Building Security In
Maturity Model

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

February 2010
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
Breaking new ground

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

- **31 Financial**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe
  - Wells Fargo
  - Goldman Sachs
  - Google
  - Qualcomm
  - Morgan Stanley
  - US Air Force
  - Dell
  - Pershing
  - The Hartford
  - Barclays Capital
  - Bank of Tokyo
  - UPS
  - Bank of Montreal
  - Sterling Commerce
  - Coke
  - Mastercard
  - Apple
  - Visa Europe
  - Thomson/Reuters
  - BP
  - SAP
  - Nokia
  - eBay
  - McKesson
- **9 ISV**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe
  - Wells Fargo
  - Goldman Sachs
  - Google
  - Qualcomm
  - Morgan Stanley
- **9 Tech**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe
  - Wells Fargo
  - Goldman Sachs
  - Google
  - Qualcomm
  - Morgan Stanley
- **2 Defense**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe
  - Wells Fargo
  - Goldman Sachs
- **5 Retail**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe
- **1 Oil**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe
- **1 Behemoth**
  - Microsoft
  - DTCC
  - EMC
  - Fidelity
  - Adobe

© 2010 Cigital Inc.
BSIMM original nine

And two unnamed financial services firms
BSIMM Europe (nine EU firms)

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) \(\leftarrow\) BSIMM 2
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

<table>
<thead>
<tr>
<th>Four domains</th>
<th>Twelve practices</th>
<th>An “archeology grid”</th>
<th>See informIT article at <a href="http://bsi-mm.com">http://bsi-mm.com</a></th>
</tr>
</thead>
</table>

The Software Security Framework (SSF)

<table>
<thead>
<tr>
<th>Governance</th>
<th>Intelligence</th>
<th>SSDL Touchpoints</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy and Metrics</td>
<td>Attack Models</td>
<td>Architecture Analysis</td>
<td>Penetration Testing</td>
</tr>
<tr>
<td>Compliance and Policy</td>
<td>Security Features and Design</td>
<td>Code Review</td>
<td>Software Environment</td>
</tr>
<tr>
<td>Training</td>
<td>Standards and Requirements</td>
<td>Security Testing</td>
<td>Configuration Management and Vulnerability Management</td>
</tr>
</tbody>
</table>

© 2010 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
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
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
A Software Security Framework

<table>
<thead>
<tr>
<th>Governance</th>
<th>Intelligence</th>
<th>SSDL Touchpoints</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy and Metrics</td>
<td>Attack Models</td>
<td>Architecture Analysis</td>
<td>Penetration Testing</td>
</tr>
<tr>
<td>Compliance and Policy</td>
<td>Security Features and Design</td>
<td>Code Review</td>
<td>Software Environment</td>
</tr>
<tr>
<td>Training</td>
<td>Standards and Requirements</td>
<td>Security Testing</td>
<td>Configuration Management and Vulnerability Management</td>
</tr>
</tbody>
</table>

- Four domains
- Twelve practices
- See informIT article on BSIMM website
  http://bsi-mm.com
## Training practice skeleton

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

- Top 10 things
  - green = good?
  - red = bad?

- “Blue shift” practices to emphasize
  - activities you should maybe think about in brown
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

<table>
<thead>
<tr>
<th>Governance</th>
<th>Intelligence</th>
<th>SSDL Touchpoints</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SM1.1]</td>
<td>4</td>
<td>8</td>
<td>[AM1.1]</td>
</tr>
<tr>
<td>[SM1.2]</td>
<td>8</td>
<td>5</td>
<td>[AM1.2]</td>
</tr>
<tr>
<td>[SM1.3]</td>
<td>6</td>
<td>4</td>
<td>[AM1.3]</td>
</tr>
<tr>
<td>[SM1.5]</td>
<td>7</td>
<td>6</td>
<td>[AM2.1]</td>
</tr>
<tr>
<td>[SM2.1]</td>
<td>7</td>
<td>3</td>
<td>[AM2.2]</td>
</tr>
<tr>
<td>[SM2.2]</td>
<td>4</td>
<td>7</td>
<td>[AM2.3]</td>
</tr>
<tr>
<td>[SM2.3]</td>
<td>7</td>
<td>3</td>
<td>[AM2.4]</td>
</tr>
<tr>
<td>[SM2.4]</td>
<td>4</td>
<td>8</td>
<td>[AM3.1]</td>
</tr>
<tr>
<td>[SM3.1]</td>
<td>3</td>
<td>2</td>
<td>[AM3.2]</td>
</tr>
<tr>
<td>[SM3.2]</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

| [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       | [SFD1.2]  | 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       | [SE3.1]   | 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       |
| [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

Ranges

© 2010 Cigital Inc.
Practices
Age matters and size matters too

<table>
<thead>
<tr>
<th>Company Facts vs Score</th>
<th>BSIMM</th>
<th>SSG_Size</th>
<th>Sat_Size</th>
<th>Dev_Size</th>
<th>SSG_Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSIMM</td>
<td>1</td>
<td>0.35</td>
<td>0.37</td>
<td>0.59</td>
<td>0.62</td>
</tr>
<tr>
<td>SSG_Size</td>
<td>0.35</td>
<td>1</td>
<td>0.62</td>
<td>0.6</td>
<td>0.29</td>
</tr>
<tr>
<td>Sat_Size</td>
<td>0.37</td>
<td>0.62</td>
<td>1</td>
<td>0.45</td>
<td>0.18</td>
</tr>
<tr>
<td>Dev_Size</td>
<td>0.59</td>
<td>0.6</td>
<td>0.45</td>
<td>1</td>
<td>0.43</td>
</tr>
<tr>
<td>SSG_Age</td>
<td>0.62</td>
<td>0.29</td>
<td>0.18</td>
<td>0.43</td>
<td>1</td>
</tr>
</tbody>
</table>

Legend: Correlation Levels

- ±0.3
- ±0.3 to ±0.6
- ±0.6 to ±0.75
- ±0.75 to ±0.9
- ±0.9 to ±1

BSIMM RecMeanScore: SSG Age Distribution
Wed Feb 3, 07:22:07 2010
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
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

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

-Bill Gates