SECURITY RISK MANAGEMENT

ISACA Atlanta Chapter, Geek Week
August 20, 2013

Scott Ritchie, Manager, HA&W
Information Assurance Services
Scott Ritchie
CISSP, CISA, PCI QSA, ISO 27001 Auditor

• Manager, HA&W Information Assurance Services
• Previous
  – AT&T, Internal Audit (Technology audits)
  – Scientific Research Corp., Information Systems Security Officer
• Academics
  – M.B.A.
  – M.S. Information Assurance

Scott.Ritchie@hawcpa.com
(770) 353-2761

http://www.linkedin.com/pub/scott-ritchie/2/308/260
# HA&W Information Assurance Services

<table>
<thead>
<tr>
<th>Key Verticals:</th>
<th>SME Domains:</th>
<th>Key Services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud &amp; Analytics</td>
<td>Security</td>
<td>• Risk and gap assessments</td>
</tr>
<tr>
<td>Healthcare IT</td>
<td>Privacy:</td>
<td>• Attest/Compliance Reporting:</td>
</tr>
<tr>
<td>Tech / Cloud Service Providers</td>
<td>o HIPAA / HITECH</td>
<td>• SSAE 16 &amp; SOC 2 Reporting</td>
</tr>
<tr>
<td>FinTech / Payments</td>
<td>o Safe Harbor</td>
<td>• PCI Compliance</td>
</tr>
<tr>
<td></td>
<td>o State Regulations</td>
<td>• ISO 27001 Certification</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>• FedRAMP Certification</td>
</tr>
<tr>
<td></td>
<td>Processing Integrity</td>
<td>• IT Internal Audit</td>
</tr>
<tr>
<td></td>
<td>Data Management</td>
<td>• IT Governance</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
<td>• Due Diligence</td>
</tr>
<tr>
<td></td>
<td>Financial Reporting</td>
<td></td>
</tr>
</tbody>
</table>
Focus of Today’s Presentation

- How to assess security risks
- Understand recognized security risk management frameworks
- Introduce security risk management practices

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Security Environment

- Explosive growth/ aggressive use of technology
- Proliferation of data
- Sophistication of threats

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Challenges

- Least privilege
- Awareness and **training**
- Insider threat
- Advanced Persistent Threats
- Trustworthiness of applications and systems
- Mobile computing
- Cloud and virtualization
- Individual/device auth
- **Resiliency** of Systems
- Privacy
- **Supply chain**

Can't cover everything - Risk management allows prioritization

http://www.linkedin.com/pub/scott-ritchie/2/308/260
"I don't think we should plug it in."
Definitions:

- **Risk**: Extent to which an entity is threatened by a potential event. (Note: Quantitative or Qualitative)
- **Risk Assessment**: Prioritization of risks based on probability and impact of an event.
- **Threat**: Circumstance with potential to adversely impact organizational operations, assets, individuals, and others.
- **Vulnerability**: Weakness in an information system, procedures, controls, or implementation.
- **Impact**: Magnitude of harm expected to result from the consequences of an event.
- **Probability**: Likelihood that a threat event will be initiated or will occur.
- **Predisposing conditions**: Condition which affects the probability that threat events, once initiated, result in adverse impacts.

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Risk Management (RM) Hierarchy

Reference: NIST 800-30

http://www.linkedin.com/pub/scott-ritchie/2/308/260
## Risk Assessment Frameworks

