


## Security Assurance: The Part You Play

Bar Biszick (cissp, csqa)  
[barb@dashmail.net](mailto:barb@dashmail.net)  
[www.QualityIT.net](http://www.QualityIT.net)  
 425-241-5391

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

1




## Agenda

- 1) Perceptions: Trends and Law
- 2) Security testing problem
- 3) Quality vs security testing
- 4) Organizational gaps
- 5) Changing Standards
- 6) QA as change agent

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

2




## Impacts global, severe

- **Code Red**—0-24 hours (350,000+ victims)
- SQL Slammer **Before** (at 0 minutes)
- SQL Slammer **After** (at 30 minutes)
  - Peaked in 3 minutes with 55 million scans
  - Affected 90% of vulnerable machines within 10 minutes

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

3




## Key Point #1

Detection and Response is no longer an effective means of mitigating security risk.

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

4




## Root Cause of Breaches

- 65% Errors and omissions
- 13% Dishonest employees
- 10% Disgruntled employees
- 5%-8% Hackers and crackers

■ Source: Current and Future Danger: a CSI Primer on Computer Crime and Information Warfare

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

5




## Liability increasing

- HIPAA
  - Transactions and Code Sets Rule
  - Privacy Rule
  - Security Rule
- Sarbanes-Oxley
  - CEO/CFO personally liable
  - Exec Management required to report issues

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved


6



## QA Responsibility

- QA is a risk management function!!!!

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 7




## Key problem: Perception

### Mgt. Thinks It's Covered!!!!

- Compartmentalized= inefficient, insufficient
- Responsibility misplaced:
  - Assumes Operations people are skilled in Quality Testing principles
  - Assumes Testers are skilled in Security Testing techniques
- Assumes policies are to be followed, not questioned


(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 8



## Security Defined

- Assessing, protecting and assuring the confidentiality, integrity and accessibility of information, information systems and data so that unauthorized persons or systems cannot accidentally or deliberately read, damage or modify them and authorized persons and systems are not denied access to them or impaired in their productivity by them.


(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 9



## Security Objectives

1. Authorized users access only what they need
2. Unauthorized users are denied access
3. Known and anticipated vulnerabilities are managed


(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 10



## Security Assurance

Testing to provide *grounds for confidence* that the **claimed security objectives** are achieved

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 11



## Motivation for Enterprise Security

- Insure Productivity
  - Access to valid, appropriate information
  - High availability (avoid interruptions)
- Manage Liability
  - Reduce Risk to acceptable levels

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 12

## OSI Security Protection Layers

- 7-Application Layer
- 6-Presentation Layer
- 5-Session Layer
- 4-Transport Layer
- 3-Network Layer
- 2-Datalink Layer
- 1-Physical Layer

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

13

## Security Zones

- Virtual Transport System
- Physical Systems
- Dependent Systems
- Organizational Policy
- Human Factors
- External Threats

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

14

Quality	Security
<ul style="list-style-type: none"> <li>■ Does what it's supposed to do</li> <li>■ Recovers successfully</li> <li>■ Errors helpful in recovery</li> <li>■ Access based on authorization</li> <li>■ Applications get resources needed</li> </ul>	<ul style="list-style-type: none"> <li>■ Does ONLY what it's supposed to do</li> <li>■ Fails safely</li> <li>■ Errors don't provide clues to technology</li> <li>■ Access based on need to know</li> <li>■ Applications never exceed range of resources needed</li> </ul>

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

15

Quality	Security
<ul style="list-style-type: none"> <li>■ Uses copied prod data as test data</li> <li>■ Checks password is valid</li> <li>■ Checks correctness/completeness of messages</li> <li>■ Assures high availability</li> </ul>	<ul style="list-style-type: none"> <li>■ Scrubs test data before use</li> <li>■ Checks user is valid</li> <li>■ Checks the origin as well as the integrity of the message</li> <li>■ Makes sure anyone who doesn't need to know doesn't have the means, motive or opportunity for access</li> </ul>

