

BSIMM Begin

1. Introduction

Welcome to the BSIMM Begin survey sponsored by Cigital. As a discipline, software security has made great progress over the last decade. In 2008, Gary McGraw, Brian Chess, and Sammy Miguez interviewed the executives running nine software security initiatives, using the twelve practices of the Software Security Framework (<http://bsi-mm.com/ssf>) as our guide. Those companies among the nine who graciously agreed to be identified include: Adobe, The Depository Trust and Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, and Wells Fargo. We used the resulting data, drawn from real programs at different levels of maturity, to guide construction of the Building Security In Maturity Model (BSIMM). A maturity model is appropriate because improving software security almost always means changing the way an organization works--people, process, and automation are all required. While not all organizations need to achieve the same software security goals, our experience is that all successful large-scale software security initiatives share common ideas and approaches. Whether you rely on the Cigital Touchpoints, Microsoft SDL, or OWASP CLASP, there is much to learn from the practical experience of others.

WHY SHOULD YOU PARTICIPATE? We are continuing our research into real-world software security activities and this is where you can make a valuable contribution to your organization and to the software security community as a whole. All data are interesting! Regardless of your organization's size or the maturity of your software security approach, we encourage you to participate. In return, you will receive a good understanding of your organization's foundational software security activities relative to both the very mature organizations originally surveyed and those participating in this survey.

WHO SHOULD COMPLETE THIS SURVEY? This survey is best completed by someone with a working knowledge of the spectrum of software security activities actually being performed within a firm.

As you continue to the next page and begin the survey, please remember the following about SurveyMonkey. You will have to run JavaScript and should accept www.surveymonkey.com cookies for the survey to work correctly. Please proceed to the survey when you have about 90 minutes to dedicate to its completion. You will not be able to leave and reenter the survey. Clicking Done on the last page will submit the results. This is contrary to our previous guidance that surveys could be re-entered and we apologize for the mistake.

2. Pre-Survey Questions

IMPORTANT: In this survey, we use the phrase "software security group" to mean those individuals responsible for the execution of the software security initiative. Of course, there are many ways this may be occurring in your organization, perhaps ranging from a named group responsible for an organization-wide initiative, to a collection of business unit leaders working together, to individual efforts in specific application portfolios. Regardless of how the software security initiative is progressing in your organization, your answers will be of tremendous value.

This is a large survey, divided into six sections. Please proceed when you feel you have about 90 minutes to dedicate to its completion.

This first survey section gathers data on the firm and its software security initiative. There are 12 questions in this section, which will require approximately 8 minutes to complete.

1. If you wish to receive a copy of the blinded survey results, enter your email address.

2. Which vertical markets does your firm serve?

- | | | |
|---|--|---|
| <input type="checkbox"/> Automotive | <input type="checkbox"/> Healthcare/Pharmaceutical | <input type="checkbox"/> Online |
| <input type="checkbox"/> Financial Services | <input type="checkbox"/> Hospitality | <input type="checkbox"/> Real Estate |
| <input type="checkbox"/> Education | <input type="checkbox"/> Independent Software Vendor | <input type="checkbox"/> Retail |
| <input type="checkbox"/> Energy | <input type="checkbox"/> Insurance | <input type="checkbox"/> Technology |
| <input type="checkbox"/> Gaming | <input type="checkbox"/> Manufacturing | <input type="checkbox"/> Telecommunications |
| <input type="checkbox"/> Government | <input type="checkbox"/> Media | <input type="checkbox"/> Travel |

3. In what year did your firm's software security initiative begin (e.g., when was budget actually assigned, when did the grass-roots efforts really take hold, etc.)?

Enter year:

4. In what city, state/region, and country is your firm headquartered?

Enter location:

5. How many developers in your firm?

Number of developers:

6. How many testers in your firm?

Number of testers:

BSIMM Begin

7. Approximately how many applications are in your firm's portfolio?

Please enter a positive integer:

8. Would you characterize your firm's software security initiative as formal or informal?

Formal

Informal

9. Would you characterize your firm's software security initiative as centralized into an appointed group or decentralized into various business units or development groups?

