Privacy, Security and Computer Ethics: It’s Everyone’s Responsibility

Presented to the Ethics & Compliance Officer Association
by Betty K. Steele, CISSP, JD
September 25, 2007
Certified Information Systems Security Professional (CISSP)

• “Gold standard” certification for information security
• Like JD for Information Security, but with experience
• ISO 17024 standard accredited by ANSI
• Increasingly required to validate credentials in 10 domains
• Very few attorneys have CISSP certification
• Information security is legally based
CISSP Domains

1. Access Control
2. Application Security
4. Cryptography
5. Information Security & Risk Management
6. Legal, Regulations, Compliance, & Investigations
7. Operations Security
8. Physical (Environmental) Security
9. Security Architecture & Design
10. Telecommunications & Network Security

See www.isc2.org for more details
Today’s Workshop

• Part I The Basics
  - Information Privacy, Security & Computer Ethics Program
    Structure & Definitions
  - Computer Ethics Overview
  - Laws & Regulations
  - Guidelines, Best Practices & Standards
  - Exercise 1: Identifying Applicable Laws & Regulations
Today’s Workshop

- Part II  Defining Roles & Responsibilities
  - Effect of Legal & IT Miscommunications
  - Preserving Evidence & Liability for Employee Misbehavior
  - Roles & Responsibilities Defined
  - Exercise 2:  Identifying Roles & Responsibilities
Today’s Workshop

• Part III  Protecting Information Assets & Managing Risk
  - Basic Concepts
  - Administrative, Technical & Physical Controls
  - Using an ISO 17799 Information Security Management Framework
  - **Exercise 3: ToDos - Tying It Together**
    - *Information Privacy, Security & Computer Ethics Program Checklist*
    - *Information Security and Privacy Policy*
    - *Acceptable Use of Information Assets Policy*
  - Top Ten Takeaways from Workshop
PART I

The Basics
Policies, Procedures, Standards, Baselines, & Guidelines

- Laws, Regulations, Requirements, Goals, Objectives
- General Organizational Policy
- Functional Implementing Policies
  - Standards
    - Specific Hardware & Software
  - Procedures
    - Step-by-Step Instructions
  - Baselines
    - Consistent Level of Security
  - Guidelines
    - Recommendations

Chart From Official (ISC)² Guide to the CISSP CBK
Policies, Procedures, Standards, Baselines, & Guidelines

• Organizational or Program Policy
  – Created by management
  – Creates authority for & scope of plan
  – Defines what an organization needs at highest level
  – Reflects laws, regulations, requirements (including ethical requirements), goals, & objectives
Policies, Procedures, Standards, Baselines, & Guidelines

- **Functional, Issue-Specific Policies**
  - Defines what an organization needs at functional level
  - Targeted at different domains
    - Access control
    - Contingency planning
  - Address specific technical areas
    - Internet usage
    - Wireless/remote system access
  - Can be combined into acceptable use of assets policy
    - All users
    - Some users
Policies, Procedures, Standards, Baselines, & Guidelines

• Standards
  – Define requirements or protocols
  – Are mechanisms for controlling security risks
  – Ex., in selecting control for remote access identification & authentication could use:
    ▪ Log-in IDs & passwords
    ▪ VPN over Internet
  – May also refer to guidelines of standardization organizations such as NIST, ISO or ANSI
Policies, Procedures, Standards, Baselines, & Guidelines

- **Procedures**
  - Are step-by-step instructions supporting policies, standards, guidelines, & baselines
  - Are best developed by employees carrying them out

Instructions

1. Position tack ¾ inch from top of cardboard
2. Push in firmly with thumb
3. Cover tack with gold star

Instructions

4. Position tack ¾ inch from bottom of cardboard
5. Push in firmly with thumb
6. Cover tack with silver star
Policies, Procedures, Standards, Baselines, & Guidelines

- Baselines
  - Provide required level of protection
  - Are descriptions of how to implement security packages consistently throughout organization
  - Are analysis of available configuration settings, form basis for future, consistent implementation
Policies, Procedures, Standards, Baselines, & Guidelines

• Guidelines
  – Are discretionary or optional controls
  – Are also recommendations, best practices, templates from ISO, NIST, ethics organizations
Why Have an Information Privacy, Security & Computer Ethics Program?

