



How to Create a Business Case for Software Security Initiatives

Marco Morana
OWASP Lead
TISO Citigroup



OWASP - Italy Day IV

"Secure Software Initiatives"

6th NOVEMBER 2009, MILAN

Copyright © 2009 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

The OWASP Foundation
<http://www.owasp.org>

Status Quo of Software Security Spending

- **"Security software budgets are expected to grow by approximately 4 % in 2010 despite overall IT budgets are shrinking "** – Gartner

...but

- **"..Security managers should continue to look for ways to maintain the same level of security for less money until the economy improves"** - *CIO MidMarket*

and

- **"Organizations that have suffered a public data breach spend more on security in the development process than those that have not"** – *OWASP*

Making the Business Cases: Essentials

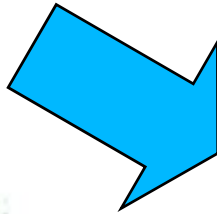
■ Secure Software Engineering Awareness

- ▶ *" Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying **to ensure that things will fail in the worst possible way at the worst possible time... again and again**"*

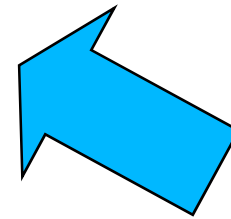
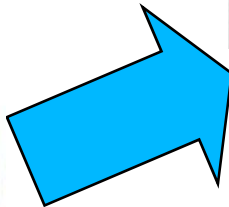
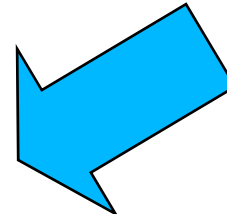
■ Prepare for Executive Management FAQs:

- ▶ Why I spend money on software security?
- ▶ How much I should spend ?
- ▶ What my competitors are doing?
- ▶ How I am doing at my vulnerabilities?
- ▶ How I get the most bang for the buck ?

Main Factors Driving Software Security Adoption



```
End Sub  
End Sub  
Private Sub tbToolBar_ButtonClicked  
On Error Resume Next  
timTimer.Enabled = True  
Select Case Button.Key  
Case "Back"  
    brwWebBrowser.GoBack  
Case "Forward"  
    brwWebBrowser.GoForward  
Case "Refresh"  
    brwWebBrowser.Refresh  
Case "Home"  
    brwWebBrowser.Home  
End Select  
End Sub
```



Lessons From the Court Room

Albert Gonzalez - Wikipedia, the free encyclopedia - Mozilla Firefox

File Edit View History Bookmarks Tools Help

W http://en.wikipedia.org/wiki/Albert_Gonzalez

Help us improve Wikipedia by [supporting it financially](#). Try Beta Log in / create account

article discussion edit this page history

Software update: 170 million card and ATM numbers

Albert Gonzalez

From Wikipedia, the free encyclopedia

Albert Gonzalez (born 1981) is a [computer hacker](#) and [computer criminal](#) who is accused of masterminding the combined [credit card theft](#) and subsequent reselling of more than 170 million card and [ATM numbers](#) from 2005 through 2007—the biggest such fraud in history.

Gonzalez and his accomplices used [sql injection](#) and [packet sniffer malware](#) software to create [backdoors](#) to several corporate systems in order to steal computer data.

During his spree he was said to have to throw away his keys because he complained about having to count \$340,000 by himself. Gonzalez stayed at lavish hotels but his lifestyle was not without problems. Gonzalez is currently awaiting the outcome of the trial.

■ May 2008 in [New York](#) for the Dave & Buster's case.
■ May 2008 in [Massachusetts](#) for the TJ Maxx case (trial scheduled early 2010)
■ August 2009 in [New Jersey](#) in connection with the Heartland Payment case.

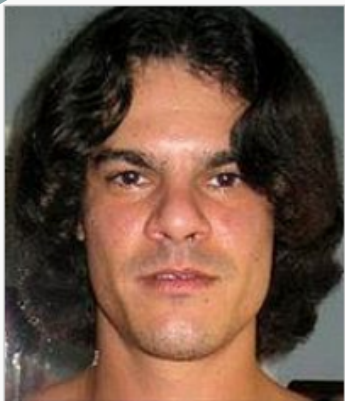


Photo of Albert Gonzalez by U.S. Secret Service

used sql injection and packet sniffers

navigation

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

search

Go Search

interaction

- [About Wikipedia](#)
- [Community portal](#)

Done

Lessons From Law Enforcement (FBI)

