The State of Application Security

A Research Study by Ponemon Institute LLC and
Security Innovation

The State of Application Security

An Organizational Maturity study by
Ponemon Institute and Security Innovation
August 2013

Part 1 - Introduction

For over 10 years, Security Innovation has been researching application security and created the Application Security Maturity (ASM) model to help organizations understand their readiness to build secure software applications.

The present study utilities Security Innovation's Secure Software Development Lifecycle (SDLC) Maturity Questionnaire, which comprises 20 objectively framed questions concerning tools usage, development team knowledge and security best practices. It is used to better understand the maturity of an organization's application security program in comparison to the core competencies of high-performing organizations.

Ponemon Institute independently surveyed 642 IT professionals in both executive and engineering positions. The majority of the respondents were at a supervisory level or higher. Over half of the respondents are employed by organizations of more than 5,000 employees.

Based on the responses, the primary finding is that a much higher percentage of executive-level respondents believe their organizations are following security procedures through the lifecycle of application development than do the engineers who are closest to executing the security processes. This is a serious and potentially dangerous misalignment. Another troubling conclusion is that most organizations are only taking minimal steps to address application security throughout their development process.

The most effective way to reduce application security risk is to implement a formal, repeatable development process that includes secure coding standards to enable the early detection and remediation of vulnerabilities. Mature organizations tend to have highly effective application security programs that include the three pillars of a secure SDLC:

1. Application Security Standards
2. Regular Security Assessments for measurement
3. Training for each role in the SDLC

The mature organizations share common characteristics by:

- Writing and adopting security architecture and development standards.
- Training their development teams on application security topics based on role, platform, and technology used.
- Conducting regular assessments on their applications and processes to make sure the implementation of standards is effective.
- Ensuring that their executives, technicians and staff understand the importance of application security as part of the organizations' overall risk management strategy and collaborate on ensuring the practices described above are in place.

The primary goal of this research is to stimulate increased awareness in the importance of application security and to encourage a dialog between executives and practitioners to ensure that there is a common understanding of organizational realities concerning their ability to build more secure software.

Follow-on Research

This research is a follow-up to last year's study released by Ponemon Institute and Security Innovation entitled, 2012 Application Security Gap Study: A Survey of IT Security & Developers. The purpose of the previous study was to measure the tolerance to risk across the established phases of application security, and define what works and hasn't worked and what gaps exist that create threats to the organization.

The importance of an organization understanding its application security maturity level and the impact it has on their overall IT security profile is critical. Research has shown that the application layer is responsible for over 90 percent of all security vulnerabilities, yet more than 80 percent of IT security spending continues to be at the network layer, primarily focused on perimeter security. The findings of this study reveal the need for making greater investment in application security programs to reduce overall organizational exposure to cybercrime.

Baseline Maturity Levels

The Application Security Maturity Model describes the three phases through that an organization typically progresses:

- Phase 1: Panic Scramble
- Phase 2: Pit of Despair
- Phase 3: Security as Core Business Process

These phases are defined as follows:

Panic Scramble

In this phase, organizations never get ahead of the threat curve and reactively respond to the most recent security event, versus making proactive and strategic considerations regarding their application security program. Their first instinct is to invest in automation tools that hold the promise of immediate impact - and do so without investing in process or staff skills.

Typical outcomes include:

- Tools yield little to no ROI and result in randomization of the team's efforts
- A frantic approach to "find and fix" vulnerabilities
- Little to no time to develop a secure development environment

Pit of Despair

In this phase, organizations rethink their security investments because progress is not being made and the use of tools is not yielding the expected results. As procedures are detailed and driven by new security awareness and requirements, management begins to realize they need to invest in long-term and company-wide training, processes, and experts to help with planning and assessments.

Typical experiences in this stage include:

- The same vulnerabilities keep recurring and developers can't properly remediate them
- Automated scans are being conducted *after* an application is built
- Tools become "shelfware" due to the organization's inability to interpret scanner output and use them effectively, and usage of these tools drops
- Retrenchment and insufficient analysis of application security program as a whole

Security as Core Business Process

In this phase, organizations have a predictable and secure SDLC that is documented, measurable and managed. Standards, Education and Assessment activities are in place to create an ecosystem of repeatable, secure software development. Each team member knows how to conduct their activities securely and automation tools are improving the effectiveness of security activities.

Typical characteristics of this stage include:

- A security training program is in place for development staff, and includes role-, platform-, and technology-specific tracks
- Application security policies and standards are in place as well as mechanisms to ensure the standards are adhered to
- Key security engineering activities are defined and conducted for each phase (e.g. threat modeling, security code reviews, security testing/verification, etc.)
- Tools are effectively integrated into the Software Development Lifecycle (SDLC)

Expanded Maturity Levels

The three phases of the Application Security Maturity Model has been further expanded in this study to include five levels of application security maturity, as aligned with the Capability Maturity Model (CMMI).[1]

- **Level 1 (Initial)**
  - Lack of discipline and maturity in the SDLC; no focus on security
- **Level 2 (Repeatable)**
  - Disciplined and repeatable SDLC but security is purely reactive
  - Security is addressed by patching issues based on penetration testing results and public incidents
- **Level 3 (Defined)**
  - Security in the SDLC is standardized and defined
  - Corporate application security policies are defined
  - Formal security requirements are defined during the development process
  - Secure coding standards are in place and the code is reviewed to these standards
  - Security testing is part of the normal testing cycle
- **Level 4 (Managed)**
  - Predictable process that is measurable and managed
  - Threat modeling is used to assess and prioritize risk in each phase of the SDLC
  - Secure architecture standards are in place and the design is reviewed to these standards
  - Development teams and the code they produce are measured against compliance security requirements as well as secure architecture and coding standards
  - Application security risk is measured and well understood across the application portfolio
  - Third party security audits are conducted for all high-risk applications
- **Level 5 (Optimized)**
  - Continuously improving process that is mature and optimizing
  - Risk metrics are used to guide application security decision making
  - Vulnerability discoveries are used to update requirements and standards
  - Security activities are analyzed and improved based on assessments of vulnerabilities in the code

[1] Capability Maturity Model Integration (CMMI) is a process improvement training and certification developed by Carnegie Mellon University. The CMMI can be used to guide process improvement across a project, division, or an entire organization according to five maturity levels.

Part 2 – Key Findings

In this section, we present the overall responses to the application security maturity questions and highlight the most significant gaps in perceptions between executives and technicians as a key research output. The complete findings are presented in the appendix of this report.

