Business Software Assurance

Identifying and Reducing Software Risk in the Enterprise

Barmak Meftah
Senior Vice President, Products and Technology
Fortify Software

$79 Billion

U.S. IT Security spend, 2007[1]

$7.3 Billion

IT security allocation in 2009 U.S. Federal Budget[2]

$288 Billion

Global IT Security spend, 2007[3]

[1]Info-Tech Research Group , November 15, 2006 baseline, 30% growth in 2007
[2]U.S. Office of Management & Budget, March 11, 2008
[3]Gartner Symposium/ITxpo, October 10, 2007

FORTIFY®

Cost of data breach at TJX soars to $256m

The Boston Globe

Suits, computer fix add t

By Ross Kerber, Globe Staff |

Shoe Company Loses Credit Card Info

A subsidiary of
credit card acc

November 8, 2007, 7:22 pm

Hackers Infect Alicia Keys's MySpace Page

By BRAD STONE

Shell, Rolls-Royce reportedly hacked by Chinese spies

MI5 has warned some 300 banks and accounting and legal firms to guard data

Jeremy Kirk Today's Top Stories ▸ or Other Cybercrime and Hac

Comments (4) Recommendations: 108 — Recomme

December 03, 2007 (IDG News Service) -- Britain's domestic intellige
perp
PLC

the

Monster Investigated by FTC Concerning Data Security

The Federal Trade Commission has launched an investigation into information

g from a 2007
f contact

Military to boost cyber-protections

AP Associated Press

RELATED VIDEO

In combat, new tastes for soldier plates
AP

» All news video

By LOLITA C. BALDOR, Associated

Wed Mar 19, 2:50 AM ET

WASHINGTON - The military is b
and improve relations with other n
fighting two wars, according to a

Data Leak in Britain Affects 25 Million

By ERIC PFANNER
Published: November 22, 2007

LONDON, Nov. 21 — The British government struggled Wednesday to
ks containing detailed personal
ons, including an unknown number of
at analysts described as potentially the
of the digital era.

