cigital

Building Security In Maturity Model

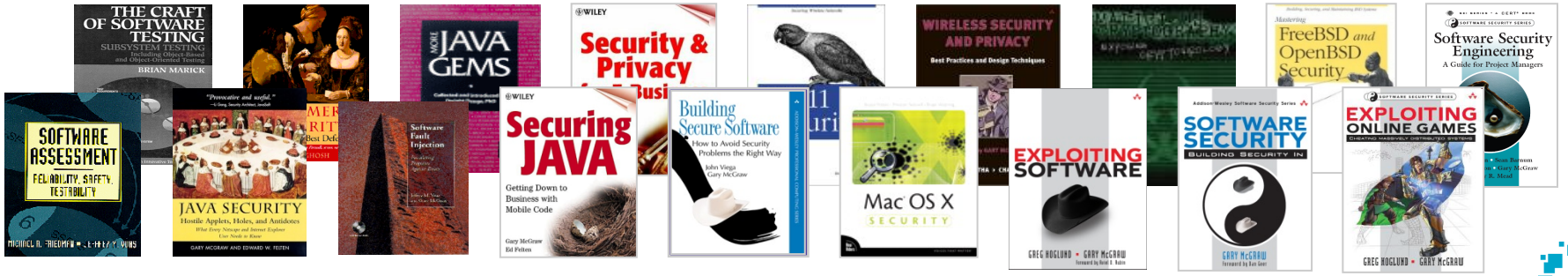
Gary McGraw, Ph.D.
Chief Technology Officer, Cigital

Software Confidence. Achieved.

October 2009

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



cigital

© 2009 Cigital Inc.

We hold these truths to be self-evident

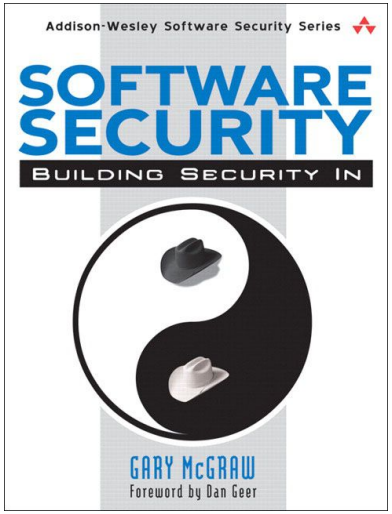
- Software security is more than a set of security functions
  - Not magic crypto fairy dust
  - Not silver-bullet security mechanisms
- Non-functional aspects of design are essential
- Bugs and flaws are 50/50
- Security is an emergent property of the entire system (just like quality)
- To end up with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

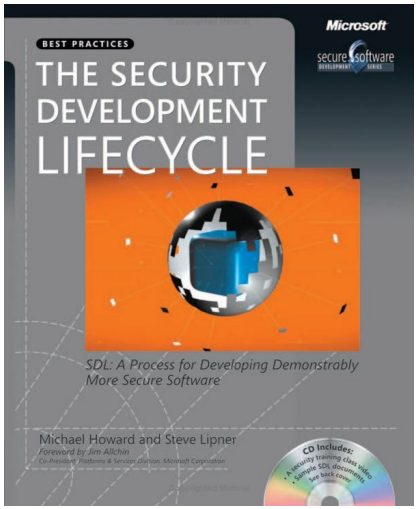
cigital

© 2009 Cigital Inc.

A shift from philosophy to HOW TO

- Integrating best practices into large organizations
  - Microsoft's SDL
  - Cigital's touchpoints
  - OWASP adopts CLASP





cigital

© 2009 Cigital Inc.

Breaking new ground

- Building Security In Maturity Model
- Real data from real initiatives
- McGraw, Chess, & Migues

cigital

FORTIFY

© 2009 Cigital Inc.

