Four Software Security Findings

Gary McGraw, Cigital

Analyzing data from 78 firms using the Building Security In Maturity Model (BSIMM) revealed four truths about software security that will help firms protect and secure their assets.

Software security continues to grow and evolve, currently accounting for more than 10 percent of global IT security revenue worldwide. On the surface, it seems obvious that we must make software systems secure from the start, but opinions vary as to implementation. Through a multiyear process of observing and measuring security initiatives, we can move beyond opinion into the realm of fact. What follows are four indisputable facts we learned about software security through our work with the Building Security In Maturity Model (BSIMM; http://bsimm.com).

THERE'S NO SPECIAL SNOWFLAKE

The BSIMM is an observation-based study of software security that began in 2008 with nine firms. The sixth release (BSIMM6) includes data gathered from 78 firms, including Adobe, Aetna, Bank of America, Experian, Fannie Mae, Fidelity, Intel, LinkedIn, McAfee, PayPal, Siemens, Sony Mobile, Symantec, Visa, VMware, Wells Fargo, and Zephyr Healthcare. This latest data set is more than 20 times larger than it was in 2008.

Using the BSIMM measurement tool, a firm can directly compare its software security approach to the BSIMM community through 112 well-defined activities—for example, performing design review for high-risk applications—organized in 12 practices. One way to represent this measurement is shown in Figure 1, which illustrates how a target firm can be scored in a high-resolution fashion using the BSIMM scorecard.

DISCLAIMER

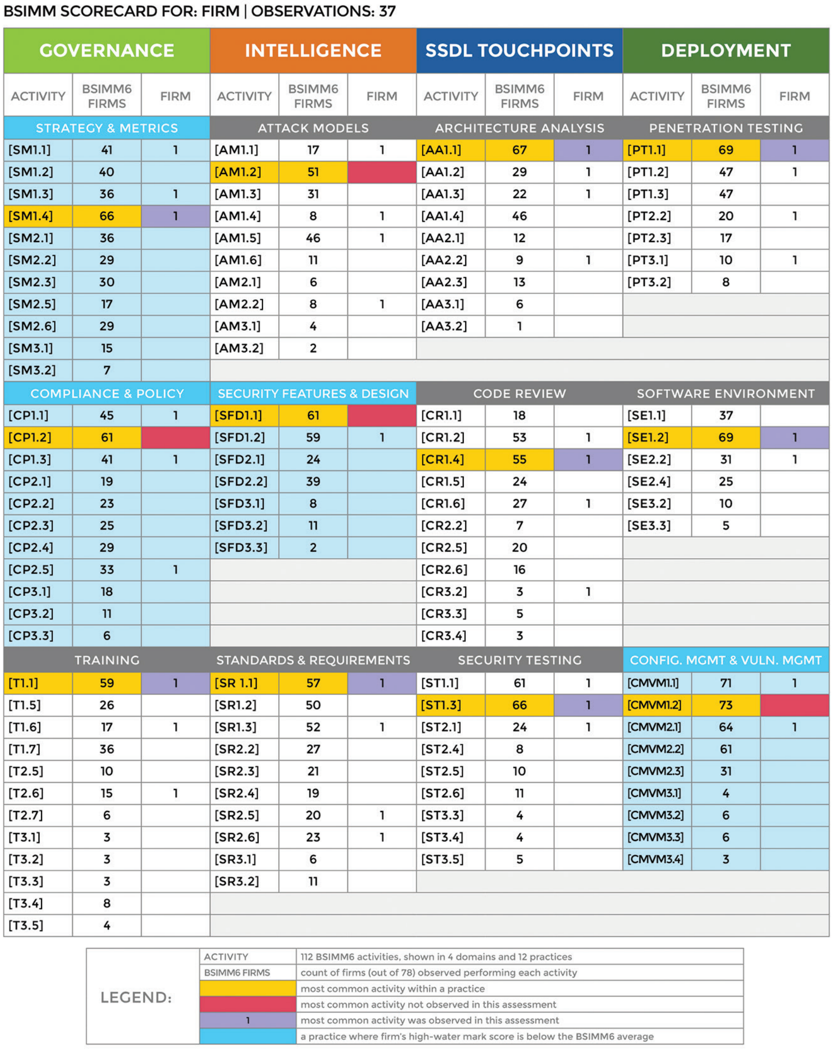
Some of the material in this article is used by permission of BSIMM coauthors Gary McGraw, Sammy Migues, and Jacob West. Download the BSIMM at http://bsimm.com.