Four Million Credit, Debit Cards Exposed in Data Breach

Tuesday, March 18, 2008

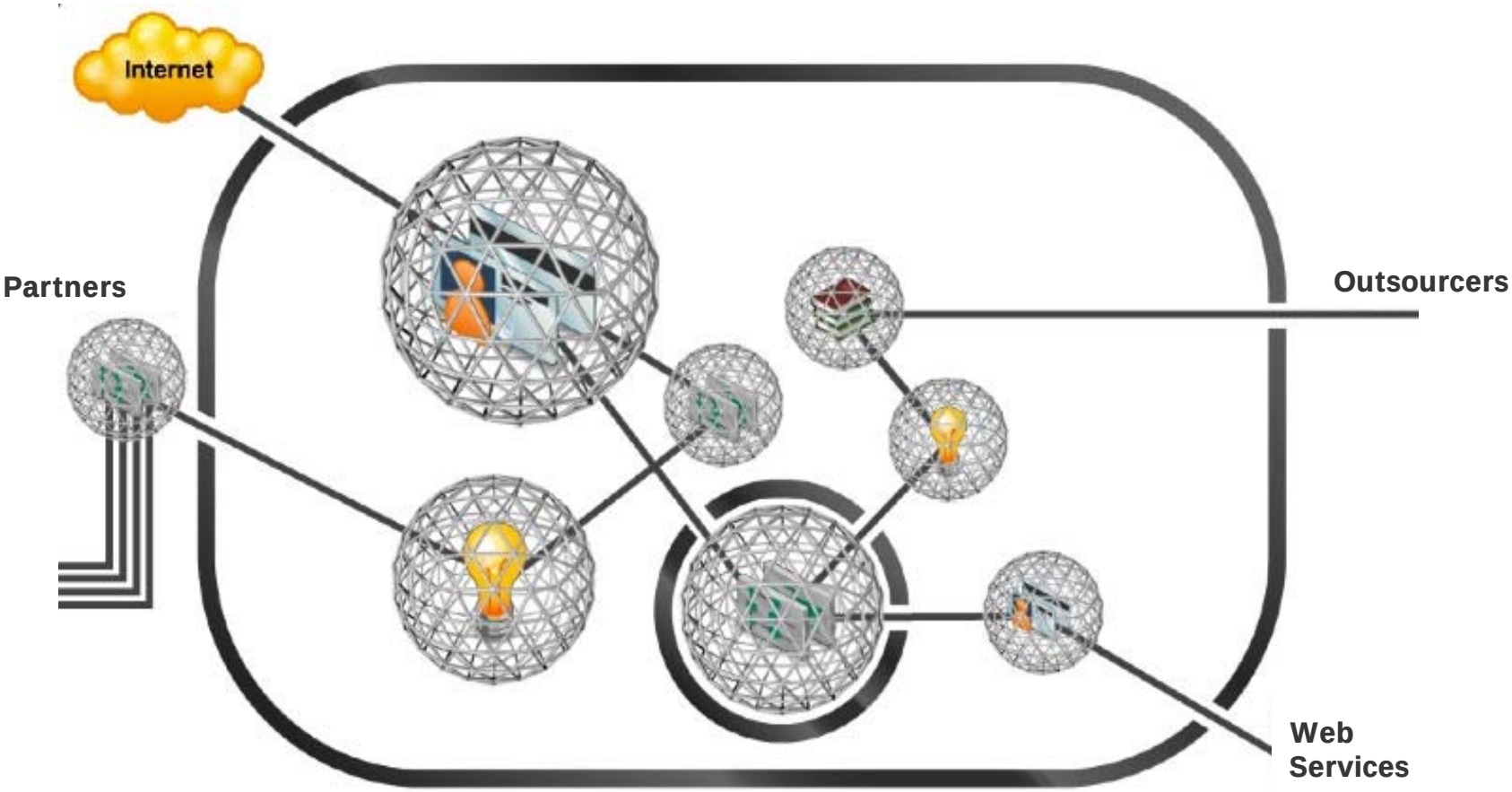
Associated Press

PORTLAND, Maine — A security breach at an East Coast supermarket chain exposed more than 4 million card numbers and led to 1,800 cases of fraud, the Hannaford Bros. grocery chain announced Monday.

FORTIFY

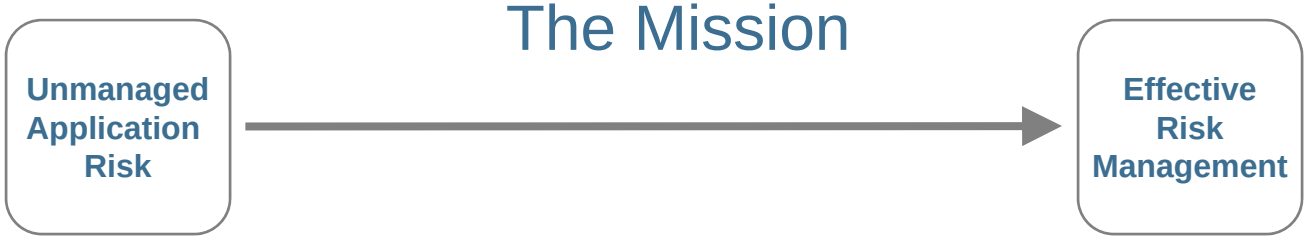
Current security gives a false sense of security

