

Sean L. Harrington
MCSE, CISSP, CSOXP, CHFI,
JD candidate (3L)

Computer & Technology Law Section
"Releasing Vulnerable Code:
Corporate and Individual Liabilities"

Nov. 8, 2011



Impact / Injury

Software Development Lifecycle

Traditional Basis of Liability

Trends

Copyright 2000 by Randy Glasbergen.
www.glasbergen.com



"OUR COMPETITION LAUNCHED THEIR WEB SITE, STOLE ALL
OF OUR CUSTOMERS AND PUT US OUT OF BUSINESS
WHILE YOU WERE IN THE JOHN."

Without Plaintiff[-employer]'s knowledge, defendant[-employee] called [the employer]'s payroll company and increased his salary from approximately \$ 40,000 per year to \$ 125,000 per year. [Plaintiff] discovered this unauthorized salary increase . . . and confronted defendant. Defendant admitted stealing . . . and gave [plaintiff] a check [that later bounced]. [Plaintiff] immediately terminated defendant and did not permit him to re-enter his office because he "was very concerned about what [defendant] could do in a very short period of time because he knew a lot about the computer."

State v. M.A., 402 N.J. Super. 353, 361 (App.Div. 2008)

IMPACT (INJURY)

Present & future business

Reputation

Goodwill

Shareholder value / Market Capitalization

Legal & Regulatory Liability

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL [COMPANY] OR ITS LICENSORS, RESELLERS, SUPPLIERS OR AGENTS BE LIABLE TO YOU FOR (i) ANY COSTS OF PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS AND SERVICES, LOSS OF PROFITS, LOSS OF USE, LOSS OF OR CORRUPTION TO DATA, BUSINESS INTERRUPTION, LOSS OF PRODUCTION, LOSS OF REVENUES, LOSS OF CONTRACTS, LOSS OF GOODWILL OR ANTICIPATED SAVINGS OR WASTED MANAGEMENT AND STAFF TIME; OR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES WHETHER ARISING DIRECTLY OR INDIRECTLY OUT OF THIS LICENSE AGREEMENT, EVEN IF [COMPANY] OR ITS LICENSORS, RESELLERS, SUPPLIERS OR AGENTS HAS BEEN ADVISED SUCH DAMAGES MIGHT OCCUR.

CYBERCRIME HIGHLIGHTS

- Average annual cost of cybercrime \$5.9M (ranging from \$1.5M - \$36.5M).
- surveyed companies experienced 72 successful attacks per week (avg. 1.4 per organization), up 44% from last year.
- most costly cybercrimes are malicious code, denial-of-service, stolen or hijacked devices, malicious insiders.
- Stolen information, attack tools, and crime services are bought and sold in an underground economy (Credit card numbers can be bought and sold for \$0.10 - \$25 per record and bank account credential prices range from \$10 - \$1,000)
- Symantec estimates that the underground market for this data is worth hundreds of millions of dollars and the aggregate value of the compromised accounts is in the billions.

CYBERCRIME HIGHLIGHTS (CONT.)

- According to the Web Application Security Consortium, today more than 87% of Web applications carry a vulnerability classified as high risk or worse.
- Cross Site Scripting, SQL Injection, *etc.* take advantage of the trust, reputation, and popularity of a site in order to infect its visitors with malware exploit toolkits. When unsuspecting users visit the site, they are silently redirected to an attacker-controlled site hosting the exploit kit and tries to download the malware onto the victims computer.
- Attacks against retail customers increased 43% in the first 9 months of 2011, resulting from an increase in popularity of web exploit kits.
- Web applications are attacked directly to steal account information, credentials, gain access to money movement functionality, and commit identity theft.

CYBERCRIME HIGHLIGHTS (CONT.)

- Recent survey of 300 IT professionals (2/3 of them working in companies with more than 10,000 employees), revealed that 25% of them knew at least one co-worker who used privileged login credentials to inappropriately access confidential information.
- 42% indicated that the IT staff freely shared passwords and access to multiple systems and applications.
- 25% indicated that at least some of the superuser passwords granting privileged access to the network were less complex than what was required of end users.
- 48% reported that privileged account passwords had remained the same for at least 90 days.

CYBERCRIME HIGHLIGHTS (CONT.)

- Federal agencies reported 41,776 incidents in 2010 - including malware, unauthorized access and denial-of-service (there were just 5,503 in 2006).
- All 24 major agencies were assessed had deficiencies related to access controls, configurations and security management. Most of the suggestions for enhancing security have not been fully implemented.
- The IRS was cited for not sufficiently restricting employee access to databases along with failure to address previously reported security issues.
- Not one of the 24 agencies have fully implemented an agency-wide information security program as required by the Federal Information Security Management Act (FISMA).

