Acknowledgments

Material is from:
- CISA Review Manual, 2009
- CISM Review Manual, 2009
- Essentials of Corporate Fraud, T L Coenen, John Wiley & Sons, 2008
- The Art of the Steal, Frank Abignale, Broadway Books, 2001

Author: Susan J Lincke, PhD CISA
Univ. of Wisconsin-Parkside
Contributors: Gabriel John, Tim Dorr, Todd Burri
Reviewers: Tim Knautz, Will Zheng

Funded by National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and/or source(s) and do not necessarily reflect the views of the National Science Foundation.
Small & Medium Businesses (SMB)

- Can employ up to 500 employees
- Make up 95% of all business in the U.S.
- Produce about 50% of our GNP
- Employ about 50% of employees [NIST]

In Europe, a Small and Medium Enterprise (SME):
- employs less than 250 people
- makes up a large portion of businesses
Research shows that SMBs/SMEs:

- Lack security – lack time, expertise, $$
- Lack security awareness
- Not aware of security regulation

Businesses in general performed according to their size: large best, medium next best, and small worst.
Small Business Adhere to Security

- Breach Notification Law
- Payment Card Industry Data Security Standard (PCI-DSS)

Specific Industry Regulation affecting SMBs:
- HIPAA: Health Insurance Portability & Accountability Act
- FERPA: Family Education Rights & Privacy
Security Standards

General Security Standards
- ISO 27001
- FIPS (NIST)
- COBIT
- CISSP – CISA – CISM

Small Business Security
- NISTIR 7621 Small Business Information Security
- Small Business Security Workbook

Small Businesses can’t devote someone to Security
Security Workbook Objectives

- Accessibility to non-professionals
- Easy to use
- Based upon professional standards
- Full-featured
- Tailored to individual organization’s requirements
- Documented
- Useful for Educational & SMB Use
- Free
Small Business Security Workbook
- Overview

3. Strategic Security Plans
   3.1 Code of Ethics
   3.2 Policy Manual
   3.3 Risk Analysis
   3.4 Business Impact Analysis & Business Continuity

4. Tactical Security Planning
   4.1 Information Security
   4.2 Network Security Plan
   4.3 Physical Security Plan
   4.4 Incident Response
   4.5 Metrics
   4.6 Personnel Information Security

5. Operational Security Plans
   5.1 ‘Absolutely Necessary’ Security Standards
   5.2 ‘Highly Recommended’ Security Practices.

6. Audit Standards
Security is a Partnership

Business
- What to protect
- How much it will cost

Technology
- How best to protect
- How to detect and recover

Purpose of Workbook: Define Security Requirements
Code of Ethics Skeleton

This code of ethics provides general guidelines, and is not intended to cover every potential scenario. Examples are provided only as necessary for the employee to understand general concepts.

**General Employee Conduct While at Work**

Employees are expected to work overtime when patients remain in the office after hours, until the doctor on staff gives permission to leave.

HIPAA guidelines are to be followed, on potential penalty of firing, fines, and jail time.

**Unethical Behavior**

- Conflict of Interest
- Confidentiality

**Relationship with Customers and Suppliers**

- Gifts & Entertainment

**Using the Organization’s Assets for Personal Activities**

**Reporting Fraud or Unethical Behavior**

Least privilege ensures that computer access is provided only on an as-needed basis, and is a mandatory aspect of HIPAA for employees and business associates alike. All computer access requires individual authentication, and access to software, hardware, and data is controlled. Data owners decide access to data views, and this access is reviewed at least annually.
Qualitative Risk
Vulnerability Assessment Quadrant Map

- Threat (Probability):
  - Hacker/Criminal
  - Loss of Electricity
  - Malware
  - Failed disk
  - Stolen Laptop
  - Stolen Backup tape

- Vulnerability (Severity):
  - Social Engineering
  - Intruder
  - Earthquake
  - Flood
  - Fire

- Slow down business:
  - 1 week
  - 1 year
  - 5 years (.2)

- Temp. shut business:
  - Snow emergency

- Threaten Business:
  - 10 years (.1)
  - 20 years (.05)
  - 50 years (.02)
Quantitative Risk

Step 1: Assign Assets to Assets

<table>
<thead>
<tr>
<th>Asset</th>
<th>Direct Loss</th>
<th>Consequential Loss</th>
<th>CIA &amp; Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Building</td>
<td>250,000</td>
<td>Daily Op (DO)</td>
<td>Avail.</td>
</tr>
<tr>
<td>Medical Database</td>
<td>10,000</td>
<td>DO + Mal + Hip + Brch</td>
<td>CIA</td>
</tr>
<tr>
<td>Laptop</td>
<td>2,000</td>
<td>DO + Mal + Hip</td>
<td>Conf/Avail</td>
</tr>
</tbody>
</table>