- Consumer concerns about identity theft
- Investor concerns about corporate fraud
- Government concerns about cyberattacks
Why Have an Information Privacy, Security & Computer Ethics Program?

- Laws & marketplace IT requirements increasingly prescriptive
- Technology used to enforce legal compliance
- Laws, technology & standards merging
- And it’s all happening fast!
What Is Computer Ethics?

- Ethics Is Generally - Standards, Values, Principles on Which to Base Decisions
- Three Truths
  - Legal ≠ Ethical
  - Compliance ≠ Security
  - Accountability ≠ Responsibility
- Ethical Computing
What Is Computer Ethics?

• Meeting the Explicit & Implicit Legitimate Expectations of Stakeholders
  - Laws, Regulations, Directives
  - Standards, Best Practices
  - Marketplace Requirements
  - Risk Management

• Ethical Computing Should Be Incorporated into Behavior
What Is Computer Ethics?

- Roots of Ethical Problems in Common Fallacies
  - Computer Game (Computer Will Prevent Cheating)
  - Law-Abiding Citizen (Confusing What One Has a Right to Do versus What Is Right to Do)
  - Shatterproof (Computer Users Can’t Hurt People)
  - Candy-from-a-Baby (Rampant Software Piracy)
  - Hacker (Primary Goal Is Learning)
  - Free Information (Information Wants to Be Free)
What Is Computer Ethics?

- Professional Codes of Ethics
  - (ISC)² www.isc2.org
  - Information Systems Security Association www.issa.org
  - Internet Architecture Board www.iab.org
  - Computer Ethics Institute www.brook.edu/its/cei
  - Generally Accepted System Security Principles
The Ethics Program

- Regulatory Requirements
  - Federal Sentencing Guidelines
  - Sarbanes - Oxley Act
  - New & Revised Regulations from Agencies
The Ethics Policy

• Regulatory Requirements
  - Consider Issues such as:
    ▪ Computer crime (i.e., internal personnel)
    ▪ Privacy & anonymity (i.e., SOX whistleblower provisions & EU Data Directive)
The Ethics Program

Good Practices

1. Computer Ethics Policy
2. Computer Ethics Training
3. Monitoring of Employee Behavior
4. Acceptable Use of Information Assets Policy
The Ethics Program

- **Roles & Responsibilities**
  - Data Owners/Collectors to Data Subjects
  - Data Custodians to Data Owners
  - Data Users to Owners/Subjects
  - System Users to System Owners
  - System Managers to Users
  - Users to Users
Major Federal Information Privacy & Security Laws

- **Federal Trade Commission Act**
  - Prevent unfair or deceptive trade practices when not keeping information privacy & security promises
  - Applies to companies using/disclosing consumer information

- **Gramm-Leach-Bliley Act**
  - Privacy & security obligations to limit disclosure of consumer financial information
  - Applies to financial institutions
Major Federal Information Privacy & Security Laws

- **Fair Credit Reporting Act**
  - Provides framework for credit reporting industry & rights to consumers
  - Applies to credit reporting agencies

- **Health Insurance Portability and Accountability Act**
  - Privacy & security obligations for individuals’ medical information
  - Applies to providers, payers [including company health plans] & health care clearinghouses
Major Federal Information Privacy & Security Laws

- **Federal Information Security Management Act**
  - Establishes requirements for security of government systems
  - Applies to non-defense related federal government

- **Children’s Online Privacy Protection Act**
  - Gives parents control over what information is collected from children online & how it can be used
  - Applies to operators of commercial Web sites
Major Federal Information Privacy & Security Laws

- **Sarbanes Oxley Act**
  - Protects financial information with internal controls for financial reporting
  - Applies to public companies
Major International Information Privacy & Security Laws

- **European Union Data Protection Directive**
  - Protects privacy rights of individuals when their personal information is processed
  - Applies to any person seeking to process personal information within the EU or transfer such information outside of the EU
Major International Information Security Laws

- **Canadian Personal Information Protection & Electronic Documents Act**
  - Prevents personally identifiable information from being collected, used or disclosed without the individual’s knowledge & consent
  - Applies to federal works, undertakings or businesses, as well as all unregulated private sector organizations engaged in commercial activity in Canada
VA & Los Alamos

• VA:
  - 1/07, hard drive with data on Drs & 500,000 vets missing
  - 5/06, home theft of laptop with data of 26 million

