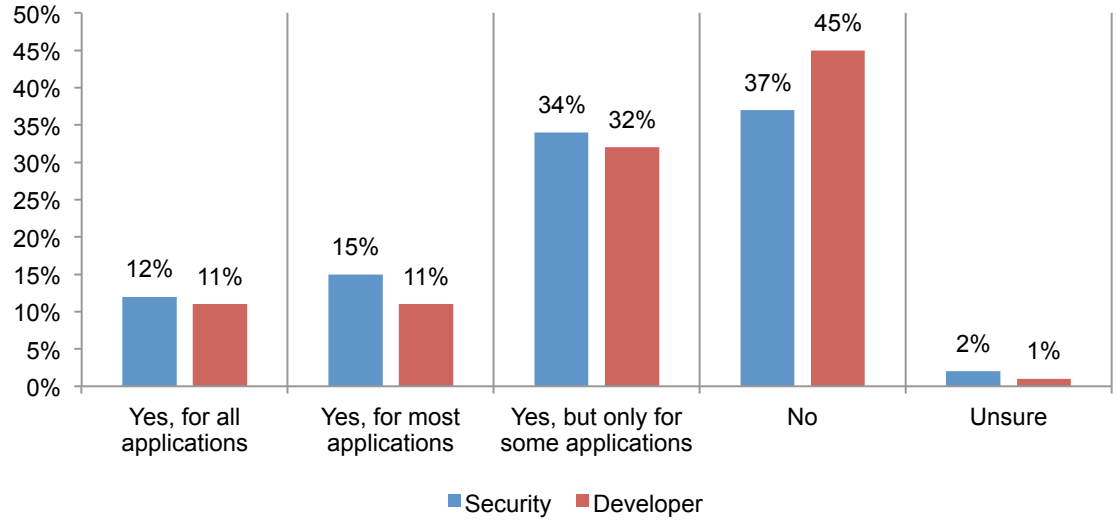
A lack of knowledge about application security is resulting in a high rate of data breaches. According to Bar Chart 9**,** compromised or hacked applications have caused at least one data breach in 68 percent of the developers' organizations and 47 percent of the security practitioners' organizations over the past 24 months. However, 19 percent of security practitioners and 16 percent of developers are not sure if they had a data breach as a result of an application being compromised or hacked.

Bar Chart 9. Frequency of data breach or security exploits due to a hacked or compromised application



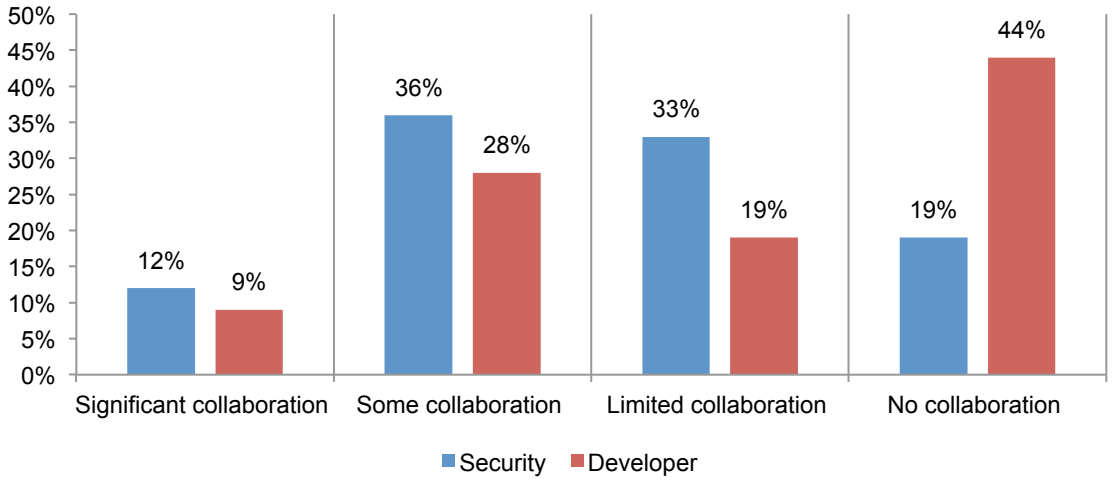
A lack of compliance with regulations could also contribute to the high occurrence of data breaches. Only 12 percent of security personnel say that all their organization's applications meet regulations for privacy, data protection and information security and only 11 percent of developers believe their organizations are in compliance.

