Making the Business Case for Software Assurance (SwA)

SEPG 2009
March 25, 2009

Julia H. Allen

© 2009 Carnegie Mellon University

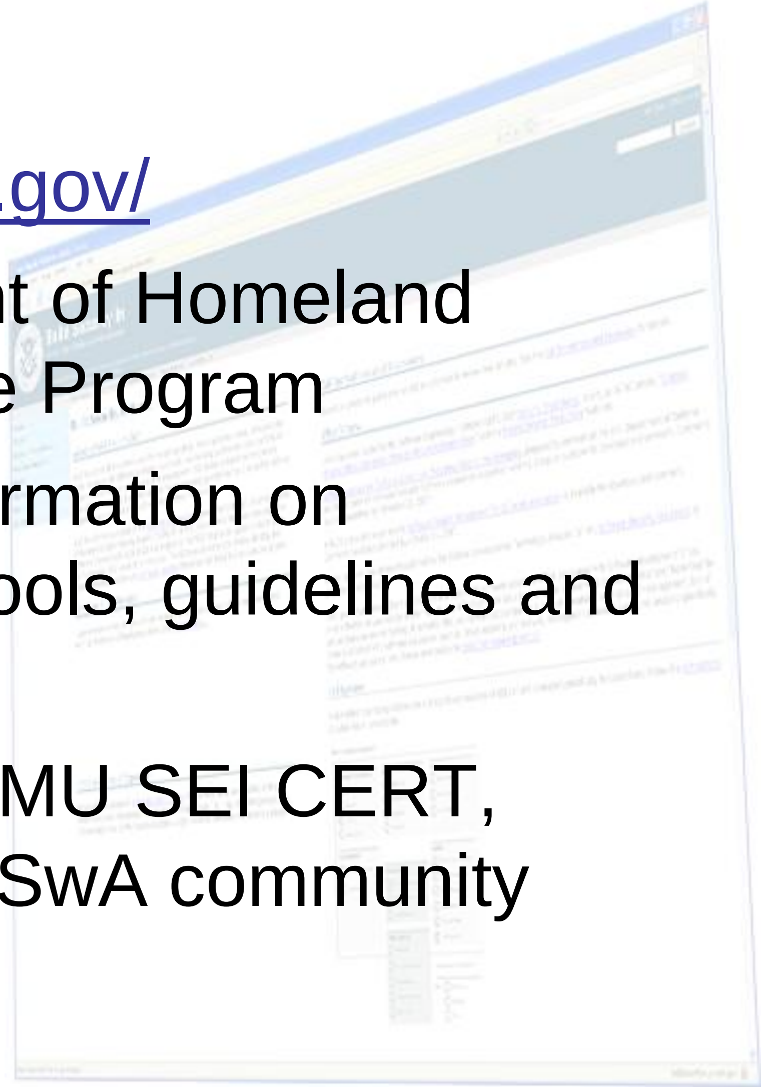
Build Security In: A Key Resource

Build Security In web site: https://buildsecurityin.us-cert.gov/

Sponsored by U.S. Department of Homeland Security, Software Assurance Program

Contains a broad range of information on principles, sound practices, tools, guidelines and resources

Contributing authors include CMU SEI CERT, Cigital, and experts from the SwA community



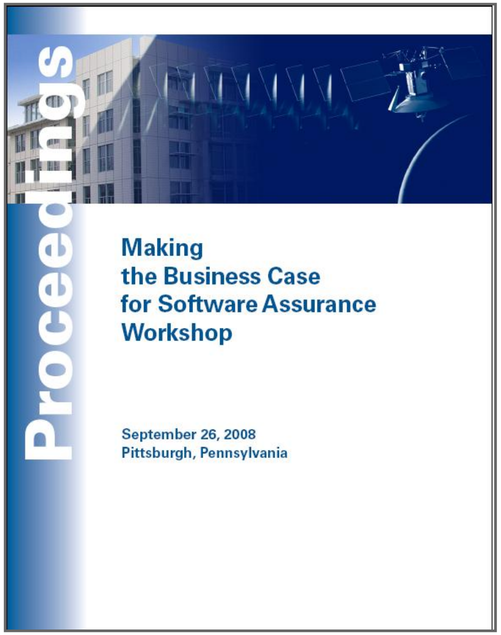
Making the Business Case for SwA Workshop