CYBERCRIME HIGHLIGHTS (CONT.)

Who is behind data breaches?

92% stemmed from external agents (+22%)

17% implicated insiders (-31%)

<1% resulted from business partners (-10%)

9% involved multiple parties (-18%)

How do breaches occur?

50% utilized some form of hacking (+10%)





49% incorporated malware (+11%)

29% involved physical attacks (+14%)

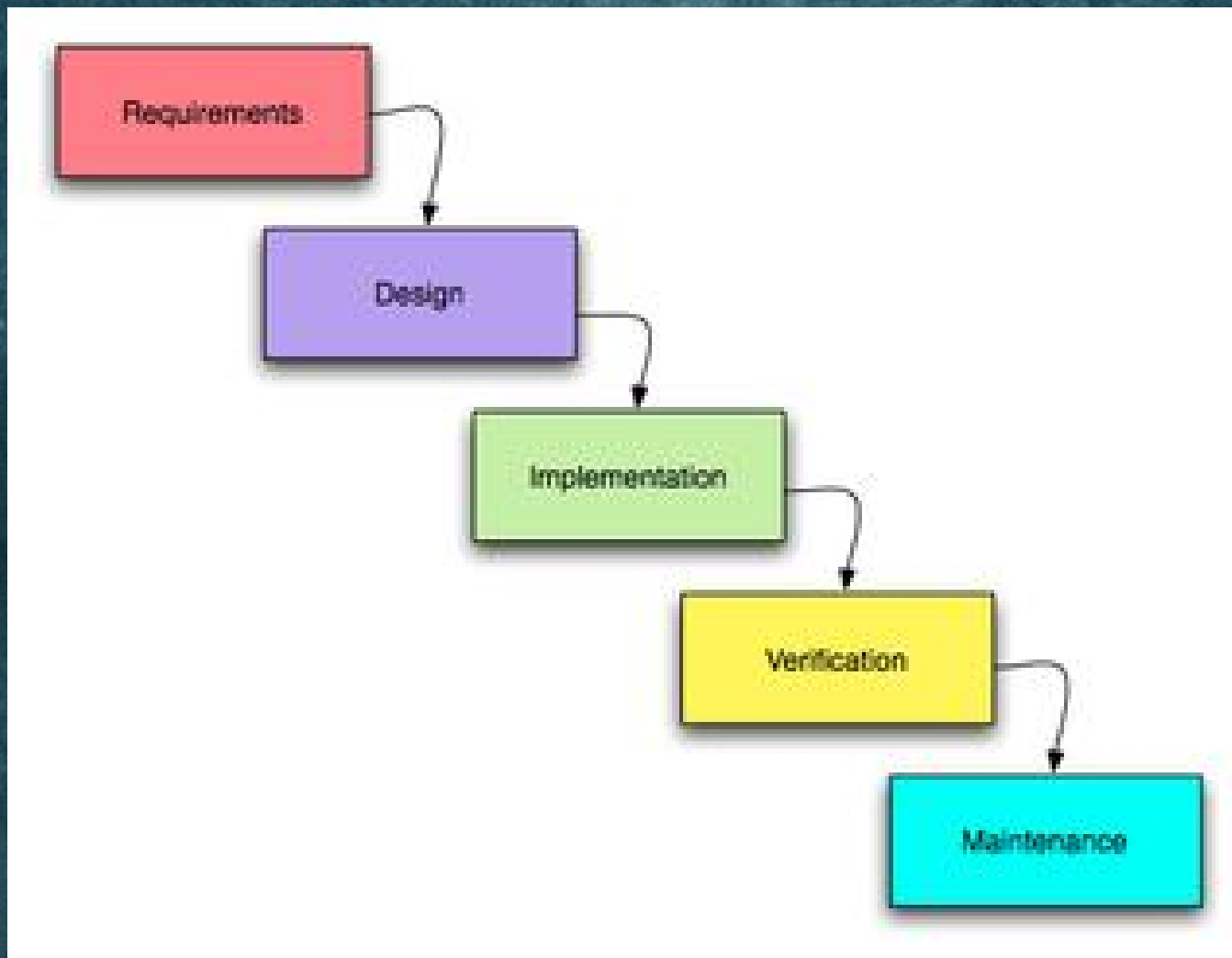
17% resulted from privilege misuse (-31%)

11% employed social tactics (-17%)