The research results have been organized into four groups that indicate the maturity of an organization's application security program:

- **Level 1** - Ensuring the adoption of security architecture and development standards
- **Level 2** - Training and assessing the effectiveness of software development teams
- **Level 3** - Ongoing assessment of the effective implementation of standards
- **Level 4** - Building a culture of collaboration among executives, technicians and staff that makes application security an important part of the organization's overall risk management strategy

Seven Key Findings

1. Most organizations do not have a defined software development process in place
2. Most organizations are not testing for application security
3. Policies and requirements are often ad-hoc and not integrated into the SDLC
4. The majority of organizations do not have a formal application security training program
5. Most development teams are not measured for compliance with regulations and standards
6. Most organizations do not identify, measure, or understand application security risks
7. Significant disconnect exists between executives and practitioners regarding perceived levels of application security maturity and activities

The four levels listed above directly relate to an organization's maturity level. For each segment, we analyzed survey responses and present them below.

Level 1

Ensuring the adoption of software security architecture and development standards

Key Finding

Most organizations do not have a defined software development process in place

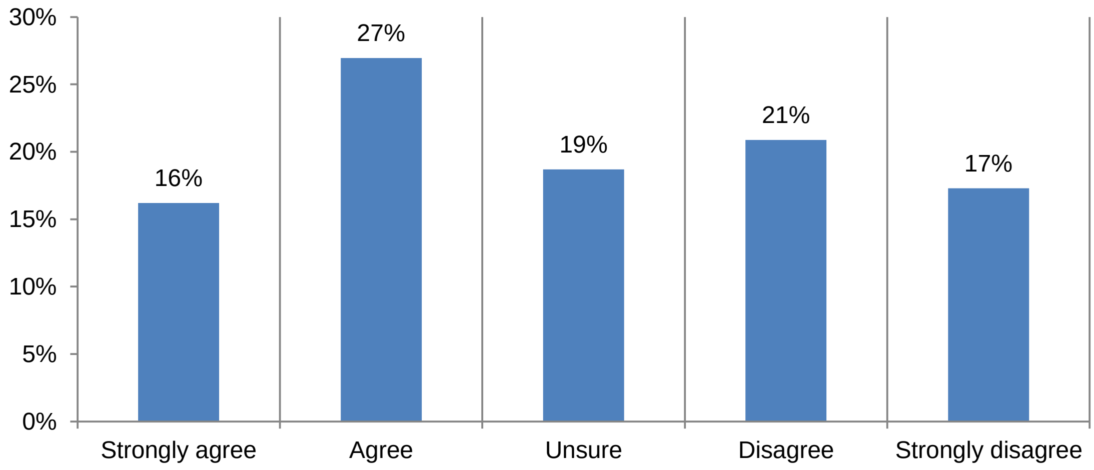
As part of a mature software development process, formal requirements, designs, implementation and testing procedures are already in place. Organizations that are mature with respect to application security *also* have security procedures defined at each phase. This finding indicates that the majority of organizations are not adequately emphasizing process, let alone security, during the application development lifecycle.

Figure 1 shows that only 43 percent of respondents say their organizations have a defined software development process in place. Of these (see Figure 2) 69 percent adhere to the defined process, meaning that only 30 percent of organizations have a defined software development process and also adhere to them.

The findings in this section reveal that approximately 43 percent of organizations represented in this study have achieved some level of maturity (level 3-5) by having the following in place:

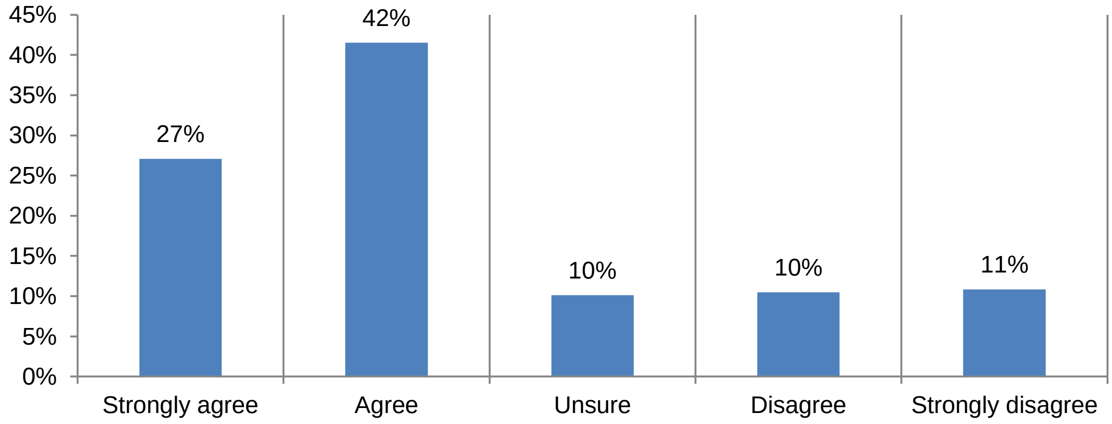
- Existence and adherence to a defined software development process
- Application testing using automated scanning tools and manual penetration
- Defined application policies and security requirements
- Defined secure coding standards and code reviewed for adherence

Figure 1: A defined software development process is in place



Among those respondents who strongly agree or agree that such a process is in place, 69 percent say they adhere to it as defined (Figure 2). However, this finding reveals only 31 percent of respondents say their organizations do not adhere to a defined process even if it exists (Level 1-2.)

Figure 2: Our organization adheres to the defined software development process



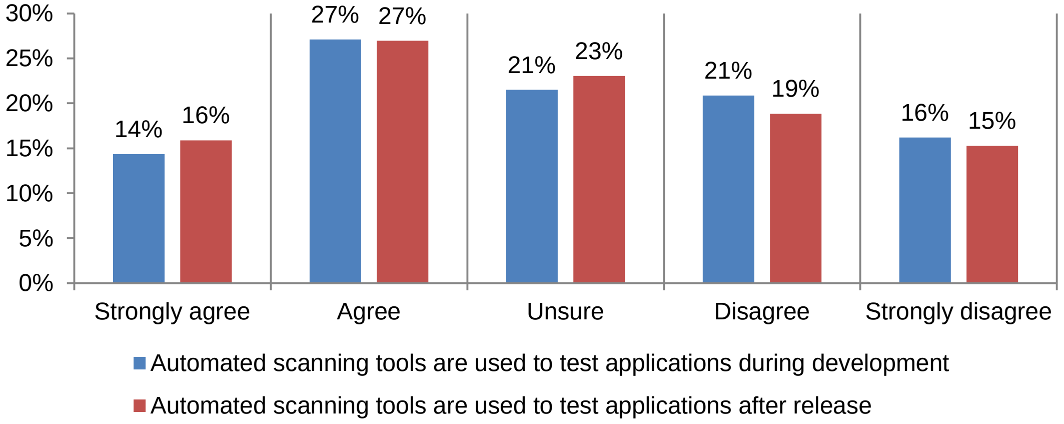
Key Finding

Most organizations are not testing for security

As discussed above, testing is included in a well-defined software development process. However, only 43 percent of respondents say their organizations have such a process in place to mitigate the risk of security bugs or defects in applications. Fifty-seven percent of organizations are at Level 1 or 2 with respect to incorporating security testing as part of the normal testing cycle.