Bar Chart 10. Compliant with privacy, data protection and information security regulations



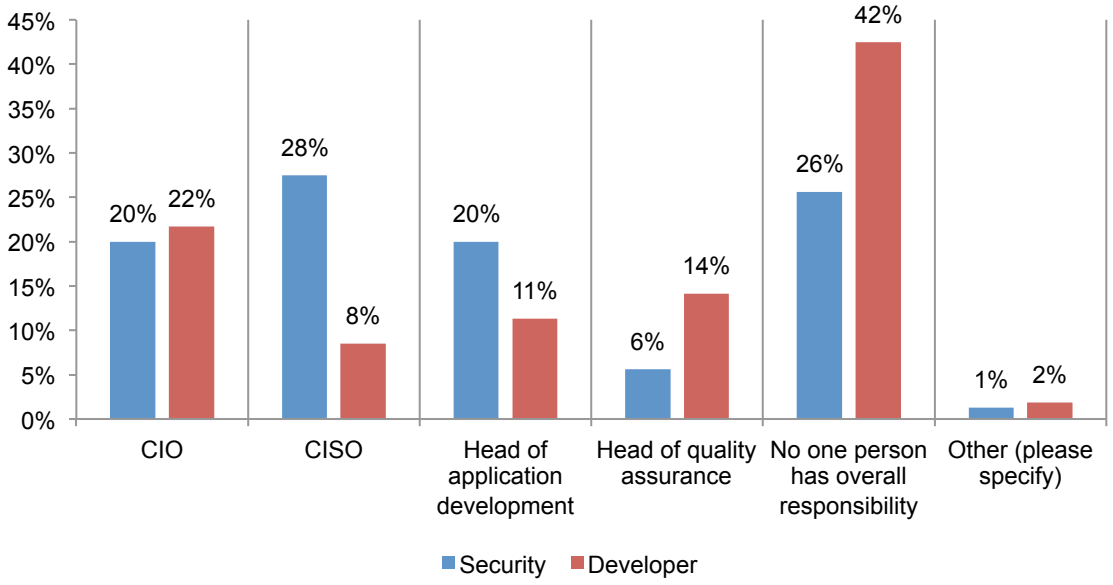
Developers and security practitioners have different perceptions about accountability and collaboration to improve application security. Bar Chart 11 presents the level of collaboration between security practitioners and developers. A lack of collaboration between developers and security practitioners in order to improve application security practices is putting data at risk. Forty-four percent of developers say there is absolutely no collaboration between their function and the security function regarding application security. However, 12 percent of security practitioners say there is significant collaboration and 69 percent say there is at least some collaboration exists with the developers.

Bar Chart 11. Collaboration between application development and security teams



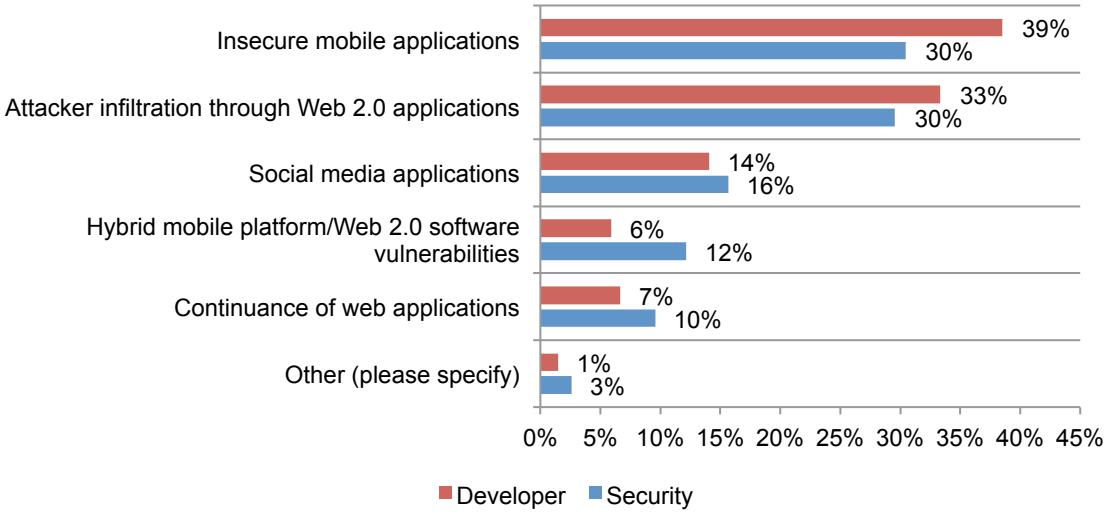
Bar Chart 12 reveals that the largest percentage of security respondents (28 percent) believe the CISO should be primarily responsible for ensuring security in the application development life cycle in their organization. However, 42 percent of developers say that no one person within their organization has primary responsibility for ensuring security in the application development life cycle.

