Building Security In Maturity Model

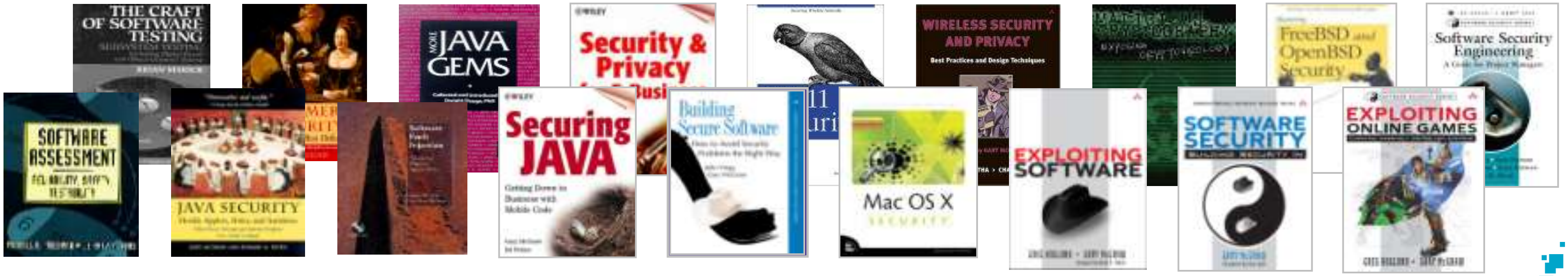
Gary McGraw, Ph.D.
Chief Technology Officer, Cigital

February 2010

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

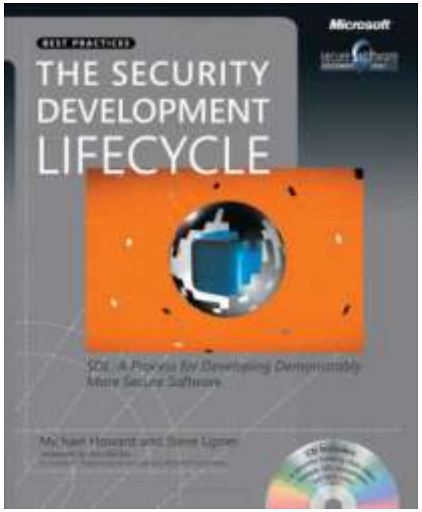


We hold these truths to be self-evident

- 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

2006: a shift from philosophy to HOW TO

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


Microsoft
BEST PRACTICES
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner

Breaking new ground

- Building Security In Maturity Model
- Real data from (30) real initiatives
- McGraw, Chess, & Migues

cigital

FORTIFY

58 software security initiatives

- 31 Financial
- 9 ISV
- 9 Tech
- 2 Defense
- 5 Retail
- 1 Oil
- 1 Behemoth

- visa europe
- thomson/reuters
- BP
- SAP
- nokia
- ebay
- mckesson

- ABN/amro
- ING
- telecom italia
- swift
- standard life
- cigna
- AON

- 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
- sterling commerce
- coke
- mastercard
- apple

- 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
- symantec
- AOL
- CA
- time warner

cigital

BSIMM original nine

EMC² where information lives®

Microsoft®

Adobe®

Google™

DTCC® The Depository Trust & Clearing Corporation

WELLS FARGO

QUALCOMM®

And two unnamed financial services firms

BSIMM Europe (nine EU firms)

NOKIA
Connecting People

STANDARD LIFE®

THOMSON REUTERS

SWIFT

TELECOM
ITALIA

And four unnamed firms

The magic 30

- SInce we have data from 30 firms we can start doing statistical analysis (RSA presentation coming soon)
  - How good is the model?
  - What activities correlate with what other activities?
  - Do high maturity firms look the same?
  - Etc

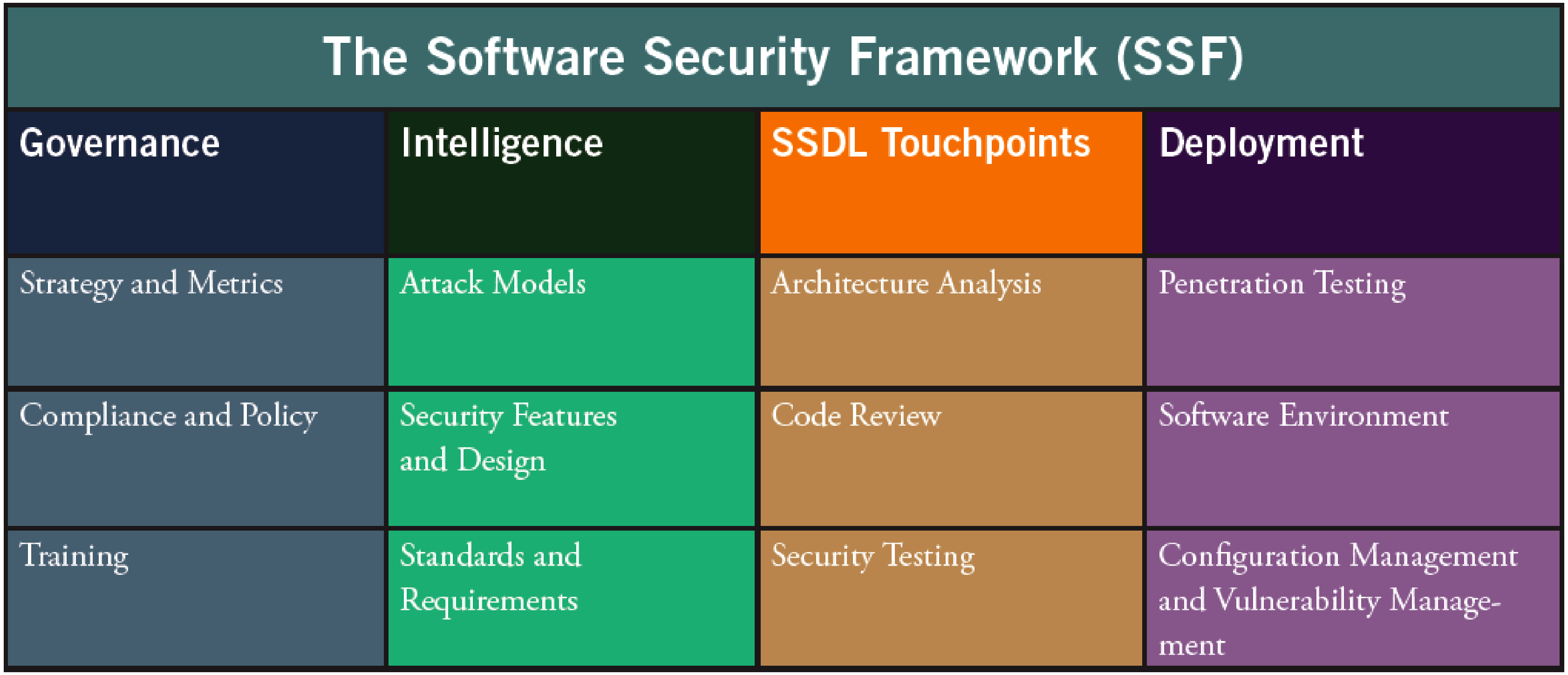
- We now have 30 (+1) firms
  - BSIMM (the nine)
  - BSIMM Europe (nine in EU)
  - 12 other firms (+ 1 underway) ← BSIMM 2

cigital

Building BSIMM (2009)

