


Case Study

Assessing Internet Application Risk

Marybeth Panock

Fidelity Investments



1



What is risk?

Risk is the possibility of suffering loss

- Loss of tangible assets
- Loss of intangible assets
 - confidentiality, integrity, and availability of information
 - reputation
 - customer loyalty



2



What is Risk Assessment?

The process of
Identifying,
analyzing,
controlling, and
communicating
the possibility of loss

Fidelity Investments

3

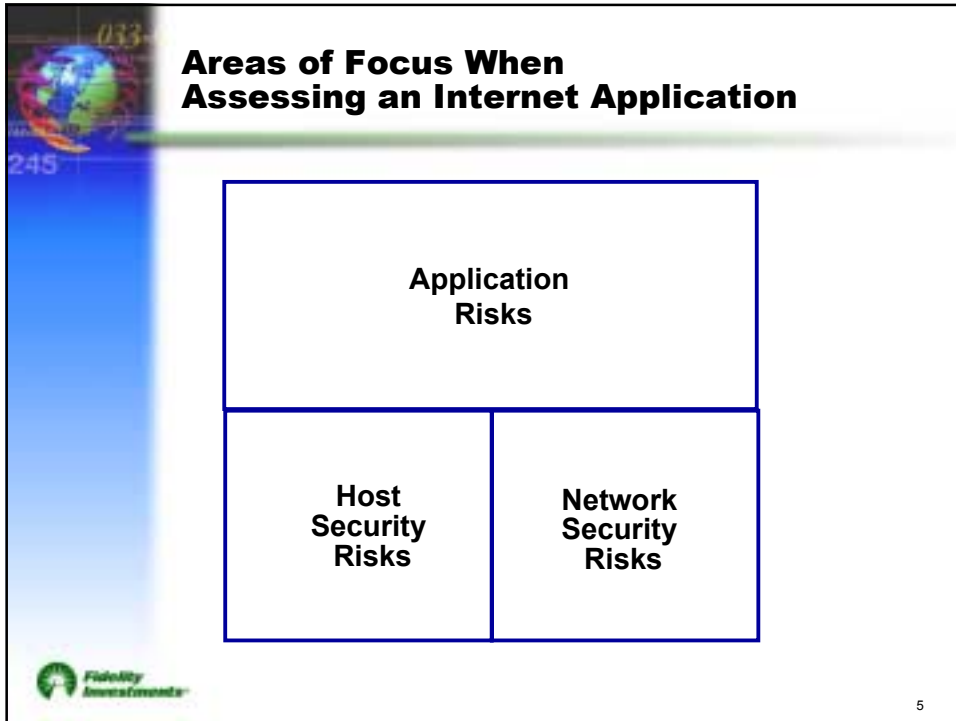



Fidelity Security Risk Assessment Methodology

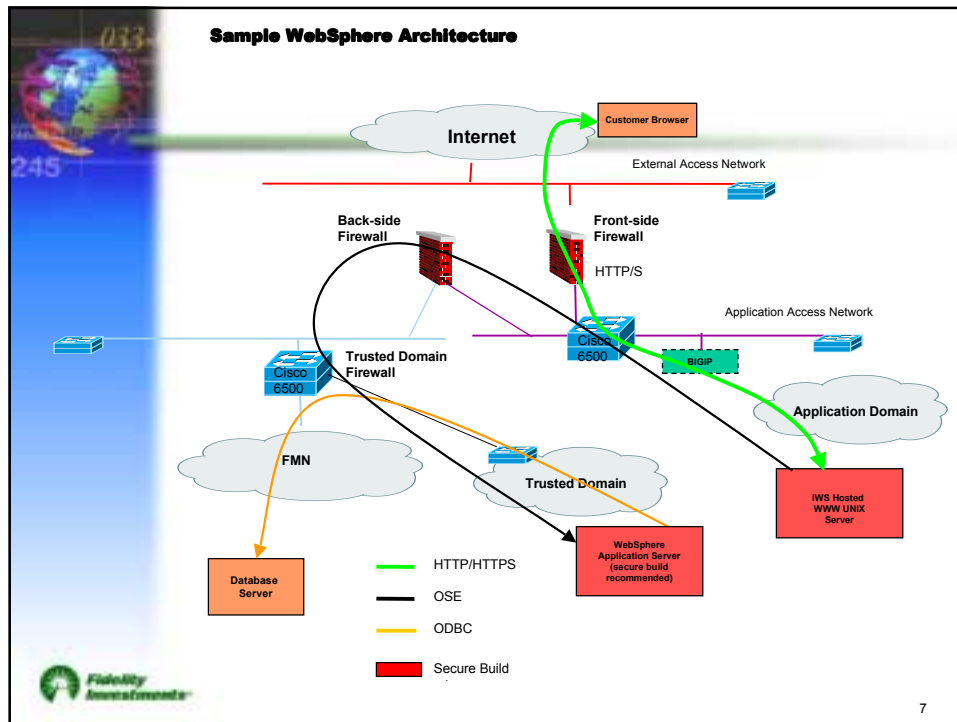
- 1 Identify assets
- 2 Identify potential risk to asset confidentiality, integrity, and availability
- 3 Analyze identified risks
- 4 Define and assign metrics to measure the severity of the risk
- 5 Develop mitigating controls
- 6 Make recommendations for implementation
- 7 Distribute coordinated risk assessment and recommendations to relevant business units
- 8 Obtain agreement and sign-off

Fidelity Investments


4



-
- Information-Gathering Tools**
- Architecture reviews**
 - Security code reviews**
 - Application security testing (e.g. Sanctum's AppScan)**
 - Demos of the application**
 - Platform compliance reviews using commercial tools**
- 
- 6




- ### What Code Review looks at
- User Input Data Validation
 - Authentication and Authorization
 - Cookie Handling and Session Management
 - Encryption schemes and methods
 - I/O
 - Logging and Error Messages
 - Race Conditions and Return Codes
- 8




User Input Data Validation

- Process of ensuring that data received from an external source e.g., web browser, is well formed and of a proper length
 - All data from the user should be considered tainted until validated
 - All validation must occur on the server side
- Length Check - only as many characters as needed
- Exact match from known list - Best Validation