<table>
<thead>
<tr>
<th>OCTAVE</th>
<th>FAIR</th>
<th>NIST SP800-30</th>
<th>ISO 27005</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Develop an Information Asset Profile</td>
<td>• Identify asset at risk</td>
<td>2. Threat Identification</td>
<td>• Identification of Assets</td>
</tr>
<tr>
<td>3. Identify Information Asset Containers</td>
<td>• Identify the threat community</td>
<td>3. Vulnerability Identification</td>
<td>• Identification of Threats</td>
</tr>
<tr>
<td>4. Identify Areas of Concern</td>
<td>2. Evaluate Loss Event Frequency</td>
<td>4. Control Analysis</td>
<td>• Identification of existing controls</td>
</tr>
<tr>
<td>5. Identify Threat Scenarios</td>
<td>• Calculate Threat Event Frequency (TEF)</td>
<td>5. Likelihood Determination</td>
<td>• Identification of vulnerabilities</td>
</tr>
<tr>
<td>6. Identify Risks</td>
<td>• Calculate Threat Capability (Tcap)</td>
<td>6. Impact Analysis</td>
<td>• Identification of Consequences</td>
</tr>
<tr>
<td>7. Analyze Risks</td>
<td>• Estimate Control Strength (CS)</td>
<td>7. Risk Determination</td>
<td>2. Risk Estimation</td>
</tr>
<tr>
<td>8. Select Mitigation Approach</td>
<td>• Derive Vulnerability (Vuln)</td>
<td>8. Control Recommendations</td>
<td>• Assessment of consequences</td>
</tr>
<tr>
<td></td>
<td>• Derive Loss Event Frequency (LEF)</td>
<td>9. Results documentation</td>
<td>• Assessment of incident likelihood</td>
</tr>
<tr>
<td></td>
<td>3. Evaluate Probable Loss Magnitude (PLM)</td>
<td></td>
<td>• Level of risk estimation</td>
</tr>
<tr>
<td></td>
<td>• Estimate Worse Case Scenarios</td>
<td></td>
<td>3. Risk Evaluation</td>
</tr>
<tr>
<td></td>
<td>• Estimate Probable Lost Magnitude (PLM)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISO 27005: IT Risk Management

- Context Definition
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Risk Acceptance

Communication and consultation

Monitoring and review

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Understand the Organization

- Governance
  - Contractual relationships
  - Organizational structure
- Policies and objectives
- Resources and knowledge
- Information flows
- Relationships with stakeholders
- Organization's culture
- Standards
Management Commitment

- Rationale for managing risk
- Accountabilities for managing risk
- Methods for resolving conflicting interests
- Commit resources
- Risk management performance metrics
- Management Review
- Response to an event or change in circumstances.
- Risk Management Policy Communication
- Democratization of Risk Management
Risk Management Approach

- Nature and types of causes and consequences
- Likelihood and impact Criteria
- How the level of risk is to be determined
- Views of stakeholders
- Risk Tolerance Level and Acceptance Criteria
- Combinations of multiple risks

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Objectives of Risk Assessment

Understand business risks
Identify improvement opportunities
Allocate resources effectively
Get support from the enterprise
Demonstrate due diligence
Meet compliance requirements

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Information Asset Inventory

- Anything of value that requires protection
  - People, Process, Technology
  - Information
  - Supporting Infrastructure
  - Business processes

- Data Sources:
  - Listings of Enterprise Applications
  - Listings of Databases
  - Software Inventory
  - Hardware Inventory
  - System Diagrams
  - Technical Design Documents

http://www.linkedin.com/pub/scott-ritchie/2/308/260
<table>
<thead>
<tr>
<th>Asset Name/Description</th>
<th>Asset Class.</th>
<th>DR Priority</th>
<th>Description</th>
<th>Exposure Level (H,M,L)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel</td>
<td>High</td>
<td>1</td>
<td>Employees</td>
<td>M</td>
</tr>
<tr>
<td>Client PII</td>
<td>High</td>
<td>1</td>
<td>Personally Identifiable Information</td>
<td>L</td>
</tr>
<tr>
<td>Production Web server</td>
<td>Medium</td>
<td>1</td>
<td>Company primary website (no sensitive data)</td>
<td>H</td>
</tr>
</tbody>
</table>
Calculating Risk (perception)

\[ \int_{\text{breaches}} f(\text{security}) \, dx = \sum_{i=\# \text{ employees}}^{n=\text{risk}} \sqrt{\frac{\text{Privacy}}{\text{Encryption}}} \log_{\text{CAPEX}} \left( \frac{\text{Legislation} \times \text{Regulation}}{\text{lawsuits}} \right) \]