46 software security initiatives

- 26 Financial
- 7 ISV
- 6 Tech
- 2 Defense
- 3 Retail
- 1 Oil
- 1 Behemoth

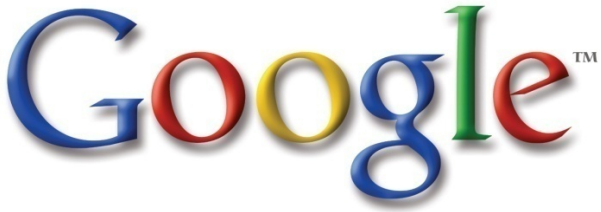
- visa europe
- thomson/reuters
- BP
- SAP
- nokia
- ABN/amro
- ING
- telecom italia
- swift
- standard life
- microsoft
- dtcc
- emc
- fidelity
- adobe
- wells fargo
- goldman sachs
- google
- qualcomm
- morgan stanley
- usaf
- dell
- pershing
- the hartford
- barclays capital
- bank of tokyo
- ups
- bank of montreal
- cisco
- bank of america
- walmart
- finra
- vanguard
- college board
- oracle
- state street
- omgeo
- motorola
- general electric
- lockheed martin
- intuit
- vmware
- amex
- bank of ny mellon
- harris bank
- paypal

cigital

© 2009 Cigital Inc.

The (original) nine

Adobe



The Depository Trust & Clearing Corporation

Two more unnamed financial services firms

cigital

© 2009 Cigital Inc.

Building BSIMM

- Big idea: Build a maturity model from actual data gathered from 9 of 46 known large-scale software security initiatives

- Create a software security framework
- Nine in-person executive interviews
- Build bullet lists (one per practice)
- Bucketize the lists to identify activities
- Create levels
  - Objectives → Activities
  - 110 activities supported by real data
  - Three levels of “maturity”

cigital

© 2009 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
- An “archeology grid”
- See informIT article at http://bsi-mm.com

cigital

© 2009 Cigital Inc.

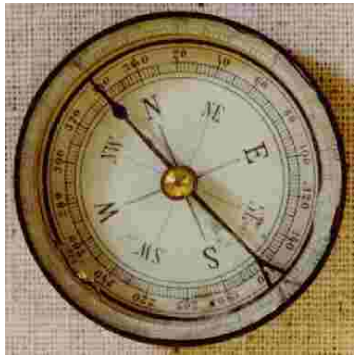
Monkeys eat bananas

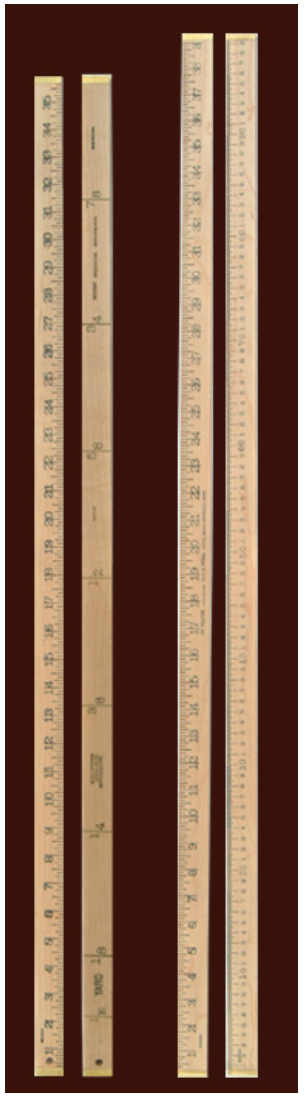
- BSIMM is not about good or bad ways to eat bananas or banana best practices
- BSIMM is about observations

cigital

© 2009 Cigital Inc.

On cargo cults and divining rods





cigital

© 2009 Cigital Inc.

Real-world data: the nine

- Initiative age: 5yrs 4months avg.
  - Newest: 2.5
  - Oldest: 10
- SSG size: 41
  - Smallest: 12
  - Largest: 100
  - Median: 35
- Satellite size: 79
  - Smallest: 0
  - Largest: 300
  - Median: 20
- Dev size: 7750
  - Smallest: 450
  - Largest: 30,000
  - Median: 5000

Average SSG size: 1% of dev

cigital

© 2009 Cigital Inc.