- Big idea: Build a maturity model from actual data gathered from 9 of ~50 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”
- The model has been validated with data from 30 firms

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

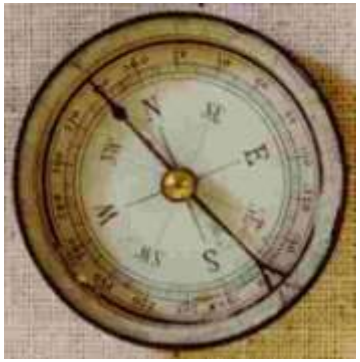
- Four domains
- Twelve practices
- An “archeology grid”
- See informIT article at http://bsi-mm.com

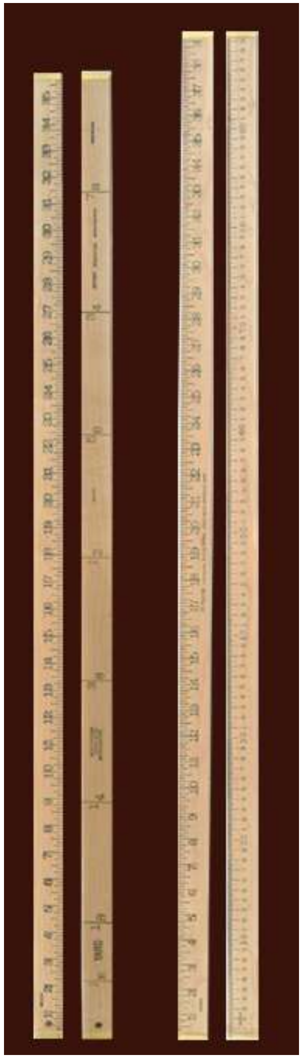
Monkeys eat bananas

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

cigital

On cargo cults and divining rods





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

Real-world data (24 firms)

- Initiative age: 5yrs 3months avg.
  - Newest: 0
  - Oldest: 14
  - Median 3.6
- SSG size: 29
  - Smallest: 0
  - Largest: 100
  - Median: 13
- Satellite size: 55
  - Smallest: 0
  - Largest: 300
  - Median: 11
- Dev size: 5878
  - Smallest: 40
  - Largest: 30,000
  - Median: 4000

Average SSG size: 1.15% of dev

cigital

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

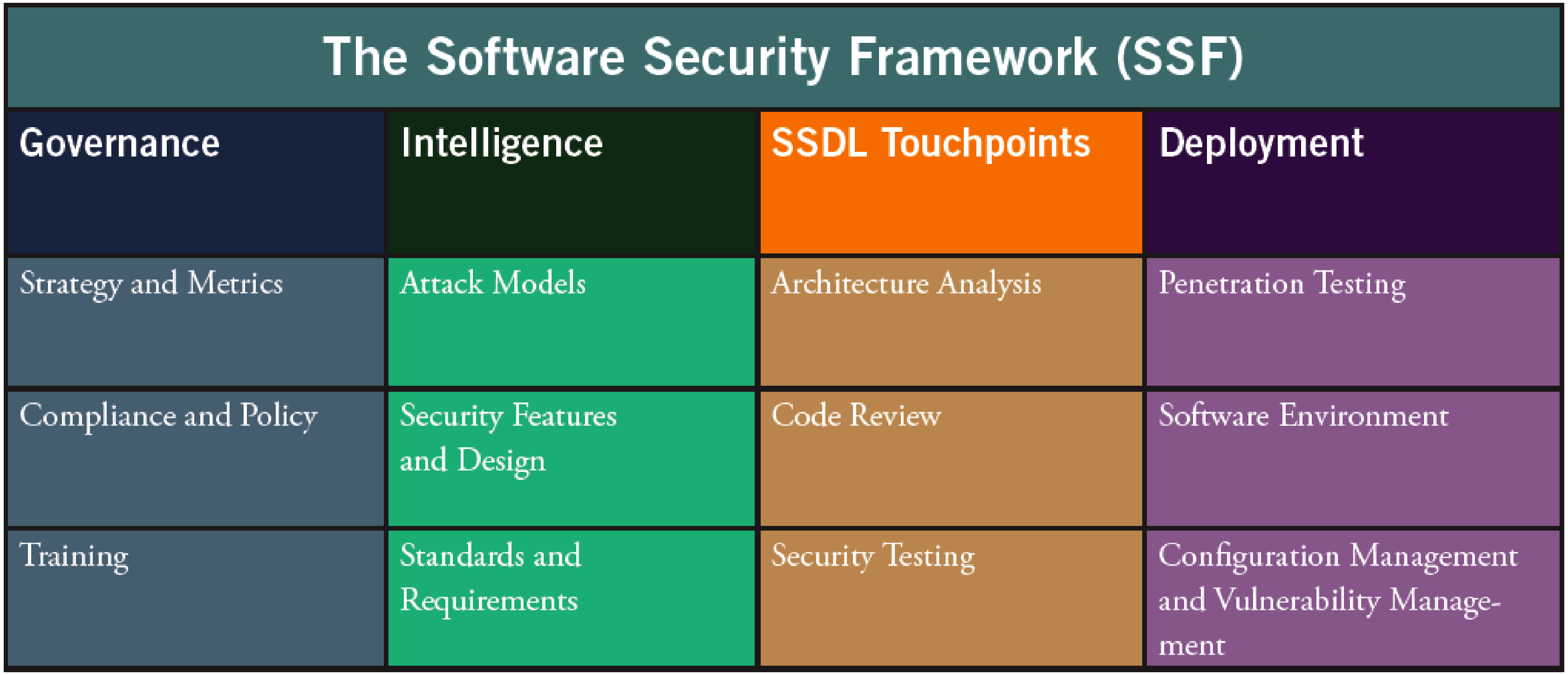
- InformIT article on BSIMM website http://bsi-mm.com