0018-9162/16/$33.00 © 2016 IEEE

The BSIMM model has been used to measure more than 110 firms to date, and many firms have been measured multiple times over several years. BSIMM measurements take the form of intensive in-person interviews with various stakeholders in a firm's software security initiative. A typical measurement process—including data gathering and analysis—takes two or three weeks to complete and results in a formal report.

The BSIMM community includes firms of various sizes in different industry verticals and with a range of levels of software security maturity. We've never come across a firm that couldn't be measured with the BSIMM—in other words, there's no special snowflake.

To give you some idea of the breadth of BSIMM6's coverage, consider that the model itself describes the work of 3,195 full-time software security professionals attempting to control the security of software developed by 287,006 developers building and evolving 69,750 applications. The BSIMM6 community includes 33 financial services firms, 27 independent software vendors, 13 consumer electronics firms, and 10 healthcare firms. Development groups in the BSIMM community range from a small group of 23 developers to a large population of 35,000 developers, with a median of 1,200 developers in a typical firm.



BSIMM SCORECARD FOR: FIRM | OBSERVATIONS: 37

GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM6 FIRMS	FIRM	ACTIVITY	BSIMM6 FIRMS	FIRM	ACTIVITY	BSIMM6 FIRMS	FIRM	ACTIVITY	BSIMM6 FIRMS	FIRM
STRATEGY & METRICS			ATTACK MODELS			ARCHITECTURE ANALYSIS			PENETRATION TESTING		
[SM1.1]	41	1	[AM1.1]	17	1	[AA1.1]	67	1	[PT1.1]	69	1
[SM1.2]	40		[AM1.2]	51	🟥	[AA1.2]	29	1	[PT1.2]	47	1
[SM1.3]	36	1	[AM1.3]	31		[AA1.3]	22	1	[PT1.3]	47	
[SM1.4]	66	1	[AM1.4]	8	1	[AA1.4]	46		[PT2.2]	20	1
[SM2.1]	36		[AM1.5]	46	1	[AA2.1]	12		[PT2.3]	17	
[SM2.2]	29		[AM1.6]	11		[AA2.2]	9	1	[PT3.1]	10	1
[SM2.3]	30		[AM2.1]	6		[AA2.3]	13		[PT3.2]	8	
[SM2.5]	17		[AM2.2]	8	1	[AA3.1]	6				
[SM2.6]	29		[AM3.1]	4		[AA3.2]	1				
[SM3.1]	15		[AM3.2]	2							
[SM3.2]	7										
COMPLIANCE & POLICY			SECURITY FEATURES & DESIGN			CODE REVIEW			SOFTWARE ENVIRONMENT		
[CP1.1]	45	1	[SFD1.1]	61	🟥	[CR1.1]	18		[SE1.1]	37	
[CP1.2]	61	🟥	[SFD1.2]	59	1	[CR1.2]	53	1	[SE1.2]	69	1
[CP1.3]	41	1	[SFD2.1]	24		[CR1.4]	55	1	[SE2.2]	31	1
[CP2.1]	19		[SFD2.2]	39		[CR1.5]	24		[SE2.4]	25	
[CP2.2]	23		[SFD3.1]	8		[CR1.6]	27	1	[SE3.2]	10	
[CP2.3]	25		[SFD3.2]	11		[CR2.2]	7		[SE3.3]	5	
[CP2.4]	29		[SFD3.3]	2		[CR2.5]	20				
[CP2.5]	33	1				[CR2.6]	16				
[CP3.1]	18					[CR3.2]	3	1			
[CP3.2]	11					[CR3.3]	5				
[CP3.3]	6					[CR3.4]	3				
TRAINING			STANDARDS & REQUIREMENTS			SECURITY TESTING			CONFIG. MGMT & VULN. MGMT		
[T1.1]	59	1	[SR 1.1]	57	1	[ST1.1]	61	1	[CMVM1.1]	71	1
[T1.5]	26		[SR1.2]	50		[ST1.3]	66	1	[CMVM1.2]	73	🟥
[T1.6]	17	1	[SR1.3]	52	1	[ST2.1]	24	1	[CMVM2.1]	64	1
[T1.7]	36		[SR2.2]	27		[ST2.4]	8		[CMVM2.2]	61	
[T2.5]	10		[SR2.3]	21		[ST2.5]	10		[CMVM2.3]	31	
[T2.6]	15	1	[SR2.4]	19		[ST2.6]	11		[CMVM3.1]	4	
[T2.7]	6		[SR2.5]	20	1	[ST3.3]	4		[CMVM3.2]	6	
[T3.1]	3		[SR2.6]	23	1	[ST3.4]	4		[CMVM3.3]	6	
[T3.2]	3		[SR3.1]	6		[ST3.5]	5		[CMVM3.4]	3	
[T3.3]	3		[SR3.2]	11							
[T3.4]	8										
[T3.5]	4										