Ten surprising things

1. Bad metrics hurt
2. Secure-by default frameworks
3. Nobody uses WAFs
4. QA can't do software security
5. Evangelize over audit
6. ARA is hard
7. Practitioners don't talk attacks
8. Training is advanced
9. Pen testing is diminishing
10. Fuzz testing

- InformIT article on BSIMM website http://bsi-mm.com

cigital

© 2009 Cigital Inc.

BSIMM basics

- Software security framework
- Top-down presentation through GOALS and OBJECTIVES
- 110 activities with examples
- Three levels of maturity
- Discussion of how to use the model

cigital

© 2009 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
- See informIT article on BSIMM website http://bsi-mm.com

cigital

© 2009 Cigital Inc.

Training practice skeleton

	GOVERNANCE: TRAINING		
	Objective	**Activity**	**Level**
[T1.1]	promote culture of security throughout the organization	provide awareness training	1
[T1.2]	ensure new hires enhance culture	include security resources in onboarding	
[T1.3]	act as informal resource to leverage teachable moments	establish SSG office hours	
[T1.4]	create social network tied into dev	identify satellite during training	
[T2.1]	build capabilities beyond awareness	offer role-specific advanced curriculum (tools, technology stacks, bug parade)	2
[T2.2]	see yourself in the problem	create/use material specific to company history	
[T2.3]	keep staff up-to-date and address turnover	require annual refresher	
[T2.4]	reduce impact on training targets and delivery staff	offer on-demand individual training	
[T2.5]	educate/strengthen social network	hold satellite training/events	
[T3.1]	align security culture with career path	reward progression through curriculum (certification or HR)	3
[T3.2]	spread security culture to providers	provide training for vendors or outsource workers	
[T3.3]	market security culture as differentiator	host external software security events	

cigital

© 2009 Cigital Inc.

Example activity

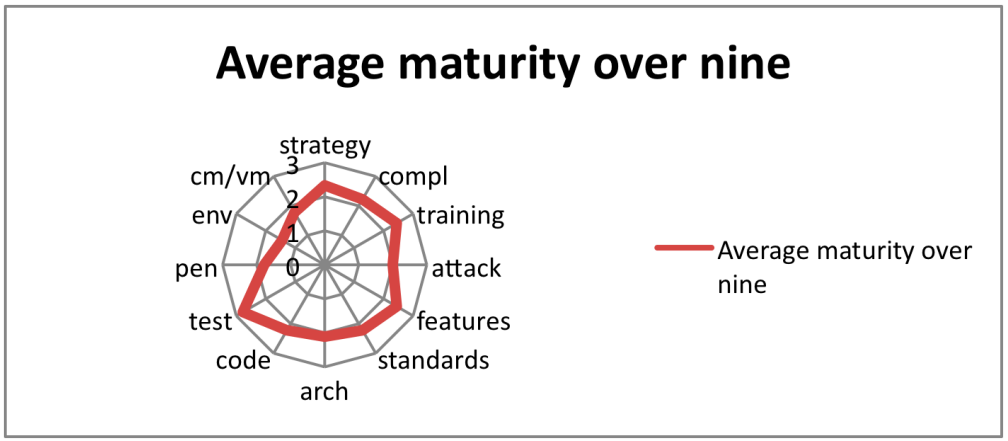
[T1.3] **Establish SSG office hours.** The SSG offers help to any and all comers during an advertised lab period or regularly scheduled office hours. By acting as an informal resource for people who want to solve security problems, the SSG leverages teachable moments and emphasizes the carrot over the stick. Office hours might be held one afternoon per week in the office of a senior SSG member.