Source: CSOOnline.com

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Calculating Risk

Risk = Impact $\times$ Probability

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Risk Identification

Possible Risks

1422. Alien Invasion
1423. City destroyed by angry Monkey God
1424. Building eaten by giant pig.

“Well he certainly does a very thorough risk analysis.”
Risk Identification Sources

- System Docs
- Surveys and Interviews
- Audits/Gap Assessments
- Previous Events
- Workshops
- Threat Catalogs
- Vulnerability Assessments
Assess Threats

• Deliberate Attacks
  – Intent
  – Capabilities
  – Operational constraints
  – Exploit characteristics

• Natural
  – Fire
  – Water
  – Earth
  – Air

• Unintentional Exposures
  – Characteristics
  – Work Environment
  – Time constraints
Likelihood Considerations

• Experience and statistics for threat likelihood
• Motivation and capabilities of the attacker
• Exposure to possible attackers
• Accident sources: geographical / weather
• Human errors and equipment malfunction
• Individual and aggregate vulnerabilities
• Effectiveness of existing controls
Vulnerabilities

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Impact criteria

- Asset classification
- Breaches of information security
- Impaired operations
- Loss of business and financial value
- Disruption of plans and deadlines
- Damage to reputation
- Breaches of requirements

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Risk evaluation criteria

- Strategic value of the assets
- Criticality of the assets
- Legal, contractual, and regulatory requirements
- Operational and business importance of confidentiality, integrity, and availability (CIA)
- Stakeholders expectations
- Damage to reputation

http://www.linkedin.com/pub/scott-ritchie/2/308/260
## Example Risk Register

<table>
<thead>
<tr>
<th>Threat</th>
<th>Predisposing Conditions</th>
<th>Vulnerable Entities</th>
<th>Confidentiality</th>
<th>Integrity (L,M,H)</th>
<th>Availability (L,M,H)</th>
<th>Overall Impact</th>
<th>Likelihood of Attack Initiation</th>
<th>Likelihood Success</th>
<th>Total Likelihood</th>
<th>Overall Risk Rating</th>
<th>Control Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of communication of Business and IT needs leads to unintended exposure of data.</td>
<td>Business objectives are not aligned with IT strategies.</td>
<td>Business Operations</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Accidental or intentional duplication and retention of data leads to unnecessary exposure.</td>
<td>Sensitive documents are retained beyond useful life</td>
<td>All data sources.</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>Lost or stolen laptop leads to exposure of sensitive data.</td>
<td>No encryption on almost all laptops.</td>
<td>All servers, network devices, and laptops.</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Improper handling of data by employees, contractors, or vendors leads to exposure of sensitive data.</td>
<td>No formal privacy awareness, data handling, or information security training.</td>
<td>Employees, contractors, and vendors.</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
</tr>
</tbody>
</table>

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Risk Treatment

Accept

Mitigate

Transfer/Share

Avoid
Risk acceptance criteria

• Multiple thresholds and provisions for senior managers to accept risks
• Ratio of estimated benefit to the estimated risk
• Different acceptance criteria for different classes of risk
• May include requirements for future additional treatment

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Executive Summary, Methodology, and Detailed Results
Share results of assessment - present risk treatment plan
Eliminates misunderstanding among decision makers and stakeholders
Supports decision-making
Improve awareness and provides new knowledge
Co-ordinate with other parties and plan responses
Give decision makers and stakeholders a sense of responsibility about risks

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Re-Assess Risks

• Assessments are an on-going exercise
• Track mitigation strategies
• Re-test control design/effectiveness
• Document test results, corrective actions, changes in business needs/requirements.

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Future

- Develop risk-aware mission and business processes
- Integrate into enterprise architecture development
- Acquire IT systems with high level of assurance
- Consider threats when deploying new technology
- Agile defense
- Implement robust continuous monitoring programs

http://www.linkedin.com/pub/scott-ritchie/2/308/260
Questions

http://www.linkedin.com/pub/scott-ritchie/2/308/260
THANK YOU!