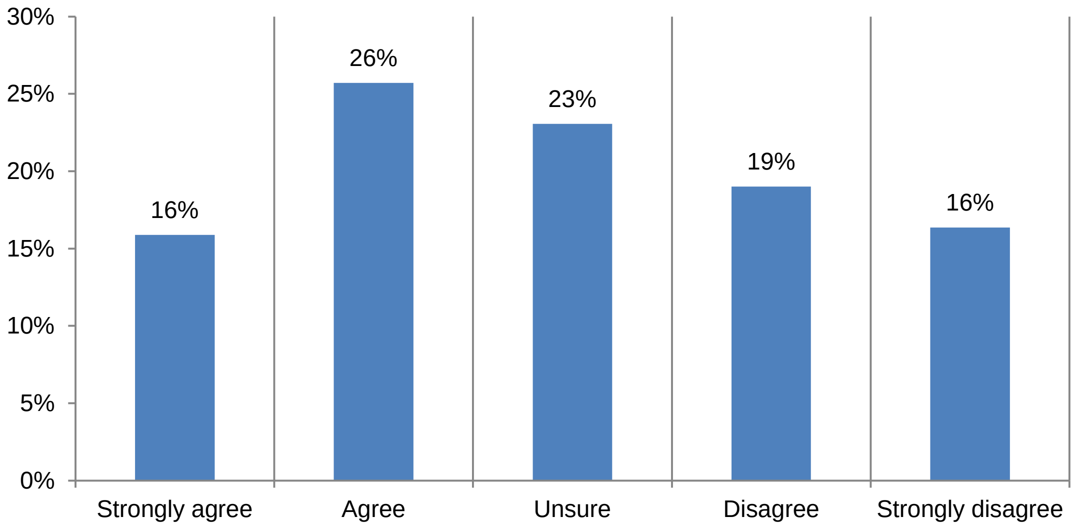
Specific tools, such as those that automatically scan for security flaws, are not used as widely as they should be. As shown in Figure 3, only 41 percent of respondents report their organizations are using automated scanning tools to test applications during development. A similar percentage (43 percent) of respondents say their organization uses these tools to test applications for vulnerabilities after release, as shown in Figure 3.

Figure 3: The use of automated scanning tools



Further**,** only 42 percent say their organizations subject applications to a manual penetration testing effort by internal teams or by a third party (Figure 4). Leveraging third party security audits for high-risk applications is an indicator of Level 4 maturity.

Figure 4: Applications are subjected to manual penetration testing

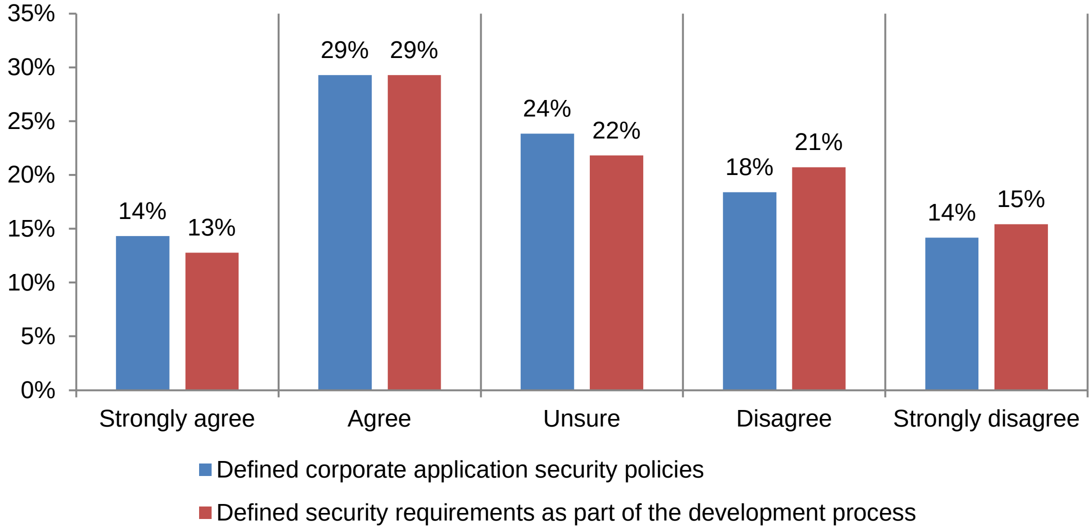


Key Finding

Policies and requirements are often ad-hoc and not integrated into the SDLC

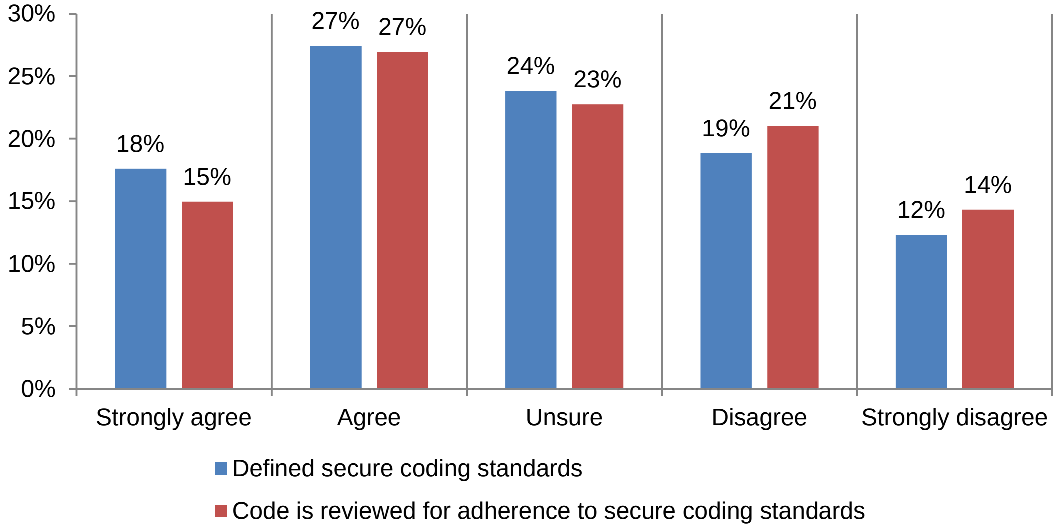
According to Figure 5, 43 percent have corporate application security policies and 42 percent say their organizations have formal security requirements as part of the development process. Lack of consistent policies and requirements in place makes it difficult to identify and remediate any security vulnerabilities (Level 1 or 2.) To achieve Level 3 maturity, an organization needs to have normal security requirements defined during the development process, secure coding standards in place, and practice review of code vs. those standards.

Figure 5: Application security policies and requirements are defined



Similarly, as shown in Figure 6, defined secure coding standards are lacking in a majority of organizations represented in this study (55 percent) and a slightly higher percentage of respondents do not review code for adherence to secure coding standards (58 percent).