Held September 26, 2008 at Carnegie Mellon

Invited speakers, refereed paper presentations, facilitated discussions; 70 researchers and practitioners

Topics:

- Measurement
- Process and decision making issues
- Legal issues
- Globalization
- Risk issues
- Organizational development issues



Proceedings

Making
the Business Case
for Software Assurance
Workshop

September 26, 2008
Pittsburgh, Pennsylvania

http://www.sei.cmu.edu/community/BCW_Proceedings.pdf

Topics

Why software assurance?

Software assurance costs and benefits

Business case perspectives

Deloitte 2007 Global Security Survey - Findings

Finding #3: Application security: generic countermeasures are no longer adequate

Applications are the primary gateway to sensitive data

87% of respondents: poor software development quality is a top threat in the next 12 months

Application security is the #1 issue for CIOs (Gartner)

Deloitte 2007 Global Security Survey: The Shifting Security Paradigm. Deloitte, September 2007.

http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901(1).pdf

Defining Software Assurance

The level of confidence that software is free from vulnerabilities

Engineering software so that it continues to function as intended, even when under attack

- Resists the exploitation of software weaknesses
- Able to recognize, resist, tolerate, and recover from events that threaten it

The goal: Better, defect-free software that can function more robustly in its operational environment

Why Software Assurance? - 1

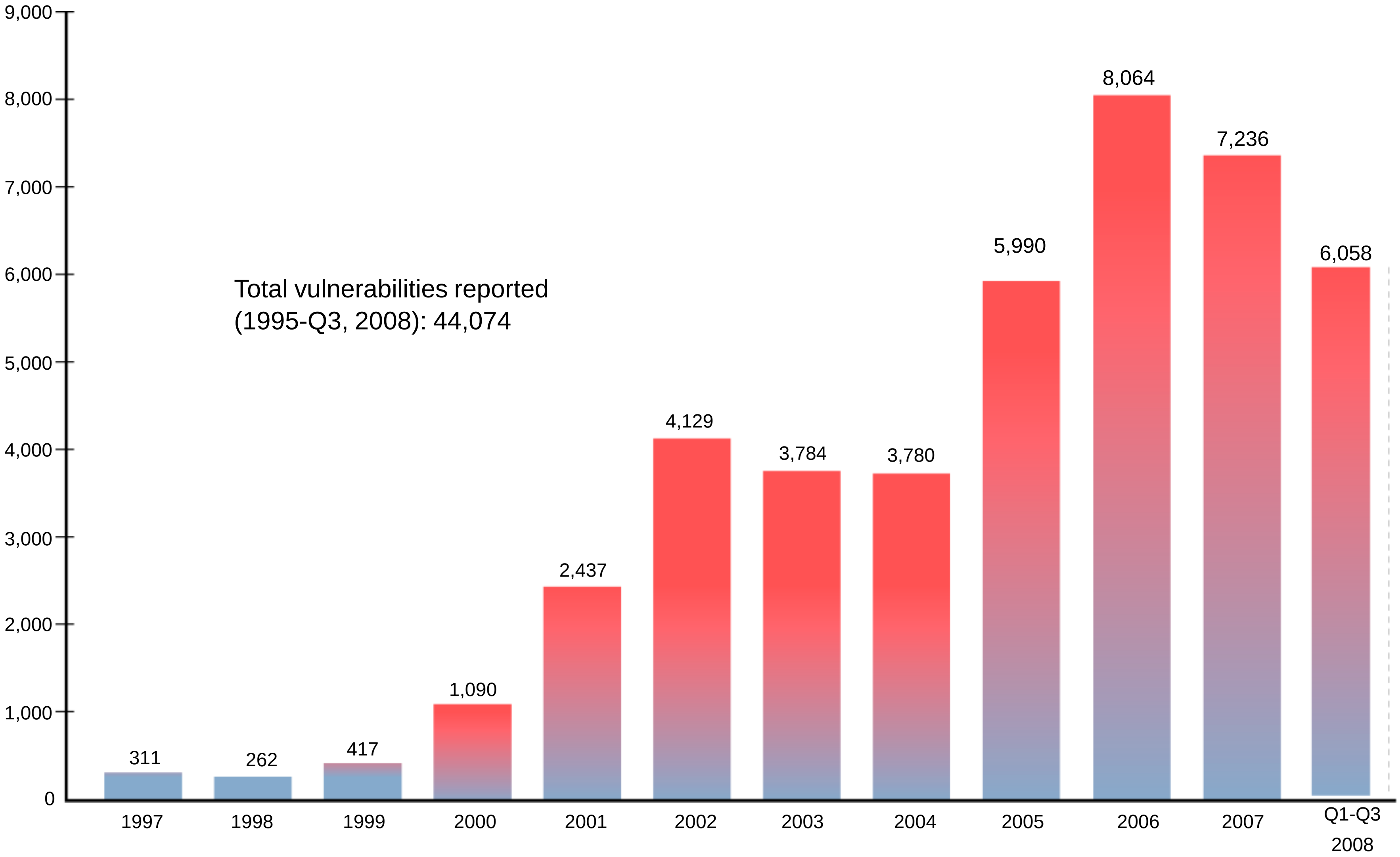
Developed nations' economies and security depend, in large part, on the reliable execution of software