- **Walls don't work. They protect the network, not the assets.**



The Enterprise Mission

The Mission



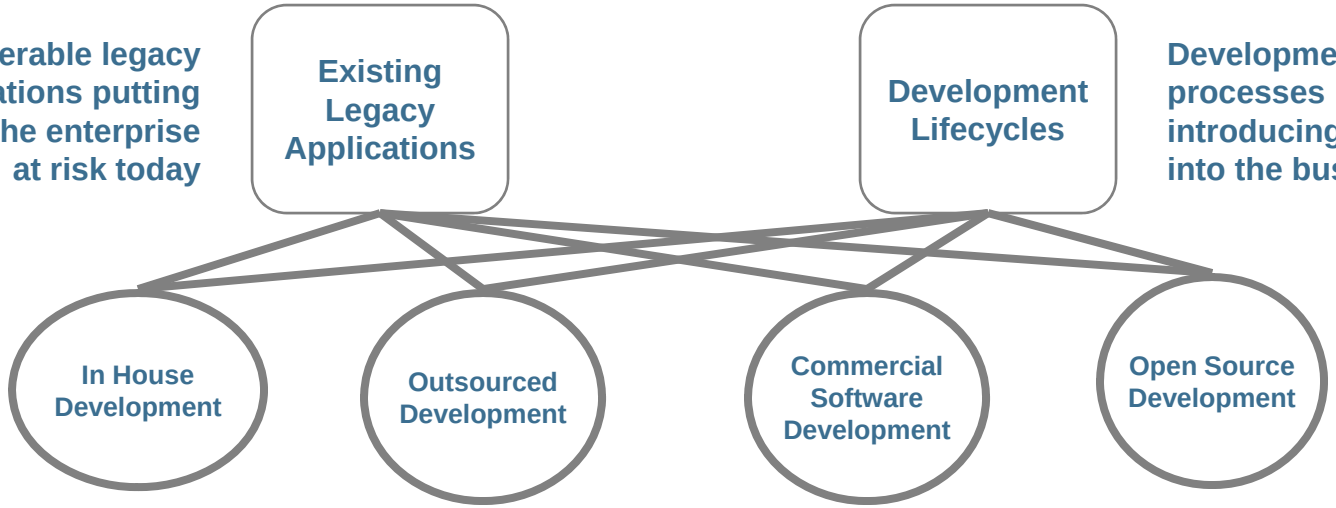
The Challenge

The Immediate Problem

Vulnerable legacy applications putting the enterprise at risk today

The Systemic Problem

Development processes introducing new risk into the business



It's not just about technology; It's organizational, too.

Business Management

- Often unaware of business risk, or mandates function over security

Development

- Rewarded primarily for features and schedule
- Security *not* mandated
- Security expertise lacking
- Complexity of software makes task significant

- No platform for collaboration
- No process that spans teams

Result: Status quo wins, *and so do the predators*

Security

- Inadequate controls to enforce policies
- Low visibility into development and software acquisition process
- Legacy of network security solutions to solve problems

FORTIFY

The Risk Factory

- **Continuing to accept insecure software and assessing it to find the vulnerabilities is a broken model (expensive)**
  - The infinite assessment loop
  - Swirling in an expensive and unproductive eddy
- **Assessing isn't bad, but it is a dead-end if you want to meet the objective of Business Software Assurance**

FORTIFY®

BSA Adoption Model

Assessment

Proving the problem or meeting the regulatory requirement

- An info-sec project
- Generates awareness & support for BSA initiative
- Services thrive
  - Pen testing& manual code review

Recurring cost that does not “fix” anything

Remediation

Fixing security issues found during assessments

- Info-sec driven project with development support
- Point of serious contention in most orgs
- Technology solutions prevail

Lowering business risk at a single point in time

Prevention

Assuring there are no issues in the first place

- Info-sec sponsored development led project
- Still an elusive goal for many
- Solutions must pass development scrutiny

