Define and Optimize Your Approach to Application Security

Avoid Common Pitfalls
Leverage Proven Tactics

Bruce C Jenkins
L&D Program Manager
bcj@hp.com

06 June 2012
What this presentation is based on...

• More than 5 years of field experience from software security consultants working with hundreds of clients
• Anecdotal accounts from over 350 software security assessments across all industry sectors
• Personal involvement in over 60 professional services engagements July 2007 – Nov 2011
Agenda

• Why Application Security?
• Obstacles to an Effective Program
• Define & Optimize (Tune)
Why Software Applications are Attacked

- Intellectual Property
- Customer Data
- Business Processes
- Trade Secrets

OWASP Tampa Day 2012
Exploiting Weaknesses: Path of Least Resistance
Security Breaches Continue

Data Security Breaches for CY2005-2012*

Source: Identity Theft Resource Center (www.idtheftcenter.org)

*As of 05 Jun 2012
Why Application Security?

1. Customer Demands
2. **Regulatory Compliance** -- CY2010
3. Breach / Data Loss
4. Well-informed, Proactive
Why Application Security?

1. Customer Demands -- CY2011
2. Regulatory Compliance
3. Breach / Data Loss
4. Well-informed, Proactive
Why Application Security?

1. Customer Demands
2. Regulatory Compliance -- CY2012
3. Breach / Data Loss
4. Well-informed, Proactive
Why Application Security?

1. Customer Demands
2. **Regulatory Compliance** -- CY2012
3. Breach / Data Loss
4. Well-informed, Proactive
   
   (This group has been breached and they’re just not admitting it.)
Motivation for Developing Secure Systems
Motivation for Developing Secure Systems

FOR IMMEDIATE RELEASE
May 25, 2012

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
REPORTS A CYBER ATTACK ON A CONTRACTOR
POTENTIALLY AFFECTING TSP PARTICIPANTS
No Indication of Any Improper Use of Data

Washington, D.C. -- The Federal Retirement Thrift Investment Board (FRTIB) announced today that a computer belonging to Serco Inc., a third party service provider, suffered a sophisticated cyber attack that resulted in the unauthorized access of the personal information of approximately 123,000 Thrift Savings Plan (TSP) participants or other recipients of TSP payments. In April of 2012, the FRTIB and Serco were informed of the unauthorized access incident by the Federal Bureau of Investigation (FBI).

Notification letters are being sent to all affected individuals offering them information on how to contact a call center that has been established to provide support and offer services such as credit monitoring. In addition, as a precautionary measure, the FRTIB will place alerts on the impacted TSP accounts to ensure that any account activity receives heightened scrutiny.
Motivation for Developing Secure Systems

FOR IMMEDIATE RELEASE
May 25, 2012

FEDERAL RETIREMENT THrift INVESTMENT BOARD
REPORTS A CYBER ATTACK ON A CONTRACTOR
POTENTIALLY AFFECTING TSP PARTICIPANTS
No Indication of Any Improper Use of Data

Washington, D.C. -- The Federal Retirement Thrift Investment Board (FRTIB) announced today that a computer belonging to Serco Inc., a third party service provider, suffered a sophisticated cyber attack that resulted in the unauthorized access of the personal information of approximately 123,000 Thrift Savings Plan (TSP) participants or other recipients of TSP payments. In April of 2012, the FRTIB and Serco were informed of the unauthorized access incident by the Federal Bureau of Investigation (FBI).

Notification letters are being sent to all affected individuals offering them information on how to contact a call center that has been established to provide support and offer services such as credit monitoring. In addition, as a precautionary measure, the FRTIB will place alerts on the impacted TSP accounts to ensure that any account activity requires heightened scrutiny.
### Regions Financial Corp. - Ernst & Young

**ITRC Breach ID**: ITRC20120131-02  
**Company or Agency**: Regions Financial Corp.  
**State**: AL  
**Est. Date**:  
**Breach Type**: Electronic  
**Breach Category**: Business  
**Records Exposed?**: Yes - Published  
**# Records Rptd**: 0

> Personal information about Regions Financial Corp. current and former employees was lost in November when a flash drive with the data came up missing after being mailed by outside auditor Ernst & Young in the same envelope as the decryption code.

### Lexington Clinic

**ITRC Breach ID**: ITRC20120131-01  
**Company or Agency**: Lexington Clinic  
**State**: KY  
**Est. Date**: 12/7/2011  
**Breach Type**: Electronic  
**Breach Category**: Medical/Healthcare  
**Records Exposed?**: Yes - Published  
**# Records Rptd**: 1,018

Following the Dec. 7 theft of an unencrypted laptop, Lexington Clinic in Kentucky is notifying 1,018 patients who received services in the neurology department.