IMPACT (INJURY)

| Victim | Attack | Business Impact | Effective Countermeasures |
|--|--|---|--|
|  Citigroup ^{2,3} 6/14/2011 | <ul style="list-style-type: none"> Account # in URL & lack of authorization checks Allowed an authenticated user to access other user's accounts | <ul style="list-style-type: none"> \$2.7 million fraudulent purchases 360K credit card records stolen | <ul style="list-style-type: none"> Security training Security requirements / guidelines Threat modeling Abuse case tests |
|  UBS ⁴ 9/15/2011 | <ul style="list-style-type: none"> Unauthorized trading due to trader with excessive access | <ul style="list-style-type: none"> Lost \$2.3 Billion over 3 months | <ul style="list-style-type: none"> Threat Modeling: identify business logic-related security requirements, controls, and security tests |
|  American Express ⁵ 10/7/2011 | <ul style="list-style-type: none"> Debug mode left enabled on website Cross site scripting vulnerability on debug page would allow attackers to access customer accounts through session hijacking | <ul style="list-style-type: none"> Customer notification and damaged reputation | <ul style="list-style-type: none"> Perform static code analysis Where possible, keep test code in a separate project from production code Don't leave dead code in production |
|  HDFC Bank ⁶ 9/6/2011 | <ul style="list-style-type: none"> Hidden SQL Injection Vulnerability Allowed full database access | <ul style="list-style-type: none"> Vulnerability made publically available, damaging HDFC's brand | <ul style="list-style-type: none"> Security training / guidelines Perform static code analysis Automated security testing |

Software Development Lifecycle (SDLC)



SLDC Traditional Views

Tradeoff: Features vs. bugs

functionality vs. security

Security a remediation afterthought

Peer code review a luxury

“Most security professionals are usually not software developers.”
Shon Harris, CISSP All-in-One Exam Guide at 906.

“Many software developers do not have security as a main focus.” *Id.*

Andrew Pardoe, Liability for Software Defects:

Software developers generally create software because they have identified a problem they want to solve. As Eric Raymond wrote, "Every good work of software starts by scratching a developer's personal itch." The programmer had a problem to solve and wrote a program to solve the problem. Having already done the work and not having intended to profit from the work the programmer releases the code for other people to use. Because the developer has minimal incentive to release software for other people to use the warranty expressed by most open-source licenses can be reduced to "if it breaks, you get to keep both pieces."

SOFTWARE

Intrinsic software: an embedded component of a product (e.g., microwave oven, automobile)

Extrinsic software: loaded onto a machine by end-user

Web-facing: Internet banking, PayPal

Back-office (middleware, database).
E.g., amortization calculations, trade settlement, record keeping, cloud storage, *etc.*

