



BSIMM3: The Building Security In Maturity Model

*Gary McGraw, Ph.D.
Chief Technology Officer, Cigital*

March 2012

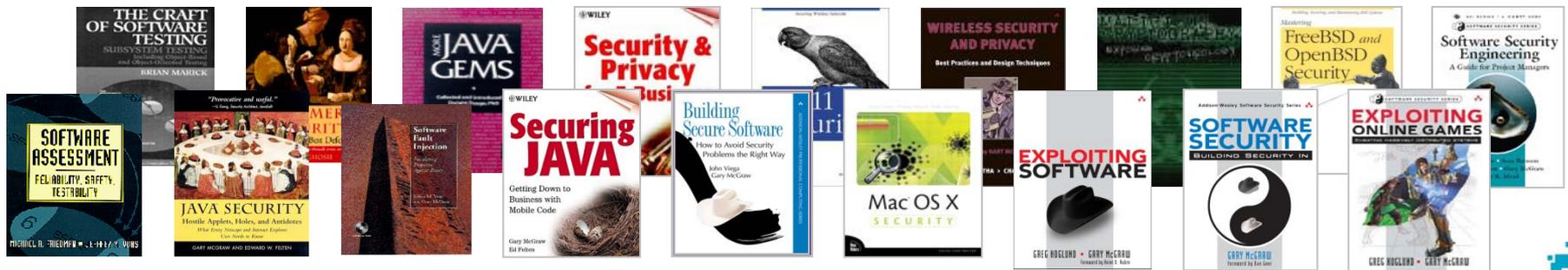


Software Confidence. Achieved.



Cigital

- Founded in 1992 to provide software security and software quality professional services
- Recognized experts in software security and software quality
 - Widely published in books, white papers, and articles
 - Industry thought leaders



We hold these truths to be self-evident

- Software security is more than a set of security functions
 - Not magic crypto fairy dust
 - Not silver-bullet security mechanisms
- Non-functional aspects of design are essential
- Bugs and flaws are 50/50
- Security is an emergent property of the entire system (just like quality)
- To end up with secure software, deep integration with the SDLC is necessary



BSIMM: Software Security Measurement



- Real data from (42) real initiatives
- 81 measurements
- 11 over time
- McGraw, Chess, & Migues



42 software security initiatives measured



BSIMM by the numbers

	BSIMM	BSIMM2	BSIMM3
Firms	9	30	42
Measurements	9	49	81
2nd Measurements	0	0	11
SSG Members	370	635	786
Satellite Members	710	1150	1750
Developers	67,950	141,175	185,316
Applications	3970	28,243	41,157
Average SSG Age (yrs)	5.32	4.49	4.32
SSG Avg of Avgs	1.13 per 100	1.02 per 100	1.99 per 100
Financials	4	12	17
ISVs	4	7	15
High Tech	2	7	10
Other	0	8	10



Monkeys eat bananas



- BSIMM is not about good or bad ways to eat bananas or banana best practices
- BSIMM is about observations
- BSIMM is descriptive, not prescriptive

A Software Security Framework

The Software Security Framework (SSF)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

- Four domains
- Twelve practices
- See informIT article on BSIMM website
<http://bsimm.com>

Architecture Analysis practice skeleton

SSDL TOUCHPOINTS: ARCHITECTURE ANALYSIS		
Capturing software architecture diagrams, applying lists of risks and threats, adopting a process for review, building an assessment and remediation plan.		
Objective	Activity	Level
[AA1.1] get started with AA	perform security feature review	1
[AA1.2] demonstrate value of AA with real data	perform design review for high-risk applications	
[AA1.3] build internal capability on security architecture	have SSG lead review efforts	
[AA1.4] have a lightweight approach to risk classification and prioritization	use risk questionnaire to rank apps	
[AA2.1] model objects	define/use AA process	2
[AA2.2] promote a common language for describing architecture	standardize architectural descriptions (include data flow)	
[AA2.3] build capability organization-wide	make SSG available as AA resource/mentor	
[AA3.1] build capabilities organization-wide	have software architects lead review efforts	3
[AA3.2] build proactive security architecture	drive analysis results into standard architectural patterns (T: sec features/design)	



Example activity

[AA1.2] Perform design review for high-risk applications. The organization learns about the benefits of architecture analysis by seeing real results for a few high-risk, high-profile applications. If the SSG is not yet equipped to perform an in-depth architecture analysis, it uses consultants to do this work. Ad hoc review paradigms that rely heavily on expertise may be used here, though in the long run they do not scale.