Bar Chart 12. Responsibility for ensuring security in the application development



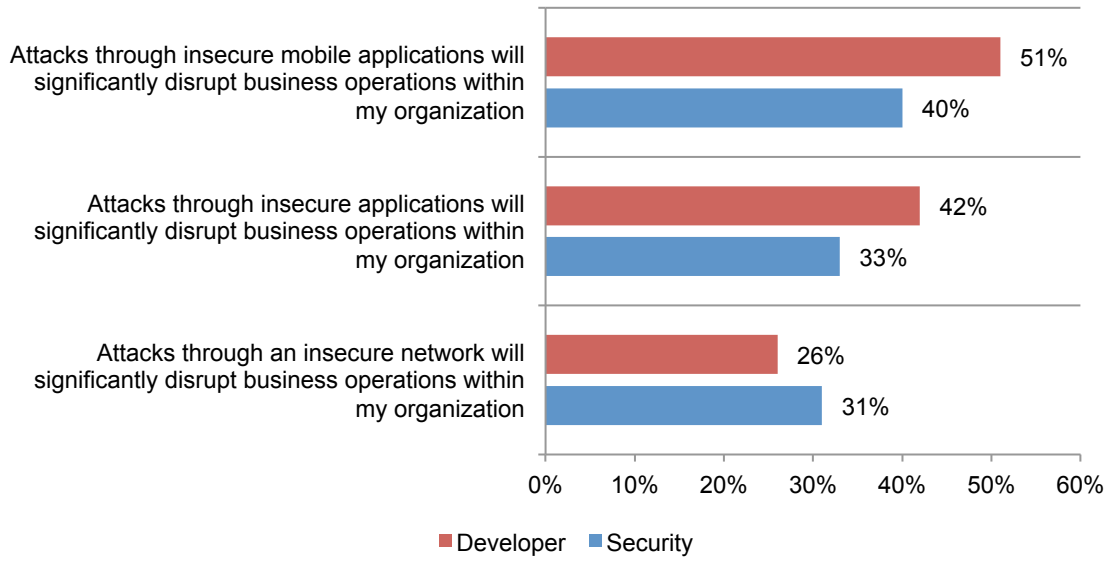
Mobile technology and Web 2.0 attacks put organizations at risk. According to Bar Chart 13, 39 percent of developers and 30 percent of security practitioners believe the most serious threat to application security in the next 12 to 24 months is insecure mobile applications. The next most significant threat is attacker infiltration through Web 2.0 applications.

Bar Chart 13. Two most serious threats to application security in the next 12 to 24 months



Bar Chart 14 reveals that 51 percent of developers and 40 percent of security respondents say insecure mobile applications will disrupt business operations at their organizations. Forty-two percent of developers and 33 percent of security practitioners worry about insecure applications.

Bar Chart 14. The most likely attacks to affect your organization



A very small percentage test mobile applications in production, development or testing and quality assurance, as shown in Bar Chart 15.

Bar Chart 15. Venues for testing mobile apps

Part 3. Conclusion

Gaps in perceptions between security practitioners and developers about application security maturity, readiness and accountability indicate why many organizations' critical applications are at risk. A lack of collaboration between the security and development teams makes it difficult to make application security part of an enterprise-wide strategy and to address serious threats.

The research reveals areas that organizations need to address. These include increasing expertise about application security, including how to fix vulnerable code in critical applications. A lack of budget may be keeping organizations from hiring individuals with the necessary knowledge and credentials to reduce application security risk. In addition, many organizations do not have a function or role that is accountable for ensuring the security of applications.

Security practitioners and developers do agree that mobile technology and social media platforms are putting organizations at risk and is expected to become more of a threat. This mutual understanding may pose an opportunity to improve collaboration in order to achieve a higher level of application security in their organizations.