Step 2: Determine Loss due to Threats & Vulnerabilities

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat</th>
<th>Single Loss Expectancy (SLE)</th>
<th>Annualized Rate of Occurrence</th>
<th>Annual Loss Expectancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility</td>
<td>Fire</td>
<td>$200,000</td>
<td>0.01</td>
<td>$2,000</td>
</tr>
<tr>
<td>Medical Office</td>
<td>Malpractice</td>
<td>$1M</td>
<td>0.05</td>
<td>$50,000</td>
</tr>
<tr>
<td>Medical Info</td>
<td>Stolen (Copied) (Hacker, malware, fraud)</td>
<td>$150,000 = $50K Liability + $100K Salary + notification</td>
<td>10</td>
<td>$150,000</td>
</tr>
</tbody>
</table>

Step 3: Estimate Likelihood of Exploitation
## Risk Table: Treat Risk

<table>
<thead>
<tr>
<th>Risk</th>
<th>ALE Score</th>
<th>Control</th>
<th>Cost of Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malpractice</td>
<td>$50,000</td>
<td>Medical server up</td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td>$25,000</td>
<td>Awareness training, HIPAA Adherence</td>
<td>Weekly HIPAA meetings, Annual training</td>
</tr>
<tr>
<td>Stolen Information/HIPAA audit</td>
<td>$15,000</td>
<td>HIPAA Adherence, Encrypted disks, VPN, firewalls, antivirus software, Audit tech/service</td>
<td>Weekly HIPAA meetings, Encryption &amp; security technology</td>
</tr>
<tr>
<td>Bad server disk</td>
<td></td>
<td>RAID system, backup</td>
<td>$800</td>
</tr>
<tr>
<td>Stolen laptop</td>
<td></td>
<td>Encrypted laptop, No stored records</td>
<td></td>
</tr>
<tr>
<td>Power Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failed Comm</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 4: Compute Expected Loss**

**Step 5: Treat Risk**
Introduce Concepts: Recovery Terms

**Interruption Window**: Time duration organization can wait between point of failure and service resumption

**Service Delivery Objective (SDO)**: Level of service in Alternate Mode

**Maximum Tolerable Outage**: Max time in Alternate Mode
Introduce Terms: RPO & RTO

Recovery Point Objective

Recovery Time Objective

- Critical
- Vital
- Sensitive
- Nonsensitive
- Patient Information
- One-week old data ok

One Week
One Day
One Hour
2 Hours
24 Hours
One Week
## BIA & Business Continuity

### Step 1: Define RPO, RTO

<table>
<thead>
<tr>
<th>Service</th>
<th>RPO (Hours)</th>
<th>RTO (Hours)</th>
<th>Critical Resources</th>
<th>Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Service</td>
<td>1 hour</td>
<td>0-2 hours</td>
<td>Computer system</td>
<td>Can operate with Patient DB being up to one week old for 2-3 days.</td>
</tr>
</tbody>
</table>

### Step 2: Define Control Technologies

<table>
<thead>
<tr>
<th>Data File and System/Directory Location</th>
<th>RPO (Hours)</th>
<th>Special Treatment (Backup period, RAID, File Retention Strategies)</th>
<th>Special Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Service</td>
<td>none, 1 day</td>
<td>RAID, Offsite backup/restore</td>
<td></td>
</tr>
</tbody>
</table>

### Step 3: Define Problem Events & Procedures (Backup/Restore…)

---
Sensitivity Classification
(Example)

- **Proprietary:** Nothing 😊
- **Confidential:** Health Info
- **Private:** Personnel records & reviews
- **Privileged:** Financial Info, Contracts
- **Public:** Web pages, Notice of Privacy Protection

CISA Review Manual 2009
## Classify Data by Sensitivity

<table>
<thead>
<tr>
<th>Sensitivity Class</th>
<th>Description</th>
<th>Information Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>Information <strong>protected by HIPAA or other law.</strong> Shall be made available or visible on a need-to-know basis only. Dissemination could result in financial liability or reputation loss.</td>
<td>Health care information: PHI &amp; EPHI Personnel records &amp; reviews</td>
</tr>
<tr>
<td>Privileged</td>
<td>Accessible to management or affected parties only. Could cause <strong>internal strife or external embarrassment</strong> if released.</td>
<td>Financial Database Budget Third party contracts</td>
</tr>
</tbody>
</table>
Define Treatment by Sensitivity Class