Figure 6: Defined secure coding standards and code reviewed for adherence



Level 2

Training and assessment of the effectiveness of software development teams

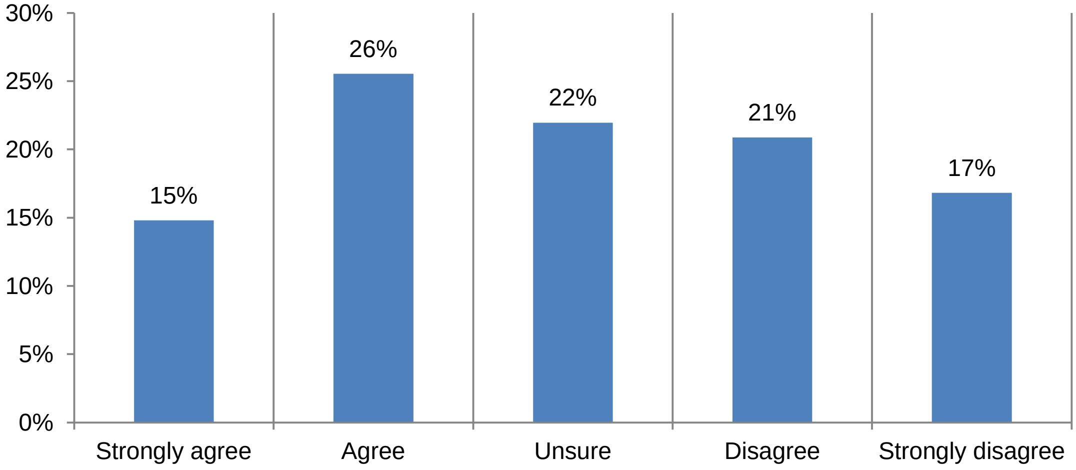
Key Finding

Majority of organizations do not have a formal training program In place

Mature organizations have application security training programs in place for their developers that focus on understanding and implementing the security requirements and policies. They also regularly update these programs to make sure developers understand the organization's application security policies, areas of vulnerability and best practices and standards to be followed.

In the *2012 Application Security Gap Study*, more than half of respondents (51 percent) said their organizations did not have an application security training program in place. This year's study has a similar finding. While the organizations may have some type of training in place, a majority of organizations are not updating internal training and education to ensure development teams are capable of adhering to application security policies and best practices (Figure 7).

Figure 7: Training updated to ensure developers' adherence to policies & best practices



Key Finding

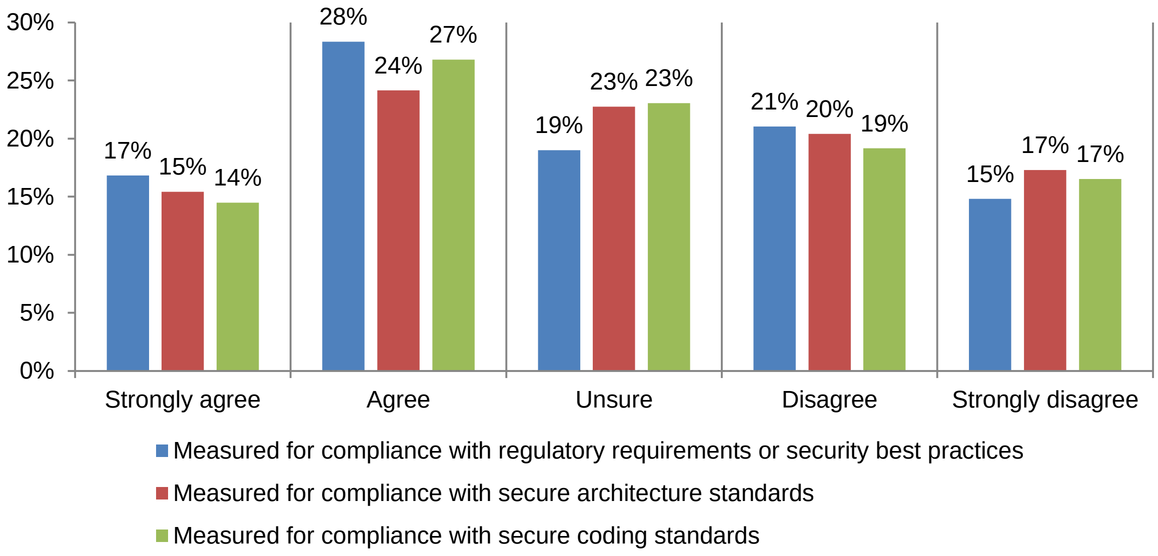
Most development teams are not measured for compliance with regulations and standards

An important part of the overall education of developers is to ensure that they are adhering to the organization's security policies and practices**.** Such assessments are critical to maintaining security in the development process and to understanding if the training program is achieving its objectives.

Figure 8 presents the findings of three questions that focused on whether organizations are measuring their development teams in the following areas: compliance with regulatory requirements, compliance with secure architecture standards and compliance with secure coding standards.

As shown, the majority of organizations in all cases do not take steps to determine compliance among programmers. Specifically, 45 percent measure development teams for their compliance with regulatory requirements or security best practices. Only 39 percent say development teams are measured for compliance with secure architecture standards and 41 percent say development teams are measured for compliance with secure coding standards.

Figure 8: Development teams are measured for compliance with regulations & standards



Level 3

Ongoing assessment of the effective implementation of standards

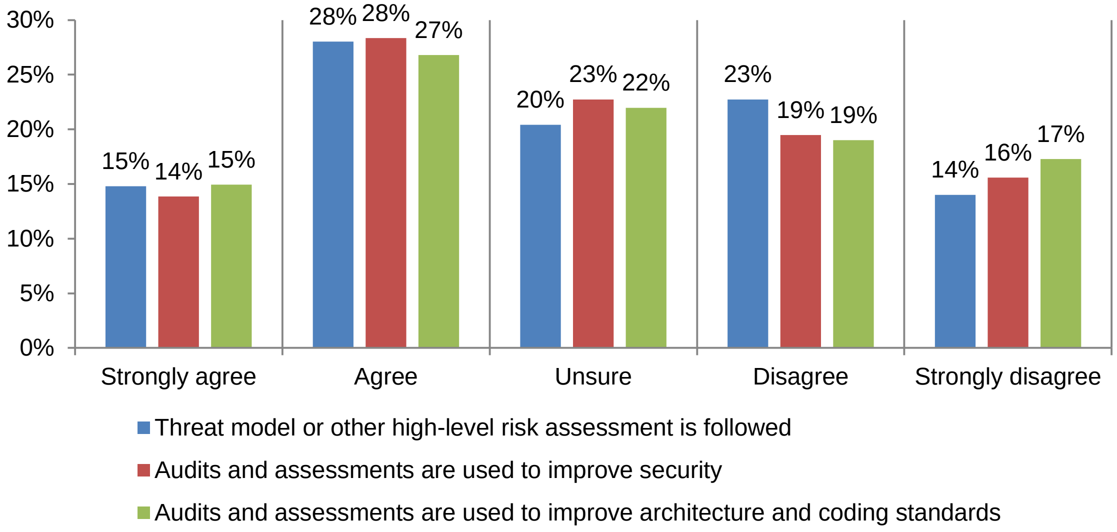
Key Finding

Most organizations don't identify, measure, or understand application security risks

Mature organizations are aware of the effectiveness of the implementation of standards because on a regular basis they conduct audits and assessments to understand the threats against their organization and to improve security, architecture and coding standards. Measures are also critical to becoming more strategic about investments in application security based on an understanding of the security risks they face.