Globalization of the IT software supply chain and software outsourcing

Software vulnerabilities jeopardizing:

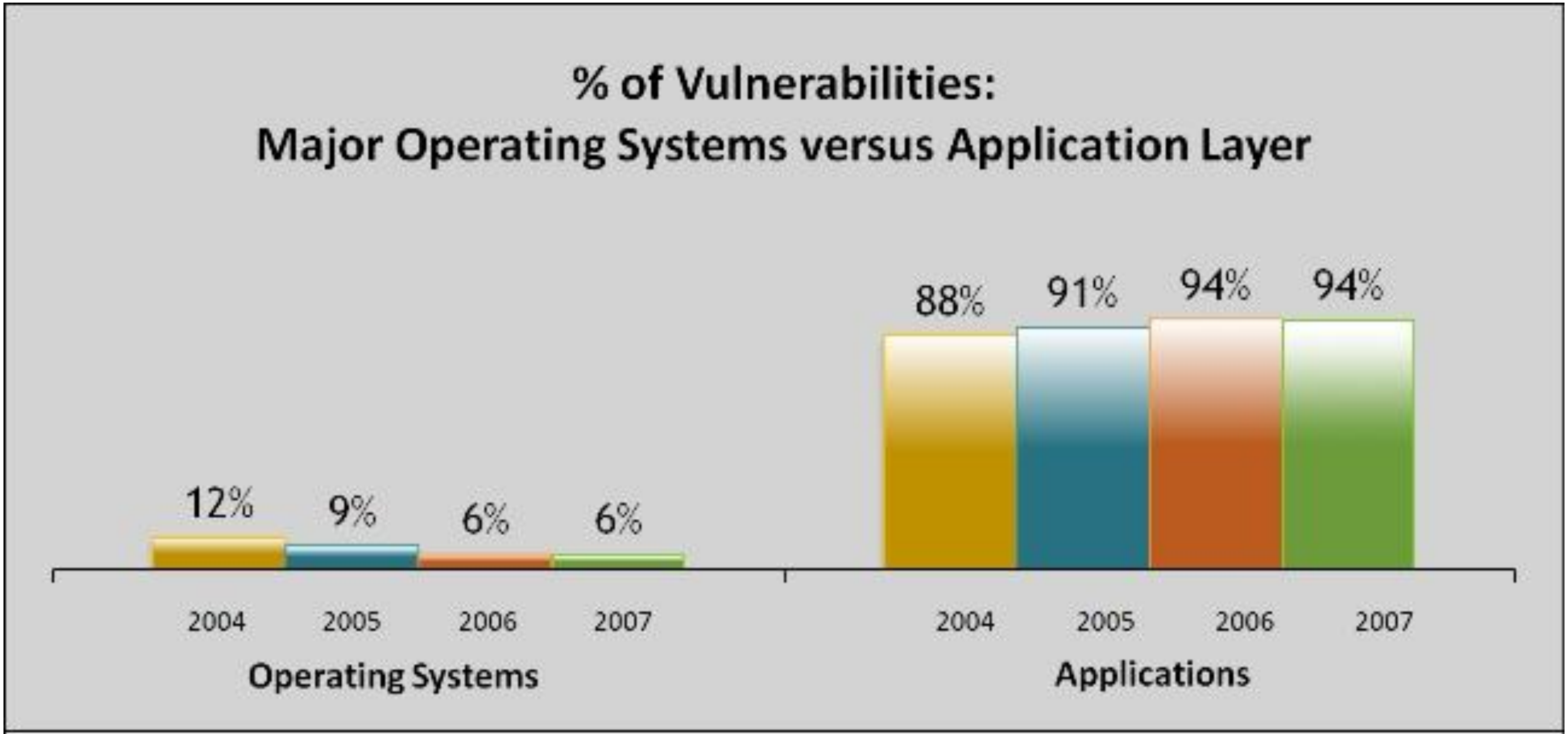
- Personal identities
- Intellectual property
- Consumer trust
- Business services, operations, & continuity
- Critical infrastructures & government