SLDC Progressive Views

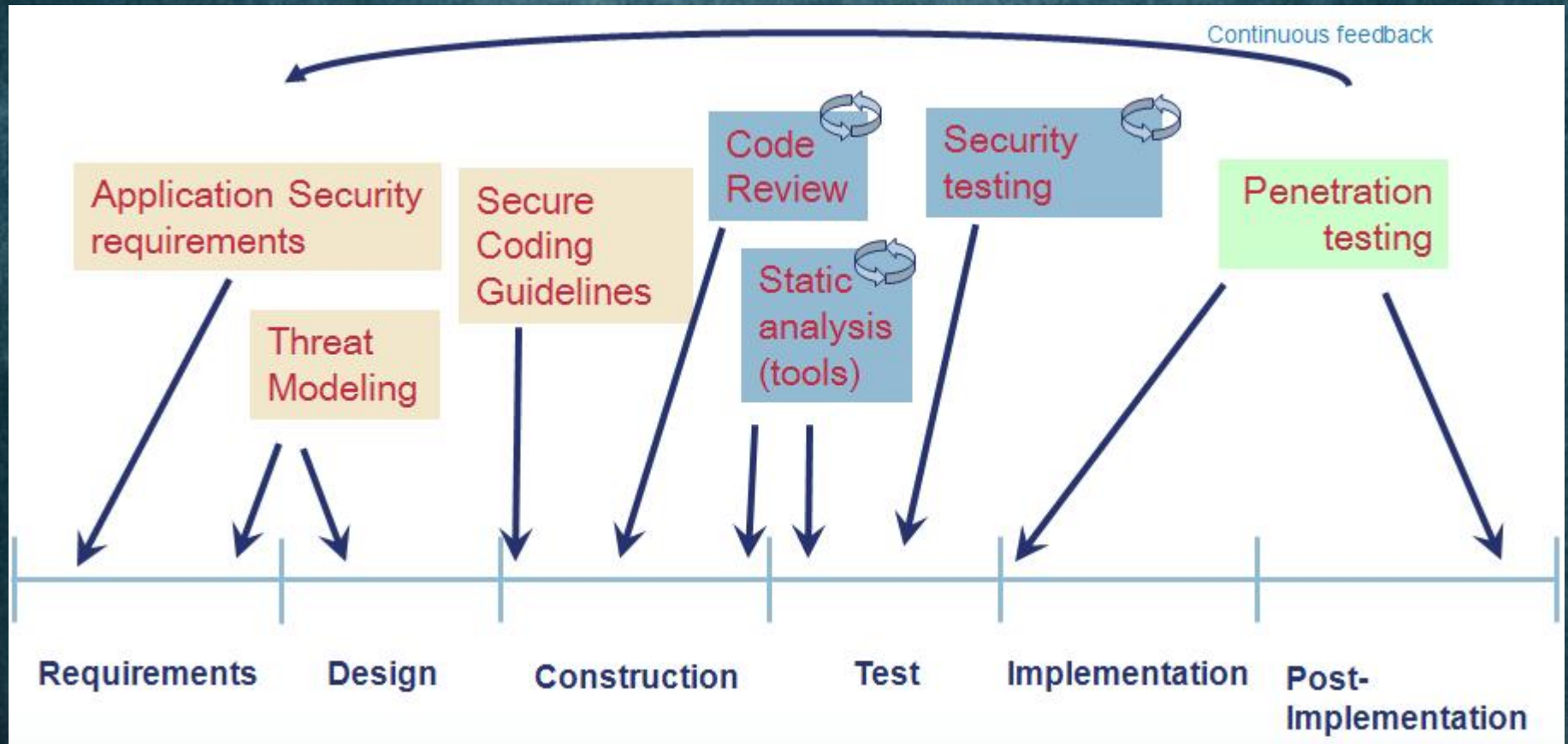
Security a non-functional requirement

Security is a feature (lack thereof is a bug)