<table>
<thead>
<tr>
<th></th>
<th>Confidential</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access</strong></td>
<td>Need to know</td>
<td>Need to know</td>
</tr>
<tr>
<td><strong>Paper Storage</strong></td>
<td>Locked cabinet,</td>
<td>Locked cabinet,</td>
</tr>
<tr>
<td></td>
<td>Locked room if unattended</td>
<td>Locked room if unattended</td>
</tr>
<tr>
<td><strong>Disk Storage</strong></td>
<td>Server-only storage</td>
<td>Password-Protected</td>
</tr>
<tr>
<td></td>
<td>Password-protected,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encrypted,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Hashed</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Labeling &amp; Handling</strong></td>
<td>‘Confidential’</td>
<td>Clean desk</td>
</tr>
<tr>
<td></td>
<td>Clean desk,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>low voice,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>shut doors</td>
<td></td>
</tr>
<tr>
<td><strong>Transmission</strong></td>
<td>Encrypted</td>
<td><strong>Local only, Encr.</strong></td>
</tr>
<tr>
<td><strong>Archive</strong></td>
<td>Encrypted</td>
<td></td>
</tr>
<tr>
<td><strong>Disposal</strong></td>
<td>Degauss &amp; damage disks</td>
<td>Reformat disks</td>
</tr>
<tr>
<td></td>
<td>Shred paper</td>
<td></td>
</tr>
</tbody>
</table>
## Define Asset Inventory

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Information Access and Permissions (e.g. RWX)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>RW Access:</td>
</tr>
<tr>
<td></td>
<td>6.1 Patient Appointment</td>
</tr>
<tr>
<td></td>
<td>6.2 Patient Information</td>
</tr>
<tr>
<td></td>
<td>6.3 Patient Medical History</td>
</tr>
<tr>
<td></td>
<td>6.5 Patient Plan Management</td>
</tr>
<tr>
<td></td>
<td>6.6 Health Plan Eligibility</td>
</tr>
<tr>
<td></td>
<td>6.8 Health Care Claim Status</td>
</tr>
<tr>
<td></td>
<td>6.10 Health Care Payment</td>
</tr>
<tr>
<td>R.D.</td>
<td>RW Access:</td>
</tr>
<tr>
<td></td>
<td>6.4 Patient Medical Treatment (R for Prescription)</td>
</tr>
<tr>
<td></td>
<td>6.7 Health Care Claim</td>
</tr>
<tr>
<td>M.D.</td>
<td>RW Access:</td>
</tr>
<tr>
<td></td>
<td>6.4 Patient Medical Treatment</td>
</tr>
<tr>
<td></td>
<td>6.7 Health Care Claim</td>
</tr>
<tr>
<td></td>
<td>6.9 Certification and Authorization of Referrals</td>
</tr>
</tbody>
</table>

### Asset Information

<table>
<thead>
<tr>
<th>Asset Name</th>
<th>Patient Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value to Org.</td>
<td>Crucial to patient health, affects liability</td>
</tr>
<tr>
<td>Location</td>
<td>Secure Data Room</td>
</tr>
<tr>
<td>Criticality &amp; Sensitivity Class</td>
<td>Confidential, Vital</td>
</tr>
<tr>
<td>IS System</td>
<td>Patient Database</td>
</tr>
<tr>
<td>Data Owner</td>
<td>Jamie</td>
</tr>
<tr>
<td>Designated Custodian</td>
<td>Backup Ops: Terry IS Operations: Pat C.</td>
</tr>
</tbody>
</table>
Network Security: From where is data accessed?

Chris: Patient Care Personnel (Local)

Terry At Health First: Patient Scheduling, Patient History

HMO/PPO: Billing Authorizations, Referrals

At home – Jamie: Patient Care, Finances (local)
# Networked Applications

## Service and Server Table

<table>
<thead>
<tr>
<th>Service</th>
<th>Sensitivity</th>
<th>Roles</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Database</td>
<td>Confidential</td>
<td>Staff</td>
<td>Medical</td>
</tr>
<tr>
<td>Finance</td>
<td>Private</td>
<td>Partner</td>
<td>Operations</td>
</tr>
</tbody>
</table>

## Applications, Sources of Entry, Servers, and Controls Table

<table>
<thead>
<tr>
<th>Applications</th>
<th>Sources of Entry</th>
<th>Servers</th>
<th>Required Controls (e.g., Encryption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Database</td>
<td>Office, Home, Hospital</td>
<td>Medical Database Server &lt;only&gt;</td>
<td>Encryption, VPN</td>
</tr>
<tr>
<td>Medical Transactions</td>
<td>HMOs/PPOs</td>
<td>Medical Database Server</td>
<td>Encryption, specialized protocols</td>
</tr>
</tbody>
</table>
Network Security Map with Color-Coding
Physical Security Map with Color-Coding