• Los Alamos (three 2007 breaches reported by media):
  - Laptop stolen from vacation hotel room
  - Scientist fired off e-mail to nuclear test site over Internet
  - Lab manager circulated e-mail over Internet about US nuclear arsenal
Laptop Rules

- Employees must access thru server
- If data saved to hard drive must be to encrypted folder
- Files must be deleted from hard drive ASAP
- Laptops must be secured in drawer or office at end of day
- If taken must be locked in trunk, drawer or safe
- Payroll employees must use cable lock
TJX 45.7 Million Credit & Debit Card Numbers & 455,000 Drivers’ License Numbers Stolen

- 8/07, announces large charge because of data breach
- 1/07, illegal access of payment systems announced
- Intrusions took place in 2005, 2006 & early 2007
- Banks & credit unions block & reissue credit cards
- Credit unions pressure to require secure system/financial responsibility
Piedmont Hospital Audit Puts Hospitals on Edge

• Audit by OIG of DHHS
• List of 42 items requested, policies & procedures for:
  - User access to ePHI
  - Emergency access to systems
  - Risk assessments
  - Employee violations & sanctions
  - Review of audit records
  - Physical access to electronic information systems
May OMB Salvo to Executive Branch Department & Agencies

- Required breach notification policy by end of September
2006 FTC Creation of Division of Privacy & Identity Protection

- **Typical violations are:**
  - Failure to have adequate passwords
  - Unnecessary storage of documents & records
  - Failure to encrypt data in transmission & storage
  - Failure to use security measures for wireless networks
  - Inadequately assessing vulnerabilities for common risks
  - Failure to have measures to detect unauthorized access

- **Enforcement action includes audits every 2 years for 20 years**
- **Plus companies are sued**
ChoicePoint

- Data broker sold credit data of 145,000 to identity thieves
- 35,000 Californians notified
- Later 110,000 from other states notified
- Government investigations
- Stock value & revenue declines
- FTC settlement - $10 M penalties & $5 M consumer redress
- 5/07, settled with states for $500,000 for ID theft education
Security Breach Notification Laws

• **Purpose:** To require notice to individuals (sometimes, notice to credit reporting agency)

• **Applies to:** Organizations that collect, use & disclose unencrypted (most states) personal information

• **Concern:** Danger in relying solely on encryption
Perils of Outsourcing

• Domestic outsourcing events:
  - Third-party payment processor CardSystems
  - Data broker ChoicePoint
  - UPS

• Controversy with outsourcing to India, China, the Philippines
Guidelines, Best Practices & Standards

  - Guidelines & general principles for security management
  - Best practices of control objectives & controls
  - De facto world standard
Guidelines, Best Practices & Standards

• **IT Infrastructure Library**
  – Series of best practice publications, including security management
  – Works with British Standards Institution
  – BS 7799 is genesis of ISO/IEC 17799
Guidelines, Best Practices & Standards

• National Institute of Standards & Technology
  – Federal agency within Dept of Commerce
  – Computer Security Division provides standards for feds
  – Standards also used by US industry for HIPAA, GLBA, etc.
  – Excellent security management publications
Guidelines, Best Practices & Standards

- **Payment Card Industry Data Security Standard**
  - Created by major credit card companies
  - Protects credit & debit card information
  - Merchants must comply
  - Used as standard for state legislation to shift costs of credit & debit card losses to merchants
Exercise 1: Identifying Applicable Laws & Regulations

   a. Determine which apply directly to your company (includes your vendor or service provider)
   b. Determine which apply indirectly to your company (includes you as vendor or service provider)
3. Consider Other Issues.
   a. Does law apply now?
   b. Will it apply soon?
   c. What enforcement actions, litigation, etc., are out there?
   d. What standards, etc., should be used?
   e. What is the competition doing?
   f. What is the marketplace requiring?
4. List Applicable Laws and Regulations, How They Apply (Directly or Indirectly) and Other Issues – Exercise 1, Worksheet 2.
Part II

Defining Roles & Responsibilities
Establishing Unambiguous Roles

- Demonstrates management support
- Increases employee efficiency
- Lowers risks to reputation damage
- Enhances capability to manage systems
- Provides personal accountability
- Reduces misunderstandings/turf protection
- Supports disciplinary action for violations
- Demonstrates compliance
- Fosters responsibility
Roles & Responsibilities – Miscommunications
## IT/Legal Communications Gap