Security must be incorporated into initial requirements gathering

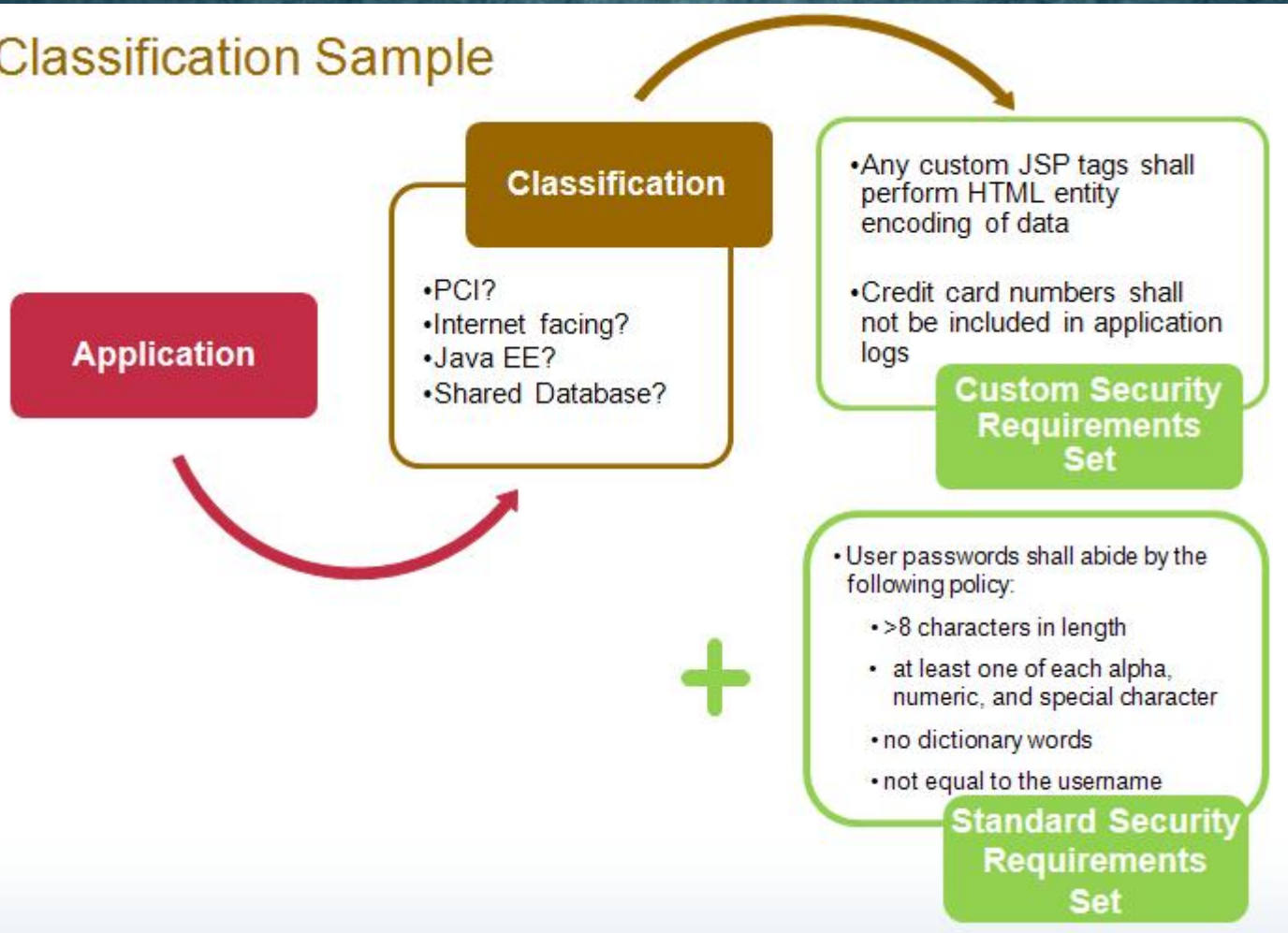
Coding best practices (e.g., peer code review) are essential

