cigital

BSIMM: Building Security In Maturity Model

Carl W. Schwarcz
Managing Consultant, Cigital

cigital

Software Confidence. Achieved.

Presented to Bay Area OWASP

June 2012

Maturity in Secure Development Processes

- We all have ideas about a secure SDLC but ..
  - What works?
  - What is worthwhile (ROI)?
  - What's in vogue this year?
- But, do we have any data to back up adoption?
  - We rely on friends, stories, PR
  - My opinion against yours

cigital

© 2011 Cigital Inc.

New Product!

Carl [tm] Security In A Can

© 2011 Cigital Inc.

Process Model Choice:

Prescriptive
vs
Descriptive

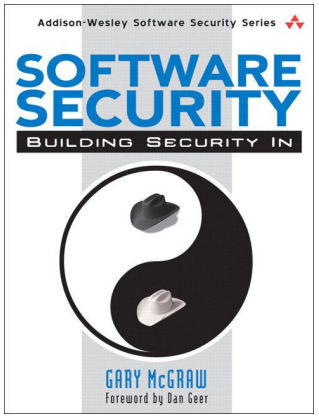
© 2011 Cigital Inc.

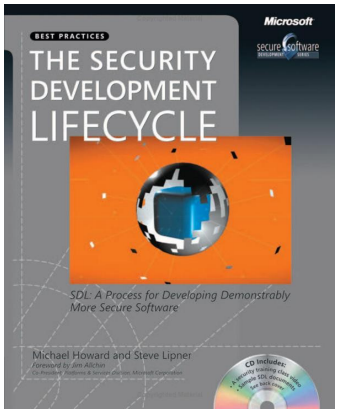
A Brief History of AppSec Best Practices

- NIST SP 800-64
- BS7799/ISO17799/27001-2
- OCTAVE
- Microsoft's SDL
- Cigital's touchpoints
- OWASP CLASP

~1990

~2006





cigital

© 2011 Cigital Inc.

What if you could collect real data?

Sony Ericsson

The Depository Trust & Clearing Corporation

+ 14 others

© 2011 Cigital Inc.

BSIMM: Software Security Measurement

McGraw, Migues, Chess

cigital

PlexLogic

FORTIFY

CSO

Minded security

VIRTUALFORGE
we harden your software

- Idea: Build a maturity model from actual data gathered from real-world software security initiatives
- Interview firms in-person
- Discover common activities through observation
- Build scorecard

© 2011 Cigital Inc.

The Evolution of BSIMM

- We now have over 42 firms with 81 distinct measurements
  - 2009: BSIMM (9 firms)
  - 2009: BSIMM Europe (9 in EU)
  - 2010: BSIMM2 (30)
  - 2011: BSIMM3 (42), Creative Commons license
- Since we have data from > 30 firms we can perform statistical analysis
  - How good is the model?
  - What activities correlate with what other activities?
  - Do high-maturity firms look the same?

cigital

© 2011 Cigital Inc.

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

bsimm.com/facts

cigital

© 2011 Cigital Inc.

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**, 109 **activities**
- Derived from observation of the first 9 firms, updated since
- A common vocabulary, NOT a methodology

cigital

© 2011 Cigital Inc.

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)	

cigital

© 2011 Cigital Inc.

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.

cigital

© 2011 Cigital Inc.

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: 5,183
  - Smallest: 11
  - Largest: 30,000
  - Median: 1675

SSG ratio to dev averages ~1-2%

cigital

© 2011 Cigital Inc.

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	[PT2.3]	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	[CR1.1]	19	[SE1.1]	19
[CP1.2]	38	[SFD1.2]	29	[CR1.2]	20	[SE1.2]	38
[CP1.3]	34	[SFD2.1]	23	[CR1.4]	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	[CMVM2.3]	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						