Centralized

Decentralized

10. Does your firm's software security initiative have a named owner or leader?

Yes

No

11. How many hops (not inclusive) between the day-to-day software security initiative owner or ownership and the CEO?

Number of hops (not inclusive):

12. Please consider providing the following OPTIONAL information.

Name of firm:

Number of employees in firm:

Your name and contact information:

3. BSIMM Domain 1 - Governance

The Governance domain includes those practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.

This second survey section gathers data on the SSG's software security activities related to Governance. There are 37 questions in this section, which will require approximately 30 minutes to complete.

13. The firm has a documented strategy for improving software security.

True

False

14. The firm has only vaguely defined goals, roles, and responsibilities in its software security strategy.

True

False

15. The firm distributes its software security strategy broadly within the firm.

True

False

16. The SSG conducts internal marketing activities to raise awareness of software security issues.

True

False

17. Managers and application owners have little or no understanding of the software security problem and its potential negative impacts.

True

False

18. Corporate executives are not able to tie the need for software security to meeting business objectives.

True

False

19. The SSG conducts real attack and vulnerability demonstrations for executives.

True

False

BSIMM Begin

20. Executives have the facts on software security breaches occurring within the firm and at similar firms.

True

False

21. Executives understand the direct links between software security failures and impacted business objectives.

True

False

22. The firm has identified SDLC gates or checkpoints where software security efforts can be validated.

True

False

23. The firm has identified SDLC gate or checkpoint locations that are compatible with the SDLC processes in use.

True

False

24. SDLC gates or checkpoints do not include gathering software security data (e.g., test results) usable for go/no go decisions.

True

False

25. The firm does not use metrics to determine ongoing effectiveness of software security efforts.

True

False

26. The firm uses software security metrics to drive software security investment.

True

False

27. The firm use metrics to define software security goals in quantitative terms.

True

False

28. The firm is largely unaware of its regulatory and statutory compliance requirements for software.

True

False

BSIMM Begin

29. The firm has harmonized its regulatory and statutory compliance requirements for software in order to remove duplication.

True

False

30. The firm's approach to regulatory and statutory compliance has been mapped to specific software security activities.

True

False

31. The firm has documented its PII (personally identifiable information) obligations as derived from regulatory, statutory, customer, contractual, and other sources.

True

False

32. The firm has documented the software security and data privacy practices that stem from its PII obligations.

True

False

33. The firm has a vaguely defined software security policy (or none at all).

True

False

34. The firm's software security policy addresses both regulatory requirements and customer-driven security requirements.

True

False

35. The firm's software security policy presents a unified approach for satisfying software security drivers.

True

False

36. The firm provides no software security awareness training.

True

False

37. The firm's software security awareness training is available to everyone involved in the software development process.

True

False

BSIMM Begin

38. The firm uses software security awareness training to promote a culture of security throughout the organization.

True

False

39. The employee onboarding process for those in the software engineering organization includes a module on software security.

True

False

40. The firm's onboarding process for developers includes training on secure coding and internal software security resources.

True

False

41. The firm makes a concerted effort to ensure new software engineering hires enhance the software security culture.

True

False

42. The SSG has little or no interest in solving software security problems.

True

False

43. The SSG consistently misses opportunities to leverage teachable moments to deliver software security knowledge.

True

False

44. Rather than advocacy, the SSG consistently emphasizes punishment as the means for maturing software security capability.

True

False

45. Employees with software security skills are identified for further contribution to the software security process.

True

False

46. Employees with software security skills are provided opportunities for social networking with each other.

True

False

BSIMM Begin

47. Employees with software security skills are used to speed adoption of software security in software development processes.

True

False

48. Software security training never includes noteworthy security events (e.g., breaches, accomplishments) from company history.

True

False

49. Software security training explains how examples from company history are relevant to the student's software development efforts.

True

False

50. Software security training explains when examples from company history should be applied to current projects.

True

False

4. BSIMM Domain 2 - Intelligence

The Intelligence domain includes practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.

This third survey section gathers data on the SSG's software security activities related to Intelligence. There are 25 questions in this section, which will require approximately 17 minutes to complete.

51. The firm does not understand which attacks are most relevant to the software portfolio.

True

False

52. The firm's list of most relevant attacks includes input from observed attacks, hacker forums, organizational knowledge, and similar sources.