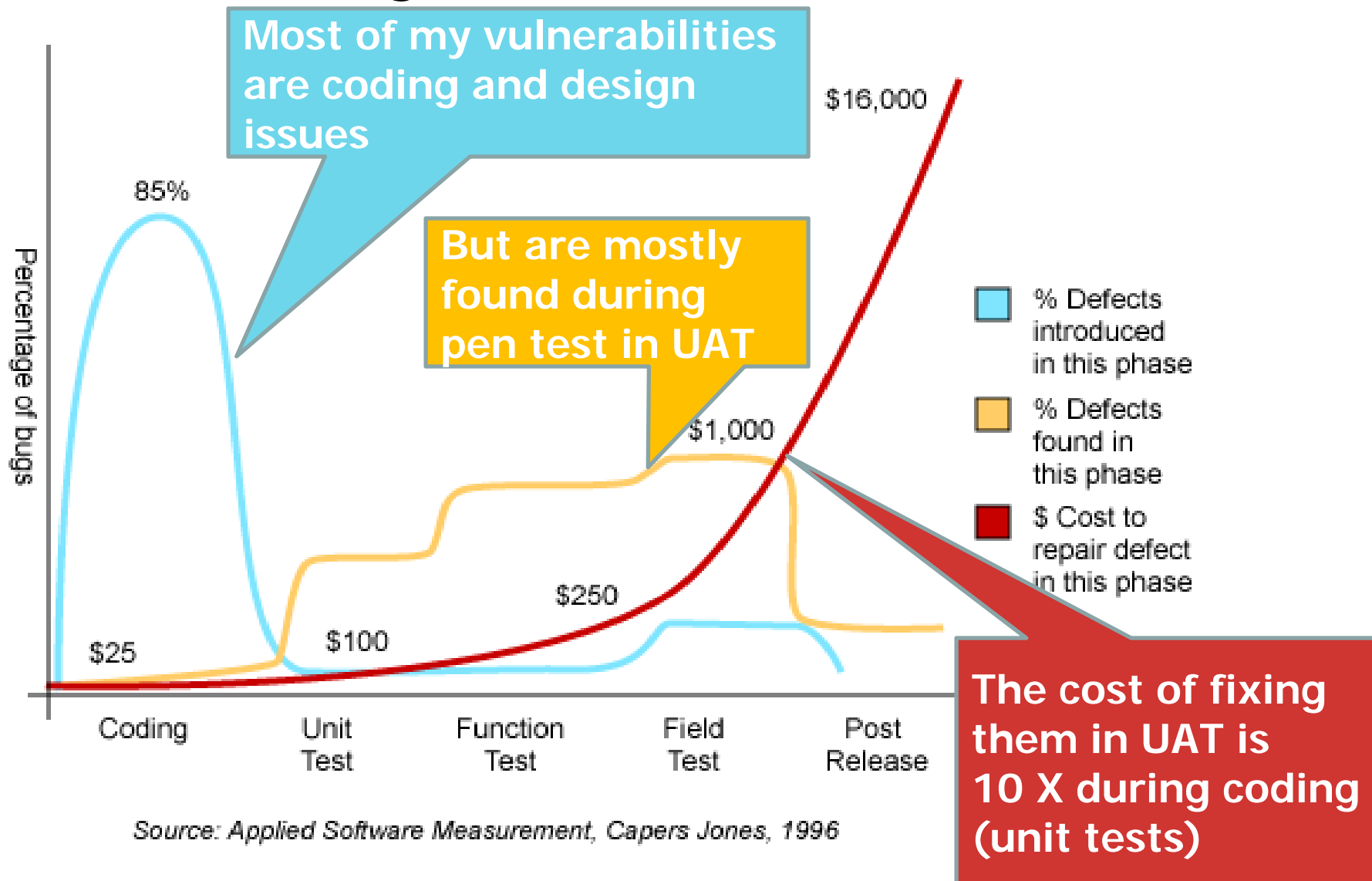
THREAT INTELLIGENCE:

Attack "xp_cmdshell on MSQL server to upload sniffers to capture CC transactions and ATM PINs from DB, HSM

RECCOMENDATIONS:

1. Disable xp_cmdshell,
2. Deny extended URL,
3. escape special characters such as "",
4. Use store procedures,
5. Run SQL Server and IIS under non-privilege,
6. Do not use "sa" hardcoded,
7. Lock account on mainframes against brute force
8. Use minimum privileges on AD/SQL server, restrict access
9. Use proxy server for internet access,
10. Implement firewall rules
11. Ensure HSM do not take commands with PIN in the clear

Defect Management/Costs Measurements



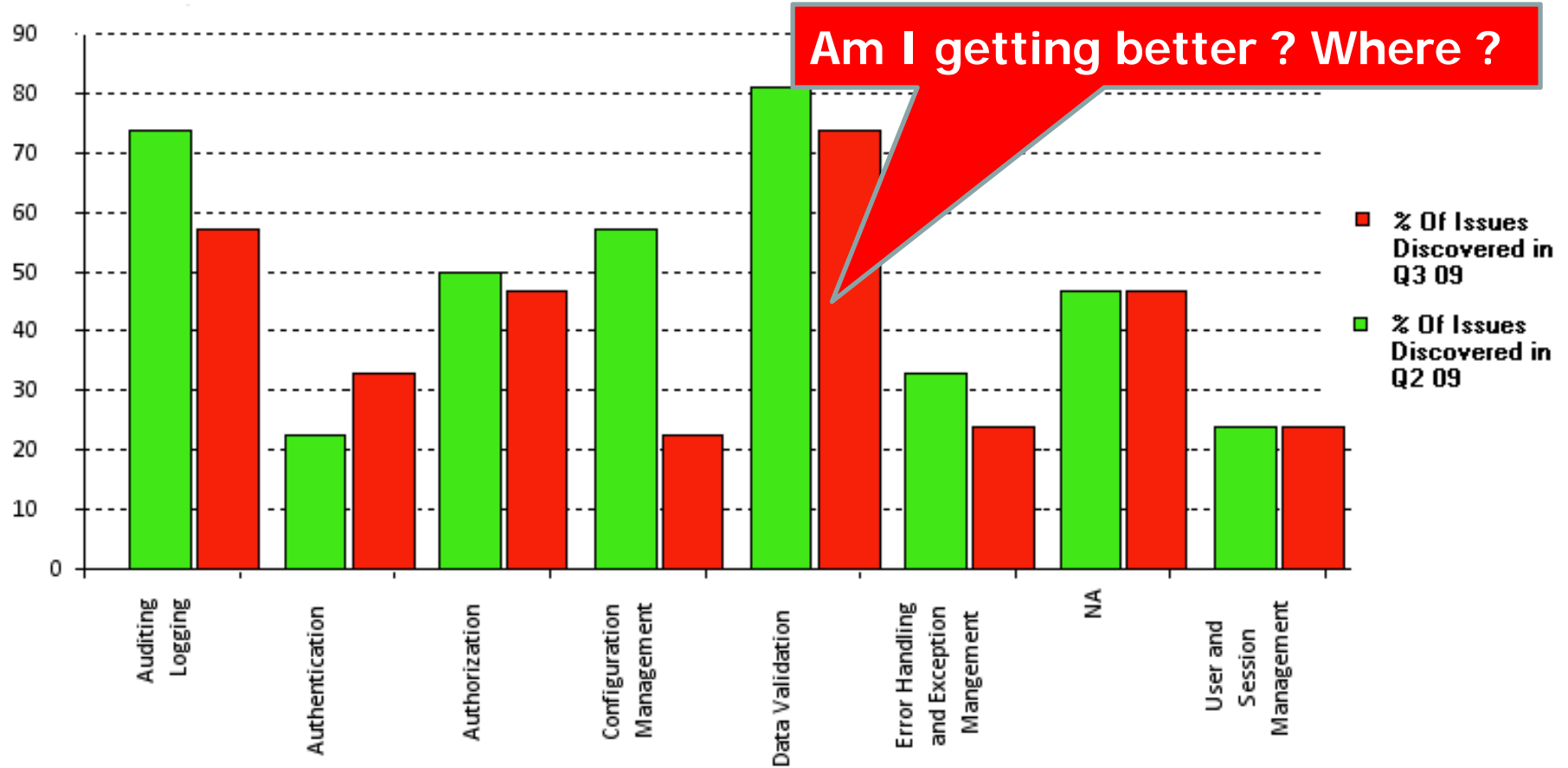
Analysts/Researchers Opinions

- **"75% of security breaches happen at the application layer"- *Gartner***
- **"Over 70 % of security vulnerabilities exist at the application layer, not the network layer" – *Gartner***
- **"If only 50 percent of software vulnerabilities were removed prior to production ... costs would be reduced by 75 percent" - *Gartner***
- **"Correction of security flaws at the requirement level is up to 100 times less the cost of correction of security flaws in fielded software" –*Fortify***

Why Using Metrics And Maturity Models?