- Only known good characters - Good Validation
- Exclude known bad characters - Last Resort Validation
- Worst (No) Validation




9




Cookie and Session ID

- Fully Baked Cookies
- Confidential data in Cookies
- Secure Flag on Cookies
- Passing Session ID
- Replay Attacks
- Timeout Values on Session ID




10




Sanctum Inc.'s AppScan

- Automates the complex, manual task of auditing web applications
 - Detects application vulnerabilities
 - Simulates application attacks
 - Points to potential security loopholes
- Used in place of manual user security testing
- It is not a substitute for Secure Code Review




11




AppScan Parameters

- Tests Methods
 - Strict Matching or Not?
 - Attack Stage; Safe or Unsafe or both
- Attack Mode
 - Manual or Automatic
- Tests
 - 1 Parameter substitution
 - 2 Path Substitution
 - 3 Database Mutation
 - 4 HTML / JavaScript attacks
 - 5 Buffer Overflow




12




Risk Assessment Document

- Risk Assessment*
 - A. Summary explanation of significant risks (application, host, and network)
 - B. Risk rating (low, medium, high)
 - C. Mitigating controls
- Requirements and Recommendations*
- Reference Documents*
- Optional: Business Unit Comments*
- Risk Acceptance (sign-off page)*
- Detailed Risk Assessment Matrix*




13




Categories and Risk Factors

| <i>Category</i> | <i>Risk Factor</i> | <i>Wt.</i> | <i>Risk</i> |
|------------------------------|----------------------------|------------|-------------|
| <i>User Input Validation</i> | • Exact Match e.g. YES/NO | 5 | 1 |
| | • Known Good Characters | | 2 |
| | • Exclude Bad Characters | | 3 |
| | • None | | 5 |
| <i>Web Server Build</i> | • Secure Unix | 3 | 1 |
| | • Secure NT | | 1 |
| | • Standard Unix | | 3 |
| | • Standard NT | | 3 |
| <i>Internet Protocol</i> | • Single TCP Connection | 2 | 1 |
| | • Multiple TCP Connections | | 2 |
| | • UDP Connections | | 3 |