True

False

53. The firm's most relevant attacks list is updated periodically.

True

False

54. The firm has a data classification scheme.

True

False

55. The firm's data classification scheme has never been used to inventory its software according to the data handled.

True

False

56. The firm's software portfolio has not been prioritized according to each application's data classification.

True

False

57. The firm maintains a list of attackers or attacker profiles most relevant to the software portfolio.

True

False

58. The firm's list of attackers or profiles includes information on motivations and capabilities.

True

False

BSIMM Begin

59. The firm's list of attackers or profiles includes detailed information for specific individuals when known.

True

False

60. The SSG collects and publishes stories about attacks, focusing solely on events that occur at other firms.

True

False

61. SSG stories about attacks on the firm's portfolio include both successful and unsuccessful attacks.

True

False

62. The SSG builds and publishes security features for others to use.

True

False

63. The firm routinely attempts to solve security feature coding problems once and then make solutions available for others.

True

False

64. Software architecture discussions rarely or never include software security topics.

True

False

65. The software architecture group has taken responsibility for security as they have for performance, availability, or scalability.

True

False

66. SSG members do not attend software architecture meetings or interact with the security architecture group.

True

False

67. Organizational software security standards explain the expected way to adhere to software security policy.

True

False

BSIMM Begin

68. Organizational software security standards address each of the major security features used (e.g., authentication in a J2EE environment) across the portfolio.

True

False

69. The firm has no central location for software security information.

True

False

70. The SSG keeps centralized software security information current.

True

False

71. The SSG steers everyone to the central location for software security information.

True

False

72. The firm's compliance constraints have not been translated into software security requirements.

True

False

73. Software development projects are provided with compliance constraints that have been translated into software requirements.

True

False

74. Secure coding standards are provided to developers.

True

False

75. The firm's secure coding standards are specific to programming languages, libraries, and frameworks actually in use.

True

False

76. The firm's secure coding standard are mature enough to assist in code reviews.

True

False

5. BSIMM Domain 3 - SSDL Touchpoints

The SSDL Touchpoints domain includes practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.

This fourth survey section gathers data on the SSG's software security activities related to SSDL Touchpoints. There are 20 questions in this section, which will require approximately 14 minutes to complete.

77. The firm has an architecture analysis process.

True

False

78. Architecture reviewers identify security features as part of the analysis process.

True

False

79. Architecture reviewers typically do not look for problems that would cause security features to fail or prove insufficient.

True

False

80. The firm does not have a clear understanding of which applications are high risk or high profile.

True

False

81. Architecture reviewers use high risk, high profile applications as examples in demonstrating the need for continued analysis.

True

False

82. To ensure continued progress, outside consultants are used when architecture reviewers are not available.

True

False

83. The SSG is proficient in conducting architecture security reviews.

True

False

84. SSG members conducting architecture security reviews seek detailed guidance from the actual architects.

True

False

BSIMM Begin

85. The SSG has no role in uncovering design flaws.

True

False

86. The firm has a risk classification scheme for the application portfolio.

True

False

87. The firm has a review prioritization scheme for the application portfolio.

True

False

88. The firm collects basic information about each application (e.g., using a questionnaire) and uses the data to determine the risk represented and assign a priority that drives review schedules.

True

False

89. The SSG publishes a list of the most important security defects to be removed from the application portfolio.

True

False

90. The firm has a 'most important security defects' list built only from anecdotal data and public lists.

True

False

91. The firm has a 'most important security defects' list that is periodically updated.

True

False

92. The SSG is not capable of performing code review on high-risk applications.

True

False

93. The SSG does not proactively look for opportunities to perform code reviews on high-risk applications.

True

False

94. The SSG makes itself available to help others.

True

False

BSIMM Begin

95. SSG members are available for assistance on some manner of announced schedule.

True

False

96. Manual security code reviews are performed.

True

False

97. There are no automated software static analysis tools used to supplement manual security code reviews.

True

False

98. Human judgment is applied to output from software static analysis tools prior to results being used.

True

False

99. QA teams perform edge case testing as part of or in addition to functional testing.

True

False

100. QA teams perform boundary condition testing as part of or in addition to functional testing.

True

False

101. QA teams approach some parts of software testing as "adversarial testing" (i.e., like an attacker).

True

False

102. The SSG does not capture security testing results from across the portfolio.

True

False

103. The SSG ensures that security testing results are shared with QA groups.

True

False

BSIMM Begin

104. The SSG helps QA in adopting a security mindset by following up after sharing security testing results.

True

False

105. Black-box security testing tools are used by QA teams.

True

False

106. Black-box security testing tools are not integrated into QA processes.

True

False

107. The black-box security testing tools integrated into QA processes do not include protocol fuzzing tools.

True

False

6. BSIMM Domain 4 - Deployment

The Deployment domain includes practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.