Real-world data (42 firms)

- Initiative age
 - Average: 5.5 years
 - Newest: 1
 - Oldest: 16
 - Median: 4
- SSG size
 - Average: 19.2
 - Smallest: 0.5
 - Largest: 100
 - Median: 8
- Satellite size
 - Average: 42.7
 - Smallest: 0
 - Largest: 350
 - Median: 15
- Dev size
 - Average: 5183
 - Smallest: 11
 - Largest: 30,000
 - Median: 1675

Average SSG size: 1.99% of dev group size

BSIMM3 Scorecard

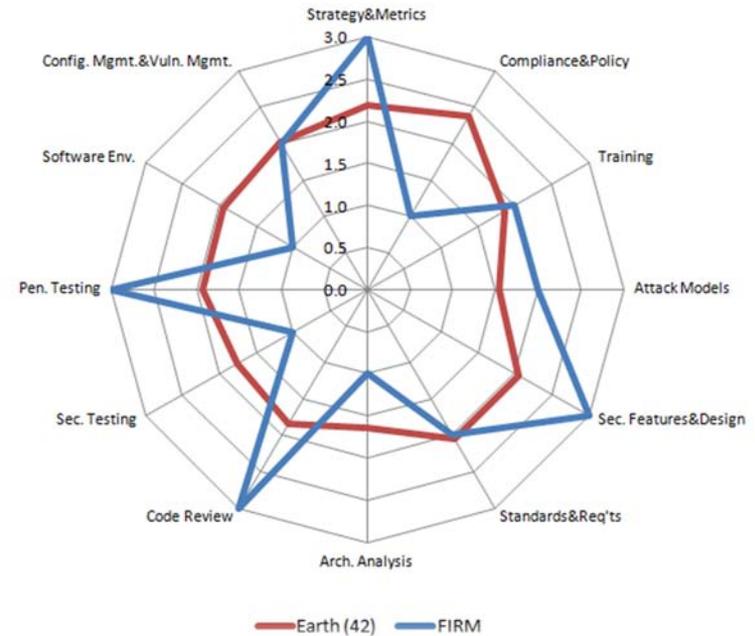
Governance		Intelligence		SSDL Touchpoints		Deployment	
Activity	Observed	Activity	Observed	Activity	Observed	Activity	Observed
[SM1.1]	30	[AM1.1]	13	[AA1.1]	34	[PT1.1]	38
[SM1.2]	26	[AM1.2]	29	[AA1.2]	29	[PT1.2]	32
[SM1.3]	28	[AM1.3]	24	[AA1.3]	24	[PT1.3]	30
[SM1.4]	38	[AM1.4]	13	[AA1.4]	28	[PT2.2]	15
[SM1.6]	30	[AM1.5]	25	[AA2.1]	9	[PT2.5]	20
[SM2.1]	18	[AM2.1]	12	[AA2.2]	6	[PT3.1]	10
[SM2.2]	22	[AM2.2]	12	[AA2.3]	12	[PT3.2]	6
[SM2.3]	22	[AM2.4]	15	[AA3.1]	8		
[SM2.5]	20	[AM3.1]	3	[AA3.2]	4		
[SM3.1]	13	[AM3.2]	5				
[SM3.2]	5						
[CP1.1]	35	[SFD1.1]	37	[CRI.1]	19	[SE1.1]	19
[CP1.2]	38	[SFD1.2]	29	[CRI.2]	20	[SE1.2]	38
[CP1.3]	34	[SFD2.1]	23	[CRI.4]	29	[SE2.2]	19
[CP2.1]	19	[SFD2.2]	15	[CR2.2]	14	[SE2.3]	7
[CP2.2]	27	[SFD2.3]	14	[CR2.3]	19	[SE2.4]	22
[CP2.3]	20	[SFD3.1]	8	[CR2.4]	17	[SE3.2]	11
[CP2.4]	18	[SFD3.2]	9	[CR2.5]	13		
[CP2.5]	26			[CR3.1]	12		
[CP3.1]	7			[CR3.2]	3		
[CP3.2]	11			[CR3.3]	5		
[CP3.3]	8						
[T1.1]	33	[SR1.1]	31	[ST1.1]	32	[CMVM1.1]	33
[T1.2]	11	[SR1.2]	22	[ST1.2]	12	[CMVM1.2]	35
[T1.3]	5	[SR1.3]	25	[ST1.3]	28	[CMVM2.1]	29
[T1.4]	11	[SR1.4]	17	[ST2.1]	20	[CMVM2.2]	27
[T2.1]	16	[SR2.1]	10	[ST2.3]	7	[CMVM3.3]	22
[T2.2]	18	[SR2.2]	17	[ST3.1]	9	[CMVM3.1]	5
[T2.4]	20	[SR2.3]	18	[ST3.2]	9	[CMVM3.2]	6
[T2.5]	9	[SR2.4]	17	[ST3.3]	4		
[T3.1]	6	[SR2.5]	19	[ST3.4]	4		
[T3.2]	4	[SR3.1]	9				
[T3.3]	7						
[T3.4]	6						