- **Use vulnerability metrics to articulate software security needs/opportunities**
 - ▶ Point to software security root causes
 - ▶ Identify vulnerability trends
 - ▶ Analyze needs for improvements
- **Use maturity models to provide visibility on the organization's security capabilities**
 - ▶ Assess organization capability levels
 - ▶ Set goals and needs to reach the goals
 - ▶ Provide the roadmap

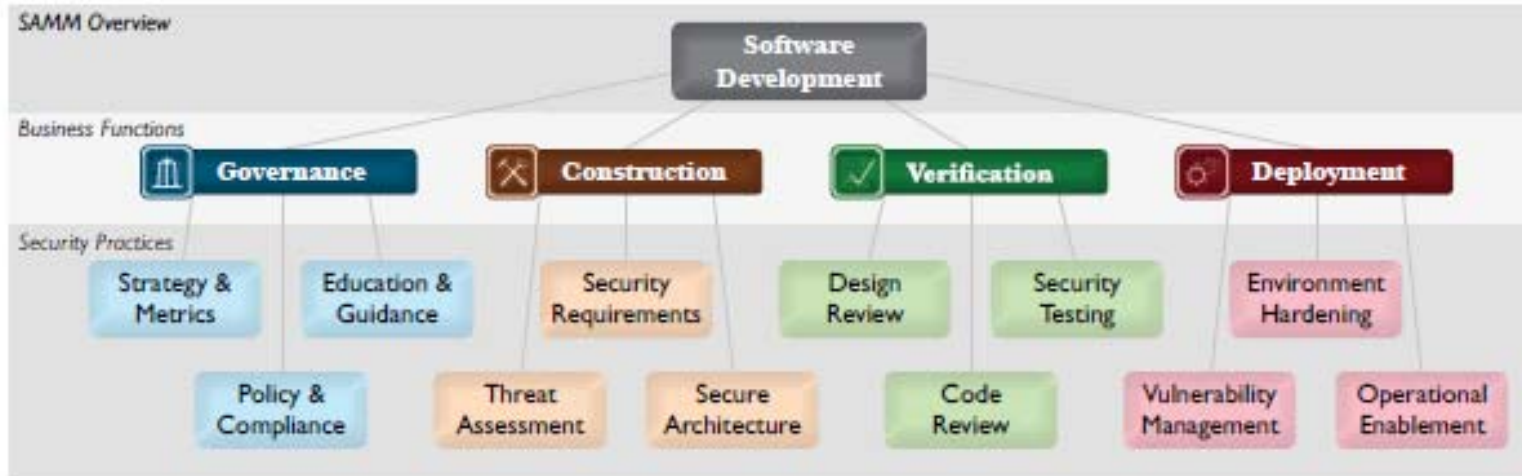
Vulnerability Taxonomies and Trends



Software Security Metrics Business Cases

- **Business Managers:** shows that projects **are on schedule and moving on target** and testing cycles for vulnerabilities are shorter translating in cost savings
- **Information Security Officers:** show that we are getting **better on reporting compliance** and manage risk reduction
- **Developer Leads:** show that **developers are getting better to write secure software** when provided with secure coding training and tools

Software Security Maturity Models: SAMM, BSIMM



Source SAMM : <http://www.opensamm.org/>

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

Source <http://www.bsi-mm.com/ssf/>

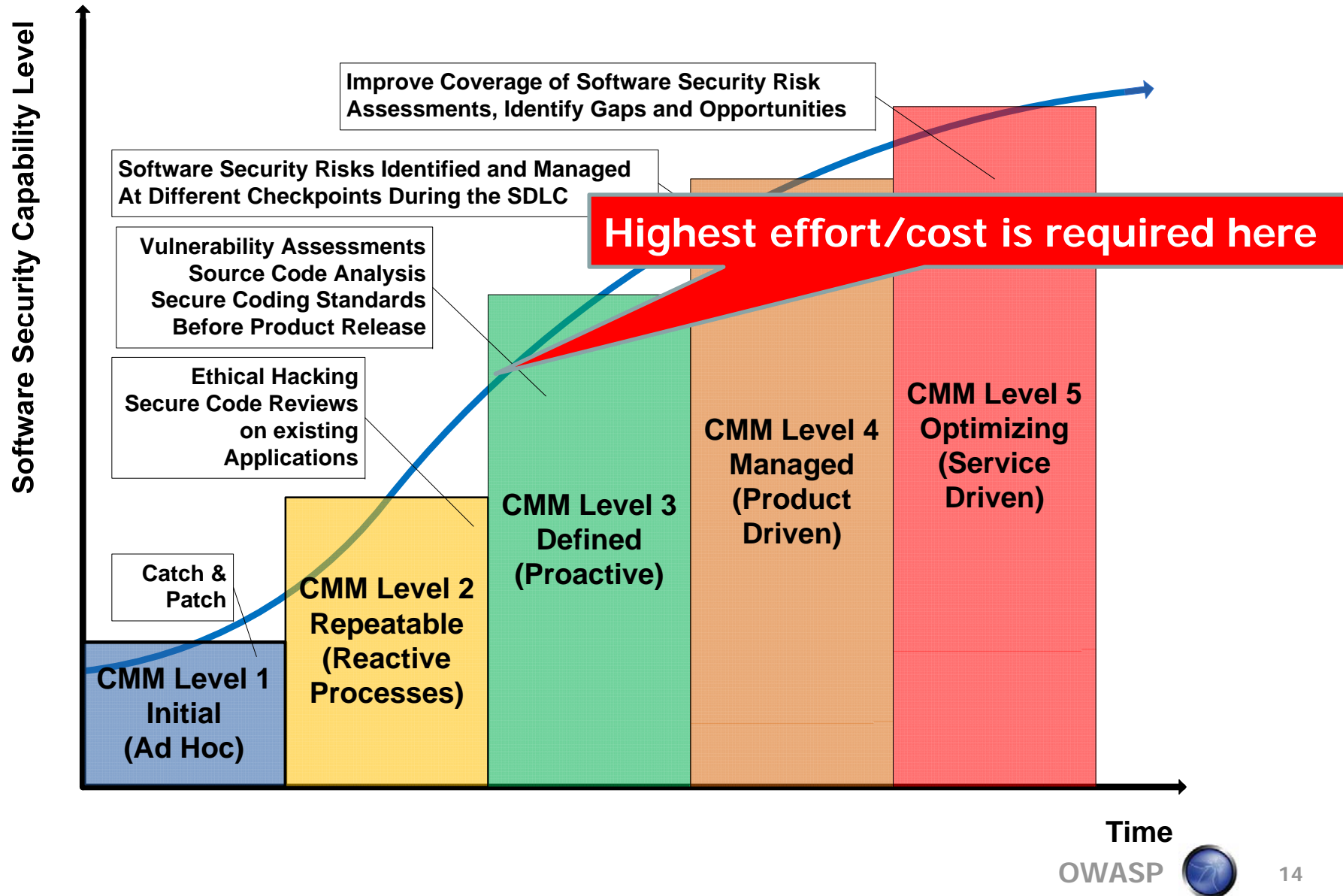
Activities, Objectives and Capability Levels