Software Development Lifecycle

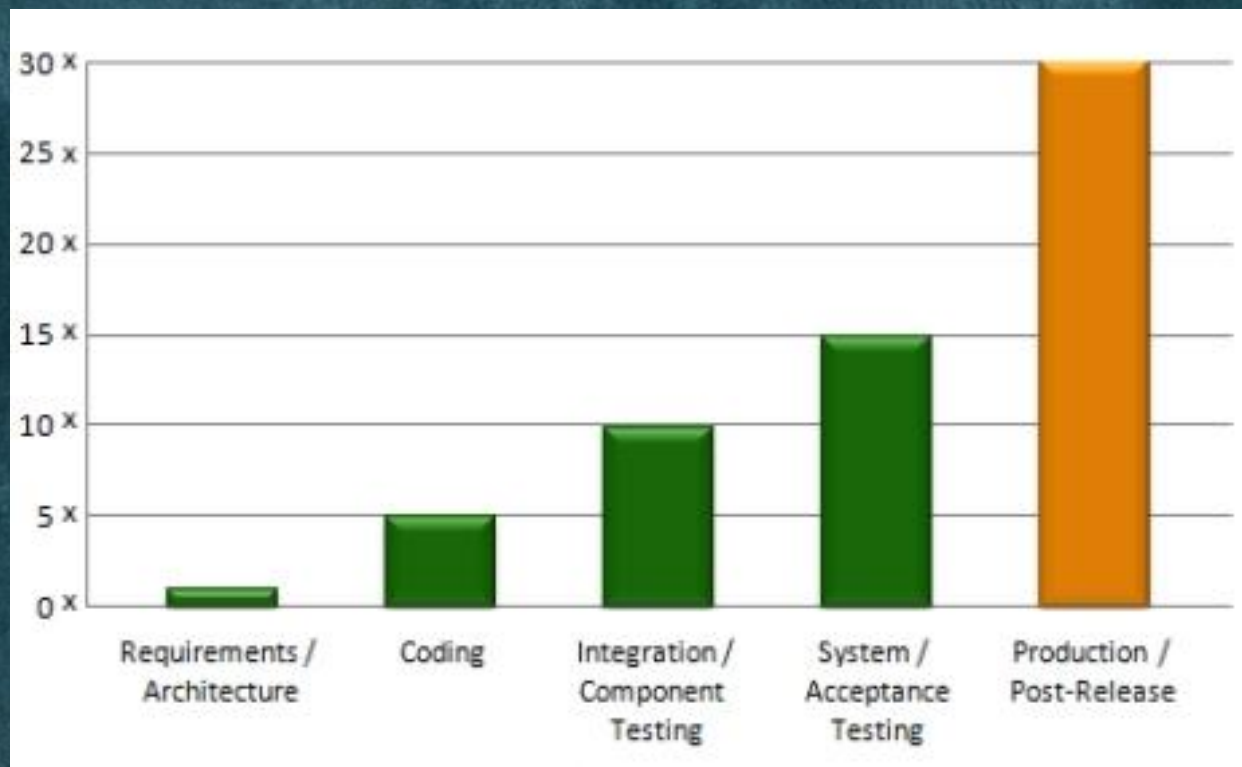


Initial Requirements

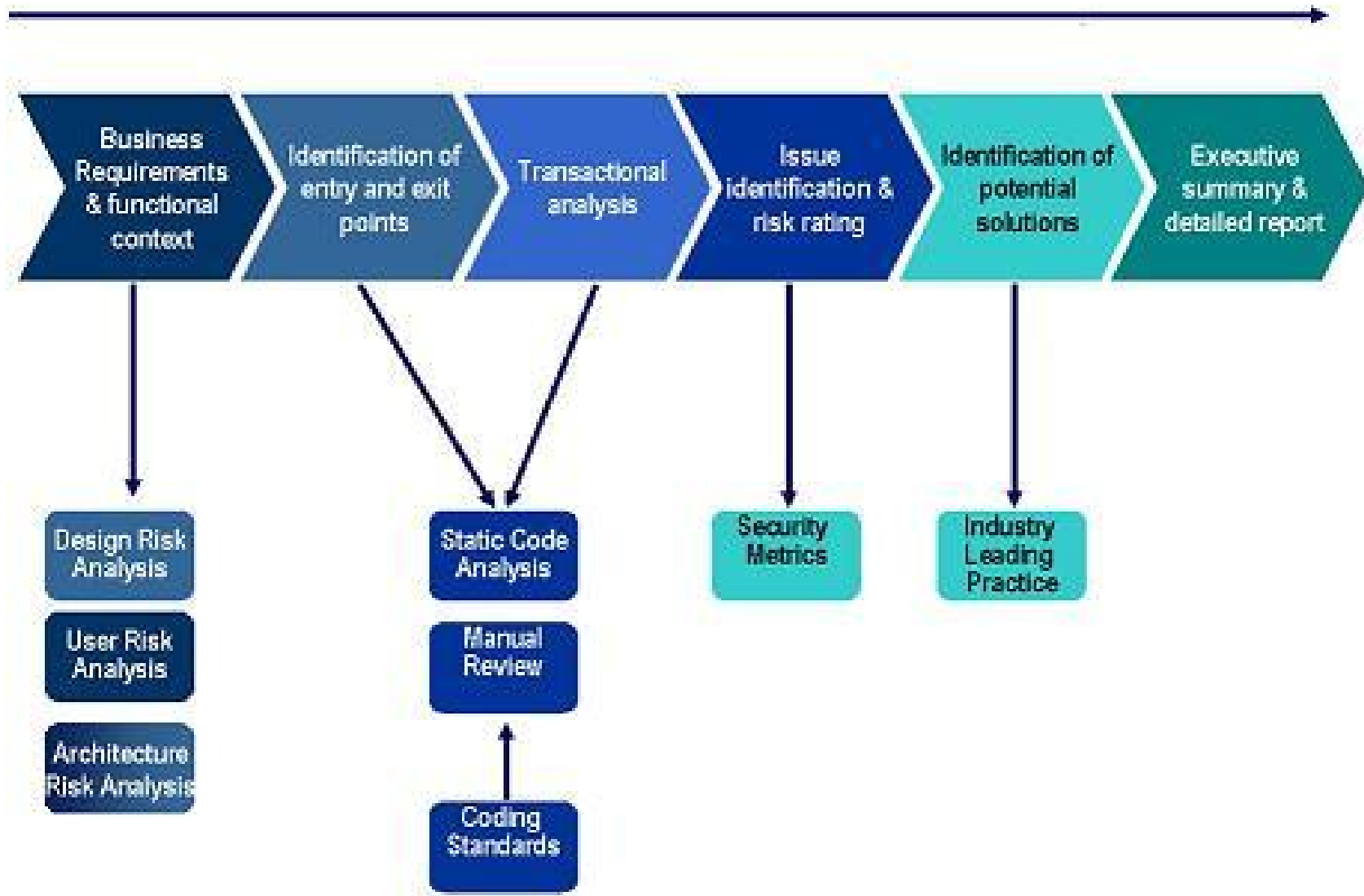
Classification Sample



The National Institute of Standards and Technologies (NIST) estimates that vulnerabilities fixed after release can result in 30 times the cost of fixes performed during the design phase.



Secure Code review process – Operational process



Security Awareness Training

Use Hibernate Encryption for Credit Card Numbers

Description

The Payment Card Industry Data Security Standard (PCI DSS) 1.2.1 states: "3.4 Render PAN [Personal Account Number], at minimum, unreadable to anyone who may have access to the system. This can be achieved by using the following approach: (a) PANs are securely stored in an encrypted format, and (b) PANs are rendered unreadable to anyone who may have access to the system to seamlessly encrypt and decrypt PANs."