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

A Software Security Framework

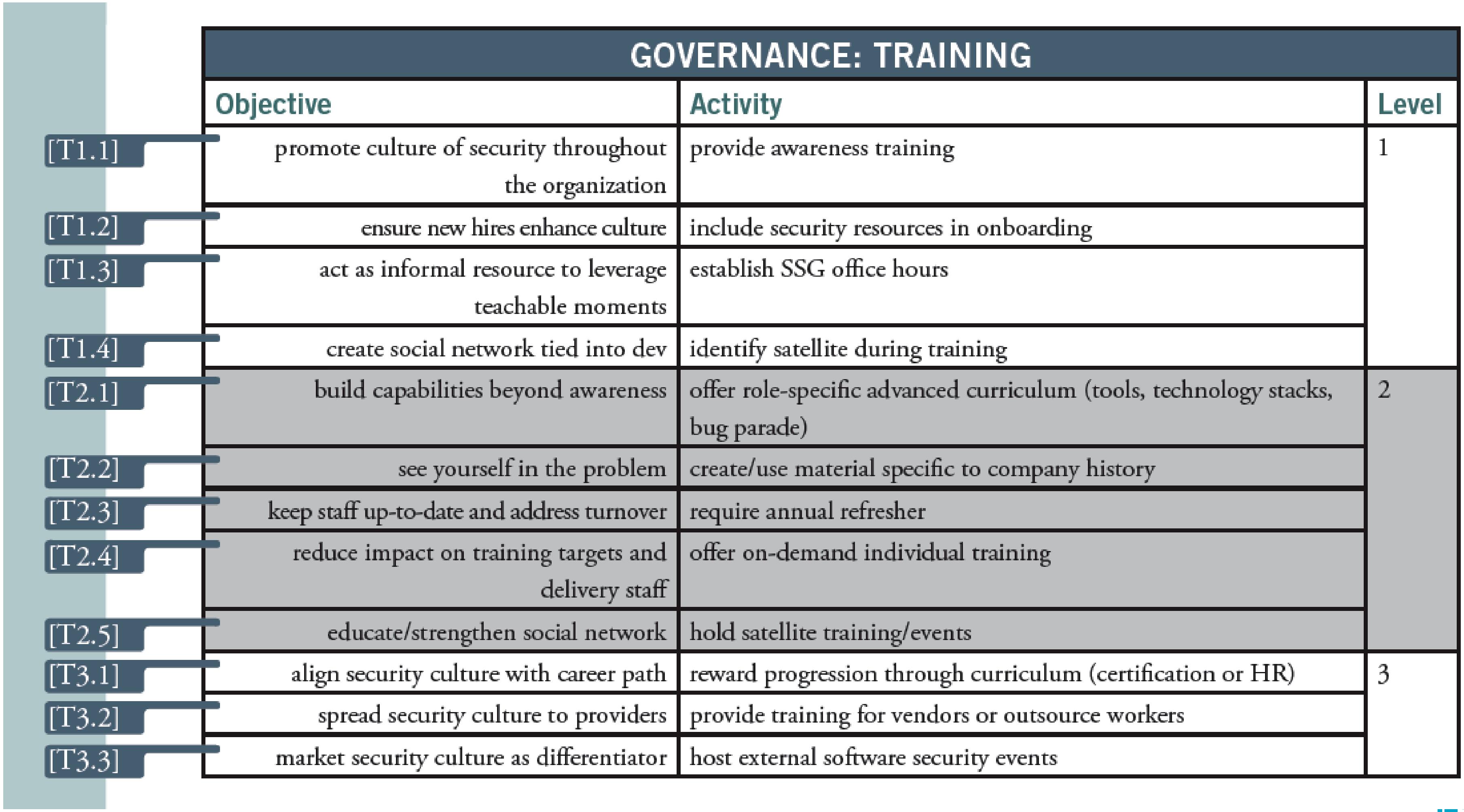


The Software Security Framework (SSF)

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

Training practice skeleton



GOVERNANCE: TRAINING

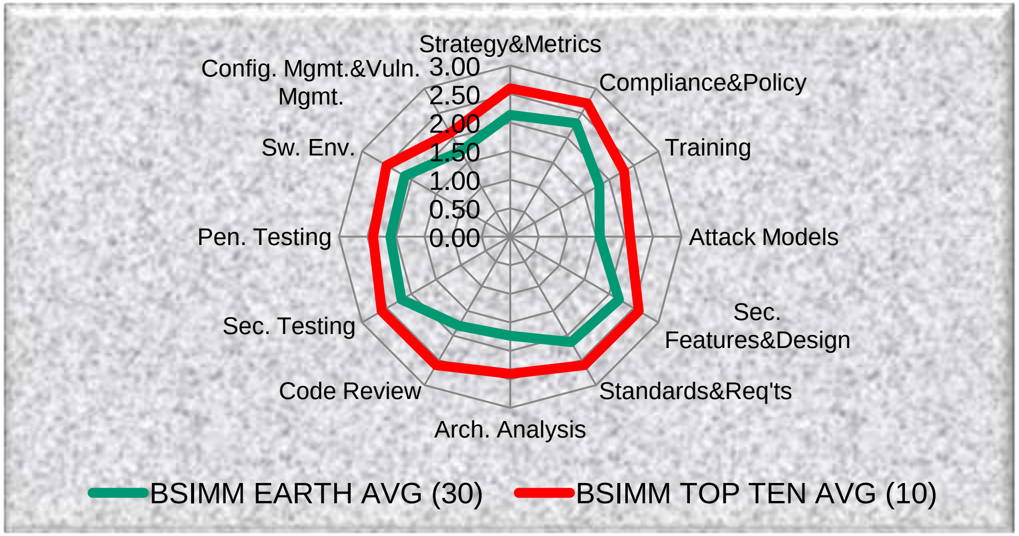
	Objective	Activity	Level
[T1.1]	promote culture of security throughout the organization	provide awareness training	1
[T1.2]	ensure new hires enhance culture	include security resources in onboarding	
[T1.3]	act as informal resource to leverage teachable moments	establish SSG office hours	
[T1.4]	create 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	

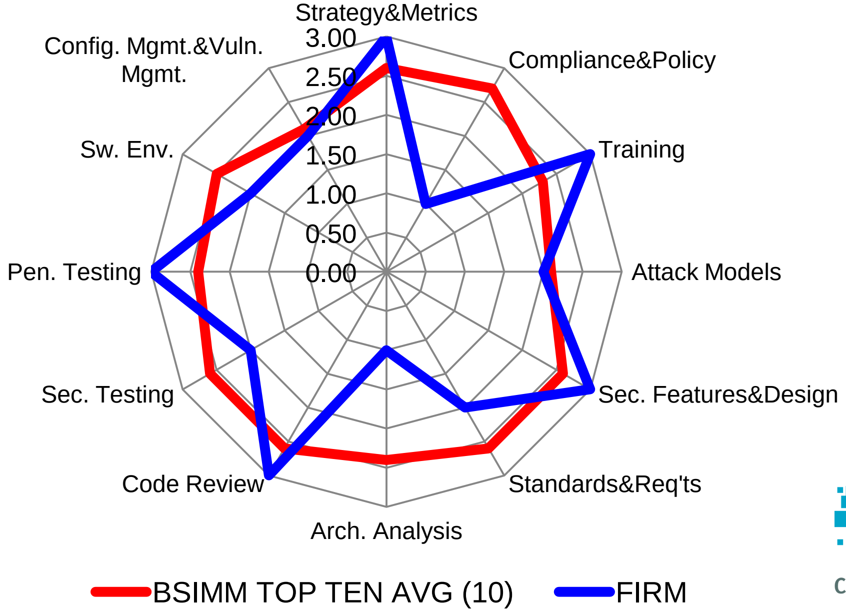
Example activity

[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.