SSDL TOUCHPOINTS: CODE REVIEW			
Use of code review tools, development of customized rules, profiles for tool use by different roles, manual analysis, ranking/measuring results.			
	Objective	Activity	Level
CR1.1	know which bugs matter to you	create top N bugs list (real data preferred) (T: training)	1
CR1.2	review high-risk applications opportunistically	have SSG perform ad hoc review	
CR1.3	spread software security around without any process	establish coding labs or office hours focused on review	
CR2.1	drive efficiency/consistency with automation	use automated tools along with manual review	2
CR2.2	drive behavior objectively	enforce coding standards	
CR2.3	find bugs earlier	make code review mandatory for all projects	
CR2.4	know which bugs matter (for training)	use centralized reporting (T: strategy)	
CR2.5	make most efficient use of tools	assign tool mentors	
CR3.1	drive efficiency/reduce false positives	use automated tools	
CR3.2	combine assessment techniques	build a factory	
CR3.3	handle new bug classes in an already scanned codebase	build capability for new codebase	

Use this as a yardstick to compare software security practices with other organizations

Source BSIMM <http://www.bsi-mm.com/ssf/>

The Software Security Maturity Curve (CMM)



Cost vs. Benefit Analysis (CBA)

- ▶ Purpose is to **weight the cost of software security initiative vs. the benefits**

$$\text{CBRatio} = \frac{\text{COST of initiative}}{\text{BENEFIT of initiative}}$$

- ▶ **Need to cost quantify factors and compare them** (to compare apples with apples) for example:

- ▶ **COSTs:**

- ▶ **Secure software engineering costs** for training, new processes and tools

- ▶ **BENEFITs:**

- ▶ **Reduced costs** in fixing with patching, lessen business impact of exploits

Assumption Costs and Failure Costs of the Software Security Initiative

■ Assumption Costs (proactive):

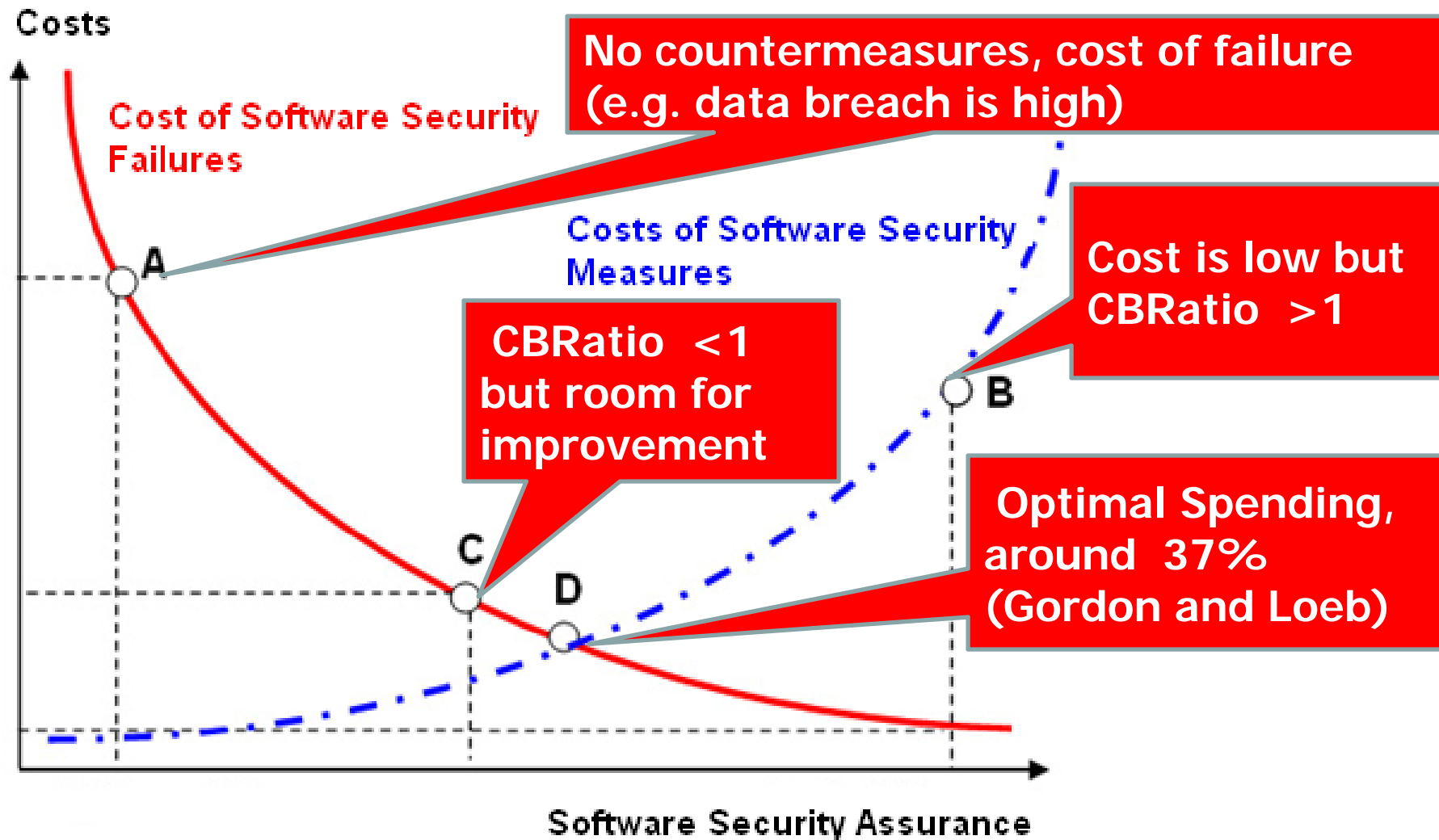
- ▶ Cost of acquiring tools, standards and processes to develop secure software
- ▶ Cost of hiring and/or training a software security team
- ▶ Costs for implement security features (e.g. estimate possible as function of KLOC)