This fifth survey section gathers data on the SSG's software security activities related to Deployment. There are 15 questions in this section, which will require approximately 11 minutes to complete.

108. The firm has no willingness to address software security even in the absence of evidence of security issues.

True

False

109. The firm never engages external penetration testers.

True

False

110. The development teams have a defined defect management and release process.

True

False

111. There are established defect management or mitigation channels for penetration testing results to get back to the development teams.

True

False

112. Penetration testing results are passed to development teams through ad hoc or informal channels only.

True

False

113. The firm has no processes or technologies that monitor input to applications.

True

False

114. The firm has processes or technologies that analyze input to applications in order to spot attacks.

True

False

BSIMM Begin

115. Host and network security decisions do not consider the applications they will support.

True

False

116. Processes are in place to maintain firewalls and patch operating systems and other acquired software.

True

False

117. There are operations personnel who focus on host and network security issues.

True

False

118. The SSG is prepared to assist in software security incidents.

True

False

119. The SSG and incident response teams meet on a regular basis.

True

False

120. The SSG and incident response teams maintain a free flow of information in both directions.

True

False

121. Production logs are rarely or never mined for data that might reveal software security issues.

True

False

122. Software security issues identified in production logs are made available to the SSG.

True

False

123. Software security issues identified in production logs and made available to development teams are used to change developer behavior.

True

False

7. Post-Survey Questions

Thank you for the data you have provided thus far. Using the insights you've gained into your firm's current software security activities, please answer the following questions.

This sixth survey section gathers data on the effectiveness of software security activities. There are 6 questions in this section, which will take approximately 15 minutes to complete.

124. On a scale of 0 (not at all) to 9 (most), how effective do you believe your current software security activities are in producing software that meets your firm's software security needs?

	Not at all effective	1	2	3	4	5	6	7	8	Most effective
Software security activity effectiveness:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

125. Across your firm's software portfolio, unacceptable software security test results (as part of release to production or while in production) or security breaches (in production) occur with what frequency?

Constantly

Quarterly

Weekly

Annually

Monthly

Hardly ever

BSIMM Begin

126. Please rate each of the following BSIMM software security practices according to the current investment levels in your firm:

	None	Way too little	Not really enough	About right	A little too much	Way too much
Strategy and Metrics	ja	ja	ja	ja	ja	ja
Compliance and Policy	ja	ja	ja	ja	ja	ja
Training	ja	ja	ja	ja	ja	ja
Attack Models	ja	ja	ja	ja	ja	ja
Security Features and Design	ja	ja	ja	ja	ja	ja
Standards and Requirements	ja	ja	ja	ja	ja	ja
Architecture Analysis	ja	ja	ja	ja	ja	ja
Code Review	ja	ja	ja	ja	ja	ja
Security Testing	ja	ja	ja	ja	ja	ja
Penetration Testing	ja	ja	ja	ja	ja	ja
Software Environment	ja	ja	ja	ja	ja	ja
Configuration Management and Vulnerability Management	ja	ja	ja	ja	ja	ja

127. Please rank order, from 1 (most investment) to 12 (least investment), the following BSIMM software security practices according to the investment levels you believe would be appropriate for your firm:

	1	2	3	4	5	6	7	8	9	10	11	12
Strategy and Metrics	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Compliance and Policy	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Training	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Attack Models	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Security Features and Design	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Standards and Requirements	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Architecture Analysis	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Code Review	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Security Testing	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Penetration Testing	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Software Environment	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Configuration Management and Vulnerability Management	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja

BSIMM Begin

128. Please accept our sincere appreciation for completing this survey. Your participation will directly improve the empirical data available for software security research and we thank you.

Please use the space below to provide any comments or feedback on any survey question, on the BSIMM, or on any software security topic you feel we overlooked.

Thank you.