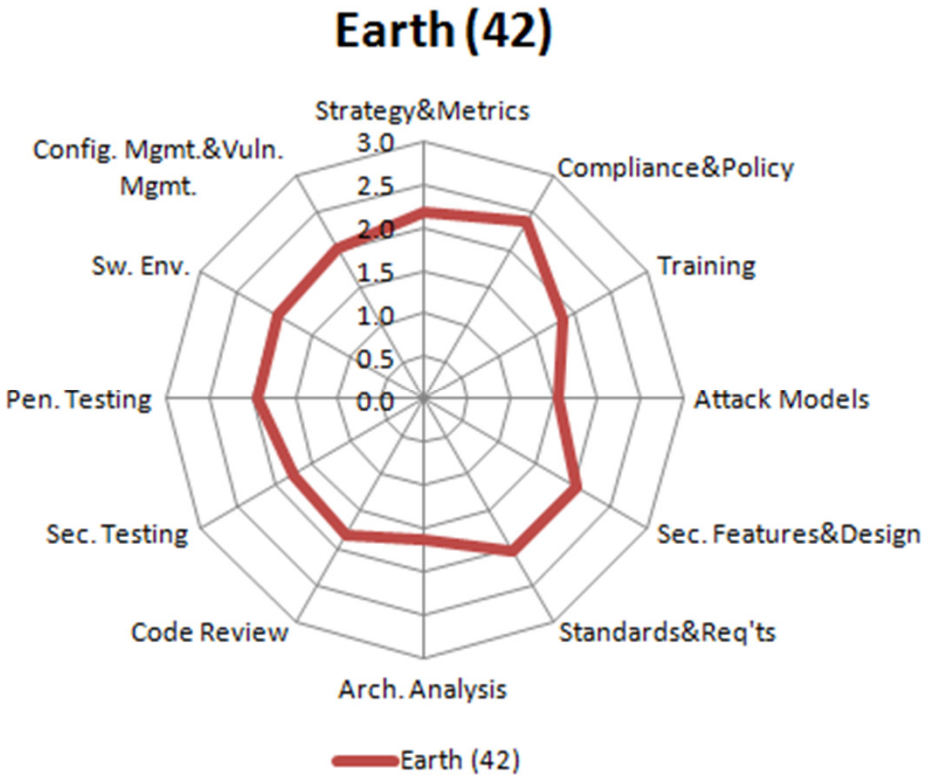
- 109 Activities
- 3 levels
- Top 12 activities
  - 69% cutoff
  - 29 of 42 firms
- Comparing scorecards between releases is interesting

cigital

© 2011 Cigital Inc.

Twelve things “everybody” does (well, 66%)

- Core activities
  - identify gates
  - know PII obligations
  - awareness training
  - data classification
  - identify features
  - security standards
  - review security features
  - static analysis tool
  - QA boundary testing
  - external pen testers
  - good network security
  - close ops bugs loop