LEGEND:		
	ACTIVITY	112 BSIMM6 activities, shown in 4 domains and 12 practices
	BSIMM6 FIRMS	count of firms (out of 78) observed performing each activity
	🟨	most common activity within a practice
	🟥	most common activity not observed in this assessment
	1	most common activity was observed in this assessment
	🟦	a practice where firm's high-water mark score is below the BSIMM6 average

Figure 1. The Building Security In Maturity Model 6 (BSIMM6) scorecard can be used to rate a target firm against the BSIMM population on II2 activities. To read about particular activities, download the BSIMM at http://bsimm.com.

YOUR FIRM NEEDS A SOFTWARE SECURITY GROUP

Each of the 78 software security initiatives described in BSIMM6 has a software security group (SSG). Successfully carrying out the BSIMM activities without an SSG is very unlikely (and hasn't been observed in the field to date), so it's essential to create an SSG before you start working to adopt the BSIMM activities.

SSGs come in a variety of shapes and sizes. Strong SSGs tend to include people with deep coding experience and architectural chops. Software security can't only be about finding specific bugs such as the Open Web Application Security Project Top 10 (www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). Code review is a very important best practice, but reviewers must actually understand code (not to mention the huge piles of security bugs). However, the best code reviewers sometimes make very poor software architects, and asking them to perform an architecture risk analysis will only result in blank stares. Make sure code and architectural capabilities are equally covered in your SSG.

An SSG is often asked to mentor, train, and work directly with hundreds of developers. Communication skills,

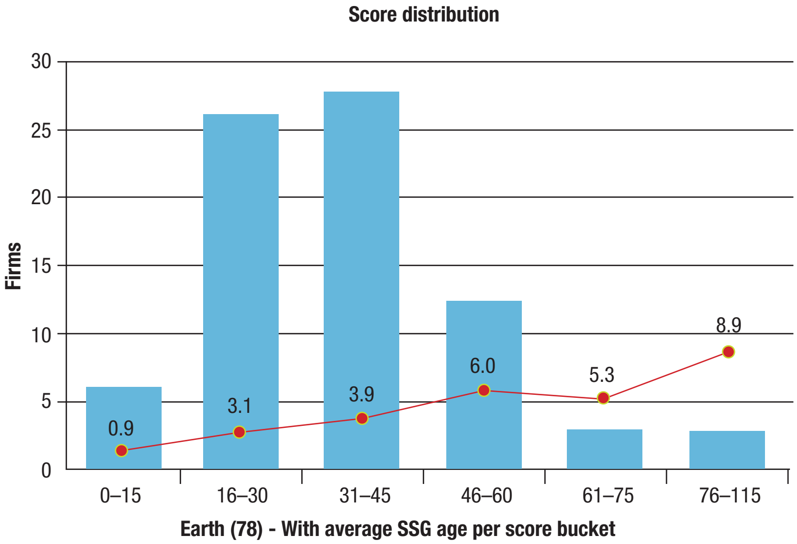


Figure 2. Distribution of BSIMM maturity scores among 78 firms (referred to as "Earth" in the BSIMM). SSG is software security group.

teaching capability, and good consulting sense are must-haves for at least a portion of the SSG staff. For more about this, see SearchSecurity's article "How to Build a Team for Software Security Management," which was based on SSG structure data gathered at the 2014 BSIMM Community Conference (http://searchsecurity.techtarget.com/opinion/McGraw-How-to-build-a-team-for-software-security-management).

Though no two of the 78 firms we examined had exactly the same SSG structure—suggesting that there are multiple ways to structure an SSG—we did observe some commonalities. At the highest level of organization, SSGs have five major roles:

- provide software security services,
- set policy,
- mirror business unit organizations,
- use a hybrid policy and services approach,
- and manage a distributed network of those doing software security work.