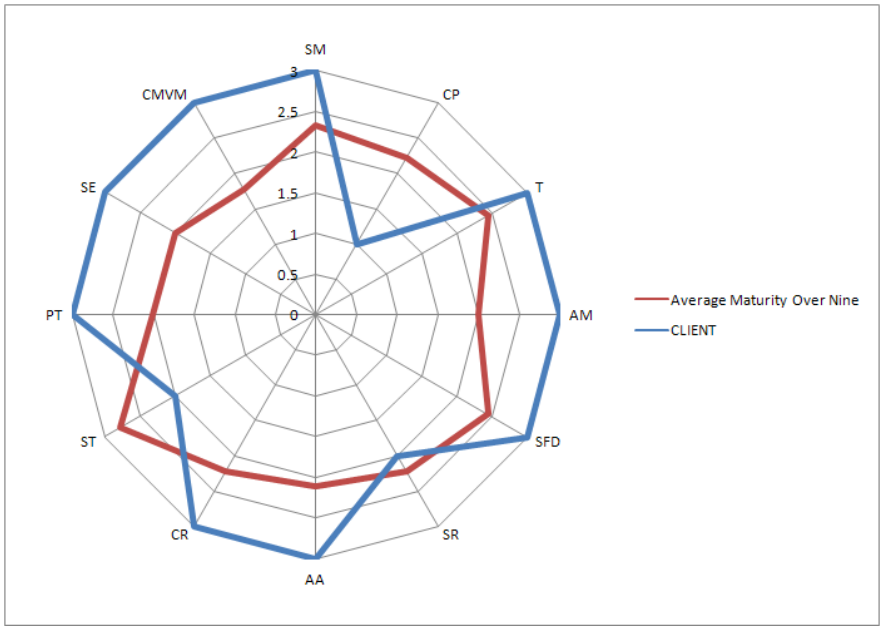
cigital

© 2009 Cigital Inc.

Ten things everybody does

- Activities that ALL do
  - evangelist role
  - policy
  - awareness training
  - history in training
  - security features
  - SSG does ARA
  - code review tools
  - black box tools
  - external pen testing
  - good network security





cigital

© 2009 Cigital Inc.