■ Failure Costs (reactive):

- ▶ Cost of develop and/or deploy patches
- ▶ Cost of incident response
- ▶ Cost of vulnerability exploits resulting in data breach, fraud, denial of service, quantifiable damage to the organization

The most difficult to estimate

Assumption Costs vs. Failure Costs



Data Loss Liabilities Estimates

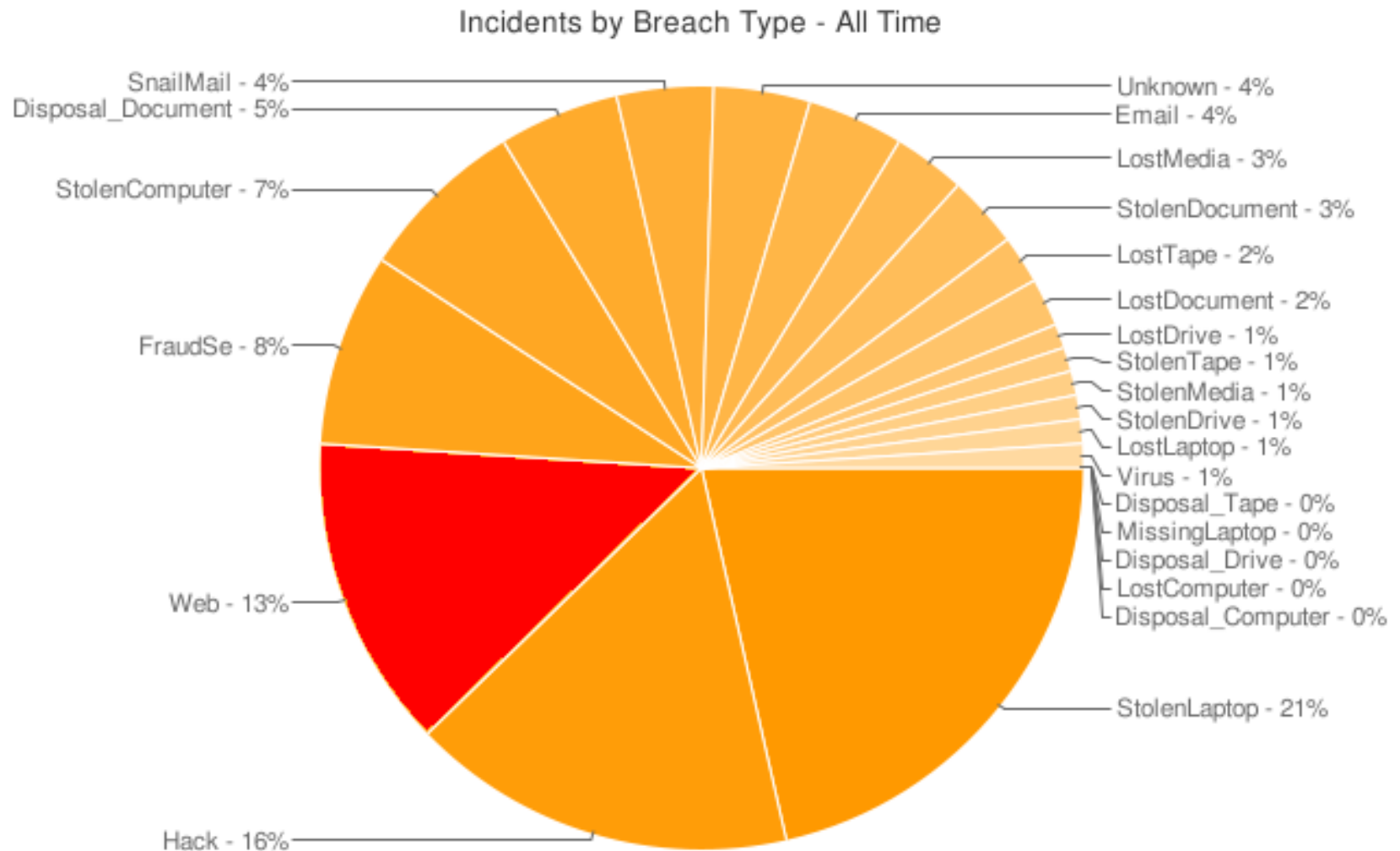
■ Consider FTC data (2003)

- ▶ 4.6 % of US population suffered identity fraud
- ▶ Companies spent 3×10^8 hours repairing the troubles caused + \$ 5 Billion dollar spent out of pocket
- ▶ Minimum wage of 5.15 \$/hr (in 2003)
- ▶ 10 Million people involved
 - $P = 4.6 \%$
 - $L = \frac{3 \times 10^8 \times \$ 5.15/\text{hr} + \$ 5 \times 10^9}{10^7 \text{ victims}} = \text{\$ 655/victim}$