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

16

## Security Dependencies

- Robust Fault Testing
- Resources, Tools and Skill sets
- Current Operational Security controls
- Security State of Dependent Systems
- Regulatory Policies & Procedures
- External Security Perimeter controls

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

17

## Key Point # 4

To be effective,  
security must be  
addressed comprehensively  
on software projects

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

18

## IEEE P1074

- **Standard for Developing Software Life Cycle Processes**
  - Foundation Life Cycle Standard
  - Not specific to any model
  - Huge traceability matrix
  - Describes inputs and outputs

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 19

## P1074 Key changes

- Quantifying security risk (objectives)
- Implementing Threat Modeling (failure point analysis)
- Assuring verification (accountability)

**General Process**

1220 Systems Engineering Process

1362 Concept of Operations

1233 Guide – System Requirements Spec

1490 Guide to PM Body of Knowledge

1058 SW Project Mgt Plans

1074 Developing SWLC Processes

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 20

## QA Focus

- Comprehensive approach
- Minimize damage
- Analyze for failure points
- QA as risk management
- Change Perception

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 21

## QA Strategy

- 1) Baseline perception of IT security
- 2) Implement Threat Modeling in all IT projects
- 3) Test products end to end from Master Test Plan (don't push out tasks to different groups, pull in members to participate in centralized Test team as needed)
  - 1) QA contributes testers and test managers
  - 2) Ops contributes SMEs and test resources
- 4) Measure against security objectives
- 5) Verify Accreditation

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 22

## Key Points

- Require formalized Security Objectives
- Control Master Security Test Plan
- Engage SMEs in planning
- Communicate responsibilities and expectations
- Expect Threat Modeling participation & results
- Verify Operational readiness
- Communicate Risk in Liability terms

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 23

## Security Assurance: The Part You Play Curriculum

- 4 tracks (Mgt., PM, Dev/QA; Ops/Support)
- Each track obtains 30 page handbook
- Each track 2 hours a day over 7 days
- Each class 2 hours:
  - First hour presentation/instruction
  - Second hour workbook and topic discussion
- Tracks yield evaluation of current processes and 5 action items
- Fully aligned with ISO 17799, ISO 15408 and IEEE P1074

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved 24

## Management Track

- Session 1: Your Part in the Secure System Life Cycle
- Session 2: Security Leadership
- Session 3: Security Role Management
- Session 4: Determining Security Objectives
- Session 5: Determining Acceptable Risk
- Session 6: Assessing policies and procedures
- Session 7: Security Accreditation

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

25

## Project Management Track

- Session 1: Your Part in the Secure System Life Cycle
- Session 2: Evaluating Security Approaches
- Session 3: Setting Appropriate Project Controls
- Session 4: Identifying and Engaging Security Stakeholders
- Session 5: Evaluating Cost/Benefit of Security Controls
- Session 6: Justifying Acceptable Risk Level
- Session 7: Distributing Obtained Security Knowledge

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

26

## Development & Testing Track

- Session 1: Your Part in the Secure System Life Cycle
- Session 2: Threat Modeling for Security
- Session 3: Assuring compliance with Security Policies & Objectives
- Session 4: Justifying product security controls
- Session 5: End to End System Security Testing
- Session 6: Assuring Secure Product Upgrade and Integration
- Session 7: Assuring security operational readiness

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

27

## Operations Track

- Session 1: Your Part in the Secure System Life Cycle
- Session 2: Physical Security
- Session 3: Access Control Models
- Session 4: Building System Security Profiles
- Session 5: Determining Maintenance and Support Risk
- Session 6: Assessing System Integration Risk
- Session 7: Intrusion Detection Strategy and Response

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

28

## Source Information

- Contact: Bar Biszick
- [barb@dashmail.net](mailto:barb@dashmail.net); 425-241-5391
- [www.qualityit.net](http://www.qualityit.net)

Harris, Shon, CISSP Certification Exam Guide (McGraw Hill, 2002)

Peltier, Thomas R. Information Security Policies, Procedures and Standards (Auerbach Press, 2002)

(c) Bar Biszick-July, 2003  
Redmond WA-All Rights Reserved

29