BSIMM Scorecard

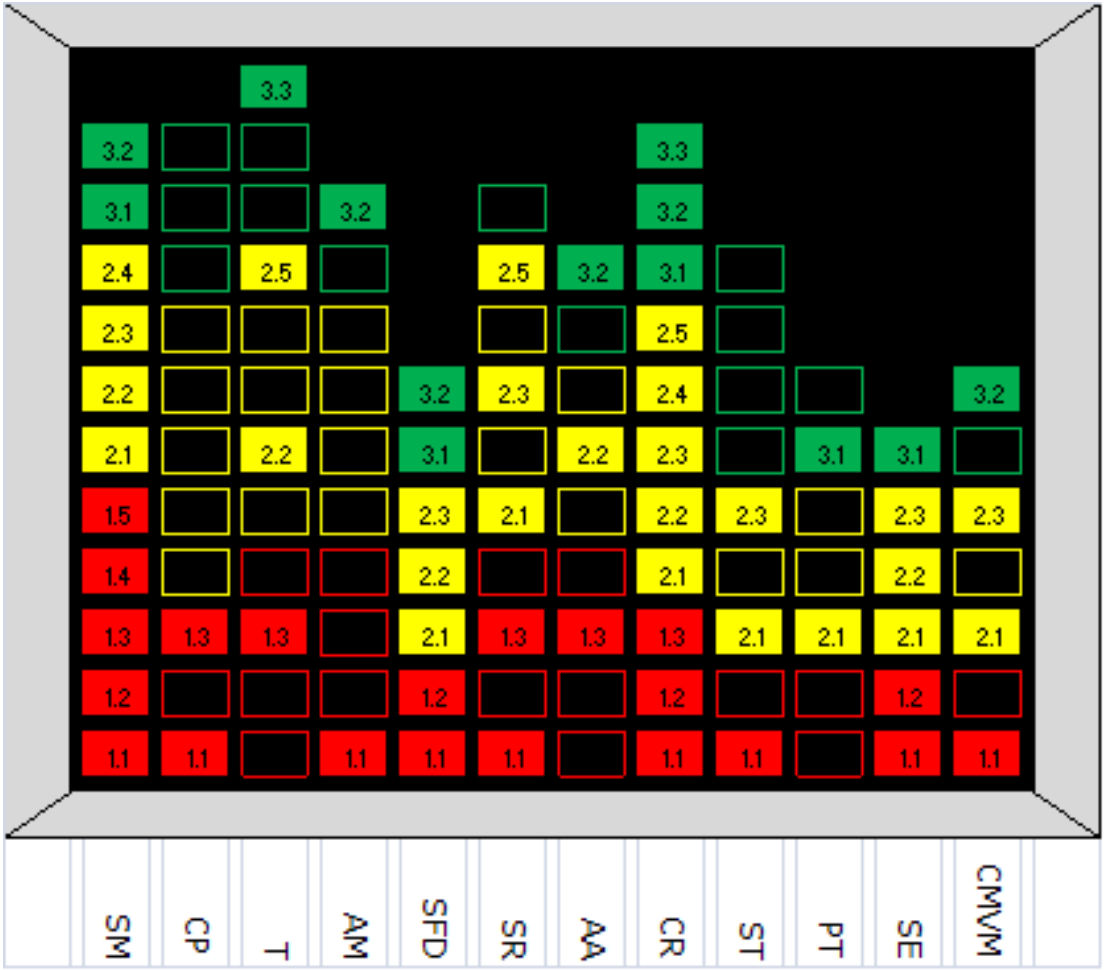
Governance			Intelligence			SDL Touchpoints			Deployment		
Activity	*Observed*	CLIENT	Activity	*Observed*	CLIENT	Activity	*Observed*	CLIENT	Activity	*Observed*	CLIENT
[SM1.1]	*4*	1	[AM1.1]	*5*	1	[AA1.1]	*5*		[PT1.1]	*9*	
[SM1.2]	*8*	1	[AM1.2]	*6*		[AA1.2]	*4*		[PT1.2]	*2*	
[SM1.3]	*6*	1	[AM1.3]	*2*		[AA1.3]	*8*	1	[PT2.1]	*3*	1
[SM1.4]	*7*	1	[AM1.4]	*7*		[AA1.4]	*3*		[PT2.2]	*2*	
[SM1.5]	*7*	1	[AM2.1]	*3*		[AA2.1]	*4*		[PT2.3]	*1*	
[SM2.1]	*7*	1	[AM2.2]	*6*		[AA2.2]	*2*	1	[PT3.1]	*2*	1
[SM2.2]	*4*	1	[AM2.3]	*5*		[AA2.3]	*5*		[PT3.2]	*2*	
[SM2.3]	*7*	1	[AM2.4]	*5*		[AA3.1]	*2*				
[SM2.4]	*4*	1	[AM3.1]	*1*		[AA3.2]	*1*	1			
[SM3.1]	*3*	1	[AM3.2]	*1*	1						
[SM3.2]	*1*	1									
[CP1.1]	*6*	1	[SFD1.1]	*9*	1	[CR1.1]	*3*	1	[SE1.1]	*2*	1
[CP1.2]	*6*		[SFD1.2]	*6*	1	[CR1.2]	*7*	1	[SE1.2]	*9*	1
[CP1.3]	*9*	1	[SFD2.1]	*6*	1	[CR1.3]	*3*	1	[SE2.1]	*1*	1
[CP2.1]	*3*		[SFD2.2]	*5*	1	[CR2.1]	*7*	1	[SE2.2]	*4*	1
[CP2.2]	*4*		[SFD2.3]	*4*	1	[CR2.2]	*5*	1	[SE2.3]	*2*	1
[CP2.3]	*5*		[SFD3.1]	*1*	1	[CR2.3]	*4*	1	[SE3.1]	*3*	1
[CP2.4]	*3*		[SFD3.2]	*5*	1	[CR2.4]	*5*	1			
[CP2.5]	*5*					[CR2.5]	*5*	1			
[CP3.1]	*1*					[CR3.1]	*2*	1			
[CP3.2]	*2*					[CR3.2]	*1*	1			
[CP3.3]	*2*					[CR3.3]	*1*	1			
[T1.1]	*9*		[SR1.1]	*5*	1	[ST1.1]	*5*	1	[CMVM1.1]	*4*	1
[T1.2]	*5*		[SR1.2]	*3*		[ST1.2]	*5*		[CMVM1.2]	*6*	
[T1.3]	*5*	1	[SR1.3]	*3*	1	[ST2.1]	*9*	1	[CMVM2.1]	*6*	1
[T1.4]	*7*		[SR1.4]	*4*		[ST2.2]	*2*		[CMVM2.2]	*4*	
[T2.1]	*6*		[SR2.1]	*3*	1	[ST2.3]	*3*	1	[CMVM2.3]	*2*	1
[T2.2]	*8*	1	[SR2.2]	*1*		[ST3.1]	*5*		[CMVM3.1]	*1*	
[T2.3]	*1*		[SR2.3]	*4*	1	[ST3.2]	*7*		[CMVM3.2]	*2*	1
[T2.4]	*6*		[SR2.4]	*5*		[ST3.3]	*2*				
[T2.5]	*4*	1	[SR2.5]	*4*	1	[ST3.4]	*2*				
[T3.1]	*2*		[SR3.1]	*3*							
[T3.2]	*1*										
[T3.3]	*1*	1									