Vulnerabilities Reported to CERT



Total vulnerabilities reported
(1995-Q3, 2008): 44,074

Increase in Application Layer Vulnerabilities



Calculated from the Microsoft Security Intelligence Report 2008

http://msdn.microsoft.com/en-us/security/cc420637.aspx

Why Software Assurance? - 2

Most successful attacks result from:

- Targeting and exploiting known, non-patched software vulnerabilities
- Insecure software configurations

Many vulnerabilities introduced during software design & development

Increasing trend of assembling systems from purchased parts means getting software acquisition* right with respect to assurance

* Refer to Polydys & Wisseman. “Software Assurance in Acquisition: Mitigating Risks to the Enterprise.” October 2008. https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf

Topics

Why software assurance?

Software assurance costs and benefits

Business case perspectives

Software Development vs. Assurance Costs

Development:

Costs to produce correct software aka software quality

- should include reworking design flaws and coding bugs

Assurance:

Costs to make the software secure

- remediate any identifiable means of exploitation (specification, design, coding)
- minimize attack damage, ensure a systematic recovery
- meet security functional requirements
- include certification

Sample Benefits

Reduced levels of patching and favorable customer feedback [Microsoft 08]

Reduced costs of fixing security flaws early in the SDLC [Fortify]

Capitalized dollar value of losses averted as a result of SwA practices [Arora 08]

Estimated monetary value of avoided risk of regulatory penalties, contractual penalties, and other sanctions [Arora 08]

Software products with built-in SwA are more resilient, cost less to sustain, require less rework [Jarzombek 08]

Current State

No widely accepted single, common model for calculating cost/benefit for early investment in SwA during software development

What We Can Offer: A variety of models and other considerations that may be useful for conveying the value of SwA

Cost/Benefit Models

Thirteen most commonly cited models for IT valuation

Investment-oriented (3)

- For example, Microsoft's Rapid Economic Justification

Cost-oriented (3)

- For example, Total Cost of Ownership

Environmental/Contextual-oriented (4)

- For example, Balanced Scorecard

Quantitative estimation (3)

- For example, CoCoMo II and security extensions

Shoemaker, Dan et al. "Models for Assessing the Cost and Value of Software Assurance." November 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/684-BSI.html

Topics

Why software assurance?