■ My annual liability ($P \times L$) for each data theft victim is \$ 30.11

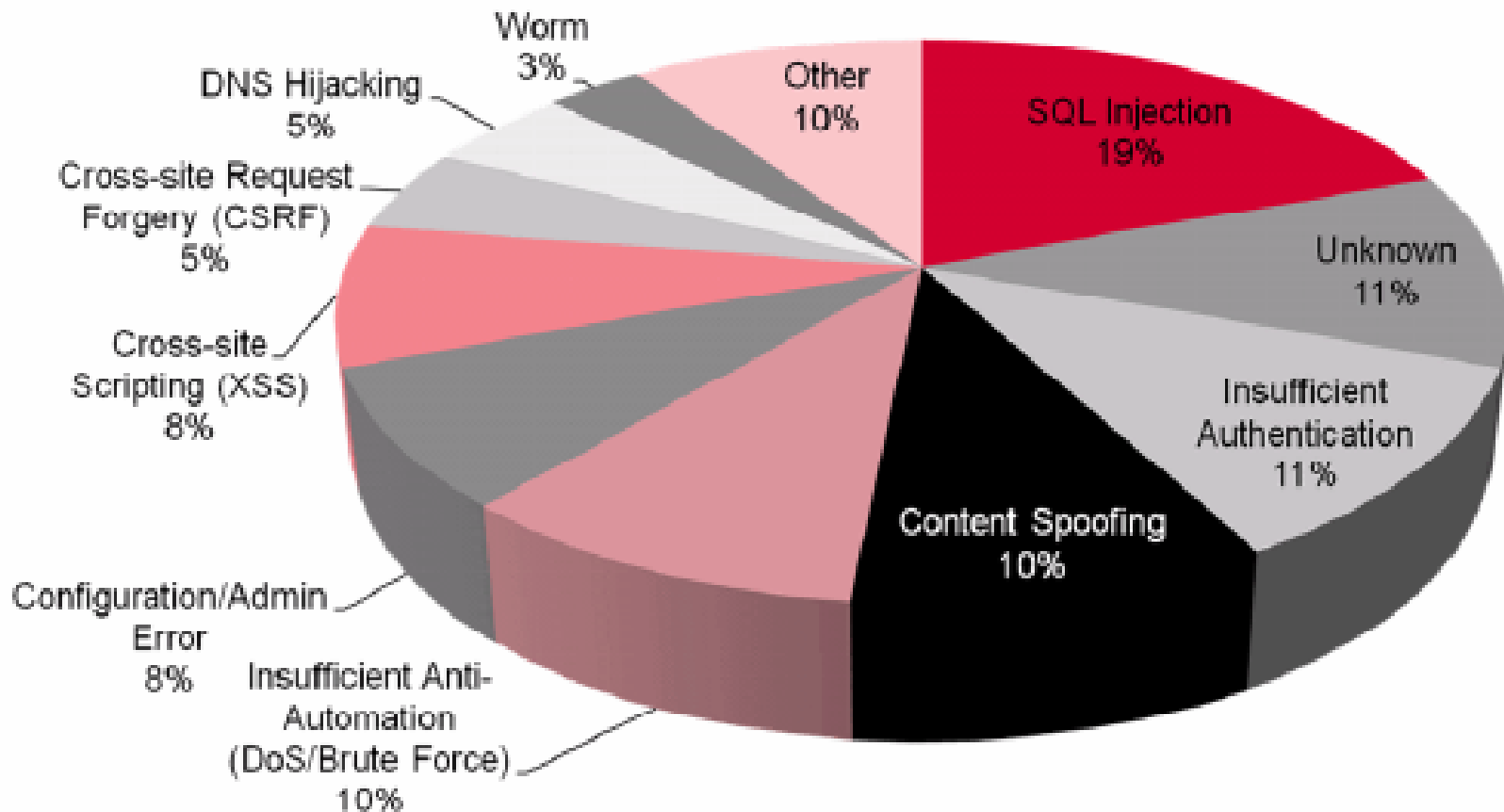
SOURCE: Dan. E. Geer, Economics & Strategies of Data Security

Data Losses As Web Breaches (datalossdb.org)



SOURCE: Open Security Foundation Data Loss Statistics

Which Vulnerabilities Are Exploited? (WHID)



SOURCE: Breach Security The WHID 2009, August 2009

Estimating SQL Injection Attack Liability

■ **Probability of attack** by type and attack vector incident (identity theft) data:

- ▶ **13 % of incidents involve breaches of web channel** (datalossdb.org)
- ▶ **19 % of incidents use SQL injection as attack vector** (WHID)
- ▶ $P = 0.13 \times 0.19 = 0.025$ (2.5 %)