Sensitivity Classification:
- Green = Public
- Yellow = Sensitive
  - Confidential Access
- Orange = Private
- Red = Confidential
  - Confidential Data Storage
  - No patients
  - Cabinets locked
  - Room locked

Criticality Classification:
- Critical: Air conditioning, UPS, fire suppressant, etc.
Incident Response Plan

**Preparation**

- Identify Incident
- Limit Incident
- Analysis & Eradication
- Recovery
- Lessons Learned

<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
<th>Methods of Detection</th>
<th>Procedural Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker Intrusion</td>
<td>An intruder has entered the local network.</td>
<td>Last login; Weekly log checks; Antivirus Email alarm</td>
<td>Table 4.4.2 Hacker Intrusion Incident Response</td>
</tr>
</tbody>
</table>

**Incident Type:** Hacker intrusion  
**Contact Name & Info:**  
**Emergency Triage Proc:**  
**Escalation Conditions and Steps:**

**Analysis & Eradication Proc:**
**Other Notes (Prevention techniques):**

Determine and remove root cause

Return operations to normal

Process improvement: Plan for the future
Top-Down Information Security → Security System

- **Risk** → $Assets $Threats
- **Info Sec.** → Sensitivity, Inventory, Access Cntrl
- **Network Sec.** → Path of Logical Access, network diagram
- **Physical Security** → Map, standards
- **BIA/BCP** → Criticality → RTO & RPO
- **Incident Resp.** → Detection, Procedures
- **Personnel Info. Sec.** → Segregated Duties, Policy, Training
- **Sensitivity, Roles**
- **Sensitivity**
- **Metrics**
- **Threats**
- **Assets**
- **Measure Threats**
- **Compliance & Audit**
Personnel Security:
Define Segregation of Duties

Authorization

Approves

Acts on

Double-checks

Origination

Distribution

Verification
Who could subvert the system?

<table>
<thead>
<tr>
<th>Fraud Problem</th>
<th>Legal Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>False new patient</td>
<td>➢ Medicare/HMO fraud</td>
</tr>
<tr>
<td>Unreported cash patients</td>
<td>➢ Theft or tax evasion</td>
</tr>
<tr>
<td>Selling drugs</td>
<td>➢ Malpractice</td>
</tr>
<tr>
<td>Selling health info</td>
<td>➢ HIPAA, Notification Act violation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat</th>
<th>Role</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>False new patient</td>
<td>Admin</td>
<td>Weekly audit meeting to review: Medical DB Access Report</td>
</tr>
<tr>
<td>Unreported cash patients</td>
<td>Admin</td>
<td>Weekly audit meeting to review: Medical DB Access Report</td>
</tr>
</tbody>
</table>
Allocate responsibility for security

<table>
<thead>
<tr>
<th><strong>Chief Security Officer:</strong> Terry</th>
</tr>
</thead>
</table>

Person responsible for security project management
- Take backup tapes daily
- Take backup tapes daily
- Lead weekly audit meeting, providing Medical DB Access Report
- Perform physical inventory weekly (except partners’ laptops)
- Collect security metrics
- Provide HIPAA and procedural security training
- Complete Incident Response Report when necessary
# Developing Metrics

## Threats
- HIPAA Audit
- Malpractice: Failed Disk/System
- Power Outage

## Metrics

<table>
<thead>
<tr>
<th>Category</th>
<th>Metric</th>
<th>Calculation &amp; Collection Method</th>
<th>Period Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>HIPAA Audit Performance</td>
<td>Health First Team</td>
<td>Annual</td>
</tr>
<tr>
<td></td>
<td>Computer Security Audit</td>
<td>Kenosha Software Audit Plan</td>
<td>Twice yearly</td>
</tr>
<tr>
<td>Tactical</td>
<td>Hours without DB service</td>
<td>Patient DB Outage Form</td>
<td>Twice yearly</td>
</tr>
<tr>
<td></td>
<td>Attendance at Audit meetings</td>
<td>Monthly audit meetings</td>
<td>Twice yearly</td>
</tr>
</tbody>
</table>
Conclusion
Goals are to...

Help small businesses
- Plan for security
  - Achieve near-COBIT Level 3
- Security Awareness Training
- Audit

Train Students
- Provide lectures on security
- Train students for CISA & CISM certification
- Help students gain valuable experience
Security Workbook Features

- Just-in-time security concepts
- Skeleton versions of text/tables
- Visual aids (color-coded maps)
- Build system of security
- Phased approach
- Security & teaching aids
Download of Workbook & Materials Available

If you would like to use the Security Workbook, Lectures, or Case Study
Indicate so on the form…

lincke@uwp.edu