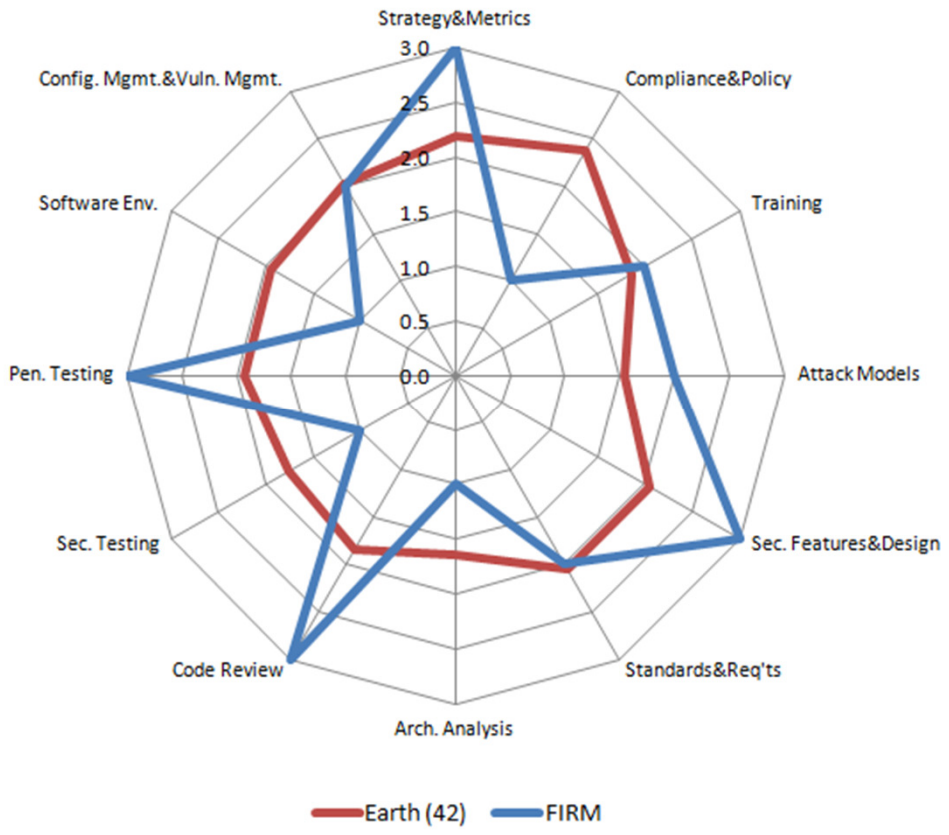


cigital

© 2011 Cigital Inc.

BSIMM3 as a measuring stick

- Compare a (fake) firm with peers using the high water mark view
- Descriptive (not prescriptive)
- Incredible insight for planning



cigital

© 2011 Cigital Inc.

BSIMM3 scorecard with firm data

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		[PT1.1]	38	
[SM1.2]	26		[AM1.2]	29		[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		[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		[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	
[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										

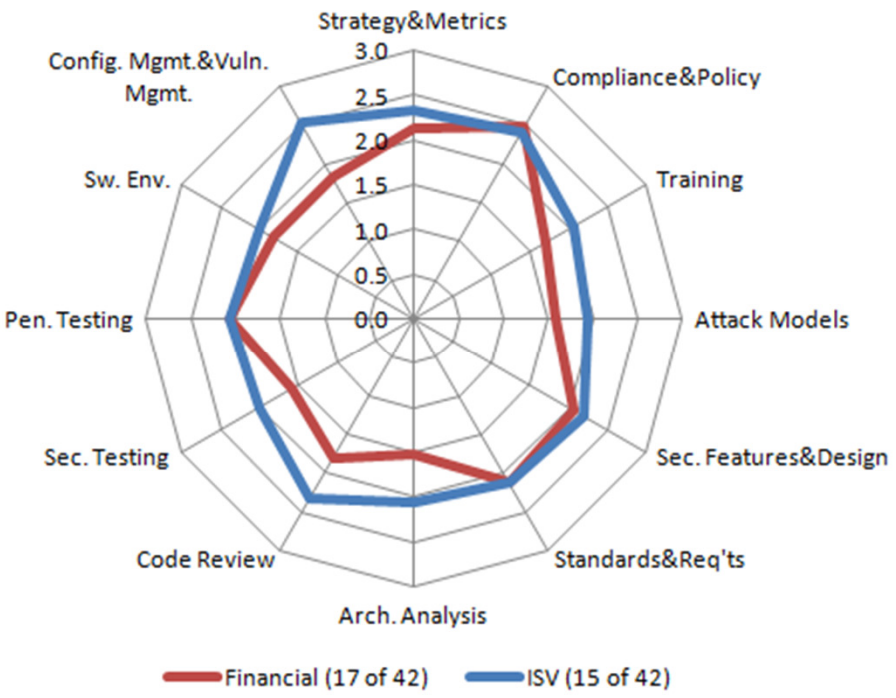
Legend:
- Activity: 109 activities from BSIMM, shown in 4 domains and 12 practices
- Data Pool: count of firms (out of 42) observed performing this activity
- one of the most commonly observed activities across all participants
- where we did not observe a most common activity
- where we did observe 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

- Top 12 activities
  - green = good?
  - red = bad?
- "Blue shift" practices to emphasize
  - activities you should maybe think about in blue

cigital

© 2011 Cigital Inc.