**“The Battle of the Acronyms”**

<table>
<thead>
<tr>
<th>IT</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>AMT</td>
</tr>
<tr>
<td>BSB</td>
<td>BSA</td>
</tr>
<tr>
<td>CMM</td>
<td>CGC</td>
</tr>
<tr>
<td>DBMS</td>
<td>DISC</td>
</tr>
<tr>
<td>EAP</td>
<td>EAA</td>
</tr>
</tbody>
</table>
## IT/Legal Communications Gap

### “The Cheat Sheet”

<table>
<thead>
<tr>
<th>IT</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ACL</td>
<td>• AMT</td>
</tr>
<tr>
<td>Access Control List</td>
<td>Alternative Minimum Tax</td>
</tr>
<tr>
<td>• BSB</td>
<td>• BSA</td>
</tr>
<tr>
<td>Back Side Bus</td>
<td>Bank Secrecy Act</td>
</tr>
<tr>
<td>• CMM</td>
<td>• CGC</td>
</tr>
<tr>
<td>Capability Maturity Model</td>
<td>Controlled Foreign Corporation</td>
</tr>
<tr>
<td>• DBMS</td>
<td>• DISC</td>
</tr>
<tr>
<td>Database Management System</td>
<td>Domestic Int’l Sales Corporation</td>
</tr>
<tr>
<td>• EAP</td>
<td>• EAA</td>
</tr>
<tr>
<td>Extensible Authentication Protocol</td>
<td>Export Administration Act</td>
</tr>
</tbody>
</table>
IT/Legal Communications Gap
Different Goals

• Different Goals
  – Keep systems up &
    secure
  – Ensure clients comply
    with law
Big Bucks at Stake
“The $140,000 Miscommunication”

- Lawsuit for fraudulent inducement to buy products
- Lawyers ask IT for information
- IT provides it in requested format
- Lawyers manually enter into litigation application

**Solution:** Someone who understands data structure of CRM & sales automation applications & legal side needs to mediate.
Big Bucks at Stake
“The Almost $12.5 Million Bill”

- Large healthcare provider outsourced IT management
- It needed to produce emails for 10 custodians for 2 yr period
- 20 separate Microsoft Exchange servers were backed up daily
- 12,500 backup tapes for email systems alone
- IT solution included restoration of all Exchange environments to online ‘live” format so individuals’ mailboxes could be searched
- Solution required 500 Terabytes of storage & cost $12.48 million
### Big Bucks at Stake

**“The Almost $12.5 Million Bill”**

<table>
<thead>
<tr>
<th>Solutions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Legal requested restoration of custodians’ email</td>
</tr>
<tr>
<td>• Legal uncertain of scope they wanted to cover</td>
</tr>
<tr>
<td>• IT heard as need for “live” environment for 20 servers</td>
</tr>
<tr>
<td>• IT heard daily backups</td>
</tr>
</tbody>
</table>

**Solutions:** Exchange backups contain backup file (.EDB) which can be read & searched w/o restoring entire environment – cost $3.1M. Because no mailbox limits (& email deletion spotty), they decide to sample backups on monthly rather than daily basis. (Risk of missing email considered small & final cost $1.1M, or 10% of original quote).
Talking Past Each Other
“Just Ask Why”

- Large gov’t agency defending Title VII case
- Broad request from legal included all email & other HR ESI
- IT said backups did not exist & Legal kept asking
- Until … 5 million messages recovered

**Solution:** Ask or tell what’s behind the request.
The Dog Ate My Homework & Duty to Preserve Evidence

- *US v. Quattrone* – Investigation by SEC, NASD & grand jury
- Q sends document destruction policy to employees
- Some employees deleted emails & purged files
- Q’s actions provide nexus for his conviction

**Lesson:** The cover-up is always worse.
Employer Liability for Employee On-Line Activities

• *Doe v. XYC Corporation* – Company liable for employee child porn because of failure to enforce its own policy.

**Lesson:** Have acceptable use policy, train & enforce it.
Employee Expectation of Privacy in Workplace

- *US v. Barrow* – City worker who brought personal computer to work had no expectation of privacy when child porn found on hard drive.