Positive Code Example

This example shows how to first configure Hibernate with Jasypt, and then seamlessly apply the encryption to the Personal Account Number (PAN). The example makes use of a password-based encryptor where the password is stored in the environment variable "pbePasswordVar". Using an environment variable Password Based Encryptor (PBE) allows you to set the password in an environment variable upon launching the application server and then unset it after the application server has been launched. This is particularly useful if you set the environment variable from a different machine and then unset it quickly afterwards.

```
//First, configure Jasypt Encryptor when the application loads
org.jasypt.digest.common.util.DigestUtils.setAlgorithm("SHA-256");
new org.jasypt.encryptor.PasswordBasedEncryptor().setPassword("pbePasswordVar");
// Register the encryptor with the Hibernate configuration
hibernate.cfg.setJasyptEncryptor(new org.jasypt.encryptor.PasswordBasedEncryptor());
hibernate.cfg.registerHibernatePBEEncryptor(true);
```

Negative Code Example

In this example, the Hibernate configuration will not encrypt the PAN. This violates PCI requirements.

```
<hibernate-mapping package="com.yourApplication">
    <class name="CreditCardNumber" table="CARD_DATA" >
        <id name="ID" column="ID">
            <generator class="native" />
        </id>
    </class>
</hibernate-mapping>
```

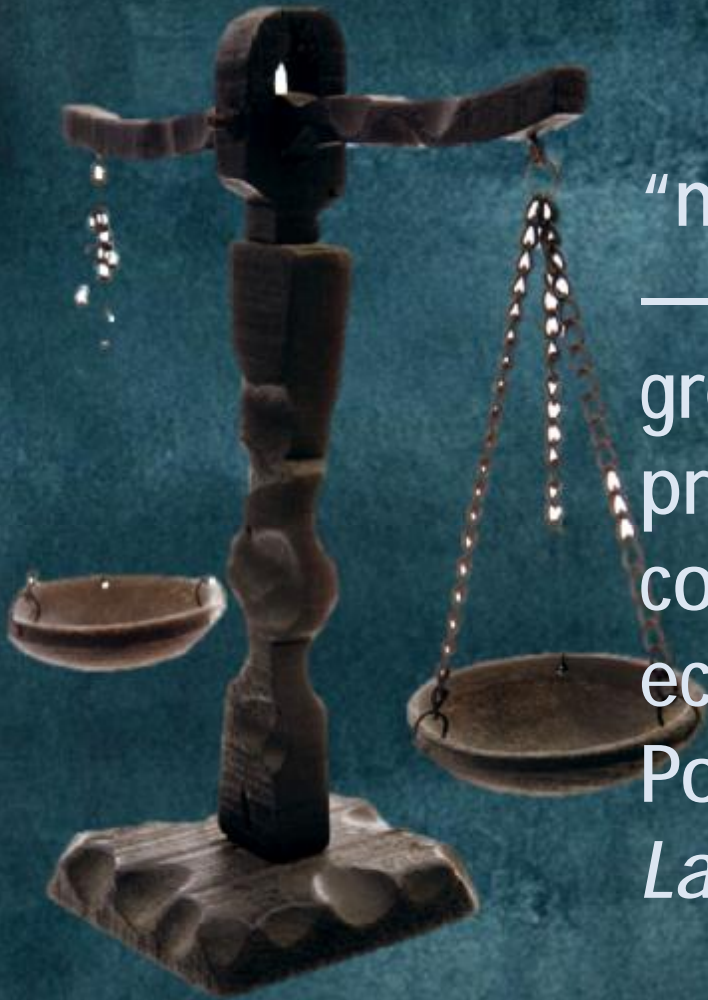
As Traditional Views

Give Way

To More Progressive Views

Duty of Care Owed

LIABILITY



“many areas of the law, especially —but by no means only— the great common law fields of property, torts, crimes, and contracts, bear the stamp of economic reasoning.” Richard A. Posner, *The Economic Analysis of Law* 18 (1977).

Shareholder derivative liability

- Tort liability
 - Negligence
 - strict products liability
 - misrepresentation
- Contract liability
 - Implied warranty of merchantability
 - Quasi-contract (promissory estoppel)
- Statutory Civil Liabilities

Criminal Liabilities

Regulatory (SOX, GLBA, HIPAA)



TORT LIABILITY

- NEGLIGENCE
 - Breach of the duty of reasonable care
 - Plaintiff must be owed that duty
 - Harm must be foreseeable ("*The risk reasonably to be perceived defines the duty that must be obeyed.*" Palsgraf, 248 N.Y. at 344.)
 - Defendant's conduct (act or omission) must be unreasonable
 - Purely economic losses usually not recoverable

TORT LIABILITY (cont.)