Minimizing business risk systematically

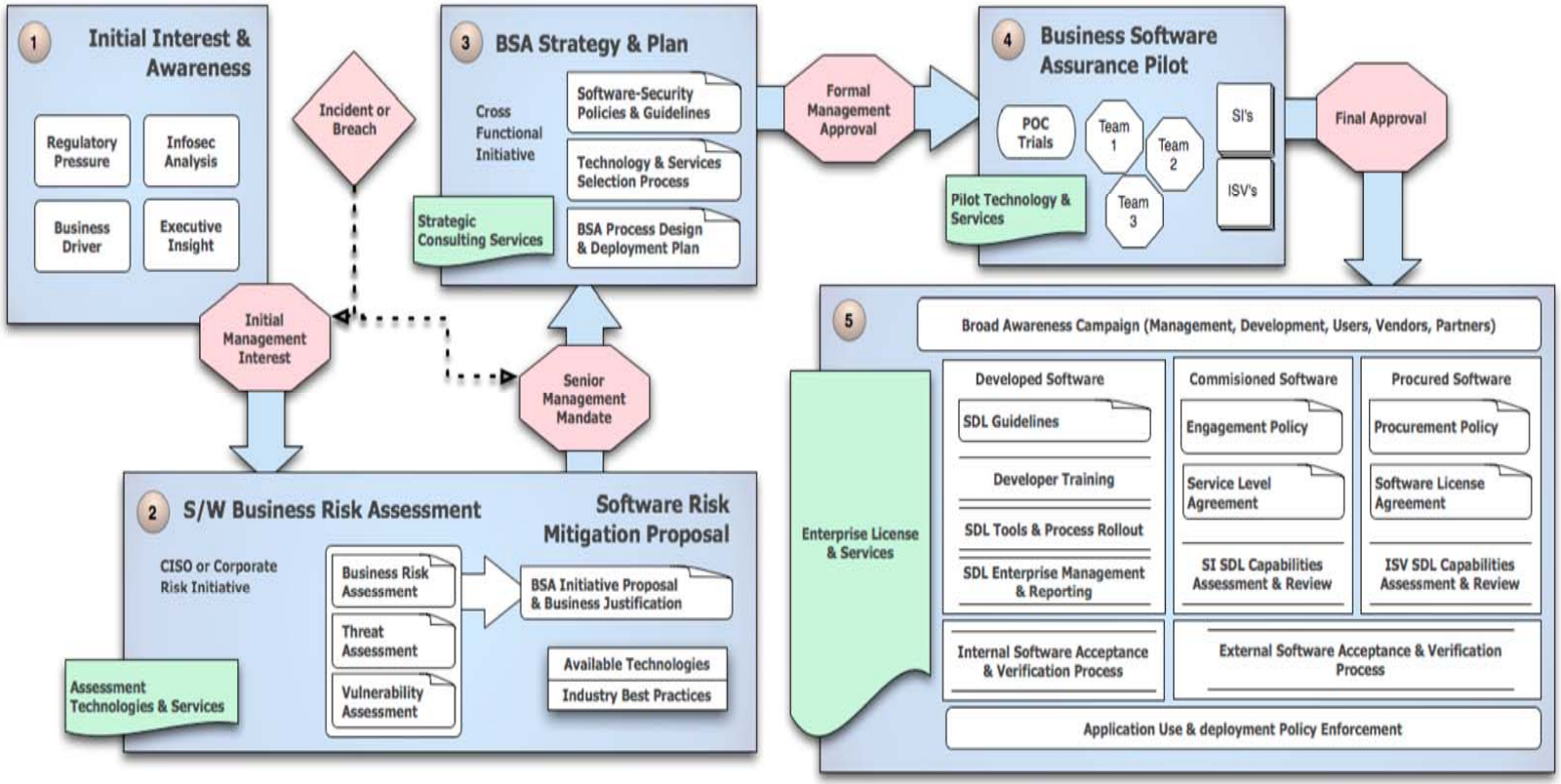
Example: Cost of Fixing Critical Defects

Cost of Fixing Vulnerabilities Later

Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs
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 Vulnerabilities Early

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

Identifying the critical bugs earlier in the lifecycle reduced costs by about $2.0MM

The CISO Journey