14



Risk Factor Calculations

Application Risk Category example : User Input Validation


Risk Factor = *None*
 Category Weight * Risk = Risk Factor Calculation
 5 x 5 = 25

Host Risk Category example : Web Server Build


Risk Factor = *Secure Unix*
 Category Weight * Risk = Risk Factor Calculation
 3 x 1 = 3

Network Risk Category example : Internet Protocol

Risk Factor = *Single TCP Connection*
 Category Weight * Risk = Risk Factor Calculation
 2 x 1 = 2



15



Risk Calculations

Risk Factor Calculation = Category Weight * Risk


Calculated Risk = Σ Risk Factor Calculations

Overall Rating = $\frac{(\text{Calculated Risk} - \text{Lowest Risk}) * 100}{(\text{Highest Risk} - \text{Lowest Risk})}$


Low Risk = 0-33%

Medium Risk = 34-67%

High Risk = 68-100%




16




Results to date 2/00 - 11/01

- Over 70 Internet and Extranet Application Risk Assessments have been conducted
- Overall Security Risk before mitigation
 - Low Risk or Green: 22%
 - Medium Risk or Yellow: 68%
 - High Risk or Red: 10%

(Not all risk assessments were numerically rated)




17




Internet Applications risk findings

- Application Risk
 - Low Risk or Green: 15%
 - Medium Risk or Yellow: 48%
 - High Risk or Red: 37%
- Host Risk
 - Low Risk or Green: 33%
 - Medium Risk or Yellow: 45%
 - High Risk or Red: 22%
- Network Risk
 - Low Risk or Green: 35%
 - Medium Risk or Yellow: 55%
 - High Risk or Red: 10%




18




Internet Applications Biggest Issues

- Application Security
 - Lack of sufficient Data Validation
 - Non-compliant Authentication strategies
 - Insufficient verification of Secure Coding standards
 - Vendor code
 - Legacy Applications (behind generic plug-ins)
- Host Security
 - Non-standard Secure Build: e.g., additional files
- Network Security
 - Non-validated HTTP into internal network
 - Architectures non-compliant with Corporate Policy
 - Lack of sufficient Network Isolation



19



Lessons Learned

- A well-run Risk Assessment practice can influence business units to deploy more secure Internet Applications
 - People do listen
- Senior Management who must accept the risk want applications to be secure while Development wants them to be finished
 - Target the right level for sign-off
- Integrating risk assessment into the business process helps gain acceptance and cooperation



20




Assessing Internet Application Risks

Worked Example




21



Example: WebSphere Sample Application Risks

| Application Security Risks | | | | | |
|---|----|------------------|-----|-----|------|
| Category/ Risk Factor | Wt | Risk | Min | Max | Calc |
| Authentication 1. PIN Authentication 2. Digital Certificates 3. Basic Authentication | 3 | 1 2 3 | 3 | 9 | 3 |
| Session Mgmt 1. Adequate. Cookie Handling 2. Inadequate Cookie Handling | 3 | 1 2 | 3 | 6 | 6 |
| Authorization 1. User limited to resources authorized for individual user 2. User limited to group resources 3. Insufficient control of sensitive application resources | 3 | 1 2 3 | 3 | 9 | 6 |
| Input Validation 1. Exact match from known values (e.g. YES/NO) 2. Match against known good characters (e.g. A-Z, 0-1) 3. Exclude Bad Characters 4. None or unknown | 5 | 1 2 3 5 | 5 | 25 | 25 |
| Buffer Overflows, etc 1. Buffer Overflow protection, error handling, adequate logging 2. Buffer Overflow protection, error handling/logging inadequate 3. Inadequate Buffer Overflow protection | 3 | 1 2 3 | 3 | 9 | 3 |
| Confidentiality 1. 128 Bit Encryption 2. 40 Bit Encryption 3. No Encryption | 2 | 1 2 3 | 2 | 6 | 2 |
| Totals | | | 19 | 64 | 45 |