**Lesson**: Have acceptable use policy, train & enforce it.
Roles & Responsibilities

- **Data Owners/Collectors to Data Subjects**
  - Ex., Employer (CEO) to Employees

- **Data Custodians to Data Owners**
  - Ex., Electronic Records Administrator to Plant Manager

- **Data Users to Owners/Subjects**
  - Ex., Health Plan Employee to Employer/Patient

- **System Users to System Owners**
  - Ex., Employee (Authorized to Use System) to Employer

- **System Managers to Users**
  - Ex., Systems Administrator to System Subscribers

- **Users to Users**
  - Ex., Peer-to-Peer Network
Role Playing

- **Board of Directors/Management**
  - Overall responsibility for information assets
  - Responsible for ensuring information availability, accuracy & protection
  - Should be aware of risks that they are accepting

**Role:** Employer/Data – System Owner
Role Playing

• Security Officer
  – Directs, coordinates, plans, & organizes security activities
  – Communicates risks to management
  – Budgets for information security activities
  – Ensures development of policies, procedures, baselines, standards, & guidelines
  – Develops & provides security awareness training program
  – Understands business objectives
  – Maintains awareness of emerging threats & vulnerabilities
Role Playing

• **Security Officer**
  – Evaluates security incidents & responses
  – Develops security compliance plan
  – Establishes security metrics
  – Ensures compliance with government regulations & client requirements
  – Assists internal & external auditors
  – Stays abreast of emerging technologies
  – Listens

Role: Data Custodian
Role Playing

• **General Counsel**
  – Identifies applicable laws & regulations
  – Drafts & recommends general organizational policy in conjunction with security officer
  – Coordinates with security officer on other applicable policies, procedures, standards, baselines, & guidelines

**Role:** Data Collector/Custodian
Role Playing

• **Chief Information Officer**
  – Heads up IT department
  – Aligns technology & business strategy

Role: Data/System Owner - Data Custodian/System Manager
Role Playing

• **End Users**
  – Protects data through adherence to security policies
    ▪ i.e., Does not download unauthorized software, open attachments from unknown senders, etc.
  – Can report security incidents for investigation

**Role: Data/System Users**
Role Playing

• **Information Systems Security Professionals**
  – Develop security policies, procedures, standards, baselines, & guidelines
  – Implement & review same
  – Provide guidance for technical security issues & threats
  – Provide technical interpretation of government regulations
  – Provide technical interpretation of industry trends & determine vendor solutions in security architecture

Role: Data Custodians/System Managers
Role Playing

• Division, Department Heads/Directors
  – Classify information assets & ensure protection with appropriate controls
  – Review controls & access rights

Role: Data Owners/Collectors - System Owners
Role Playing

- IT Department Employees (Generally)
  - Take care of information on behalf of data owner
  - Ensure information available to end users
  - Ensure information backed up to enable recovery

Role: Data Custodians/System Managers
Role Playing

• **Information Systems Auditors**
  – Determine compliance
  – Provide independent assurance to management
  – Examine systems to determine organizational objects met

**Role: Data Collectors/Users**
Role Playing

- **Physical Security Professionals**
  - Manage installation, maintenance & ongoing operations of CCTV, burglar alarms, etc.
  - Manage guards
  - Establish relationships with external law enforcement, FBI
  - Interface with systems security, HR, facilities, etc.

Role: Data Custodians
Role Playing

- **Administrative Assistants/Secretaries/Receptionists**
  - Greet visitors, sign in packages, screen phone, etc.
  - Recognize individuals at place of business

**Role: Data Custodians**
Role Playing

- **Help Desk Administrator**
  - Fields questions from users
  - Contacts computer incident response teams

**Role: Data Custodian/User**
Role Playing

- **Directors/Teams for Quality, Six Sigma, etc.**
  - Understand linkages with processes, metrics, etc.
  - Are critical to effectiveness of implementation & success of program

**Role: Data Custodians/Users**
Four Types of Responsibilities

1. To lead information security governance & be externally accountable (CEO)
2. To lead the information security program (CISO)
3. To participate in implementation & follow security policies (GC)
4. To be a general user following security policies (employee)
Exercise 2: Identifying Roles & Responsibilities

1. Circle Types of Information (on Exercise 2, Worksheet 1) You
   a. Collect
   b. Use
   c. Request
   d. Disclose
   e. Store
   f. Destroy.