Software assurance costs and benefits

Business case perspectives

Business Case Perspectives

Vendors

Process

Global Supply Chain

Organizational Development

Explored at the September 2008 Making the Business Case for SwA Workshop

Business Case for Security Vendors

Why

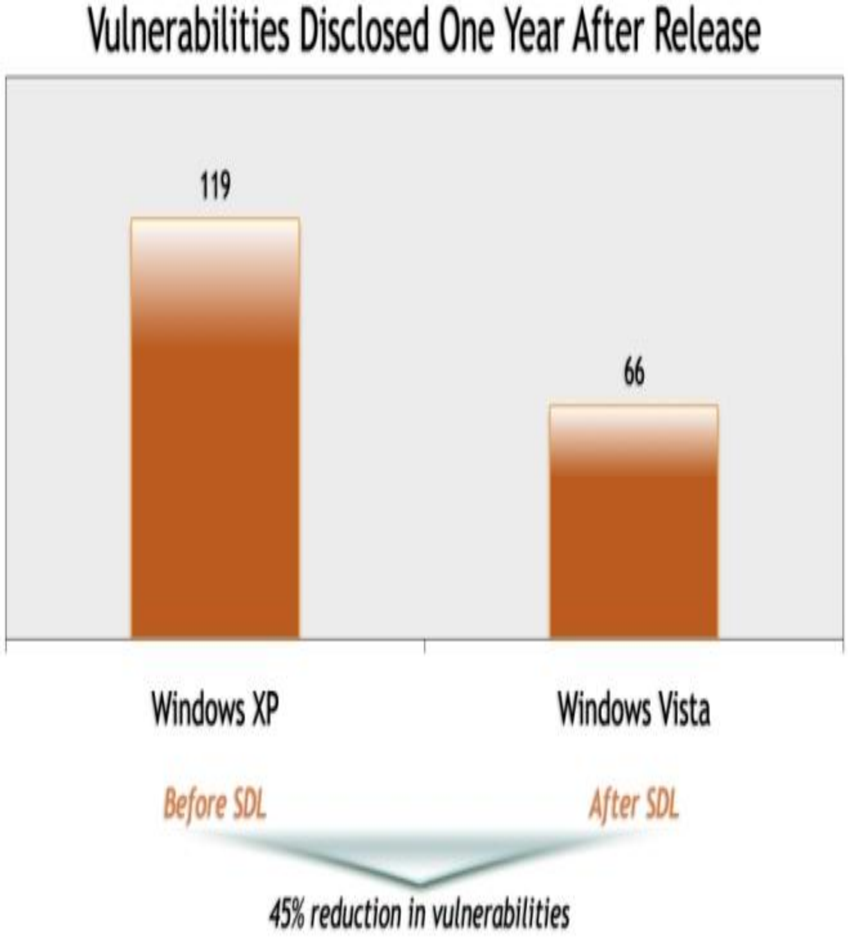
- Customer expectations; profit/loss of sales
- Fear of bad publicity; stock price impacts
- Explicit requests (primarily government customers; Common Criteria)

What

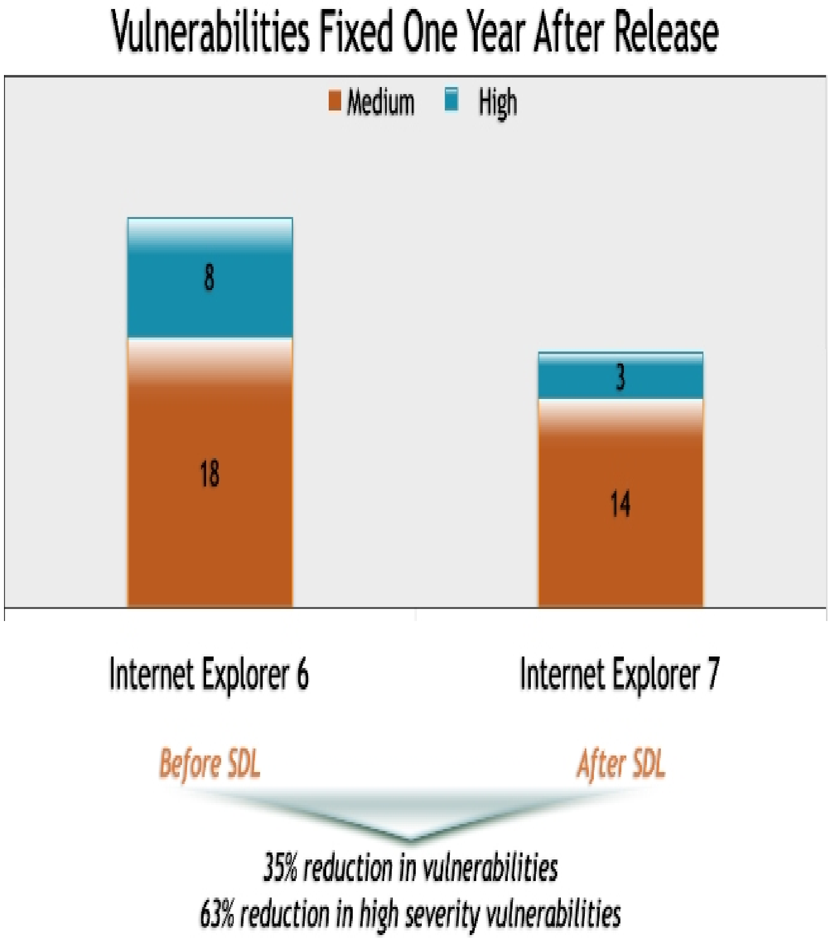
- Developer training
- Penetration testing
- Dynamic (black box) testing
- Source code analysis
- Design reviews