Some SSGs are highly distributed across a firm and others are very centralized. Looking at all the SSGs in our study, we see several common "subgroups": people dedicated to policy, strategy, and metrics; internal services groups that (often separately) cover tools, penetration testing, middleware development, and shepherding; incident response groups; training development and delivery groups; externally facing marketing and communications groups; and vendor-control groups.

We observed an average ratio of SSG to development of 1.51 percent across the entire group of organizations, meaning there's one SSG member for every 75 developers when we average the ratios for each participating firm. The largest ratio found was 16.7 percent and the smallest, 0.03 percent. The average SSG size among the 78 firms is approximately 14 people (range = 1–130, median = 6).

If you intend to take on software security in a firm-wide fashion, start by forming an SSG that's the right size to get the job done.

EXPERIENCE AND MATURITY MAKE A BIG DIFFERENCE

With a larger BSIMM data set than ever before, we can now analyze large-scale trends. For example, we were able to graph the distribution of maturity scores among the participating firms by dividing the scores into six bins (see Figure 2). The scores represent a slightly skewed bell curve. We also plotted the firms' average age in each bin, represented by the orange line on the graph. In general, firms with more observed BSIMM activities have older software security initiatives.

We also compared groups of firms by maturity. On average, the top 11 firms in the BSIMM population have a development group size of 10,000, have been doing software security at the enterprise level for 6.8 years, have an SSG with 29 members, and have a satellite (developers, architects, and others who are directly engaged in software security but aren't part of the SSG) of 118 people. In contrast, the bottom 11 firms have an average development group size of 600, have been doing software security at the enterprise level for 1.25 years, have an SSG with 3.4 members, and don't have a satellite.

Comparing activities commonly found among the top 11 versus bottom 11 firms is telling. Although six of the same activities are found in both populations (ranging from code review and training activities to data classification and standards activities), nine are observed in the top firms and none are observed in the bottom firms. These nine activities emphasize governance and outreach:

- SM1.1: Publish process (roles, responsibilities, plan); evolve as necessary.
- SM1.3: Educate executives.
- SM2.1: Publish data about software security internally.
- SM2.2: Enforce gates with measurements and track exceptions.
- CP1.3: Create policy.
- CP2.5: Ensure executive awareness of compliance and privacy obligations.
- SR1.2: Create a security portal.
- AM1.3: Identify potential attackers.

- AA1.4: Use a risk questionnaire to rank applications.

With this analysis, not only do we know the kinds of activities undertaken in more mature software security initiatives, but we also generally know when those activities are undertaken in the initiative's life cycle. Less mature firms, or those just getting started with software security, have plenty to learn from their more experienced peers.

We know what to do for software security and even how and when to do it. Now we just need to make it so everywhere.

SOFTWARE SECURITY SHOULD BE EVENLY DISTRIBUTED

One of the most commonly held myths of software security is that developers and development staff should just "take care of" software security. The theory is that with some training, developers can do it all. Our work with the BSIMM shows that this isn't the case, and that an SSG is necessary.

However, development staff and other members of a firm should eventually be directly involved in software security. In fact, satellites play a major role in executing software security activities among the most mature BSIMM community firms. BSIMM6 describes the work of 1,084 SSG members working directly with a satellite of 2,111 people (that's right—the satellite population is twice as large as the SSG population).

A satellite can be widely distributed with one or two members in each product group, or it can be more focused, getting together regularly to compare notes, learn new technologies, and expand the understanding of software security in an organization. Identifying and fostering a strong satellite is important to the success of many software security initiatives, but not all of them. Some BSIMM activities target the satellite explicitly.

Each of the 10 firms with the highest BSIMM scores has a satellite (100 percent) with an average size of 131 people. Thirty of the remaining 68 firms have a satellite (44.1 percent), and none of the 10 firms with the lowest BSIMM scores has a satellite. This suggests that as a software security initiative matures, its activities become distributed and institutionalized into the organizational structure. Among the BSIMM population of 78 firms, initiatives tend to evolve from centralized and specialized to decentralized and distributed, with an SSG orchestrating things at the core.

The time has come to put away the bug parade boogeyman (www.informit.com/articles/article.aspx?p=1248057), the top 10 tea leaves, the black box Web app goat sacrifice, and the occult reading of penetration testing entrails. It's science time. The BSIMM provides an important step forward in the institutionalization of software security as a discipline. Improvement is only possible when measurement is in place, and the BSIMM remains the only measurement tool in the software security field. C

GARY MCGRAW, PhD, is Cigital's chief technology officer. Contact him at gem@cigital.com.