"[T]he owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions."

The Hand Formula: $B < P * L$

Where B is the cost (burden) of taking precautions, and P is the probability of loss (L). L is the gravity of loss. The product of $P \times L$ must be a greater amount than B to create a duty of due care for the defendant.

TORT LIABILITY (cont.)

- STRICT PRODUCTS LIABILITY
 - sellers are strictly liable for injuries caused by a defective product even if they have exercised all possible care
 - defects in the product
 - that cause physical harm to person or property
 - Ordinarily only apply to tangible things

TORT LIABILITY (cont.)

STRICT PRODUCTS LIABILITY (cont.)

The purpose of liability is to shape and deter conduct by parties so that the productive potential of society is maximized. In order for efficiency to be achieved, actions that cause more harm to society than good must be appropriately deterred. As a result, the law ascribes to parties different forms of responsibility or liability for "bad acts," "wrongful" conduct, or actions that harm others or property.

TORT LIABILITY (cont.)

- Negligent Enablement of Cybercrime?
- Liability for the intentional conduct of others?

In general, parties are not expected to predict the illegal acts of third parties. However, misconduct is foreseeable when a company acts "with the knowledge of peculiar conditions [that] create a high degree of risk of intentional misconduct."

TORT LIABILITY (cont.)

- Misrepresentation
 - Intentional
 - negligent
- fraud

STATUTORY CIVIL

- Electronic Communications Privacy Act
 - \$10,000 per violation
- Computer Fraud and Abuse Act
 - Minimum \$5,000 per violation

STATUTORY CIVIL (cont.)

Flash Cookie litigation (Advertising companies in alleged collusion with affiliates' Web sites set "flash-cookies" on online users' web browsers to circumvent privacy and security control settings) asserted:

- Computer Fraud and Abuse Act
- Cal. Computer Crime Law
- Cal. Invasion of Privacy Penal Law
- Cal. Consumer Legal Remedies Act
- Cal. Unfair Competition Law
- Trespass to Chattels
- Unjust Enrichment

CONTRACT LIABILITY

- IMPLIED WARRANTY OF MERCHANTABILITY
 - goods are fit for their ordinary purpose
- Software manufacturers and sellers may include language in the contract of sale limiting their liability and damages for defects. U.C.C. §§ 2-316, 2-719 (1972) permitted. *See also* UCITA.
- QUASI-CONTRACT (promissory estoppel)

REGULATORY DUTIES

- STATE & Federal (HIPAA, GLBA)
- *E.g.*, Federal Financial Institutions Examination Council (FFIEC), agency “empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions, ” publisher of *Authentication in an Internet Banking Environment guidance* (institutions should have a layered security strategy that at a minimum contains the ability to “detect anomalies and effectively respond to suspicious or anomalous activity”).

REGULATORY DUTIES (cont.)

STATE STATUTES

created affirmative duties to secure personal data for all companies that maintain the personal information of one or more state residents:

- notifying individuals when their information is released, either purposefully or inadvertently.
- "provide reasonable security" for personal information, including developing and implementing "reasonable security measures" for protecting the information.
- Organizations' subcontractors must also implement such measures.

REGULATORY DUTIES (cont.)

Gramm-Leach-Bliley Act

Under the Gramm-Leach-Bliley Act (GLB), financial institutions must develop and implement appropriate physical, technical, and management process safeguards to protect customers' personal information.

HIPAA

Requires health care providers to put in place appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of medical records. The Security Rule requires health care providers to

- Nathan D. Leadstrom, *Internet Web Sites as Products under Strict Products Liability: A Call for an Expanded Definition of Product*, 40 Washburn L.J. 532 (2001)
- Cem Kaner & David Pels, *Bad Software: What to Do When Software Fails* (1998)
- Bahn & Dressel, *Liability and Control Risks with Open Source Software*
- Nathan D. Leadstrom, *Internet Web Sites as Products Under Strict Products Liability: A Call for an Expanded Definition of Product*, 40 Washburn L.J. 532 (Spring, 2001)
- Zollers, McMullin, Hurd, & Shears, *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 Santa Clara Computer & High Tech.L.J. 745 (2005)
- Beard, Ford, Koutsky, & Spiwak, *Tort Liability for Software Developers: A Law & Economics Perspective*, 27 John Marshall Journal of Computer and Information Law 199 (2010).
- Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20. Berkeley Tech L. J. 1553 (2005)
- Jane K. Winn, *Recent Developments in the Emerging Law of Information Security*, , 38 UCC L.J. 391-402 (2006)