Part 4. Methods

Random sampling frames of 14,997 IT security practitioners and 6,962 developers who reside within the United States were used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of highly experienced security and IT developers with bona fide credentials. As shown in Table 1, 665 IT security respondents completed the survey and 301 developers completed the response. After removing 98 surveys from IT security practitioners and 45 developers that failed reliability checks the final sample was 567 IT security practitioners (or a 3.8 percent response rate) and 256 developers (or a 3.7 percent response rate.

Table 1. Sample response	Security	Developer
U.S. Sample frame	14,997	6,962
Returned surveys	665	301
Rejected surveys	98	45
Final sample	567	256
Response rate	3.8%	3.7%

Table 2. Experience	Security	Developer
Years in software development	0	8.03
Years in IT or IT security	9.35	0
Years in current position	3.99	3.87

Table 3 reports the respondents' headquarters according to region.

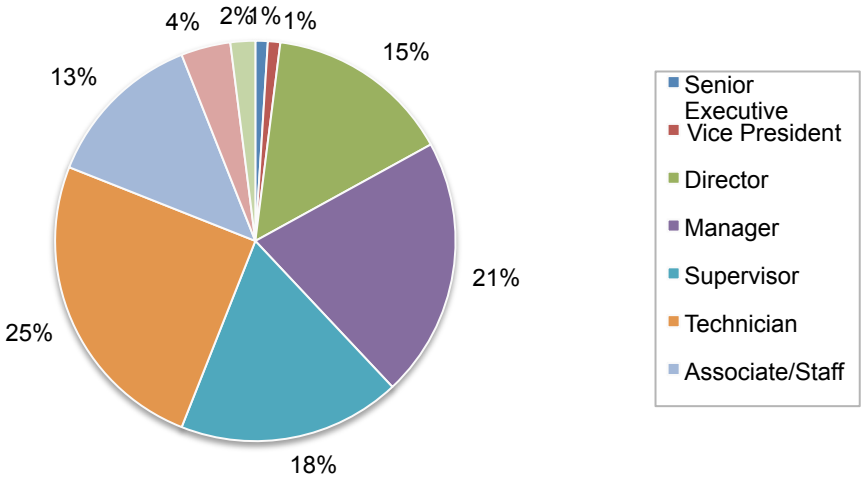
Table 3. Check the country or U.S. region where your company's primary headquarters is located.	**Security**	**Developer**
Northeast	20%	19%
Mid-Atlantic	17%	19%
Midwest	18%	16%
Southeast	13%	14%
Southwest	14%	12%
Pacific-West	18%	20%

Table 4. Reports the worldwide headcount of participating organizations.

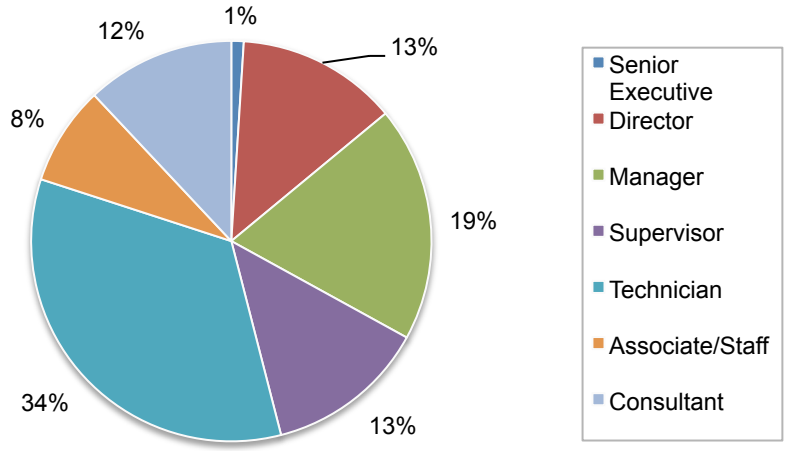
Table 4. What is the worldwide headcount of your organization?	**Security**	**Developer**
< 100	9%	14%
100 to 500	21%	20%
501 to 5,000	19%	21%
5,001 to 10,000	16%	13%
10,001 to 25,000	13%	11%
25,001 to 75,000	12%	12%
> 75,000	10%	9%

Pie Chart 1a and 1b report the security and developer respondent's organizational level within participating organizations. Fifty-six percent of security practitioners and 46 percent of developers are at the supervisor or higher level.

Pie Chart 1a: What organizational level best describes security practitioners' current position?