**Attribution 1**  
**Publication**: Health Data Management  
**Article Title**: Laptop Loaded with PHI Stolen from Lexington Clinic
What has TSP done in response to the cyber attack?

First, on May 25th, we sent notification letters to everyone whose personal information was in the affected files. The FRTIB and our service provider have been working to avoid future incidents. Steps taken include an immediate shutdown of the compromised computer, a response team that is conducting a systemwide review of all computer security procedures, and further enhanced computer security.

Point: We, as a security industry, still have a lot of work to do!
Obstacles to an Effective AppSec Program

- Awareness
- Education, Training
- Source Integrity (*this is about trust*)
- Issue Management
Obstacles to an Effective AppSec Program

• **Awareness (lack of)**
  - Don’t know about the issue
  - Don’t know about the *requirement*

• **Education, Training (little or none)**
  - Don’t know how to fix it
  - Definitely don’t have time to get trained on how to fix it

• **Source (Messenger) Integrity**
  - Lack of trust between Security and Development teams
  - Poor understanding (by Security) of how software is developed; poor understanding (by Developers) of Security team’s strategic mandate

• **Issue Management (huh?)**
  - Too many issues: “What am I going to do with 35,000 findings?”
  - Improper focus on “everything” instead of on what is most important
Who is Responsible for Software Security?

“I just want to be a coder; I’m really not interested in security.”

– Anonymous
Elements of Success
Elements of Success

1. Define Program Goals
   - Associate AppSec goals with organizational goals
   - Consider tying to bonus / promotion incentives
Goals Examples

- Collaborate amongst teams to improve security
- Report the status of security risk exposure on individual or groups of applications
- Avoid being front-page news on the WSJ
- Measure security risk of individual applications
- Identify and prioritize our application portfolio
## Application Portfolio Example

<table>
<thead>
<tr>
<th>Application / Project</th>
<th>Cost of breach (H, M, L)</th>
<th>Likelihood of target (H, M, L)</th>
<th>Potential impact</th>
<th>Application owner</th>
<th>Date of Initial Deployment</th>
<th>Last update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft Use Database (ACUSE)</td>
<td>L</td>
<td>L</td>
<td></td>
<td>AIR IT</td>
<td>2/3/2001</td>
<td>3/18/2005</td>
</tr>
</tbody>
</table>
Elements of Success

1. Define Program Goals
   - Associate AppSec goals with organizational goals
   - Consider tying to bonus / promotion incentives

2. Develop a Reasoned Strategy
   (a plan with objectives) for supporting Program Goals
   - Keep it simple
   - Ensure Objectives are measurable and time-boxed
Strategy Example

“Develop and implement a five-phased approach to raising awareness of application security (by <date>), educating and training stakeholders on process changes (by <date>), and building security into the SDLC (by <date>).”
Strategy Example #2

Step 1: Implement A Security Gate

Establish security acceptance testing program by 2012Q2

Step 2: Build In Security

Reduce cost of developing secure applications at least 20 percent by July 2013
Strategy: The Technical Component
Elements of Success

1. Define Program Goals
   - Associate AppSec goals with organizational goals
   - Consider tying to MBOs

2. Develop a Reasoned Strategy (with Objectives!) for supporting Program Goals
   - Keep it simple
   - Ensure Objectives are measurable and time-boxed

3. Obtain Executive Sponsorship
   - Influence spans business units
   - Supports… and holds accountable
Elements of Success (cont’d)

4. Communicate the Plan
   - Who, what, when, where, why (and how)
   - Communicate again (and again) (and again)
Elements of Success (cont’d)

4. Communicate the Plan
   - Who, what, when, where, why (and how)
   - Communicate again (and again) (and again)

5. Measure Progress
   - Collect metrics for a specific reason, not simply because you can
   - Use the right KPIs
A bit about Metrics & KPIs…
Tough Questions

Will it be possible to perform an analysis of 100% of enterprise web applications?

Will a zero vulnerability metric be reachable, practical or even desirable?

Is vulnerability reduction the same as risk reduction?
The 5 Key Performance Indicators (KPIs)

- **WRT** – Weighted Risk Trend
- **DRW** – Defect Remediation Window
- **RDR** – Rate of Defect Recurrence
- **SCM** – Specific Coverage Metric
- **SQR** – Security to Quality defect Ratio

- KPIs provide business-level context to security-generated data
- KPIs answer the “so what?” question
- Each additional KPI indicates a step forward in program maturity
- None of these KPIs draw strictly from security data
KPI #1 – Weighted Risk Trend

Maturity Rank: 1

A business-based representation of risk from vetted web application security defects over a specified time-period, or repeated iterations of application development.