Initial sample: Eight vendors of shrink-wrapped software ranging from less than $100M annual sales to $10B; excluded Microsoft [Epstein, Jeremy. “What Measures Do Vendors Use for Software Assurance.” February 2009. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/1093-BSI.html]

Business Case for Microsoft’s SDL



Source: Windows Vista One Year Vulnerability Report, Microsoft Security Blog 23 Jan 2008



Source: Browser Vulnerability Analysis, Microsoft Security Blog 27-NOV-2007

http://msdn.microsoft.com/en-us/security/cc424866.aspx

Cost of Fixing Defects: Fortify

Cost of Fixing Defects **Later**

Stage	Critical Defects Identified	Cost of Fixing 1 Defect	Cost of Fixing All Defects
Requirements		$139	
Design		$455	
Coding		$977	
Testing	50	$7,136	$356,800
Maintenance	150	$14,102	$2,115,300
Total	200		$2,472,100

Cost of Fixing Defects **Early**

Stage	Critical Defects Identified	Cost of Fixing 1 Defect	Cost of Fixing All Defects
Requirements		$139	
Design		$455	
Coding	150	$977	$146,550
Testing	50	$7,136	$356,800
Maintenance		$14,102	
Total	200		$503,350

Identifying critical defects earlier in the lifecycle reduced costs by about $2.0M.

https://buildsecurityin.us-cert.gov/swa/downloads/Meftah.pdf

CMMI Process Reference Model for Assurance - Draft

Process Area: Assurance Process Management

Process Management (SG1.1-1.3)	Establish process environment, infrastructure, and organizational behavior
Project Management (SG2.1- 2.3)	Manage against plan inc. risks, measures, suppliers, and 3rd party applications
Assurance Engineering (SG 3.1 - 3.5)	Establish requirements, architecture, design; conduct product implementation V&V; manage life cycle vulnerabilities
Assurance Support (SG 4.1 - 4.3)	Perform audits, determine defect root causes, and protect assets

https://buildsecurityin.us-cert.gov/swa/procwg.html

https://buildsecurityin.us-cert.gov/swa/downloads/PRM_for_Assurance_to_CMMI.pdf

SwA Measurement Framework - 1

Measure the effectiveness of achieving SwA at organizational, program, and project levels

Leverages existing measurement approaches and enumerations

- ISO 15939, ISO 27004, CMMI, NIST SP 800-55
- CVE, CWE, CAPEC, CCE

Presents example goals, information needs, measures, and benefits for

- Organizations: suppliers, acquirers
- People: executives, practitioners

Bartol, et. al. *Practical Measurement Framework for Software Assurance and Information Security,* Version 1.0, October, 2008. https://buildsecurityin.us-cert.gov/swa/downloads/SwA_Measurement.pdf ; https://buildsecurityin.us-cert.gov/swa/measact.html

SwA Measurement Framework - 2

Measures help answer five questions:

- What are the defects in the design and code that have a potential to be exploited?
- Where are they?
- How did they get there?
- Have they been mitigated?
- How can they be avoided in the future?