- 109 Activities
- 3 levels
- Top 12 activities
 - 69% cutoff
 - 29 of 42 firms
- Comparing scorecards between releases is interesting

BSIMM3 as measuring stick

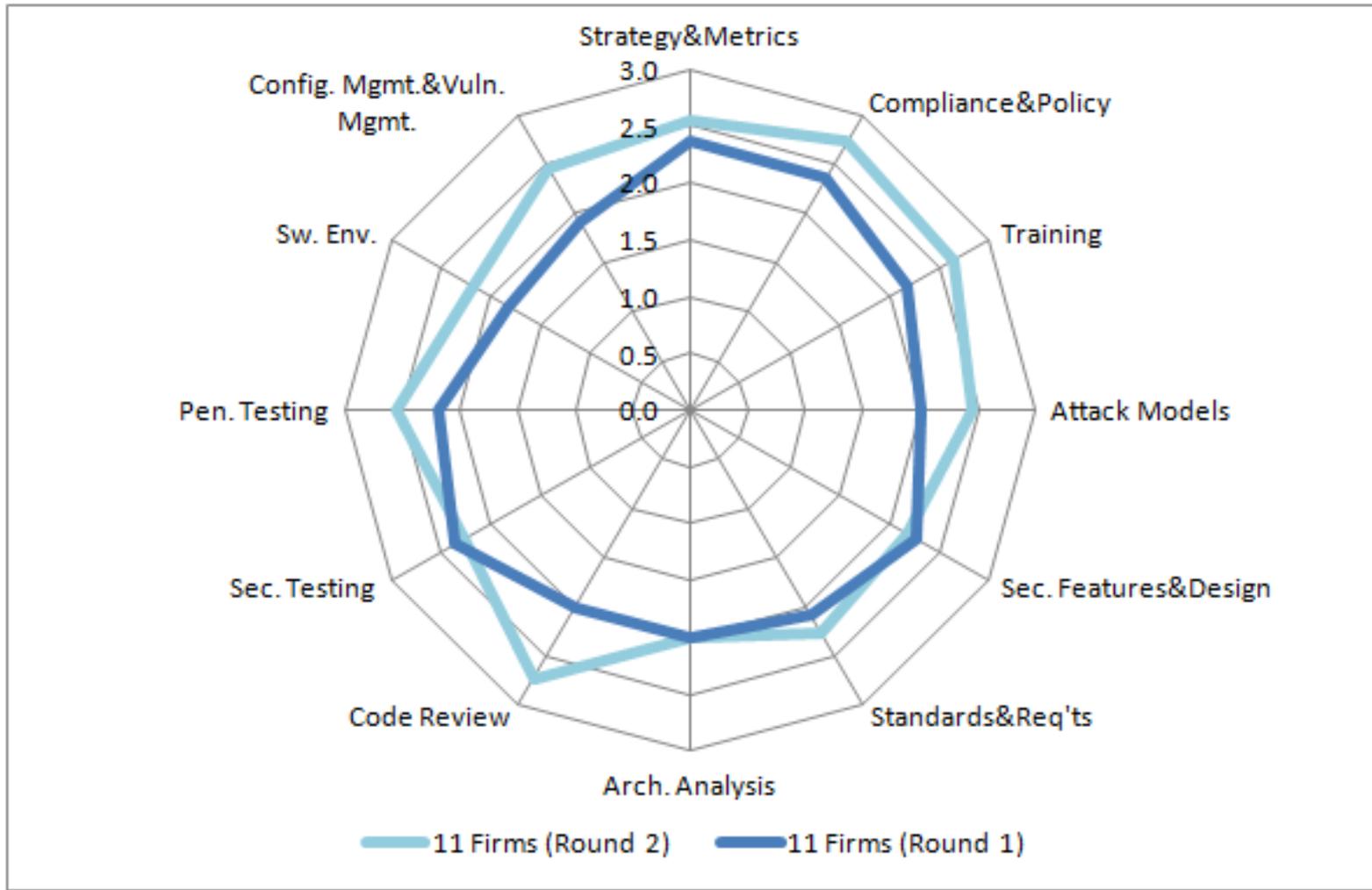
BSIMM Scorecard for: **FIRM** Raw Score: 41