Fifteen things “everybody” does

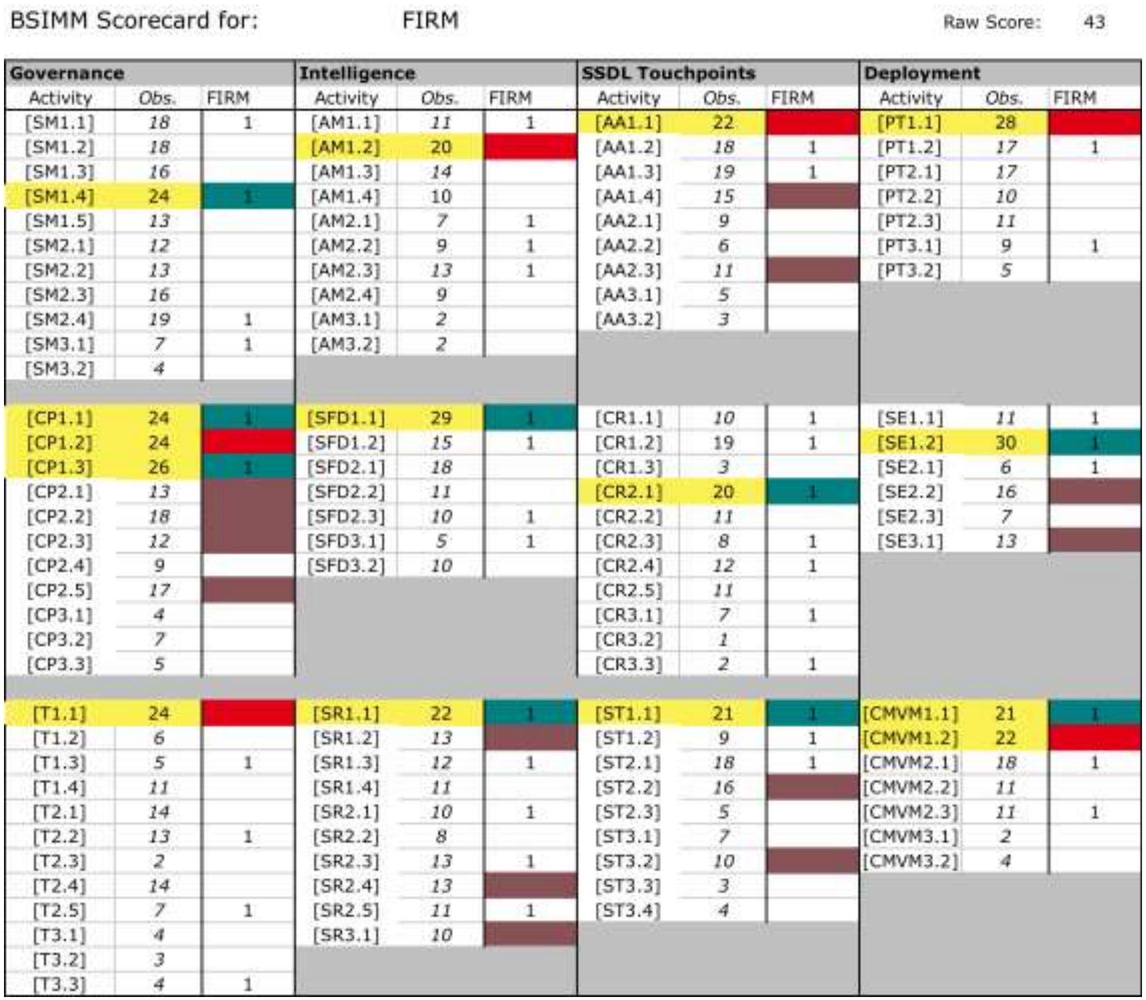
- Activities that ALL do
  - identify gates
  - unify regulations
  - know PII obligations
  - publish policy
  - awareness training
  - data classification
  - identify features
  - security standards
  - review security features
  - static analysis tool
  - QA boundary testing
  - external pen testers
  - good network security
  - incident response
  - close ops bugs loop





cigital

BSIMM Scorecard



BSIMM Scorecard for: FIRM

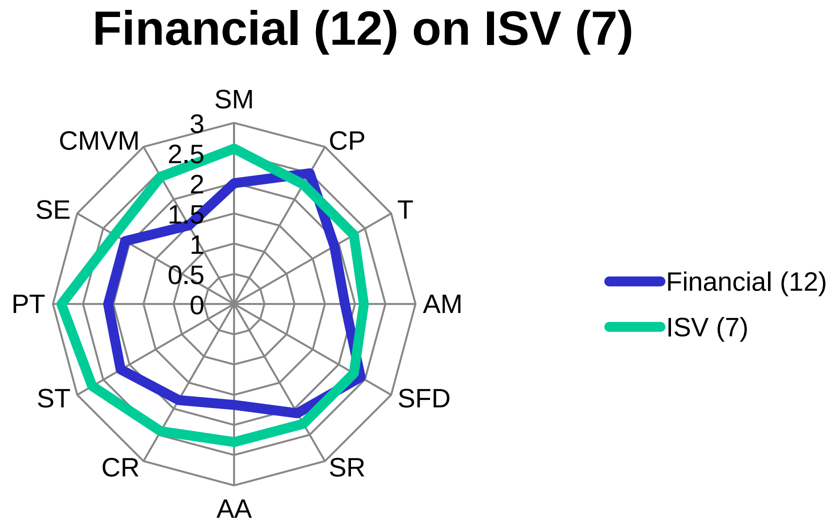
Raw Score: 43

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	Obs.	FIRM	Activity	Obs.	FIRM	Activity	Obs.	FIRM	Activity	Obs.	FIRM
[SM1.1]	18	1	[AM1.1]	11	1	[AA1.1]	22	🟥	[PT1.1]	28	🟥
[SM1.2]	18		[AM1.2]	20	🟥	[AA1.2]	18	1	[PT1.2]	17	1
[SM1.3]	16		[AM1.3]	14		[AA1.3]	19	1	[PT2.1]	17	
[SM1.4]	24	🟩 1	[AM1.4]	10		[AA1.4]	15	🟫	[PT2.2]	10	
[SM1.5]	13		[AM2.1]	7	1	[AA2.1]	9		[PT2.3]	11	
[SM2.1]	12		[AM2.2]	9	1	[AA2.2]	6		[PT3.1]	9	1
[SM2.2]	13		[AM2.3]	13	1	[AA2.3]	11	🟫	[PT3.2]	5	
[SM2.3]	16		[AM2.4]	9		[AA3.1]	5				
[SM2.4]	19	1	[AM3.1]	2		[AA3.2]	3				
[SM3.1]	7	1	[AM3.2]	2							
[SM3.2]	4										
[CP1.1]	24	🟩 1	[SFD1.1]	29	🟩 1	[CR1.1]	10	1	[SE1.1]	11	1
[CP1.2]	24	🟥	[SFD1.2]	15	1	[CR1.2]	19	1	[SE1.2]	30	🟩 1
[CP1.3]	26	🟩 1	[SFD2.1]	18		[CR1.3]	3		[SE2.1]	6	1
[CP2.1]	13	🟫	[SFD2.2]	11		[CR2.1]	20	🟩 1	[SE2.2]	16	🟫
[CP2.2]	18	🟫	[SFD2.3]	10	1	[CR2.2]	11		[SE2.3]	7	
[CP2.3]	12	🟫	[SFD3.1]	5	1	[CR2.3]	8	1	[SE3.1]	13	🟫
[CP2.4]	9		[SFD3.2]	10		[CR2.4]	12	1			
[CP2.5]	17	🟫				[CR2.5]	11				
[CP3.1]	4					[CR3.1]	7	1			
[CP3.2]	7					[CR3.2]	1				
[CP3.3]	5					[CR3.3]	2	1			
[T1.1]	24	🟥	[SR1.1]	22	🟩 1	[ST1.1]	21	🟩 1	[CMVM1.1]	21	🟩 1
[T1.2]	6		[SR1.2]	13	🟫	[ST1.2]	9	1	[CMVM1.2]	22	🟥
[T1.3]	5	1	[SR1.3]	12	1	[ST2.1]	18	1	[CMVM2.1]	18	1
[T1.4]	11		[SR1.4]	11		[ST2.2]	16	🟫	[CMVM2.2]	11	
[T2.1]	14		[SR2.1]	10	1	[ST2.3]	5		[CMVM2.3]	11	1
[T2.2]	13	1	[SR2.2]	8		[ST3.1]	7		[CMVM3.1]	2	
[T2.3]	2		[SR2.3]	13	1	[ST3.2]	10	🟫	[CMVM3.2]	4	
[T2.4]	14		[SR2.4]	13	🟫	[ST3.3]	3				
[T2.5]	7	1	[SR2.5]	11	1	[ST3.4]	4				
[T3.1]	4		[SR3.1]	10	🟫						
[T3.2]	3										
[T3.3]	4	1									