[Bartol 08]

SwA Investment Decision Making

Use business-based criteria

Cost	Estimated total costs - savings, risk reduction, TCO, cost of not doing
Criticality/Risk	Meets objectives and risk management goals
Feasibility	Likelihood of investment success
Interdependencies	With existing processes, other investments, compliance, staff skills
Involvement	Who needs to participate, buy-in?
Measurability	How measurable is the outcome?
Time & Effort	Leadership time; time to demonstrate results and reach break-even

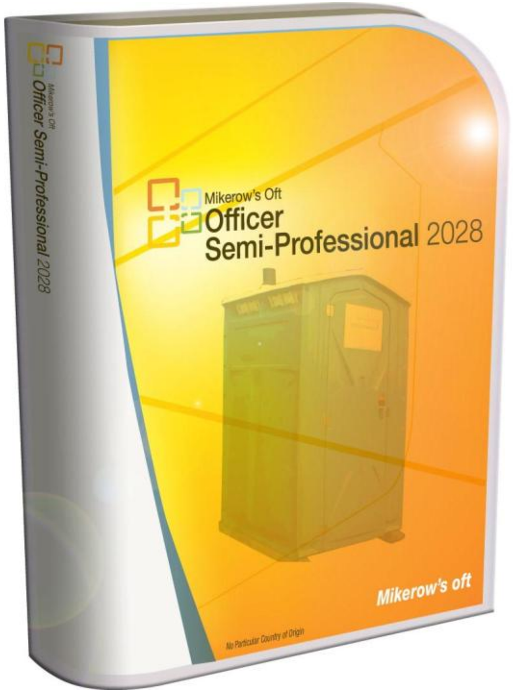
Allen, Julia. “Making Business-Based Security Investment Decisions – A Dashboard Approach,” September 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/985-BSI.html

Global Supply Chain - 1

“Software offers one of the best mechanisms for technical intelligence collection by adversaries.” [Lewis 07]

Crux of the issue: Is software made by a foreign entity less trustworthy than software made domestically?

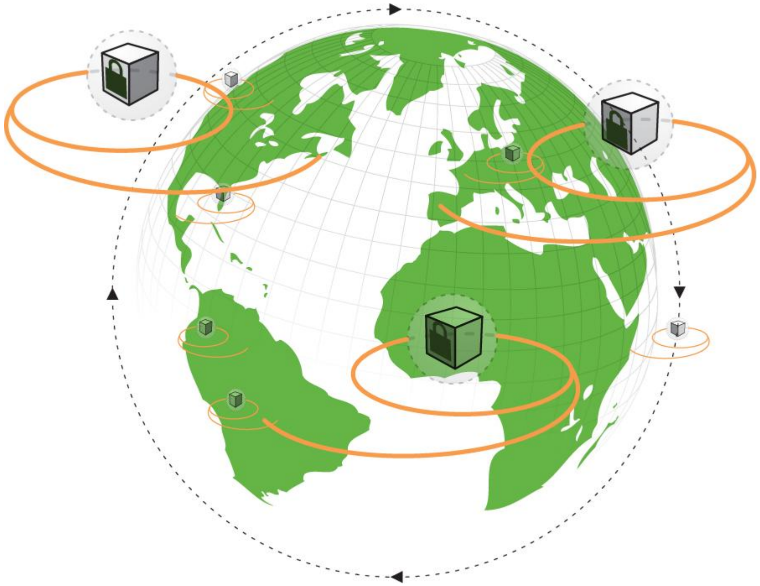
- Software of unknown pedigree or provenance
- Acquisition of foreign entities by domestic organizations and vice versa
- Insertion of malicious code into foreign-made software
- Insider threat: Developers in collusion with hostile governments and organized crime



Global Supply Chain - 2

Mitigated by

- Focusing on assurance rather than location
- Stronger acquisition policy guidance and process
- Acceptance testing and certification of acquired software
- A defined exit strategy



Organizational Development - 1

Capable performance = secure product

Awareness, training, education

Recognition	organization recognizes the need for security
Informal Realization	organization understands informal security practices
Security Understanding	security practices planned and monitored
Deliberate Control	decisions about security practices based on data
Continuous Adaptation	practices adapt to changes and are continuously improving

Shoemaker, Dan. “It’s a Nice Idea but How Do We Get Anyone to Practice It? A Staged Model for Increasing Organizational Capability in Software Assurance.” January 2009. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/1091-BSI.html.