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	Data Pool	FIRM	Activity	Data Pool	FIRM	Activity	Data Pool	FIRM	Activity	Data Pool	FIRM
[SM1.1]	30	1	[AM1.1]	13	1	[AA1.1]	34	1	[PT1.1]	38	1
[SM1.2]	26		[AM1.2]	29	1	[AA1.2]	29	1	[PT1.2]	32	1
[SM1.3]	28		[AM1.3]	24		[AA1.3]	24	1	[PT1.3]	30	
[SM1.4]	38	1	[AM1.4]	13		[AA1.4]	28		[PT2.2]	15	
[SM1.6]	30		[AM1.5]	25	1	[AA2.1]	9		[PT2.3]	20	
[SM2.1]	18		[AM2.1]	12	1	[AA2.2]	6		[PT3.1]	10	1
[SM2.2]	22		[AM2.2]	12	1	[AA2.3]	12		[PT3.2]	6	
[SM2.3]	22		[AM2.4]	15		[AA3.1]	8				
[SM2.5]	20	1	[AM3.1]	3		[AA3.2]	4				
[SM3.1]	13	1	[AM3.2]	5							
[SM3.2]	5										
[CP1.1]	35	1	[SFD1.1]	37	1	[CR1.1]	19	1	[SE1.1]	19	1
[CP1.2]	38	1	[SFD1.2]	29	1	[CR1.2]	20	1	[SE1.2]	38	1
[CP1.3]	34	1	[SFD2.1]	23		[CR1.4]	29	1	[SE2.2]	19	
[CP2.1]	19		[SFD2.2]	15		[CR2.2]	14		[SE2.3]	7	
[CP2.2]	27		[SFD2.3]	14	1	[CR2.3]	19	1	[SE2.4]	22	
[CP2.3]	20		[SFD3.1]	8	1	[CR2.4]	17	1	[SE3.2]	11	
[CP2.4]	18		[SFD3.2]	9		[CR2.5]	13				
[CP2.5]	26					[CR3.1]	12	1			
[CP3.1]	7					[CR3.2]	3				
[CP3.2]	11					[CR3.3]	5	1			
[CP3.3]	8										
[T1.1]	33	1	[SR1.1]	31	1	[ST1.1]	32	1	CMVM1.1	33	1
[T1.2]	11		[SR1.2]	22		[ST1.2]	12	1	CMVM1.2	35	1
[T1.3]	5	1	[SR1.3]	25	1	[ST1.3]	28	1	CMVM2.1	29	1
[T1.4]	11		[SR1.4]	17		[ST2.1]	20		CMVM2.2	27	
[T2.1]	16		[SR2.1]	10	1	[ST2.3]	7		CMVM2.3	22	1
[T2.2]	18	1	[SR2.2]	17		[ST3.1]	9		CMVM3.1	5	
[T2.4]	20		[SR2.3]	18	1	[ST3.2]	9		CMVM3.2	6	
[T2.5]	9	1	[SR2.4]	17		[ST3.3]	4				
[T3.1]	6		[SR2.5]	19	1	[ST3.4]	4				
[T3.2]	4		[SR3.1]	9							
[T3.3]	7										
[T3.4]	6										