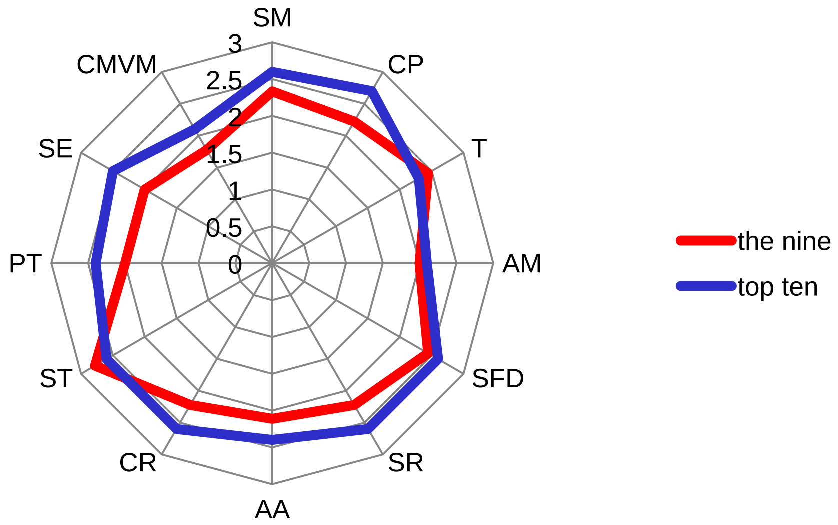
- Top 10 things
  - green = good?
  - red = bad?
- "Blue shift" practices to emphasize
  - activities you should maybe think about in brown

cigital

We are a special snowflake (NOT)

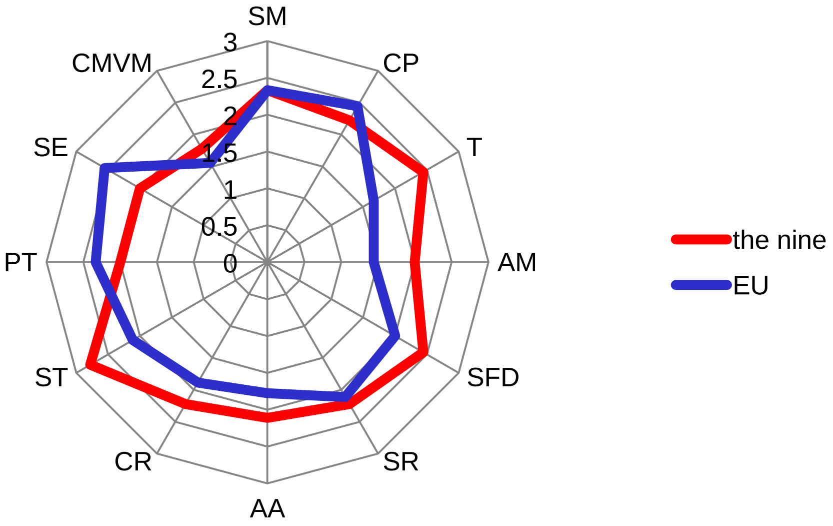


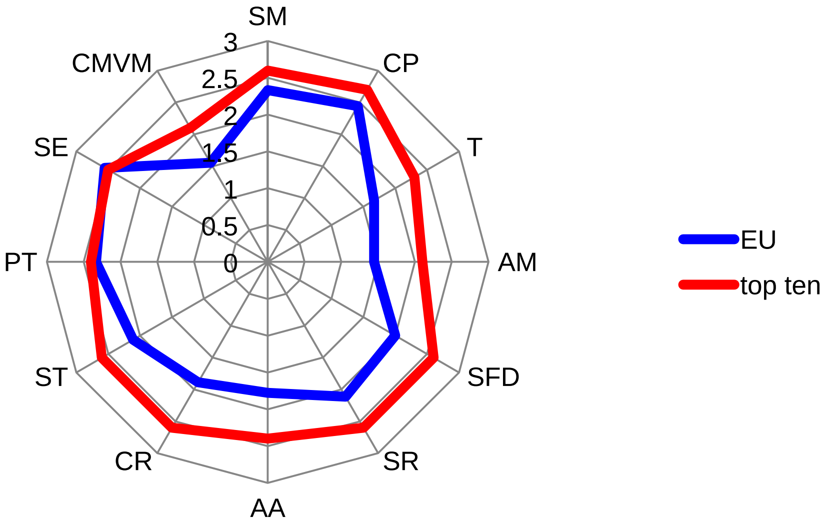
- ISV (7) results are similar to financial services (12)
- Data set range spreads