- Top 10 things
  - green = good?
  - red = bad?
- Blue shift practices to emphasize
  - activities you should maybe think about in blue

cigital

© 2009 Cigital Inc.

BSIMM Equalizer

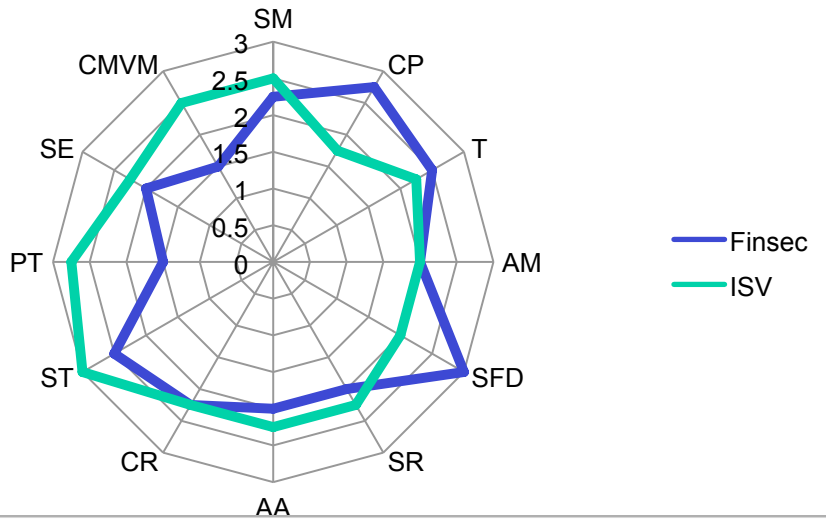


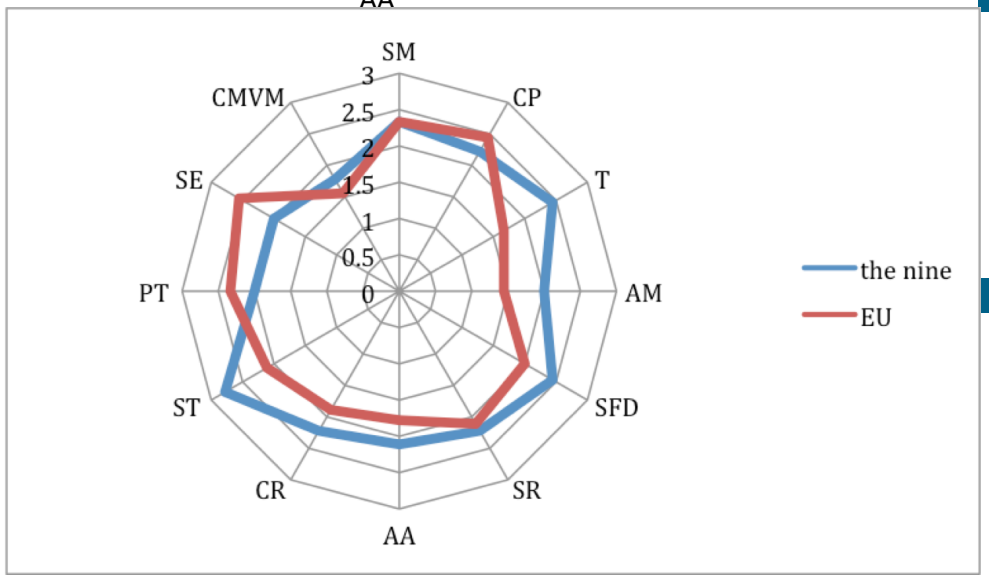
- What you do (by level)
- Gaps are apparent and lead to good conversation

cigital

© 2009 Cigital Inc.