Legend: Activity 109 activities from BSIMM, shown in 4 domains and 12 practices
 Data Pool count of firms (out of 42) observed performing this activity
 one of the most commonly observed activities across all participants
 where we did not observe a most common activity
 where we did observe a most common activity
 a practice where the firm's high-water mark score is below the average of the 42 firms
 a data-driven candidate activity for increasing practice maturity

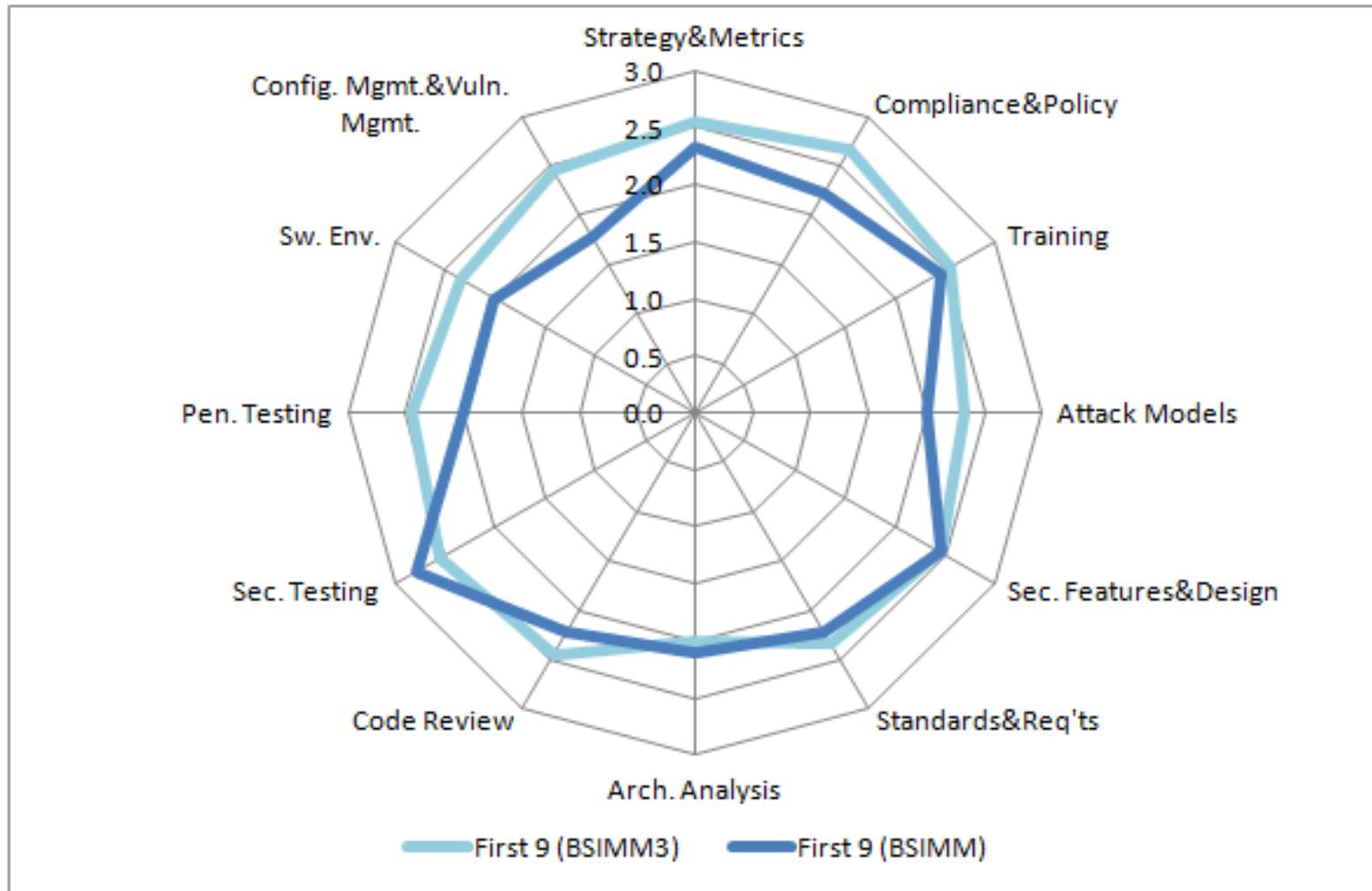
11 “movers and shakers” longitudinal



	S&M	C&P	T	AM	SF&D	S&R	AA	CR	ST	PT	SE	CMVM
% Change	7.1	13.3	17.2	18.5	-4.2	8.0	0.0	26.7	-4.0	14.3	16.7	22.2



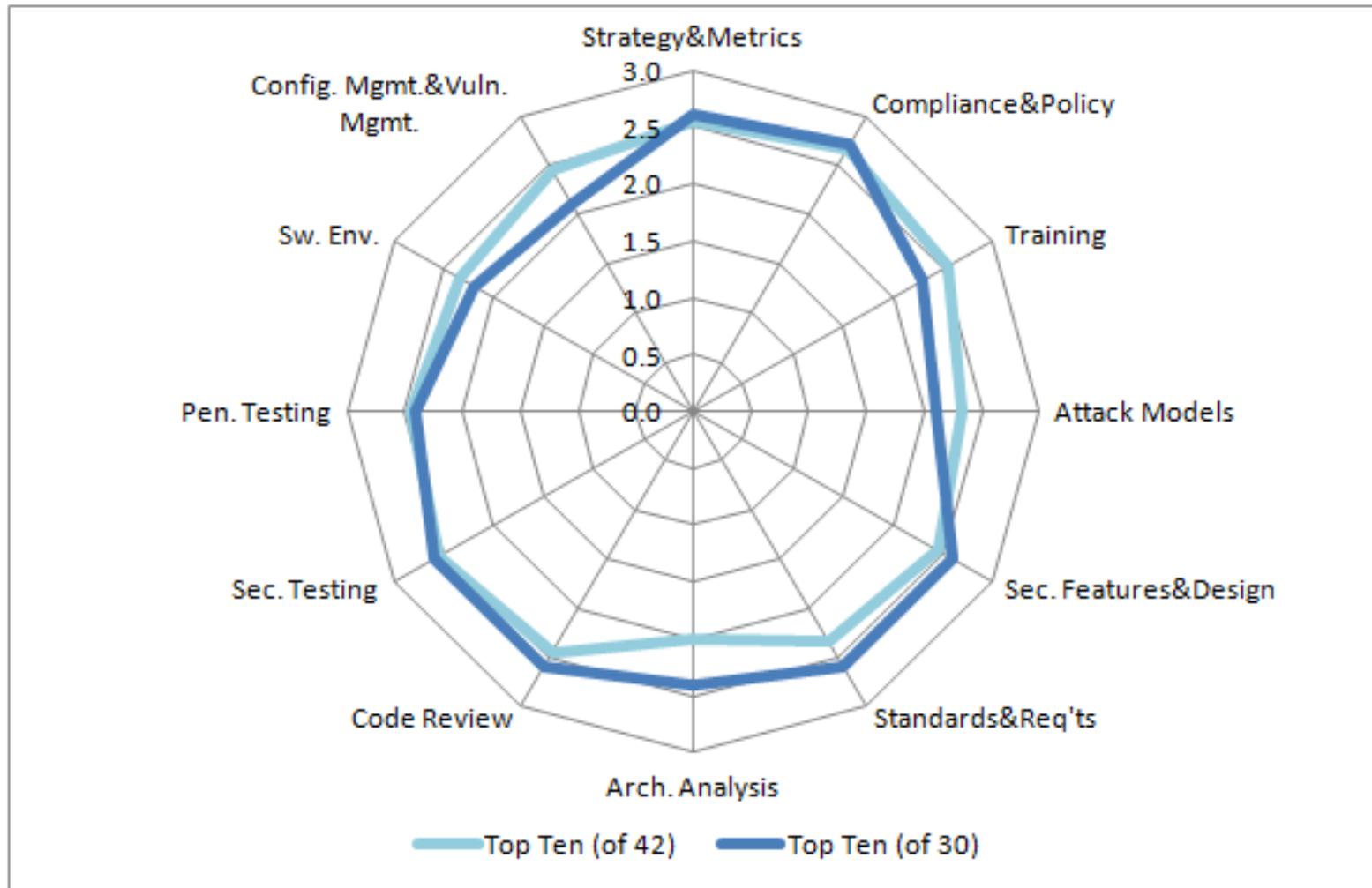
BSIMM9 longitudinal