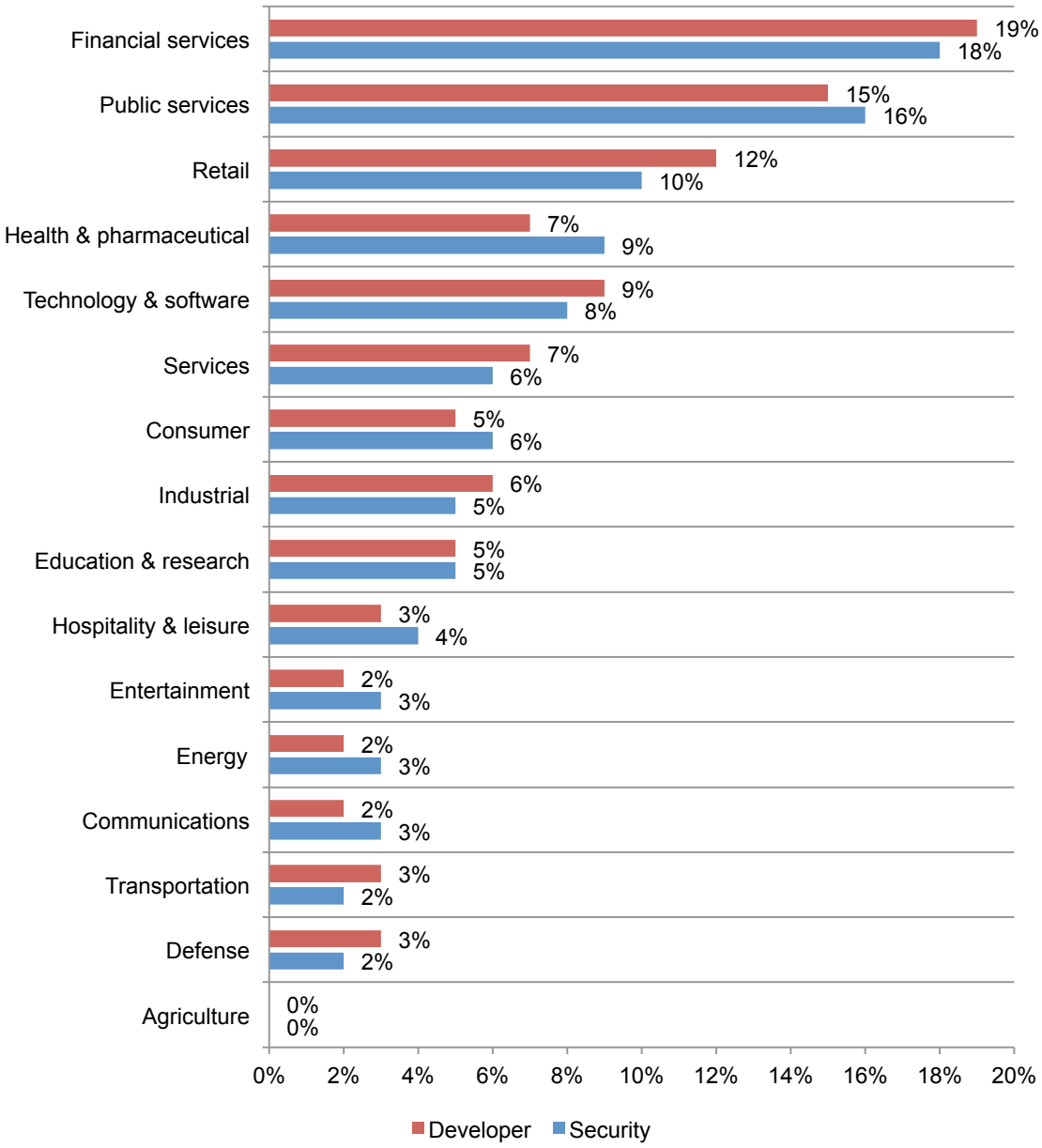


Pie Chart 1b: What organizational level best describes developers' current position?



According to Bar Chart 16, most of the respondents are in the financial services, public services and retail organizations.

Bar Chart 16. Industry distribution of respondents' organization



Caveats

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 with executive or management credentials located in the United States, 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 or perceptions about data protection activities from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the sample is representative of individuals with responsibility for reputation management issues. We also acknowledge that the results may be biased by external events.

  We also acknowledge bias caused by compensating respondents to complete this research within a holdout period. 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 certain respondents did not provide accurate responses.