We are a special snowflake (NOT)





- ISV results are similar to financial services
- You do the same things
- You can demand the same results
- BSIMM Europe coming Nov 8!

cigital

© 2009 Cigital Inc.

BSIMM Europe (brand new results)

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.
[SM1.1]	4	8	[AM1.1]	5	4	[AA1.1]	5	8	[PT1.1]	9	9
[SM1.2]	8	5	[AM1.2]	6	7	[AA1.2]	4	6	[PT1.2]	2	8
[SM1.3]	6	4	[AM1.3]	2	6	[AA1.3]	8	6	[PT2.1]	3	6
[SM1.4]	7	9	[AM1.4]	7	1	[AA1.4]	3	4	[PT2.2]	2	4
[SM1.5]	7	6	[AM2.1]	3	1	[AA2.1]	4	3	[PT2.3]	1	5
[SM2.1]	7	3	[AM2.2]	6	1	[AA2.2]	2	4	[PT3.1]	2	3
[SM2.2]	4	7	[AM2.3]	5	5	[AA2.3]	5	3	[PT3.2]	2	1
[SM2.3]	7	3	[AM2.4]	5	0	[AA3.1]	2	2			
[SM2.4]	4	8	[AM3.1]	1	0	[AA3.2]	1	1			
[SM3.1]	3	2	[AM3.2]	1	0						
[SM3.2]	1	2									
[CP1.1]	6	7	[SFD1.1]	9	8	[CR1.1]	3	5	[SE1.1]	2	3
[CP1.2]	6	8	[SFD1.2]	6	6	[CR1.2]	7	5	[SE1.2]	9	9
[CP1.3]	9	8	[SFD2.1]	6	4	[CR1.3]	3	0	[SE2.1]	1	3
[CP2.1]	3	3	[SFD2.2]	5	4	[CR2.1]	8	6	[SE2.2]	4	5
[CP2.2]	4	7	[SFD2.3]	4	3	[CR2.2]	5	3	[SE2.3]	2	2
[CP2.3]	5	4	[SFD3.1]	1	1	[CR2.3]	4	2	[SE3.1]	3	6
[CP2.4]	3	4	[SFD3.2]	5	3	[CR2.4]	5	4			
[CP2.5]	5	5				[CR2.5]	5	2			
[CP3.1]	1	1				[CR3.1]	2	2			
[CP3.2]	2	3				[CR3.2]	1	0			
[CP3.3]	2	0				[CR3.3]	1	0			
[T1.1]	9	6	[SR1.1]	5	9	[ST1.1]	5	5	[CMVM1.1]	4	6
[T1.2]	5	1	[SR1.2]	3	2	[ST1.2]	5	0	[CMVM1.2]	6	6
[T1.3]	5	0	[SR1.3]	3	3	[ST2.1]	9	5	[CMVM2.1]	6	4
[T1.4]	7	2	[SR1.4]	4	6	[ST2.2]	2	6	[CMVM2.2]	4	3
[T2.1]	6	5	[SR2.1]	3	5	[ST2.3]	3	1	[CMVM2.3]	2	2
[T2.2]	8	3	[SR2.2]	1	2	[ST3.1]	5	0	[CMVM3.1]	1	0
[T2.3]	1	0	[SR2.3]	4	4	[ST3.2]	7	1	[CMVM3.2]	2	0
[T2.4]	6	5	[SR2.4]	5	4	[ST3.3]	2	0			
[T2.5]	4	2	[SR2.5]	4	6	[ST3.4]	2	0			
[T3.1]	2	1	[SR3.1]	3	2						
[T3.2]	1	1									
[T3.3]	1	2									

© 2009 Cigital Inc.