- You do the same things
- You can demand the same results

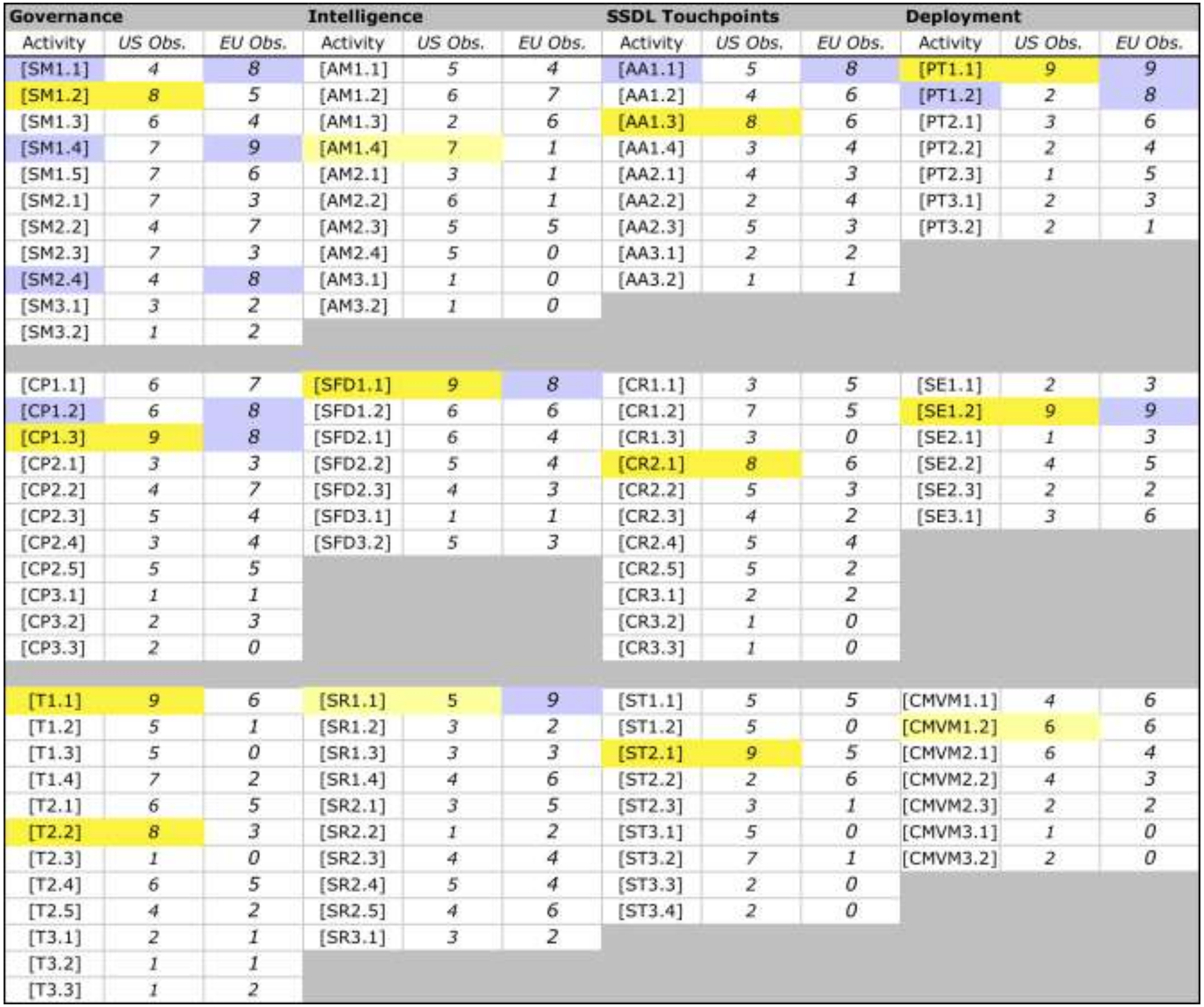
BSIMM Europe





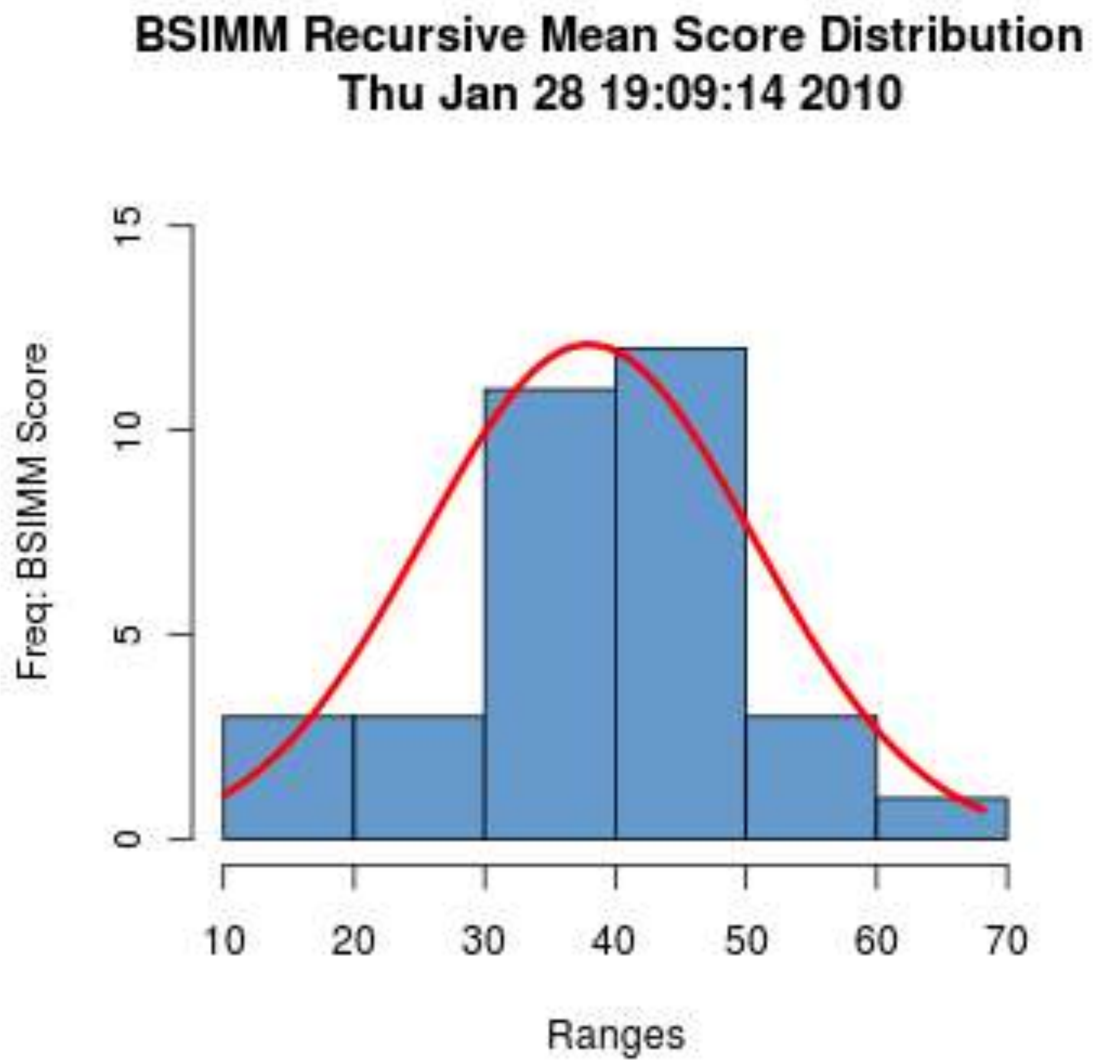
- More emphasis on privacy
- More emphasis on process
- Pen testing overemphasized
- 2 of 10 firms in the top ten