Appendix: Audited Findings

Sample response	Security	Developer
U.S. Sample frame	14,997	6,962
Returned surveys	665	301
Rejected surveys	98	45
Final sample	567	256
Response rate	3.8%	3.7%
Part 1. Attributions about the maturity of your organization's IT security activities: Following are nine (9) attributions about your organization's IT security function. Please rate each statement using the scale provided below each item to express your opinion. Strongly agree and agree response combined.	Security	Developer
Q1. Security and data protection policies are well defined and fully understood	53%	37%
Q2. Security technologies are adequate in protecting our information assets and IT infrastructure	54%	44%
Q3. Appropriate steps are taken to comply with the leading standards for IT security	48%	41%
Q4. IT security strategy is fully aligned with our business strategy	50%	39%
Q5. Ample resources ensure all IT security requirements are accomplished	36%	34%
Q6. IT security posture responds quickly to new challenges and issues	42%	31%
Q7. IT security function is able to prevent serious cyber attacks such as advanced persistent threats	46%	33%
Q8. IT security leader is a member of our company's executive team	41%	35%
Q9. My organization is able to hire and retain knowledgeable and experienced security practitioners	40%	35%
Q10. Application security is a top priority in my organization	58%	38%
Part 2. Application Security		
Q11. Please choose one statement that best describes security priorities in your organization today.	Security	Developer
Network security is a higher priority than application security	34%	38%
Network security and application security are equal in terms of security priorities	44%	39%
Network security is a lower priority than application security	22%	23%
Total	100%	100%
Q12. What percentage of your IT security budget dedicated to application security measures or activities? Your best guess is welcome.	Security	Developer
Less than 10%	38%	39%
11 to 20%	25%	24%
21 to 30%	16%	15%
31 to 40%	11%	12%
41 to 50%	8%	7%
More than 50%	2%	3%
Total	100%	100%
Q13. What percentage of your IT security budget dedicated to network security measures or activities? Your best guess is welcome.	Security	Developer
Less than 10%	9%	10%
11 to 20%	23%	20%
21 to 30%	34%	34%
31 to 40%	21%	20%
41 to 50%	8%	9%
More than 50%	5%	7%
Total	100%	100%

Q14. Please choose one statement that best describes security threats in your organization today. Please note that a human factor threat is defined as an attack involving malicious or criminal actors that attempts to gain access to the company's information assets or IT infrastructure. A code-induced threat is defined as an attack through embedding bad code such as malware into applications.	Security	Developer
Human factor threats present a greater inherent security risk than code-induced threats	43%	21%
Human and code-induced threats are equal in terms of inherent security risk	44%	41%
Code-induced threats present a greater inherent security risk than human factor threats	13%	38%
Total	100%	100%
Q15. Does your organization have a process for ensuring that security is built into new applications?	Security	Developer
Yes, we have a standardized process	36%	21%
Yes, we have a non-standardized or "ad hoc" process	43%	33%
No, we don't have a process	21%	46%
Unsure	100%	100%
Q16. Where in the application development lifecycle does your organization build in security features? Please select more than one choice if appropriate.	Security	Developer
Design phase	31%	19%
Development phase	29%	18%
Launch phase	17%	21%
Post-launch phase	13%	30%
Unsure	10%	12%
Total	100%	100%
Q17. Which phase of the application development life cycle do patching and bug fixes become the most costly and time consuming? Please select only one choice.	Security	Developer
Design phase	12%	5%
Development phase	24%	11%
Launch phase	26%	43%
Post-launch phase	31%	33%
Unsure	7%	8%
Total	100%	100%
Q18. In your opinion, is security adequately emphasized during the application development lifecycle?	Security	Developer
Yes	51%	29%
No	49%	71%
Total	100%	100%
Q19. What best describes the nature of collaboration between your organization's application development and security teams?	Security	Developer
Significant collaboration between development and security teams	12%	9%
Some collaboration between development and security teams	36%	28%
Limited collaboration between development and security teams	33%	19%
No collaboration between development and security teams	19%	44%
Total	100%	100%
Q20. Does your organization have a manual or technology-based approach that gives software developers clear guidance on how to remediate software vulnerabilities?	Security	Developer
Yes, a manual approach	19%	18%
Yes, a technology-based approach	23%	15%
Yes, both a manual and technology-based approach	28%	15%
No	21%	39%
Unsure	9%	13%
Total	100%	100%