Using BSIMM

- BSIMM released March 2009 under creative commons
  - http://bsi-mm.com
  - steal the data if you want
- BSIMM is a yardstick
  - Use it to see where you stand
  - Use it to figure out what your peers do
- BSIMM is growing
  - More BSIMM victims (9+17 and counting)
  - BSIMM Europe
  - BSIMM Begin
  - Statistics
  - Correlations

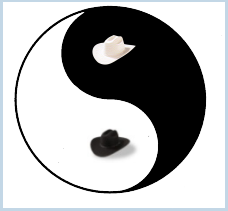
cigital

© 2009 Cigital Inc.

Take the BSIMM Begin survey today

- Web-based survey of level one activities and the ten things everybody does
- http://bsi-mm.com/begin

© 2009 Cigital Inc.



Where to Learn More

© 2009 Cigital

informIT & Justice League

informIT

- www.informIT.com
- No-nonsense monthly security column by Gary McGraw

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

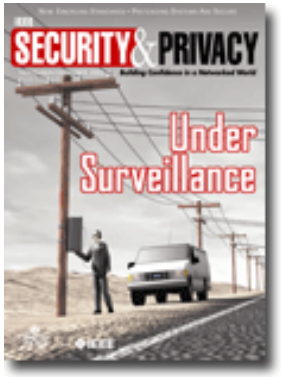
cigital

© 2009 Cigital Inc.

IEEE Security & Privacy Magazine + 2 Podcasts

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

The Silver Bullet Security Podcast with Gary McGraw

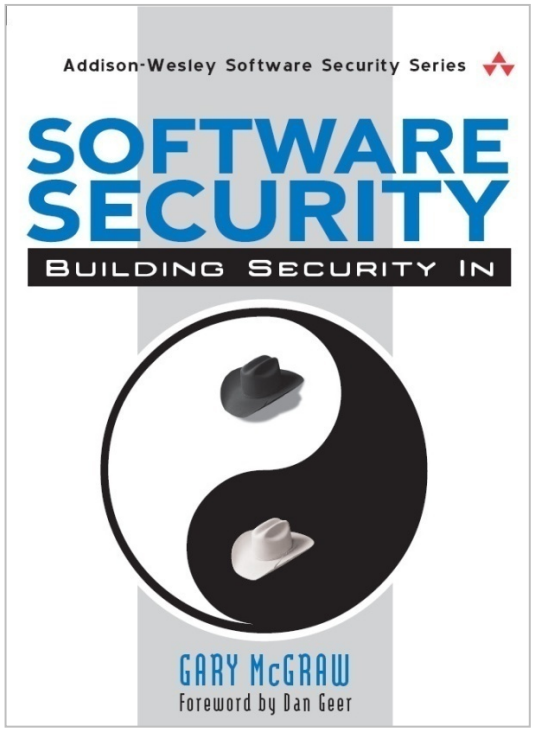


- www.cigital.com/silverbullet
- www.cigital.com/realitycheck

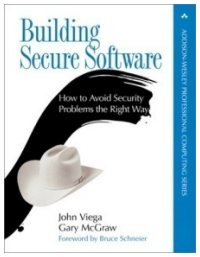
cigital

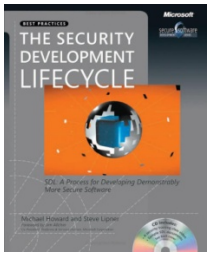
© 2009 Cigital Inc.

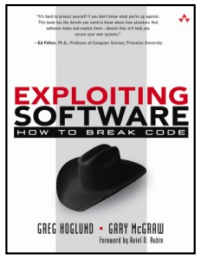
Software Security: the book



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







Addison Wesley

cigital

© 2009 Cigital Inc.

For more on BSIMM

- http://bsi-mm.com
- See the Addison-Wesley Software Security series
- Send e-mail: gem@cigital.com
  chess@fortify.com

cigital

Addison Wesley

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

-Bill Gates

© 2009 Cigital Inc.