As shown in Figure 9, use of a threat model or other high-level risk assessment is exhibited by 43 percent of the surveyed organizations. This rate of adoption is similar for audits and assessments needed to improve security, architecture and coding standards.

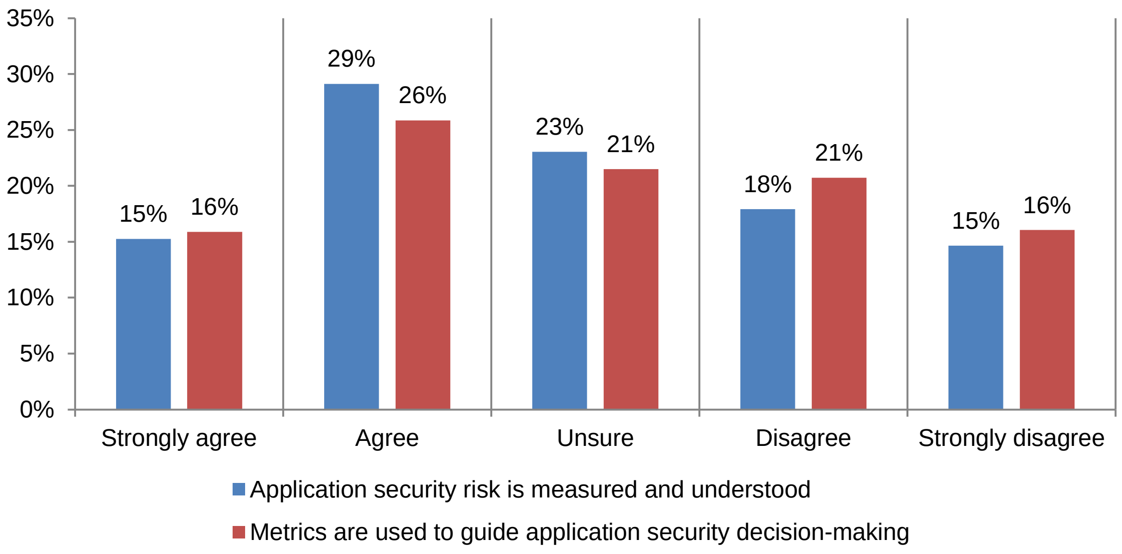
Figure 9: Audits and assessments in place to understand threats and improve standards



Programs and processes to understand application security risk are characteristics of a mature organization.

According to Figure 10, only 44 percent of respondents say their organizations measure application security risk and believe it is well understood and 42 percent use risk metrics to guide application security decision-making.

Figure 10: Measures to understand the risk and use in security decision-making



Level 4

Building a culture of collaboration among executives, technicians and staff that makes application security an important part of the organization's overall risk management strategy

Key Finding

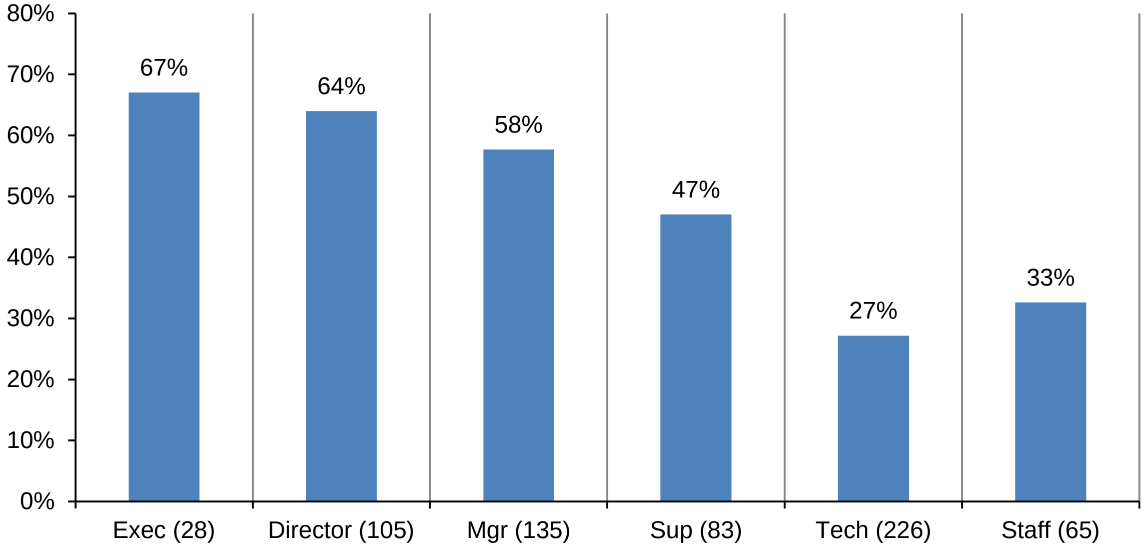
A significant disconnect exists between the responses of executives and practitioners regarding application security maturity and activities

According to the findings, executives see their organizations' application security program as far more mature than those at the managerial level and below. This may be due to poor communication and collaboration among the different roles involved in application security. Such misalignment of priorities makes it difficult for practitioners to obtain the resources necessary to invest in application security and make it an integral part of the overall risk management strategy.

As shown in Figure 11 below, executives are more than two times as likely than technicians to agree that the application security maturity questions reflect the reality of their organizations' security posture.