Formula:

\[
\text{Multiplier}_{\text{critical}} \times \text{defects} + \text{Multiplier}_{\text{high}} \times \text{defects} + \text{Multiplier}_{\text{medium}} \times \text{defects} + \text{Multiplier}_{\text{low}} \times \text{defects} \times \text{Criticality}_{\text{business}}
\]

Requirements

- Web application registry with business-level criticality assigned
- *Pull business criticality rating from DR documents
- Vetted web applications security defects by criticality level
- Mathematic plot capability
KPI #2 – Defect Remediation Window

Maturity Rank: 2

The length of time from when a vetted web application security defect is identified until it is verified closed.

Requirements

- Defect tracking system, tracking web application security vulnerabilities in development, testing, and production environments
- Self-service testing, bug tracking, and reporting capabilities
- Cooperative security enablement thru development, QA, OPS teams
KPI #3 – Rate of Defect Recurrence

The rate, over time, at which previously closed web application security defects are re-introduced into a given application, organization, or other logical unit.

Requirements

– Advanced defect tracking system
– Advanced web application security testing capabilities
– Capabilities to identify similar or like defects across an application or logical trackable unit

Maturity Rank: 3
KPI #5 – Security to Quality Defect Ratio

Maturity Rank: 4

The ratio of security defects to the total number of software quality defects being generated (functional + performance + security).

Formula: $D_s = \frac{D_{s}}{D_t}$

- $D_s = $ Total Security defects
- $D_t = $ Total Overall Quality defects

Requirements

- Mature defect reporting system (tracking combined quality defects)
  - Security as a quality defect
  - Performance as a quality defect
  - Functional (+related) as a quality defect

- Tight cooperation of Information Security & Quality Assurance
## Failures of Common Metrics

<table>
<thead>
<tr>
<th>Common Metrics</th>
<th>Failure Mode(s)</th>
<th>Options?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Number of vulnerabilities found</td>
<td>1. So what? No context!</td>
<td><strong>Business Context.</strong> KPIs provide business context to standard metrics reporting practices.</td>
</tr>
<tr>
<td>2. Number of pages scanned/tested</td>
<td>2. So what? Do “pages” matter?</td>
<td></td>
</tr>
</tbody>
</table>
When Metrics Aren’t Enough

Objective

• Conclusively prove that risk is being reduced through program effort
• Remove subjectivity of metrics by providing business context
• Bring IT Security into higher-level business discussion
• Unify “testing” methodologies

KPIs Answer

– Combine metrics with business-level context
– Provide direct feedback to the business to target ongoing effort
– Track program effectiveness including education, corporate remediation strategies
– Consolidate technical metrics into business-level dashboards
– Successfully break the “security silo”
Vulnerability reduction, without business context

More vulnerabilities = more risk?
Vulnerability reduction, with business context

App criticality + defects = more risk
Data is raw information

Metrics are refined data

KPIs are metrics with business-context

Business context makes security relevant.
The 5 Key Performance Indicators (KPIs)

- **WRT** – Weighted Risk Trend
- **DRW** – Defect Remediation Window
- **RDR** – Rate of Defect Recurrence
- **SCM** – Specific Coverage Metric
- **SQR** – Security to Quality defect Ratio

KPIs are the difference between technical data points, and the actionable intelligence that information security needs.
Elements of Success (cont’d)

4. **Communicate the Plan**
   - Who, what, when, where, why (and how)
   - Communicate again (and again) (and again)

5. **Measure Progress**
   - Collect metrics for a specific reason, not simply because you can
   - Use the right KPIs

6. **Report Results**
   - Agree on what will be reported, when and to whom
   - Be creative with rewards
   - Hold people accountable
How to Save the Day… (a few more tips)

• Put Experienced Developers on the Security Team
• Publish Secure Coding Standards
• Train Developers and Security Teams
• Collaborate on the “Top n” Security Issues for <period>
• Obtain C-level Sponsorship / Approval of Your Top n
• “Tune” Your Security Testing Product(s) to Support the Identification and Presentation of the Top n Security Issues
• Treat All Security Issues as You Would Any Other Software Defect (i.e., get the issues into your defect tracking system)
Where are you now?
Summary

• Why Application Security?
• Obstacles to an Effective Program
• Define & Optimize (Tune)
QUESTIONS?