22

Example: WebSphere Sample Host Risks


| Host Security Risks | | | | | |
|--|----|-----------------------|-----|-----|------|
| Category/ Risk Factor | Wt | Risk | Min | Max | Calc |
| Server Build 1. Secure Unix 2. Secure NT 3. Standard Unix 4. Standart NT 5. Non-standard | 3 | 1 2 3 4 5 | 3 | 15 | 3 |
| Webserver 1. Stripped version of Netscape 2. Stripped version of IIS 3. Standard Netscape 4. Standard IIS 5. Non-standard | 2 | 1 2 3 4 5 | 2 | 10 | 2 |
| Server Location 1. Fidelity Firewall Application Domain 2. Remote Hosting Site – Fidelity controlled 3. Third Party Site – not Fidelity controlled | 2 | 1 2 3 | 2 | 6 | 2 |
| Server Change Management 1. FISC 2. Non-FISC 3. None | 1 | 1 2 3 | 1 | 3 | 1 |
| Security Policy Compliance Verification 1. Security Compliance tool present and used 2. Security compliance tool not used | 2 | 1 2 | 2 | 4 | 4 |
| Server Security Vulnerability Protection 1. Verified at Go-Live & periodically 2. Verified at Go-Live 3. No Verification | 2 | 1 2 3 | 2 | 6 | 4 |
| Totals | | | 12 | 44 | 16 |

23

Example: WebSphere Sample Network Risks

| Network Security Risks | | | | | |
|---|----|----------------------------|-----|-----|------|
| Category/ Risk Factor | Wt | Risk | Min | Max | Calc |
| Architecture 1. Standard Reference Architecture 2. Non-Standard Reference Architecture 3. Non-Compliant Architecture | 5 | 1 3 5 | 5 | 25 | 5 |
| Protocols and Ports into Firewall 1. Single TCP Connection 2. Multiple TCP Connections 3. Other e.g., UDP Connections | 2 | 1 2 3 | 2 | 6 | 2 |
| Protocols and Ports into Fidelity Intranet 1. Single TCP Connection originating from Intranet 2. Single TCP Connection originating from Firewall 3. Multiple TCP Connections from Intranet 4. Multiple TCP Connections from Firewall 5. Other e.g., UDP Connections from Intranet 6. Other e.g., UDP Connections from Firewall | 2 | 1 2 3 4 5 6 | 2 | 12 | 4 |
| Firewall Protection 1. Application Proxy 2. Plug 3. Packet Filter | 3 | 1 2 3 | 3 | 9 | 9 |
| Firewall Location 1. FISC Firewall 2. Non-FISC Data Center 3. Non-Fidelity | 1 | 1 2 3 | 1 | 3 | 1 |
| Firewall Support 4. FISC Data Center 5. Non-FISC Data Center 1. Non-Data Center | 1 | 1 2 3 | 1 | 3 | 1 |
| Totals | | | 14 | 58 | 22 |

24



Risk Calculations

Risk Factor Calculation = **Category Weight * Risk**


Calculated Risk = Σ **Risk Factor Calculations**

Overall Rating = $\frac{(\text{Calculated Risk} - \text{Lowest Risk}) * 100}{(\text{Highest Risk} - \text{Lowest Risk})}$


Low Risk = **0-33%**

Medium Risk = **34-67%**

High Risk = **68-100%**



25




WebSphere Sample Overall Risk Rating

Application Security Risk Rating = $\frac{(45 - 19) * 100}{(64 - 19)} = 58 \%$

Host Security Risk Rating = $\frac{(16 - 12) * 100}{(44 - 12)} = 13 \%$

Network Security Risk Rating = $\frac{(22 - 14) * 100}{(58 - 14)} = 18 \%$

Overall Calculated Risk = $\frac{(83 - 45) * 100}{(166 - 45)} = 31 \%$



26



Assessing Internet Application Risks



27