Figure 11: The application security maturity gap between executives and other levels in the organization

Strongly agree and agree response are combined



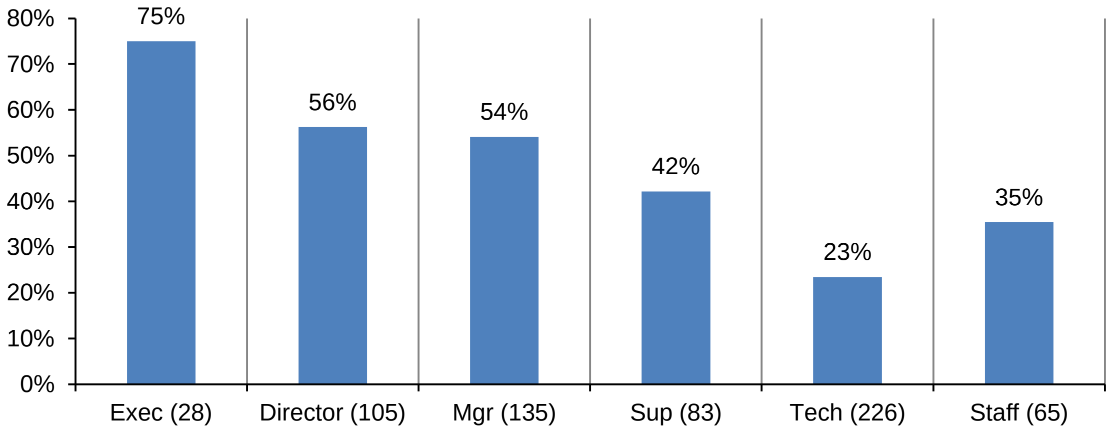
The next three charts show the most significant gaps based on the position level of the respondent, which are:

- The existence (or lack of) of defined secure architecture standards
- Measurement of development teams compliance with secure architecture standards
- Up-to-date internal training and education programs for development teams.

Figure 12 shows the different perceptions concerning the use of defined secure architecture standards. As shown, 75 percent of executives believe such standards are in place as opposed to only 23 percent of technicians who strongly agree or agree their organizations have defined secure architecture standards.

Figure 12: Existence of defined secure architecture standards

Strongly agree and agree response combined



Once more, executives are far more likely to agree that their organizations measure developers for compliance with secure architecture standards (Figure 13) while only 23 percent of technicians and staff believe such measures are taken.

Figure 13: Development teams are measured to determine compliance with secure architecture standards

Strongly agree and agree response combined

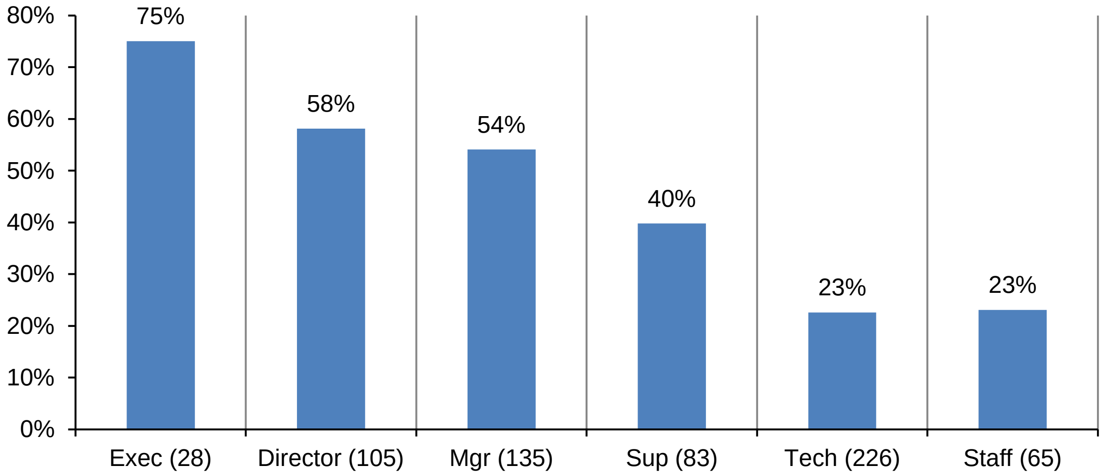
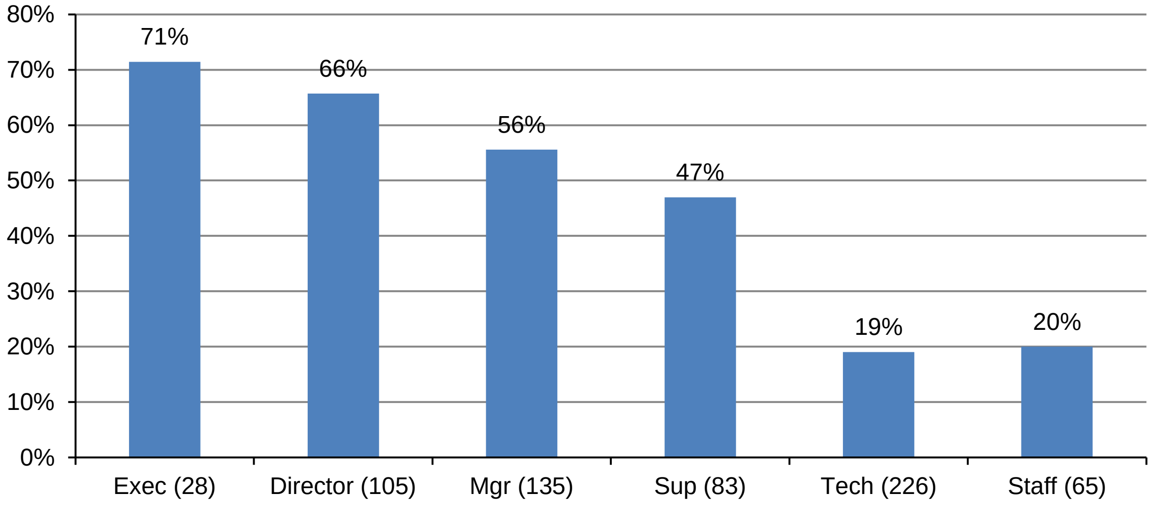


Figure 14 reveals that most executives believe internal training and education programs are updated to ensure that the development teams are capable of adhering to the latest threats, application security policies and best practices.

Figure 14: Updated internal training and education programs for development teams

Strongly agree and agree responses combined



Part 3 – Concluding Thoughts

Security Innovation's application security questions are the basis of this research and used to gauge the maturity of an application security process. By understanding the components of a mature process and how they compare in their overall approach to software security, organizations can make better decisions about investments in people and processes.

Following are the processes that organizations require to improve their application and IT security posture:

- Existence and adherence to a defined software development process
- Application testing using automated scanning tools and manual penetration
- Defined application policies and security requirements
- Defined secure coding standards and code reviewed for adherence
- Application security training programs for development teams that are specific to roles and technology
- Metrics that determine development teams' compliance with regulations, best practices, secure architecture standards and secure coding standards
- Ongoing audits and assessments to understand threats and improve standards
- Ongoing risk assessments to measure and understand the application security risk
- Management feedback to guide application security decision making

Another hurdle to overcome is the application security perception gap that exists in most organizations that has been revealed in this study. We believe these findings can be useful as a first step to initiating a productive discussion about the positive impact of closing these gaps can have on achieving a stronger allocation security posture.