	S&M	C&P	T	AM	SF&D	S&R	AA	CR	ST	PT	SE	CMVM
% Change	8.7	16.7	4.3	14.3	0.0	4.8	-5.6	9.1	-8.7	18.2	14.3	27.3

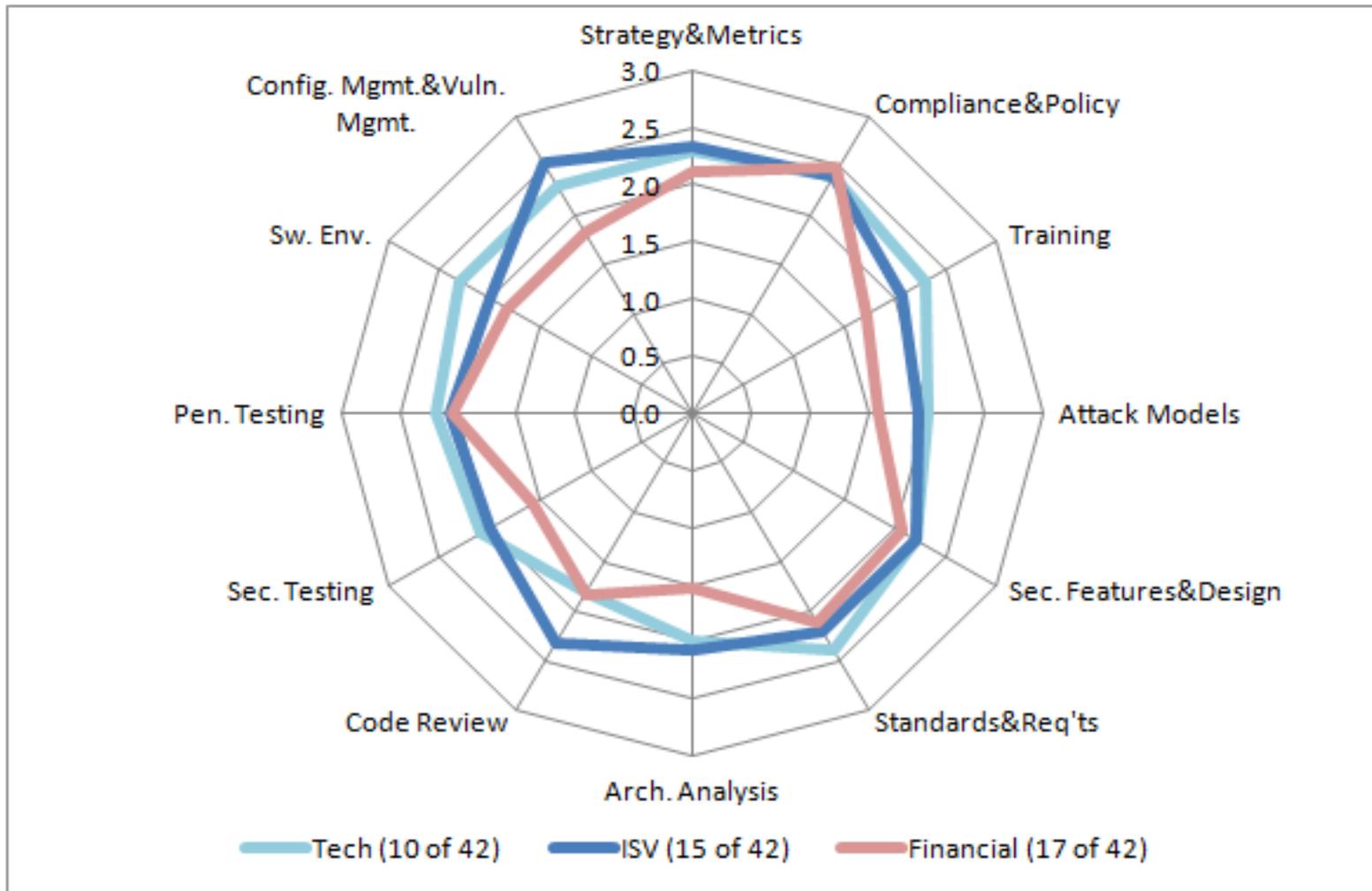


Top ten longitudinal



	S&M	C&P	T	AM	SF&D	S&R	AA	CR	ST	PT	SE	CMVM
% Change	-1.7	-1.3	10.0	10.0	-6.4	-11.4	-20.0	-6.4	-1.7	1.8	5.7	14.1

ISVs and tech pull ahead of financials



What about the government?