BSIMM Europe vs BSIMM US

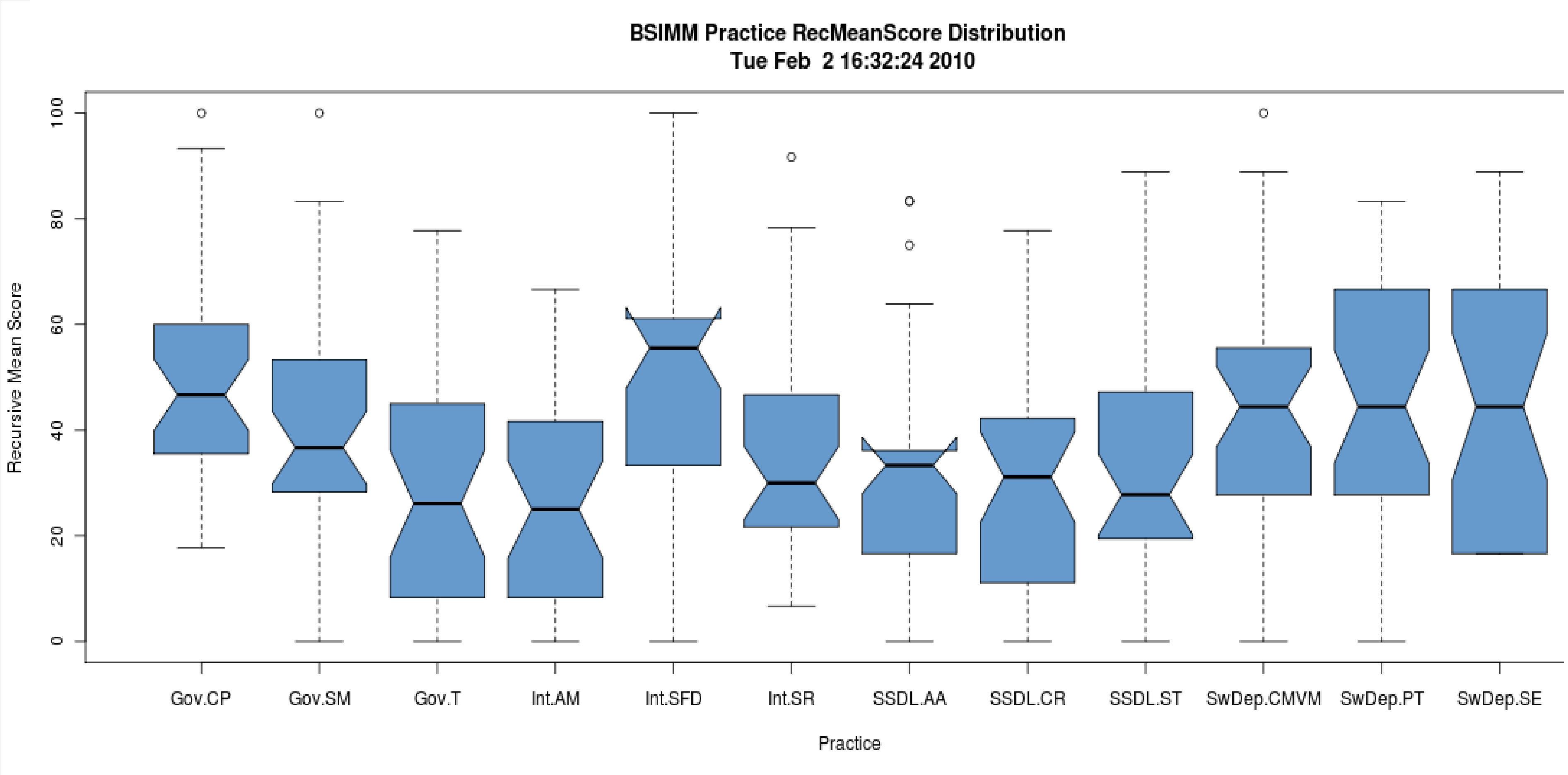


Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.
[SM1.1]	4	8	[AM1.1]	5	4	[AA1.1]	5	8	[PT1.1]	9	9
[SM1.2]	8	5	[AM1.2]	6	7	[AA1.2]	4	6	[PT1.2]	2	8
[SM1.3]	6	4	[AM1.3]	2	6	[AA1.3]	8	6	[PT2.1]	3	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									

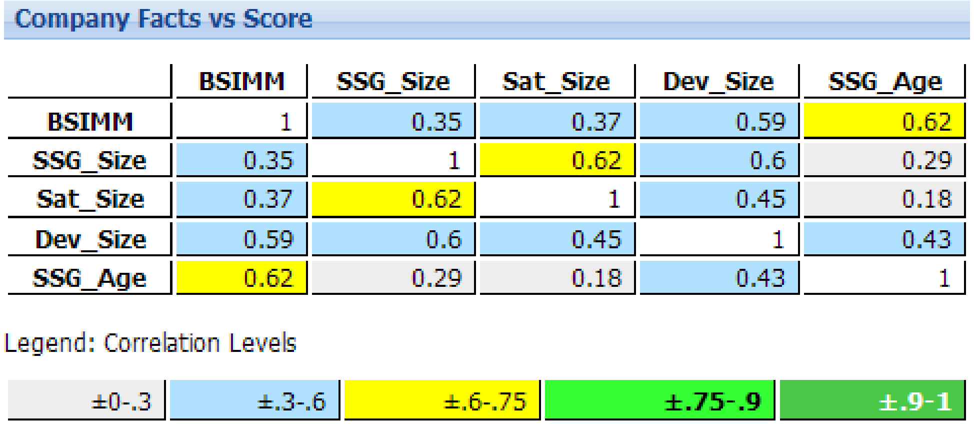
Analysis


BSIMM Recursive Mean Score Distribution
Thu Jan 28 19:09:14 2010
Freq: BSIMM Score
0
5
10
15
10
20
30
40
50
60
70
Ranges

Practices


BSIMM Practice RecMeanScore Distribution
Tue Feb 2 16:32:24 2010
Recursive Mean Score
0
20
40
60
80
100
Gov.CP
Gov.SM
Gov.T
Int.AM
Int.SFD
Int.SR
SSDL.AA
SSDL.CR
SSDL.ST
SwDep.CMVM
SwDep.PT
SwDep.SE
Practice