Organizational Development - 2

Train developers on best-known SwA practices [1] [2]

Integrate SwA practices into a well-defined, in-use SDLC

Consider emerging secure coding standards [3] [4]

Consider emerging professional certifications [5]

[1] DHS Build Security In; https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

[2] SAFECode *Fundamental Practices for Secure Software Development;* http://www.safecode.org/

[3] Application security additions to the Payment Card Industry Data Security Standard; https://www.pcisecuritystandards.org/

[4] CERT's C, C++, Java Secure Coding Standards; https://www.cert.org/secure-coding

[5] (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP) certification due June 2009; http://www.isc2.org/

Ask the Right Questions: Fortify

Can your developers describe

- the 10-25 most dangerous application security vulnerabilities?
- how their programming will mitigate the associated risk?

Which of your applications has the highest associated risk?

- What type of intruder is most likely to attack it?
- How would they attack it?

Do you have a checklist of security requirements?

- To perform code reviews?
- To develop and evaluate security-specific test cases?

[Fortify; OWASP; SANS]

SwA Business Case Challenges

It is conceptually simple yet

- Requires educating decision makers
- Not glamorous and will likely require convincing
- Might take a long time for an organization not set up for it

Must be done strategically and methodically

Requires behavioral and organizational change

To succeed you must have leadership support

Moss, Michele & Bartol, Nadya. “Benchmarking Assurance Practices: Contributions to a Business Case for Assurance.” BC Workshop presentation, September 2008.

Moving Forward

Treat SwA as a risk management issue

Address SwA in all contexts

- Development, outsourcing, acquisition, purchase, with partners, hosting another party's product/service

For internally developed software, integrate SwA practices into your SDLC

Tackle SwA as early in the life cycle as possible

References - 1

[Arora 08] Arora, Ashish, et al. “Estimating Benefits from Investing in Secure Software Development.” November 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/267-BSI.html

[Fortify] The Case for Business Software Assurance. http://www.fortify.com/security-resources/library/basics.jsp

Howard, Michael & Lipner, Steve. *The Security Development Lifecycle*. Redmond, WA: Microsoft Press, 2006.

[Jarzombek 08] Jarzombek, Joe. “Making the Business Case for Security-Enhanced Processes & Practices.” BC Workshop presentation, September 2008.

[Lewis 07] Lewis, James. “Foreign Influence on Software: Risks and Recourse.” The Center for Strategic and International Studies, March 2007. http://www.csis.org/index.php?option=com_csis_pubs&task=view&id=3772

References - 2

The Microsoft Security Development Lifecycle (SDL): Measurable Improvements for Flagship Microsoft Products. http://msdn.microsoft.com/en-us/security/cc424866.aspx

[Microsoft 08] The Business Case for the Microsoft Security Development Lifecycle (SDL). http://msdn.microsoft.com/en-us/security/cc420637.aspx

Shoemaker, Dan et al. “A Common Sense Way to Make the Business Case for Software Assurance.” November 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/952-BSI.html

The Software Assurance Forum for Excellent in Code (SAFECode); http://www.safecode.org/

Woody, Carol. “Strengthening Ties between Process and Security.”August 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/sdlc/1049-BSI.html

References - 3

Open Web Application Security Project (OWASP): Top Ten Project

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

CWE/SANS Top 25 Most Dangerous Programming Errors

http://www.sans.org/top25errors/

New York State Disseminates Application Security Procurement Language and Launches Cyber Academy To Ensure Students Learn To Program Securely (January 12, 2009)

http://www.internetnews.com/dev-news/article.php/3796091

http://www.sans.org/appseccontract/

McGraw, Gary; Chess, Brian; Migues, Sammy. *Building Security In Maturity Model,* March 2009.
http://www.informit.com/articles/article.aspx?p=1326511

http://bsi-mm.com/ (active on March 5)

For More Information

Build Security In web site; Business Case Models content area https://buildsecurityin.us-cert.gov/

Making the Business Case for Software Assurance; SEI special report [Mead 09]

Julia Allen: jha@sei.cmu.edu

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.