About Security Innovation

Security Innovation focuses on the most difficult IT Security problem, and the root cause of most data breaches — insecure software applications. Our solutions are based on the three pillars of a secure Software Development Lifecycle (SDLC), which feed into one another to create an ecosystem of repeatable, secure software development: Standards, Education, and Assessment. The company's flagship products include TeamProfessor, the industry's largest library of application security eLearning courses, and TeamMentor, "out of the box" secure development standards.

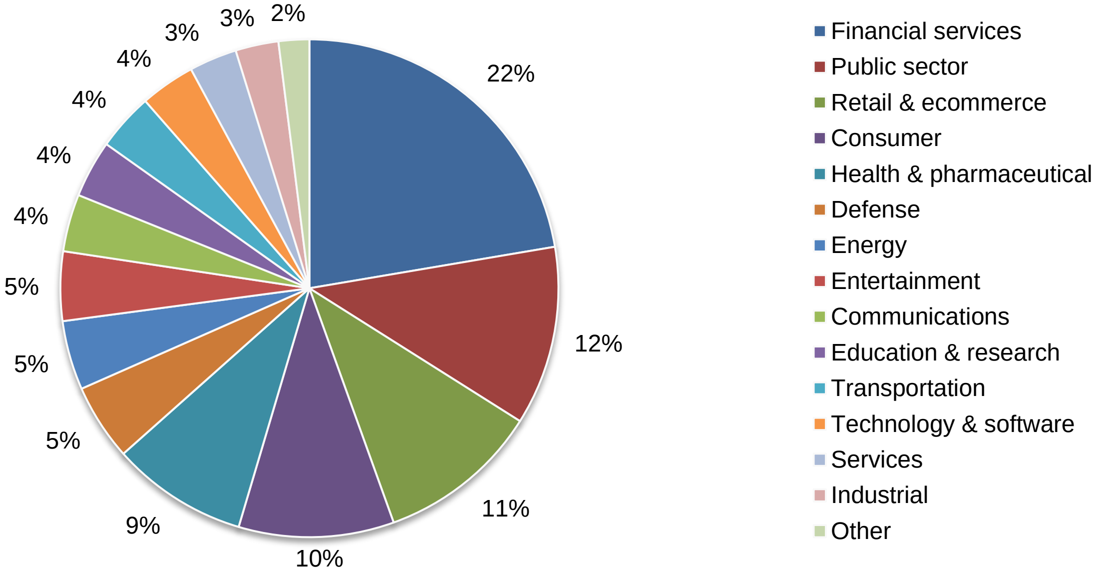
Part 4 - Methods

A random sample of 18,117 Information technology professionals located in all regions of the United States was selected to participate in this survey. As shown in Table 1 below, 687 respondents completed the survey. Forty-five surveys were removed that failed reliability checks. The final sample was 642 surveys (or a 3.5 percent response rate).

Table 1: Sample response	Freq	Pct%
Total sampling frame	18,117	100%
Total returns	687	4.8%
Rejected surveys	45	0.3%
Final sample	642	3.5%

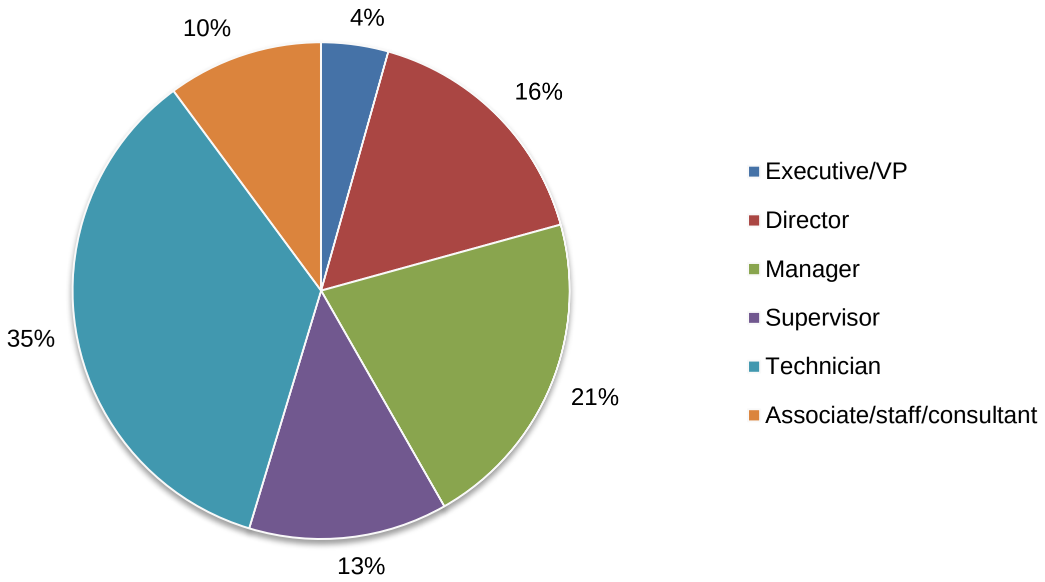
Pie Chart 1 reflects the industry distribution of respondents' organizations, with financial services (22 percent) as the largest segment, followed by public sector (12 percent) and retail and ecommerce (11 percent).

Pie Chart 1: Industry distribution of respondents' organizations



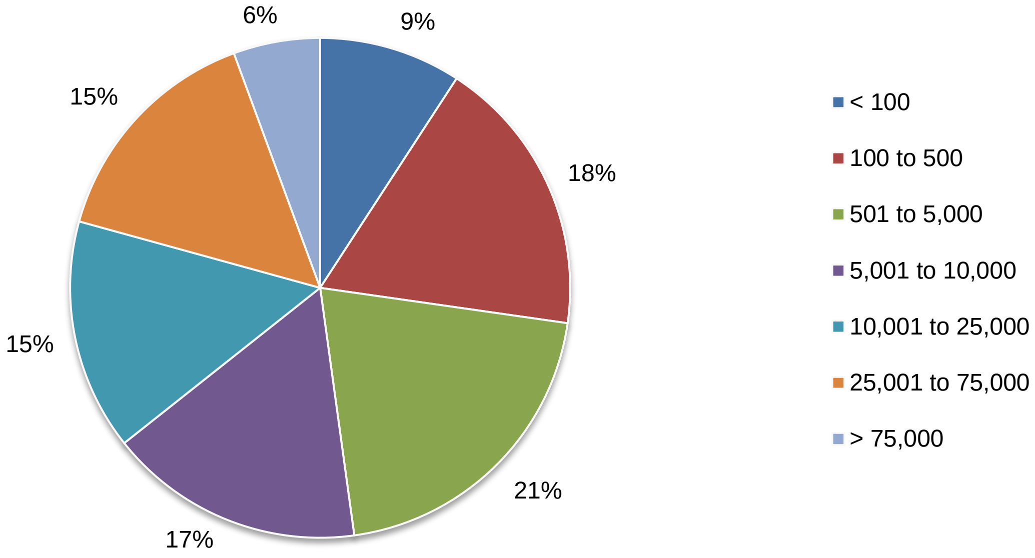
Pie Chart 2 reports the respondent’s organizational level within participating organizations. Fifty-four percent of respondents are at or above the supervisory levels.