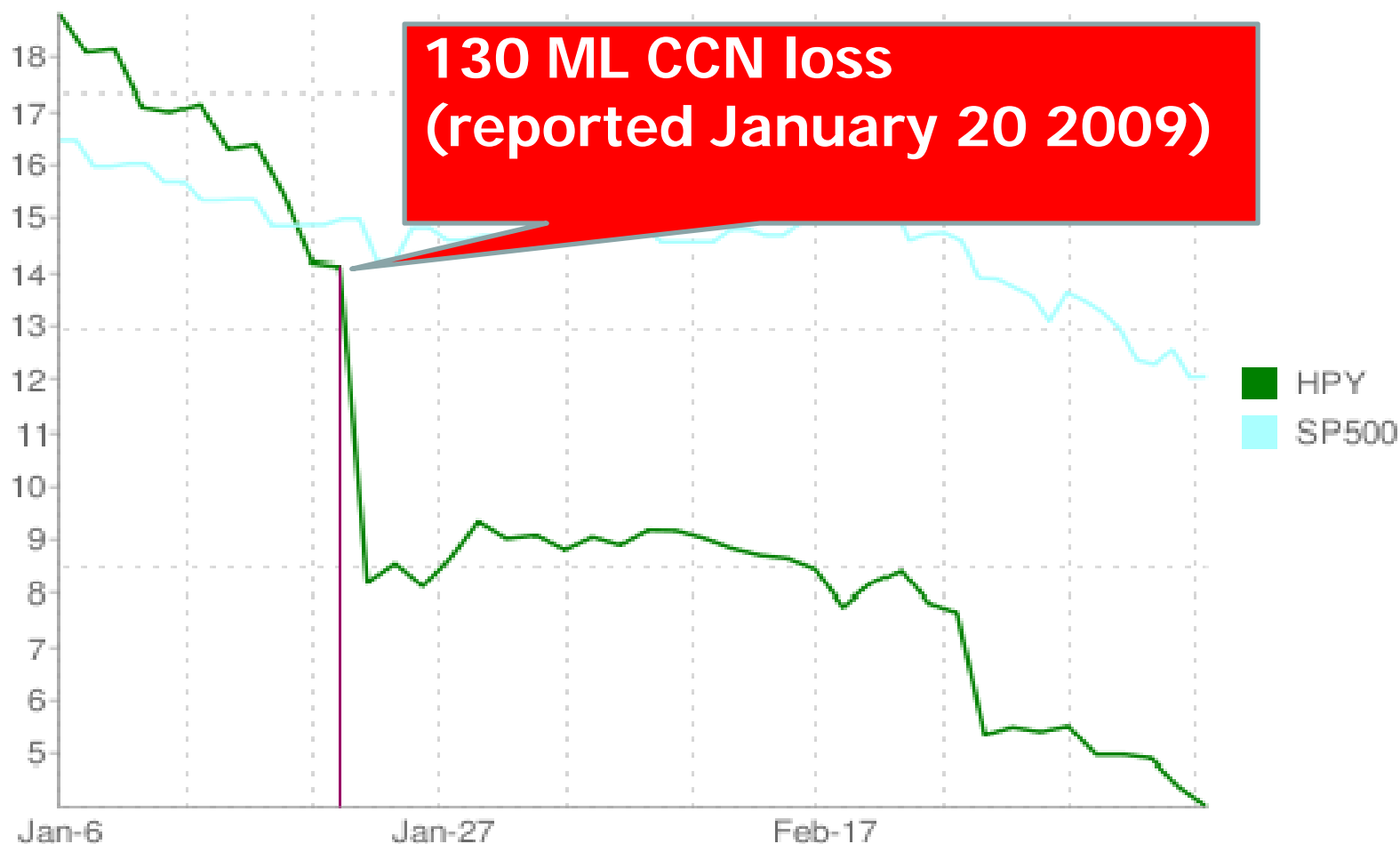
■ **Estimate data loss for this attack:**

- ▶ \$ 655 per identity theft victim (2003 FTC data)
- ▶ 94 million individual records stolen (TJX incident)
- ▶ $L = 94 \times 10^6 \times 0.025 \times 655 = \$ 1.5 \text{ Billion}$

Reporting of Losses in Quarterly Earnings

- The cyber attack on the retailer Marshalls and TJ Maxx (94 Million CCN reported in Jan/2007): **after-tax cash charge of approximately \$118 million**, or \$.25 per share.
- The company increased its estimate of pre-tax charges for the compromise to nearly **\$216 million**.
- According to some experts, **TJX may have to spend in the end a total between \$ 500 Million to \$ 1 Billion** (BankInfoSecurity.com), including non compliance fees (e.g. PCI-DSS) litigation fees and government fines.

Another Way to Look at Business Impact Of Data Breaches : Drop in Stock Price



Quantitative Risk Analysis

■ Goal:

- ▶ **Justify spending to improve security by assigning an objective monetary value to risk**

■ Risk Analysis Methodology:

- ▶ **Determine the Exposure Factor:** Percentage of asset loss caused by identified threat (e.g. 20%)
- ▶ **Determine Single Loss Expectancy (SLE):**
EF x the value of assets (e.g. \$ 1 ML * 30% = \$ 200 K)
- ▶ **Estimate Annualized Rate of Occurrence (ARO):**
twice in ten years $2/10=0.2$, 1 every year = 1
- ▶ **Determine the Annualized Loss Expectancy (ALE)**
 $ALE = SLE \times ARO = \$ 40 \text{ K}$

Use Quantitative Risk Analysis to Estimate Annual Loss Due to SQL Injection Exploit

- Exposure Factor (likelihood) of data loss via SQL injection attack: 2.5%
 - ▶ Based upon data loss db and WHID calculated probability data)
- SLE (EF x Value Assets): \$ 43 Million
 - ▶ Asset Value: assume SQL injection attack will cause fraud for 3 million credit card accounts (on-line web site for major bank) at a 580 \$/account (use SANS data)
- ARO: 40 % (four every 10 years)
- ALE (ALO X SLE): = **\$ 17 Million**

ROSI Of Secure Software Initiatives

■ ROSI (Return Of Security Investment)

▶ $\text{ROSI} = \text{Savings (Avoided loss)} / \text{Total Cost Of Solution}$

■ Goal:

▶ Answer the question on how much I can save by investing in Software Security

■ According to previous studies (Soo Hoo-IBM):

- ▶ For every 100,000 \$ spent in software security I save:
 - \$21,000 (21%) when defects are fixed and identified during design
 - \$15,000 (15%) when defects are fixed during implementation
 - \$12,000 (12%) when defects are fixed during testing

Using ROSI to justify software security investments

$$\blacksquare \text{ ROSI} = \frac{[(\text{ALE} \times \% \text{ Risk Mitigation}) - \text{SCost}]}{\text{SCost}}$$

■ Calculation example:

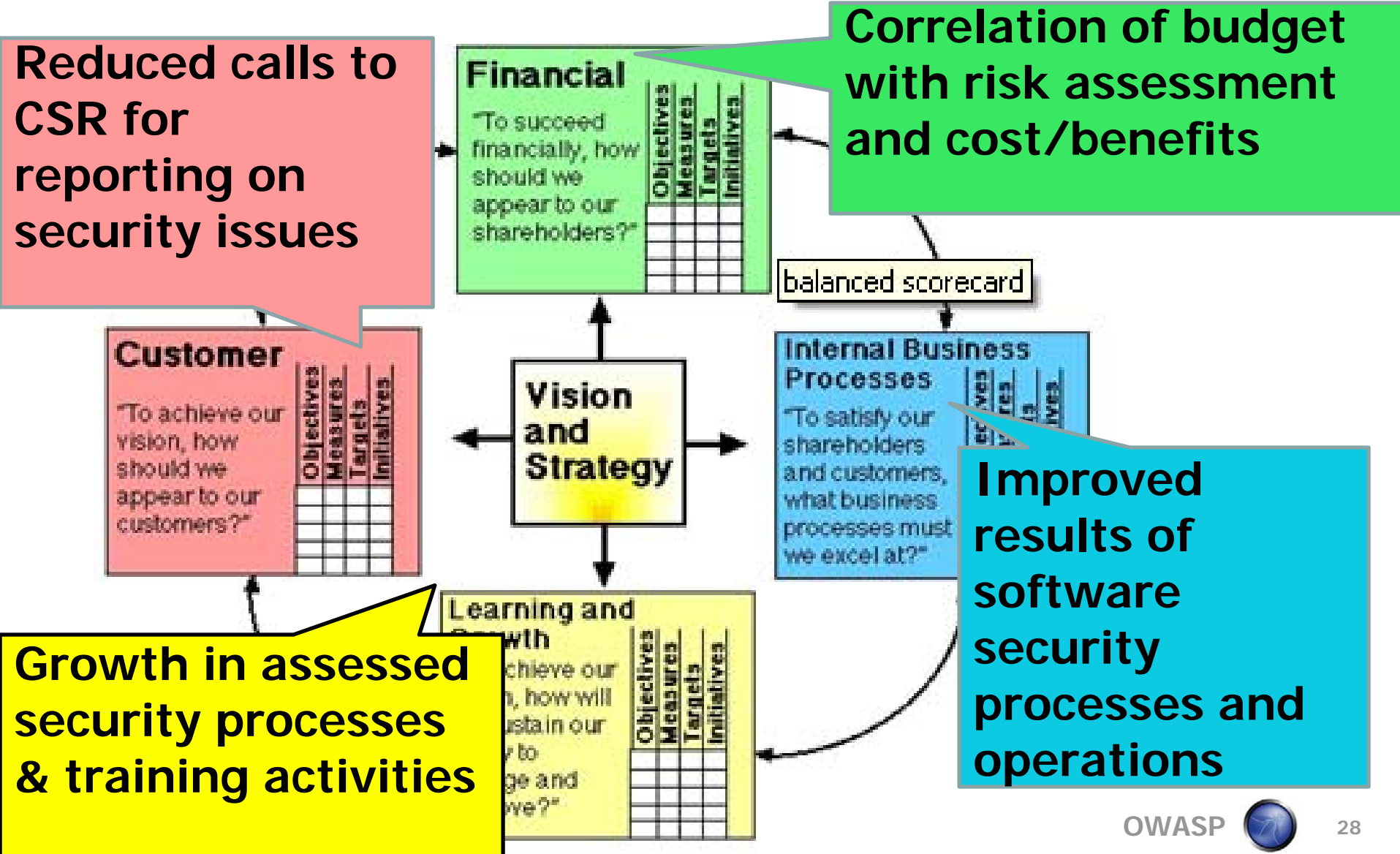
- ▶ ALE: \$ 17 Million, risk exposure for SQL injection
- ▶ Risk Mitigation: 75 % of risk mitigated by software security solution source code analysis, filtering
- ▶ SCost: \$ 4 Million, Total Cost of Ownership (TCO) software security solution
- ▶ Savings = \$ 8.75 Million, loss prevention savings
- ▶ ROSI = 210 %

Negative = investment not justifiable

Null = no return on investment

Positive = justifiable as compared with other solutions

Security Software Assurance Metrics: Balanced Scorecards



Software Security Metrics In Support Of Business Cases

■ Metrics of technical value

- ▶ Costs for testing and fixing vulnerabilities
- ▶ Percent security requirements satisfied
- ▶ Percent developers with software sec. certifications

■ Metrics of comparative value

- ▶ TCO of software security activities vs. unit revenue
- ▶ Secure software engineering costs vs. patching costs

■ Metrics of business value

- ▶ Estimate for vulnerability & risk assessment costs
- ▶ Budget to address gaps in software sec. processes
- ▶ Costs for security certifications per business unit

Come on is not so hard..



In Summary

- ✓ Rationale For Software Security Business Case
- ✓ Preparing the Business Case
 - ✓ Maturity Models
 - ✓ Metrics and Measurements
- ✓ Making the Business Case
 - ✓ Software Security Assurance Awareness
 - ✓ Failure Costs vs. Assumption Costs
 - ✓ Qualitative Risk Assessments
 - ✓ Return Of Security Investment (ROSI)
 - ✓ Performance Measurement Metrics
- Questions & Answers

Thanks for listening, further references

■ Applied Software Measurement: Assuring Productivity and Quality

- ▶ <http://www.amazon.com/Applied-Software-Measurement-Assuring-Productivity/dp/0070328269>

■ PCI-Data Security Standard (PCI DSS)

- ▶ https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

■ A CISO's Guide to Application Security

- ▶ http://www.nysforum.org/committees/security/051409_pdfs/A%20CISO'S%20Guide%20to%20Application%20Security.pdf

Further references con't

■ Gartner 2004 Press Release

- ▶ http://www.gartner.com/press_releases/asset_106327_11.html

■ Making The Business Case For Software Assurance

- ▶ <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/685-BSI.html>

■ SEI Capability Maturity Model Integration CMMi

- ▶ <http://www.sei.cmu.edu/cmmi/>

Further references con't

- Software Assurance Maturity Model
 - ▶ <http://www.opensamm.org/>
- The Software Security Framework (SSF)
 - ▶ <http://www.bsi-mm.com/ssf/>
- National Information Assurance Glossary
 - ▶ http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
- Dan. E. Geer, Economics & Strategies of Data Security
 - ▶ <http://www.verdasys.com/thoughtleadership/>

Further references con't

- Open Security Foundation, Data Loss Statistics
 - ▶ <http://datalossdb.org/statistics>
- The WHID 2009 BI-Annual Report, August 2009
 - ▶ http://www.breach.com/resources/whitepapers/downloads/WP_TheWebHackingIncidents-2009.pdf
- Quantitative Risk Analysis Step-By-Step
 - ▶ http://www.sans.org/reading_room/whitepapers/auditing/quantitative_risk_analysis_stepbystep_849?show=849.php&cat=auditing
- Breach Worse Than Reported..
 - ▶ http://www.bankinfosecurity.com/articles.php?art_id=606

Further references con't

■ Estimating Benefits from Investing in Secure Software Development

- ▶ <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/267-BSI.html>

■ Return On Security Investment (ROSI)

- ▶ http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf

■ Models for Assessing the Cost and Value of Software Assurance

- ▶ <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/684-BSI.html>