The government is **way** behind.



BSIMM3 to BSIMM4

- BSIMM3 released September 2011 under creative commons
 - <http://bsimm.com>
 - Italian and German translations available
- BSIMM is a yardstick
 - Use it to see where you stand
 - Use it to figure out what your peers do
- BSIMM3→BSIMM4
 - BSIMM is growing
 - Target 50 firms
 - Target 100 measurements



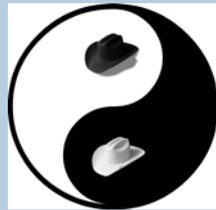
Join the BSIMM Community

- BSIMM Community Conference Annapolis 2010
- BSIMM Mixer RSA 2011
- BSIMM Community Conference Skamania 2011
- BSIMM Mixer RSA 2012
- BSIMM Europe Community Conference Amsterdam 2012
- BSIMM Community Conference <NY/Boston> 2012

- Moderated highly-functional mailing list

- The BSIMM describes the work of 786 full time software security professionals





Where to Learn More

SearchSecurity & Justiceleague Blog



- www.searchsecurity.com
- No-nonsense monthly security column by Gary McGraw debuts in April
- www.cigital.com/~gem/writing

- www.cigital.com/justiceleague
- In-depth thought leadership blog from the Cigital Principals
 - Scott Matsumoto
 - Gary McGraw
 - Sammy Migues
 - John Steven
 - Paco Hope

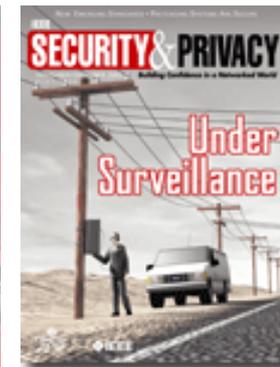
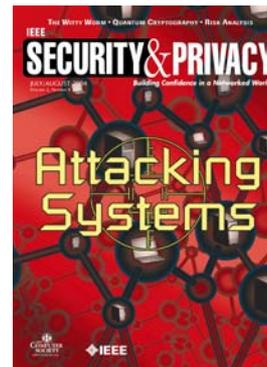


IEEE Security & Privacy + Silver Bullet Podcast

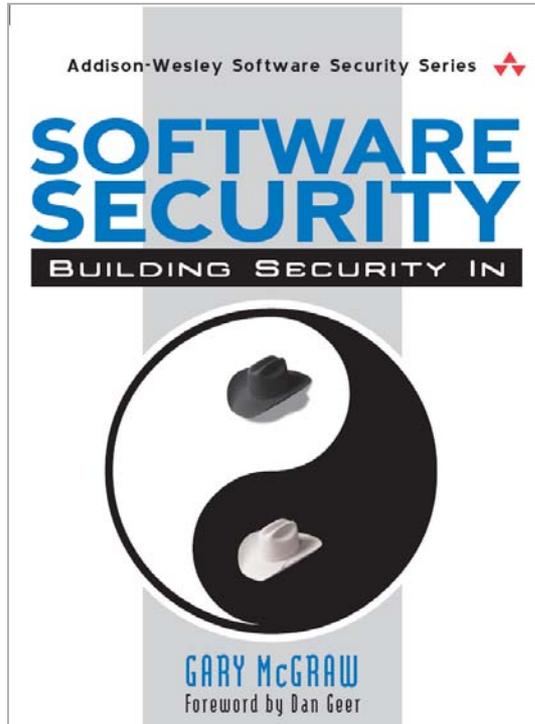


- www.cigital.com/silverbullet

- Building Security In
- Software Security Best Practices column edited by John Steven
- www.computer.org/security/bsisub/



Software Security: The HOW TO Book



- How to DO software security
 - Best practices
 - Tools
 - Knowledge
- Cornerstone of the Addison-Wesley Software Security Series
- www.swsec.com



Get Involved in the BSIMM Community

- <http://bsimm.com>
- **WE NEED GREAT PEOPLE**
- See the Addison-Wesley Software Security series
- Send e-mail: gem@digital.com

“So now, when we face a choice between adding features and resolving security issues, we need to choose security.”

-Bill Gates