Pie Chart 2: What organizational level best describes your current position?



Pie Chart 3 reports the respondent’s organizational size. Fifty-three percent of respondents are from organizations with more than 5,000 employees.

Pie Chart 3: Size of the organization



Part 5 - 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.

<u>Non-response bias</u>
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.

<u>Sampling-frame bias</u>
The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

<u>Self-reported results</u>
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 a truthful response.

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 December 2012.

Survey response	Freq	Pct%
Sample frame	18,117	100.0%
Total returns	687	3.8%
Total rejects	45	0.2%
Final sample	642	3.5%

Organizational characteristics

D1. Select the organizational level that best describes your current position.	Freq	Pct%
Executive/VP	28	4%
Director	105	16%
Manager	135	21%
Supervisor	83	13%
Technician	226	35%
Associate/staff/consultant	65	10%
Total	642	100%

D3. Select the sector that best describes your organization’s concentration or focus.	Freq	Pct%
Agriculture	6	1%
Communications	24	4%
Consumer	65	10%
Defense	32	5%
Education & research	24	4%
Energy	29	5%
Entertainment	29	5%
Financial services	144	22%
Health & pharmaceutical	57	9%
Industrial	18	3%
Public sector	75	12%
Retail & ecommerce	68	11%
Services	20	3%
Technology & software	23	4%
Transportation	24	4%
Other	4	1%
Total	642	100%

D4. Select the size of your company.	Freq	Pct%
< 100	59	9%
100 to 500	116	18%
501 to 5,000	132	21%
5,001 to 10,000	106	17%
10,001 to 25,000	96	15%
25,001 to 75,000	97	15%
> 75,000	36	6%
Total	642	100%

Survey questions

Q1. Your organization has a defined software development process that includes activities for requirements, design, implementation, and test.	Freq	Pct%
Strongly agree	104	16%
Agree	173	27%
Unsure	120	19%
Disagree	134	21%
Strongly disagree	111	17%
Total	642	100%

Q2. [1b] Your organization adheres to the software development process as defined.	Freq	Pct%
Strongly agree	75	27%
Agree	115	42%
Unsure	28	10%
Disagree	29	10%
Strongly disagree	30	11%
Total	277	100%

Q3. Your organization uses automated scanning tools to test applications during development.	Freq	Pct%
Strongly agree	92	14%
Agree	174	27%
Unsure	138	21%
Disagree	134	21%
Strongly disagree	104	16%
Total	642	100%

Q4. Your organization uses automated scanning tools to test applications for vulnerabilities after they have been released.	Freq	Pct%
Strongly agree	102	16%
Agree	173	27%
Unsure	148	23%
Disagree	121	19%
Strongly disagree	98	15%
Total	642	100%

Q5. Applications in your organization are subject to a manual penetration testing effort either by internal teams or by a third party.	Freq	Pct%
Strongly agree	102	16%
Agree	165	26%
Unsure	148	23%
Disagree	122	19%
Strongly disagree	105	16%
Total	642	100%

Q6. Your organization has corporate application security policies defined.	Freq	Pct%
Strongly agree	92	14%
Agree	188	29%
Unsure	153	24%
Disagree	118	18%
Strongly disagree	91	14%
Total	642	100%

Q7. Formal security requirements are defined as part of the development process.	Freq	Pct%
Strongly agree	82	13%
Agree	188	29%
Unsure	140	22%
Disagree	133	21%
Strongly disagree	99	15%
Total	642	100%

Q8. Your organization has defined secure coding standards.	Freq	Pct%
Strongly agree	113	18%
Agree	176	27%
Unsure	153	24%
Disagree	121	19%
Strongly disagree	79	12%
Total	642	100%

Q9. Your organization reviews code for adherence to secure coding standards.	Freq	Pct%
Strongly agree	96	15%
Agree	173	27%
Unsure	146	23%
Disagree	135	21%
Strongly disagree	92	14%
Total	642	100%

Q10. A threat model or other high-level risk assessment process is followed during the development process.	Freq	Pct%
Strongly agree	95	15%
Agree	180	28%
Unsure	131	20%
Disagree	146	23%
Strongly disagree	90	14%
Total	642	100%

Q11. Your organization has defined secure architecture standards.	Freq	Pct%
Strongly agree	89	14%
Agree	175	27%
Unsure	139	22%
Disagree	129	20%
Strongly disagree	110	17%
Total	642	100%

Q12. [11b] Application architecture is reviewed against the secure architecture standards.	Freq	Pct%
Strongly agree	60	23%
Agree	127	48%
Unsure	34	13%
Disagree	23	9%
Strongly disagree	22	8%
Total	266	100%

Q13. Development teams are measured for their compliance with regulatory requirements or security best practices.	Freq	Pct%
Strongly agree	108	17%
Agree	182	28%
Unsure	122	19%
Disagree	135	21%
Strongly disagree	95	15%
Total	642	100%

Q14. Development teams are measured for compliance with secure architecture standards.	Freq	Pct%
Strongly agree	99	15%
Agree	155	24%
Unsure	146	23%
Disagree	131	20%
Strongly disagree	111	17%
Total	642	100%

Q15. Development teams are measured for compliance with secure coding standards.	Freq	Pct%
Strongly agree	93	14%
Agree	172	27%
Unsure	148	23%
Disagree	123	19%
Strongly disagree	106	17%
Total	642	100%

Q16. In your organization, application security risk is measured and well understood across the application portfolio.	Freq	Pct%
Strongly agree	98	15%
Agree	187	29%
Unsure	148	23%
Disagree	115	18%
Strongly disagree	94	15%
Total	642	100%

Q17. Your organization uses the results of audits and assessments to improve application security policies and processes.	Freq	Pct%
Strongly agree	89	14%
Agree	182	28%
Unsure	146	23%
Disagree	125	19%
Strongly disagree	100	16%
Total	642	100%

Q18. Your organization uses the results of audits and assessments to improve architecture and coding standards.	Freq	Pct%
Strongly agree	96	15%
Agree	172	27%
Unsure	141	22%
Disagree	122	19%
Strongly disagree	111	17%
Total	642	100%

Q19. Your organization updates internal training and education to ensure development teams are capable of adhering to application security policies and best practices.	Freq	Pct%
Strongly agree	95	15%
Agree	164	26%
Unsure	141	22%
Disagree	134	21%
Strongly disagree	108	17%
Total	642	100%

Q20. Your organization uses risk metrics to guide application security decision-making.	Freq	Pct%
Strongly agree	102	16%
Agree	166	26%
Unsure	138	21%
Disagree	133	21%
Strongly disagree	103	16%
Total	642	100%