Q21. Who in your organization is most responsible for ensuring security in the application development lifecycle? One best choice.	Security	Developer
CIO	20%	22%
CISO	28%	8%
Head of application development	20%	11%
Head of quality assurance	6%	14%
No one person has overall responsibility	26%	42%
Other (please specify)	1%	2%
Total	100%	100%
Q22. Do your security or development teams use an analytical solution as part of application testing in the quality assurance process?	Security	Developer
Yes, static analysis solution	24%	23%
Yes, dynamic analysis solution	19%	24%
Yes, both a static and dynamic analysis solution	14%	15%
No	30%	36%
Unsure	13%	2%
Total	100%	100%
Q23. How does your organization mandate the remediation of vulnerable code? One best choice.	Security	Developer
It's driven through the security organization, where they require the development organization to remediate according to best practices	28%	9%
Development or engineering drives the process without any mandate from security	21%	19%
Compliance mandates typically drive the entire process and as a result our risk group is responsible for the pushing the directive down to security and development teams	11%	13%
External auditors provide the mandate to my organization, which then gets pushed down through the corporate risk group	6%	5%
No formal mandate to remediate vulnerable code exists in my organization	29%	47%
Other (please specify)	5%	7%
Total	100%	100%
Q24. What does your development team use to ensure they are successful in remediating potentially vulnerable code or fixing bugs? Please check all that apply.	Security	Developer
An IDE system (Integrated Development Environment)	18%	15%
A bug tracking/de-bugging tool	18%	16%
Static analysis solution	24%	23%
Dynamic analysis solution	14%	15%
Homegrown solution	46%	51%
Google as a reference	5%	13%
Wikipedia as a reference	5%	12%
Training or education as needed	45%	49%
Other (please specify)	5%	4%
Total	180%	198%
Q25a. Has your organization deployed a training program on application security?	Security	Developer
Yes, fully deployed	22%	11%
Yes, partially deployed	23%	37%
No, but we plan to deploy in the next 12 to 24 months	15%	14%
No	36%	37%
Unsure	4%	1%
Total	100%	100%

Q25b. If Yes, who was the targeted audience for this training event? Select all that apply.	Security	Developer
Members of the security team	32%	33%
Members of the development team	75%	69%
Non-technical employees	23%	19%
Management	13%	8%
Entire organization	25%	25%
Total	168%	154%
Q25c. What topics were covered in your application security training program?	Security	Developer
Application security best practices	33%	40%
Compliance-based topics	35%	31%
Threat-specific topics	28%	39%
General awareness	41%	39%
Technology-specific topics	9%	12%
Issues and best practices around emerging platforms such as mobile and Web 2.0	7%	11%
Other (please specify)	1%	2%
Total	154%	174%
Q25d. If Yes, what were the benefits of this training program? Check all that apply.	Security	Developer
Reduced time to deliver secure applications	12%	16%
Reduced the total cost of application development	13%	29%
Enhanced state of compliance	65%	43%
A decrease in attacks at the application layer over time	39%	53%
Other (please specify)	4%	2%
Total	133%	143%
Q26. How often over the past 24 months has your organization experienced a data breach or security exploit as a result of an application being compromised or hacked?	Security	Developer
Zero (0) [skip Q27]	34%	16%
1 to 5	32%	40%
6 to 10	11%	19%
More than 10	4%	9%
Unsure	19%	16%
Total	100%	100%
Q27. What type of attack methods may have compromised your organization's data in a recent breach or security exploit? Please select all that apply.	Security	Developer
SQL injection attack at the application layer	46%	42%
Cross-site scripting attack at the application layer	23%	25%
Privilege escalation attack at the application layer.	17%	18%
Other attack methodology at the application layer	8%	5%
Exploit of insecure software code on a mobile device	13%	19%
Exploit of insecure code through use of a Web 2.0 application	24%	29%
Unsure	19%	17%
Total	150%	155%
Q28. Does your organization test Web apps in the following venues? Please check all that apply.	Security	Developer
Production	23%	25%
Development	45%	46%
Testing and quality assurance	41%	46%
None of the above	42%	47%
Total	151%	164%