3. List in Roles & Responsibilities Identified - Exercise 2, Worksheet 3
   a. Types of Information Circled in Exercise 2, Worksheet 1,
   b. Whether You Collect, Use, Request, Disclose, Store, or Destroy It
   c. Your Role for each type of Information
   d. To Whom a Duty Is Owed.

Part III

Protecting Information Assets & Managing Risk
Protecting Information Assets & Managing Risk

Protect CIA Triad

Confidentiality  

![Diagram with Confidentiality and Integrity linked to Availability]

Integrity

Availability

of Sensitive Information
Types of Controls – Layered Defense

- **Administrative**
  - Security Awareness Training
  - Access Authorization
  - Security Incident Management

- **Technical**
  - Logical Access
  - Authentication (Person/Entity)
  - Transmission Security

- **Physical**
  - Facility Access
  - Workstation Security
  - Device & Media Disposal
ISO 17799 Information Security Management Standard

1. Organization of Information Security
2. Asset Management
3. Risk Management
4. Human Resources Security
5. Physical & Environmental Security
6. Communications & Operations Management
7. Access Control
8. Information Systems Acquisition, Development & Management
9. Information Security Incident Management
11. Compliance
Organization of Information Security (ISO 17799)

- **Internal Organization**
  - Management Commitment
  - Allocation of Responsibilities
  - Confidentiality Agreements
  - Independent Review

- **External Parties**
  - Identify Risk
  - Security & Customers
  - Security in Third Party Agreements
Asset Management (ISO 17799)

• Responsibility for Assets
  – Inventory
  – Ownership
  – Acceptable Use

• Information Classification
  – Guidelines
  – Labeling & Handling
Risk Management (ISO 17799)

- Assessing Security Risks
  - Qualitative
  - Quantitative

- Treating Security Risks
  - Transfer it
  - Reduce it
  - Accept it
  - Deny it
### Human Resources Security (ISO 17799)

<table>
<thead>
<tr>
<th>Prior to Employment</th>
<th>During Employment</th>
<th>Termination or Change in Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles &amp; Responsibilities</td>
<td>Management Responsibilities</td>
<td>Termination Responsibilities</td>
</tr>
<tr>
<td>Screening</td>
<td>Security Awareness, Education &amp; Training</td>
<td>Return of Assets</td>
</tr>
<tr>
<td>Terms &amp; Conditions of Employment</td>
<td>Disciplinary Process</td>
<td>Removal of Access Rights</td>
</tr>
</tbody>
</table>
Physical & Environmental Security (ISO 17799)

• Secure Areas
  – Physical Security Perimeter
  – Physical Entry Controls
  – Securing Offices, Rooms, & Facilities
  – Protecting Against External & Environmental Threats
  – Working in Secure Areas
  – Public Access, Delivery, & Loading Areas

• Equipment Security
  – Equipment Siting & Protection
  – Supporting Utilities
  – Cabling Security
  – Equipment Maintenance
  – Security of Equipment Off-Premises
  – Secure Disposal or Re-Use of Equipment
  – Removal of Property
Communications & Operations Management (ISO 17799)

- Operational Procedures
- Third Party Delivery Management
- System Planning & Acceptance
- Protection Against Malicious & Mobile Code
- Back-Up
- Network Security Management
- Media Handling
- Exchange of Information
- Electronic Commerce Services
- Monitoring
Access Control (ISO 17799)

- Business Requirement for Access Control
- User Access Management
- User Responsibilities
- Network Access Control
- Operating System Access Control
- Application & Information Access Control
- Mobile Computing & Teleworking
Information Systems Acquisition, Development & Maintenance (ISO 17799)

- Security Requirements of Information Systems
- Correct Processing in Applications
- Cryptographic Control
- Security of System Files
- Security in Development & Support Processes
- Technical Vulnerability Management
Information Security Incident Management (ISO 17799)

• Reporting Information Security Events & Weaknesses
  – Reporting Information Security Events
  – Reporting Security Weaknesses

• Management of Information Security Incidents & Improvements
  – Responsibilities & Procedures
  – Learning from Security Incidents
  – Collection of Evidence
Business Continuity Management (ISO 17799)

• Information Security Aspects of Business Continuity Management
  – Business Continuity & Risk Assessment
  – Developing & Implementing Continuity Plans
  – Planning Framework
  – Testing, Maintaining & Re-Assessing
Compliance (ISO 17799)