Age matters and size matters too

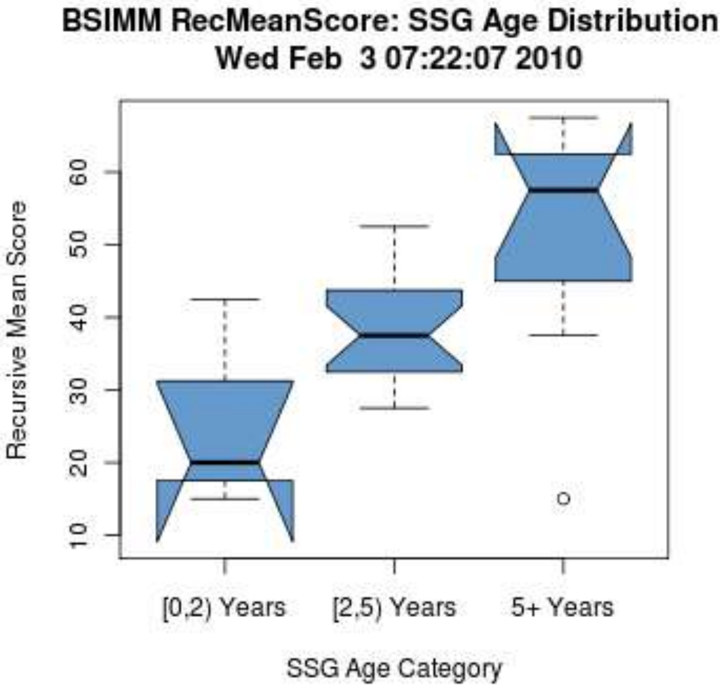


Company Facts vs Score

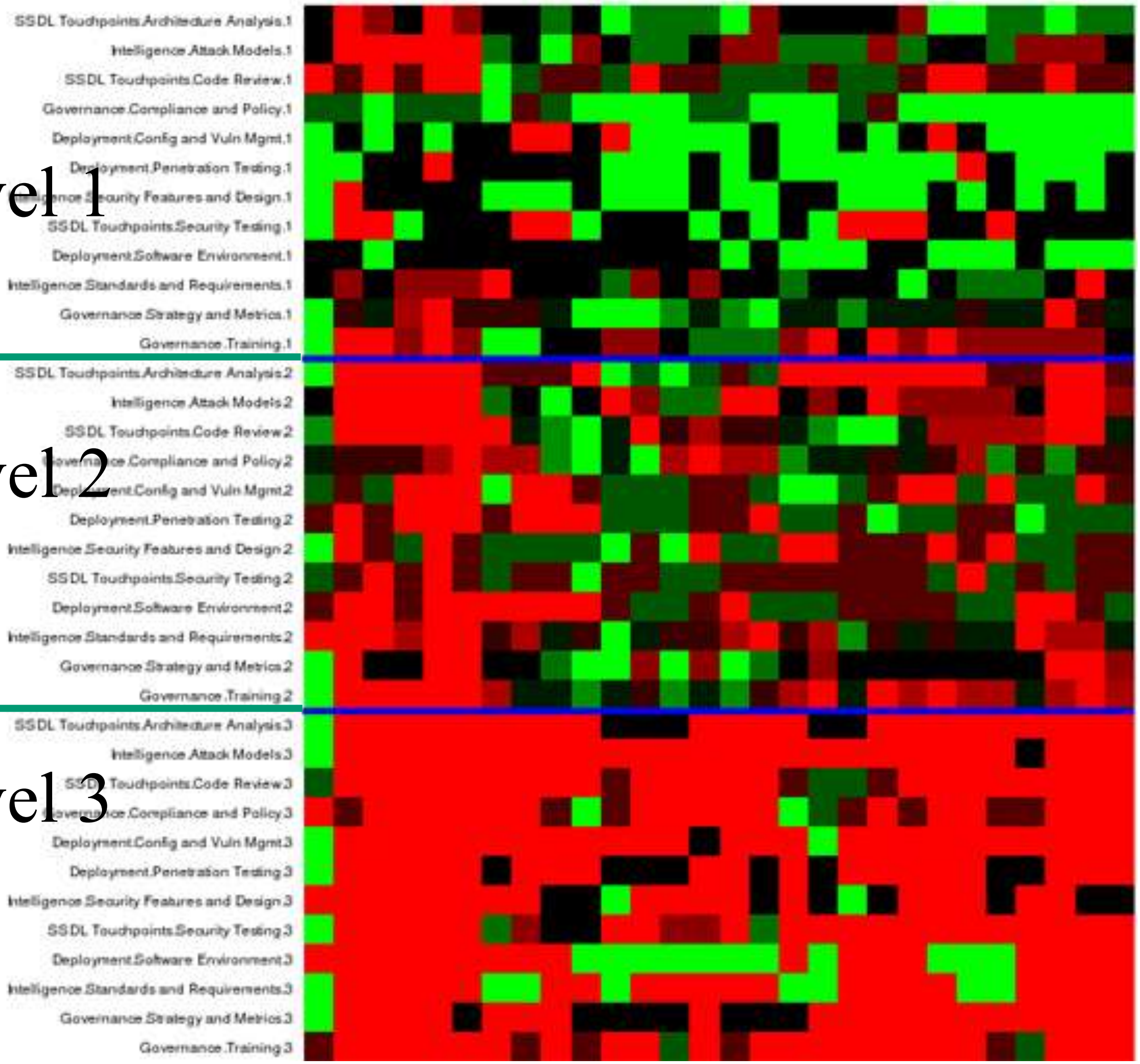
	BSIMM	SSG_Size	Sat_Size	Dev_Size	SSG_Age
BSIMM	1	0.35	0.37	0.59	0.62
SSG_Size	0.35	1	0.62	0.6	0.29
Sat_Size	0.37	0.62	1	0.45	0.18
Dev_Size	0.59	0.6	0.45	1	0.43
SSG_Age	0.62	0.29	0.18	0.43	1

Legend: Correlation Levels

±0-.3	±.3-.6	±.6-.75	±.75-.9	±.9-1



How good are the levels we chose?



Maturity Level 1

Maturity Level 2

Maturity Level 3

Using BSIMM

- BSIMM released March 2009 under creative commons
  - http://bsi-mm.com
  - v1.5 includes Europe (November 2009)
  - Italian and German translations
  - 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 (30+)
  - BSIMM Europe
  - BSIMM Begin

cigital

Where to Learn More

informIT & Justice League

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

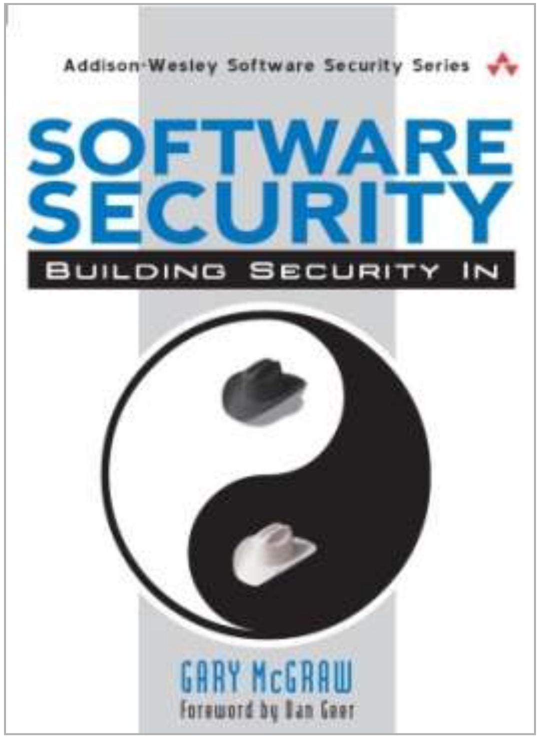
- www.cigital.com/justiceleague
- In-depth thought leadership blog from the Cigital Principals
  - Scott Matsumoto
  - Gary McGraw
  - Sammy Migues
  - Craig Miller
  - John Steven

IEEE Security & Privacy Magazine + 2 Podcasts

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

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

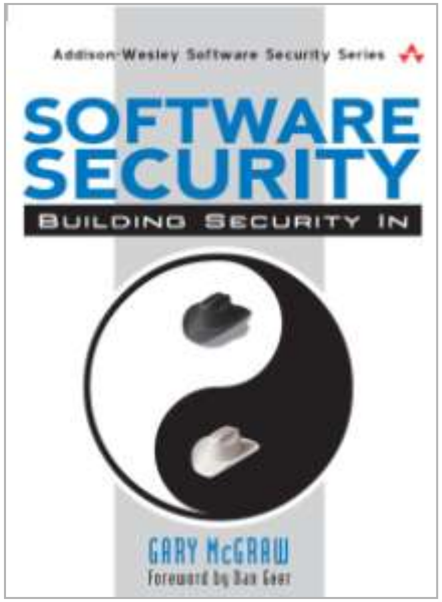
Software Security: the book



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

For more on BSIMM

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