Q29. Does your organization test mobile apps in the following venues? Please check all that apply.	Security	Developer
Production	12%	14%
Development	33%	25%
Testing and quality assurance	16%	14%
None of the above	60%	65%
Total	121%	118%
Q30. What is your primary means of securing Web facing applications? Please select all that apply.	Security	Developer
Intrusion prevention system (IPS)	45%	43%
Web application firewall (WAF)	41%	43%
Network firewall	81%	79%
Reverse proxy	34%	35%
Web application vulnerability scanning	40%	38%
Managed service	44%	45%
External pen testing	26%	29%
Internal pen testing	25%	26%
Others (please specify)	5%	9%
Unsure	8%	11%
Total	349%	358%
Q31. To the best of your knowledge, are your organization's applications compliant with all regulations for privacy, data protection and information security?	Security	Developer
Yes, for all applications	12%	11%
Yes, for most applications	15%	11%
Yes, but only for some applications	34%	32%
No	37%	45%
Unsure	2%	1%
Total	100%	100%
Q32. Following are three scenarios about attacks that may significantly impact your organization. Please rate each scenario using the five-point likelihood scale provided below. Assume a 12 to 24 months timeframe. Imminent and very likely response combined.	Security	Developer
Q32a. Attacks through insecure applications will significantly disrupt business operations within my organization.	33%	42%
Q32b. Attacks through an insecure network will significantly disrupt business operations within my organization.	31%	26%
Q32c. Attacks through insecure mobile applications will significantly disrupt business operations within my organization.	40%	51%
Q33. What do you see as the two most serious emerging threat relative to application security over the next 12 to 24 months?	Security	Developer
Insecure mobile applications	30%	39%
Attacker infiltration through Web 2.0 applications	30%	33%
Hybrid mobile platform/Web 2.0 software vulnerabilities	12%	6%
Continuance of web applications	10%	7%
Social media applications	16%	14%
Other (please specify)	3%	1%
Total	100%	100%

Q34. Fixing bugs and patching applications to security holes exposed during the development life cycle or post-release is a significant drain on my organization's time and money.	Security	Developer
Strongly agree and agree response.	26%	54%
Part 3. Organizational characteristics		
D1. What organizational level best describes your current position?	Security	Developer
Senior Executive	1%	1%
Vice President	1%	0%
Director	15%	13%
Manager	21%	19%
Supervisor	18%	13%
Technician	25%	34%
Associate/Staff	13%	8%
Consultant	4%	12%
Other (please specify)	2%	0%
Total	100%	100%
D2. Check the Primary Person you or your supervisor reports to within your organization.	Security	Developer
Business unit	2%	5%
CEO/President	0%	0%
Chief Financial Officer	1%	0%
Chief Information Officer	53%	36%
Chief Information Security Officer	24%	0%
Applications development Leader	0%	43%
Quality assurance	0%	8%
Compliance Officer	5%	2%
Chief Privacy Officer	0%	0%
Director of Internal Audit	2%	0%
General Counsel	1%	0%
Chief Technology Officer	6%	6%
Human Resources VP	0%	0%
Chief Security Officer	3%	0%
Chief Risk Officer	3%	0%
Other (please specify)	0%	0%
Total	100%	100%
D3. Check the country or U.S. region where your company's primary headquarters is located.	Security	Developer
Northeast	20%	19%
Mid-Atlantic	17%	19%
Midwest	18%	16%
Southeast	13%	14%
Southwest	14%	12%
Pacific-West	18%	20%
Total	100%	100%
D4. Experiences (mean values)	Security	Developer
Years in software development	0	8.03
Years in IT or IT security	9.35	0
Years in current position	3.99	3.87

D5. What industry best describes your organization's industry concentration or focus?	Security	Developer
Agriculture	0%	0%
Communications	3%	2%
Consumer	6%	5%
Defense	2%	3%
Education & research	5%	5%
Energy	3%	2%
Entertainment	3%	2%
Financial services	18%	19%
Health & pharmaceutical	9%	7%
Hospitality & leisure	4%	3%
Industrial	5%	6%
Public services	16%	15%
Retail	10%	12%
Services	6%	7%
Technology & software	8%	9%
Transportation	2%	3%
Total	100%	100%
D6. What is the worldwide headcount of your organization?	Security	Developer
< 100	9%	14%
100 to 500	21%	20%
501 to 5,000	19%	21%
5,001 to 10,000	16%	13%
10,001 to 25,000	13%	11%
25,001 to 75,000	12%	12%
> 75,000	10%	9%
Total	100%	100%

Thank you for your participation. If you have any questions about this research, please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

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

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