We are a special snowflake (NOT)

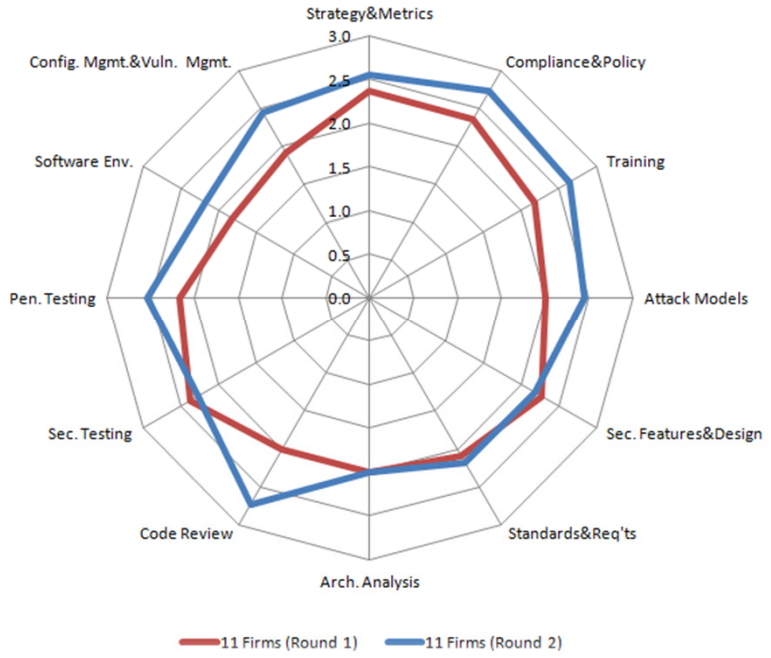


- ISV (15) results are similar to financial services (17)
- You do the same things
- You can demand the same results
- Measurement works for all

cigital

© 2011 Cigital Inc.

BSIMM Longitudinal: Improvement over time



- 11 firms measured twice (19 months apart)
- BSIMM measurements show how firms improve
  - 32% increase

cigital

© 2011 Cigital Inc.

BSIMM Over Time (3 studies)

Governance				Intelligence				SSDL Touchpoints				Deployment			
Activity	BSIMM3 Observed (of 42)	BSIMM2 Observed (of 30)	BSIMM Observed (of 9)	Activity	BSIMM3 Observed (of 42)	BSIMM2 Observed (of 30)	BSIMM Observed (of 9)	Activity	BSIMM3 Observed (of 42)	BSIMM2 Observed (of 30)	BSIMM Observed (of 9)	Activity	BSIMM3 Observed (of 42)	BSIMM2 Observed (of 30)	BSIMM Observed (of 9)
[SM1.1]	30	18	4	[AM1.1]	13	12	5	[AA1.1]	34	22	5	[PT1.1]	38	28	9
[SM1.2]	26	18	8	[AM1.2]	29	20	6	[AA1.2]	29	18	4	[PT1.2]	32	17	2
[SM1.3]	28	16	6	[AM1.3]	24	14	2	[AA1.3]	24	19	8	[PT1.3]	30	17	3
[SM1.4]	38	24	7	[AM1.4]	13	10	7	[AA1.4]	28	15	3	[PT2.2]	15	10	2
[SM1.6]	30	13	7	[AM1.5]	25	7	3	[AA2.1]	9	9	4	[PT2.3]	20	11	1
[SM2.1]	18	12	7	[AM2.1]	12	9	6	[AA2.2]	6	6	2	[PT3.1]	10	9	2
[SM2.2]	22	13	4	[AM2.2]	12	13	5	[AA2.3]	12	11	5	[PT3.2]	6	5	2
[SM2.3]	22	16	7	[AM2.4]	15	9	5	[AA3.1]	8	5	2				
[SM2.5]	20	19	4	[AM3.1]	3	2	1	[AA3.2]	4	3	1				
[SM3.1]	13	7	3	[AM3.2]	5	2	1								
[SM3.2]	5	4	1												
[CP1.1]	35	24	6	[SFD1.1]	37	29	9	[CR1.1]	19	10	3	[SE1.1]	19	11	2
[CP1.2]	38	24	6	[SFD1.2]	29	16	6	[CR1.2]	20	19	7	[SE1.2]	38	30	9
[CP1.3]	34	26	9	[SFD2.1]	23	18	6	[CR1.4]	29	20	8	[SE2.2]	19	16	4
[CP2.1]	19	13	3	[SFD2.2]	15	11	5	[CR2.2]	14	11	5	[SE2.3]	7	7	2
[CP2.2]	27	18	4	[SFD2.3]	14	10	4	[CR2.3]	19	8	4	[SE2.4]	22	13	3
[CP2.3]	20	13	5	[SFD3.1]	8	5	1	[CR2.4]	17	12	5	[SE3.2]	11	6	1
[CP2.4]	18	9	3	[SFD3.2]	9	10	5	[CR2.5]	13	11	5				
[CP2.5]	26	17	5					[CR3.1]	12	7	2				
[CP3.1]	7	4	1					[CR3.2]	3	1	1				
[CP3.2]	11	7	2					[CR3.3]	5	2	1				
[CP3.3]	8	5	2												
[T1.1]	33	24	9	[SR1.1]	31	22	5	[ST1.1]	32	21	5	[CMVM1.1]	33	21	4
[T1.2]	11	6	5	[SR1.2]	22	13	3	[ST1.2]	12	9	5	[CMVM1.2]	35	22	6
[T1.3]	5	5	5	[SR1.3]	25	12	3	[ST1.3]	28	18	9	[CMVM2.1]	29	18	6
[T1.4]	11	11	7	[SR1.4]	17	11	4	[ST2.1]	20	16	2	[CMVM2.2]	27	11	4
[T2.1]	16	14	6	[SR2.1]	10	10	3	[ST2.3]	7	5	3	[CMVM2.3]	22	11	2
[T2.2]	18	13	8	[SR2.2]	17	8	1	[ST3.1]	9	7	5	[CMVM3.1]	5	2	1
[T2.4]	20	14	6	[SR2.3]	18	13	4	[ST3.2]	9	10	7	[CMVM3.2]	6	4	2
[T2.5]	9	7	4	[SR2.4]	17	13	5	[ST3.3]	4	3	2				
[T3.1]	6	4	2	[SR2.5]	19	11	4	[ST3.4]	4	4	2				
[T3.2]	4	3	1	[SR3.1]	9	10	3								
[T3.3]	7	4	1												
[T3.4]	6	2	1												