• Compliance with Legal Requirements
  – Identification of Applicable Legislation
  – Intellectual Property Rights
  – Protection of Records
  – Data Protection & Privacy of Personal Information
  – Prevention of Misuse of Information Processing Facilities
  – Regulation of Cryptographic Controls

• Compliance with Security Policies & Standards, & Technical Compliance

• Information Systems Audit Considerations
Problems with Complexity

- Expensive
- Training Intensive
- Policies & Procedures By-Passed by Employees
- This Occurs Because of:
  - Attempted integration of poorly understood systems
  - Poorly understood business & technical issues
  - Non aligned, linear approach to compliance
  - Poorly understood legal requirements
  - Lack of documentation
  - Lack of interoperability
  - Lack of change control

• **Most incidents required little sophistication**
  – Exploitation of non-technical vulnerabilities such as policies
  – Carried out by employees with limited technical expertise

• **Perpetrators planned their actions**

• **Financial gain motivated most perpetrators**

• **Perpetrators did not share a common profile**
  – Most did not have a technical position
  – Most were not problem employees

• Incidents were detected by various methods & people
  – Detected by internal & external people
  – Detection procedures were both manual & automated

• Victim organizations suffered financial loss
  – Low of $168
  – High over $691 million
  – Significant decline in stock value (which can lead to SEC investigations & shareholder law suits)

• Perpetrators committed acts while on the job
So How Are We Doing?
Recent Surveys of IT & Compliance

• It’s Getting Worse! Ponemon Study Reports
  - 45% say couldn’t notify customers & users if breach
  - IT more pessimistic than compliance about ability to control data breaches (42% to 33%)

• 1/3rd Said Major Breach Could Put Them Out of Business! McAfee Study Reports
What’s Coming Up?

• More enforcement
• More prescriptive regs & guidance
• More marketplace consensus on common standards
  - PCI
  - ISO 17799
  - CCHIT
• More accountability for outsourcing
• More reason to have a comprehensive security incident response plan
Privacy, Security & Computer Ethics Maturity Model

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lack of understanding of interdependencies</td>
<td>• Some understanding of interdependencies</td>
<td>• Unified approach</td>
<td>• Alignment with business strategies</td>
<td>• Strategic approach &amp; continuous improvement</td>
</tr>
<tr>
<td>• Ad hoc approach to technology</td>
<td>• Siloed approach to technology</td>
<td>• Silos are taken down</td>
<td>• No silos</td>
<td>• Lack of distinction between technology used for requirements &amp; other technology</td>
</tr>
<tr>
<td>• Hard to address new requirements</td>
<td>• New requirements in a silo do not take into account other areas</td>
<td>• New requirements addressed using common platform</td>
<td>• Technology consolidated</td>
<td>• Requirements embedded into business systems</td>
</tr>
<tr>
<td>• No metrics</td>
<td>• Difficult to measure</td>
<td>• Benefits measured</td>
<td>• Business benefits measured</td>
<td>• Business benefits measured/improved</td>
</tr>
</tbody>
</table>

Adapted from IT Roadmap for GRC, Compliance & Technology, July 2007
Exercise 3: To Dos – Tying It Together

   a. Note that the most time consuming part of the Program is information gathering.
   b. Also note that the success of the risk assessment is predicated on the accuracy and comprehensiveness of the information gathering.
   c. Determine types of controls based on quantitative and qualitative risk assessment and organizational “appetite for risk.”
   d. Determine standards, best practices, metrics, and the like based on a variety of factors including industry type, organizational size and sophistication and regulatory environment.
   e. Ensure role/job specific training, consistent deployment across the organization and measurable compliance and enforcement.
   f. Incorporate into capital planning process.


Top Ten Takeaways from Workshop

1. Understanding of Interdependencies & How Policies, Procedures, Standards, Baselines, & Guidelines Are Used
2. Legal & Marketplace Reasons for Plan
3. What Computer Ethics Is
4. Importance of Planning & Documentation
5. Why Defined Roles & Responsibilities Are Essential
6. Recognizing Pitfalls of Miscommunications
7. The Importance of Risk Management
8. Types of Controls & How to Use Them
9. Using an ISO 17799 Framework
10. Exercise Materials Including
   a. Privacy & Security Laws & Regulations
   b. Security Policy
   c. Acceptable Use of Information Assets Policy
   d. Information Privacy, Security & Computer Ethics Checklist