cigital

© 2011 Cigital Inc.

How will you use it?

- Gap assessment
  - Building a new program
  - Evolving an existing program
- Benchmark
  - How are we doing relative to the “market”? Peers?
  - How are we doing over time?
- Business justification
  - Spend more here, less there
  - Data-driven, management approved ☺
- Internal alignment
  - Business unit A vs. B vs. central policy etc.
- Assess 3rd parties

cigital

© 2011 Cigital Inc.

Get Involved

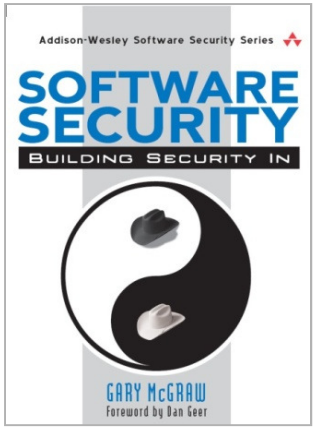
- http://bsimm.com
- WE NEED MORE FIRMS TO MEASURE

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

-Bill Gates

cschwarcz at Cigital.com

More info from CTO, Gary McGraw and other Cigital-ites:



www.informIT.com
www.cigital.com/justiceleague
www.cigital.com/silverbullet
www.computer.org/security/bsisub/
www.swsec.com

cigital

© 2011 Cigital Inc.

Membership Has Its Benefits

- The 42 firms participating in the BSIMM Project make up the BSIMM Community.
- BSIMM Community resources include:
  - A moderated private mailing list
  - An annual BSIMM Conference (invitation only)
  - A members only section of the BSIMM web site.

cigital

© 2011 Cigital Inc.

References

- bsimm.com/facts
- bsimm.com/resources
- “Cargo Cult Computer Security” (January 28, 2010); http://www.informit.com/articles/article.aspx?p=1562220
- A Software Security Framework: Working Towards a Realistic Maturity Model (October 15, 2008); http://www.informit.com/articles/article.aspx?p=1271382
- “You Really Need a Software Security Group” (December 21, 2009); http://www.informit.com/articles/article.aspx?p=1434903
- vBSIMM; http://bsimm.com/vbsimm/
- vBSIMM article on InformIT; http://www.informit.com/articles/article.aspx?p=1832574

cigital

© 2011 Cigital Inc.