Electronic Records Security and Privacy

Tuesday, May 16

2006 AIIM Annual Conference and Expo

Daryl L. Thompson
darylthompson@thompsnet.com

Why is Security essential?

- The state of Rhode Island was forced to take down its online vehicle registration system in January after hackers stole user information, including credit card numbers
- In Seattle, a hospital lab technician gained unauthorized access to patient records and stole patient personal data
- A Blue Cross and Blue Shield contractor sent names and SS numbers of employees and vendors to their home computer
- At Honeywell International, employee information including Social Security Numbers and Bank Accounts were exposed on company website
- A laptop belonging to Fidelity Investments that held the names, addresses, birth dates, Social Security numbers and other information of 196,000 retirement account customers was stolen

- Electronic Records Privacy
  - Knowledge and control of how records are maintained, utilized and disclosed
- Electronic Records Security
  - Management process through which Electronic Records Privacy is achieved
- Security supports:
  - Compliance with regulations
  - Productive IT infrastructure
  - Business operation data protection

Electronic Records Security Agenda

- Electronic Records Definition
- Security Threats
  - Threat Agents
  - Threat Types
- Security Management
  - Principles
  - Concepts
  - Process
- Workshop Objective
  - Discuss Record Management role in managing Information Security

Electronic Records Definition

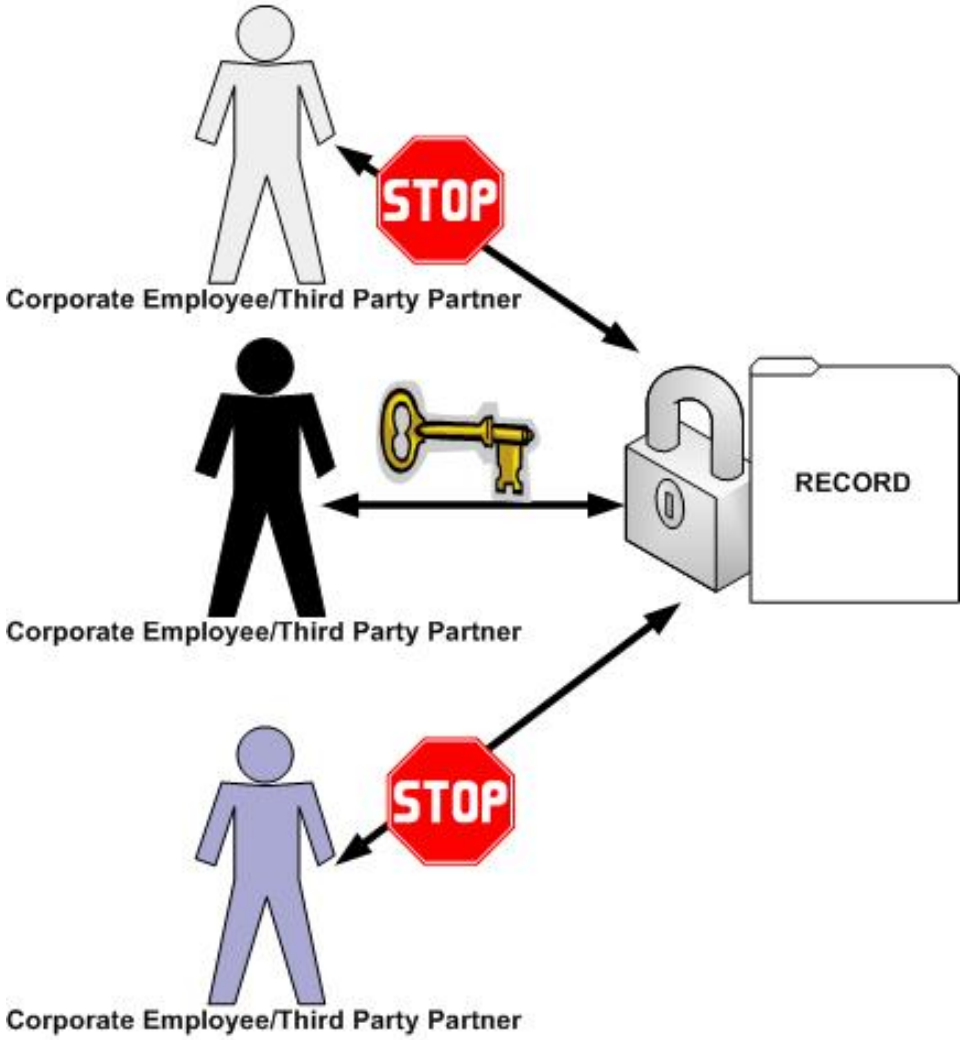
- An Electronic Record is essential for business operations:
  - Document
  - Database entry
  - E-mail/Instant Message
  - Other types of content
- Electronic Records are:
  - Created under a variety of circumstances
  - Assigned LifeCycle and Retention schedules
  - Subject to regulatory compliance
  - Stored in a Repository (Application/File Server, Storage Network)

Electronic Records Definition

- Electronic Record Users are:
  - Employees
  - Third Party Partners
  - Customers/Clients/Patients
  - Computer Systems (Web Services)
- Electronic Records can be Accessed Through:
  - Company Intranet
  - Internet
- Electronic Record User Authentication Credentials
  - Something You Know: Usernames/Passwords
  - Something You Are: Fingerprint/Eye Scan
  - Something You Have: Token
  - Something You Trust: Certificate Authority

Electronic Records Definition

- Electronic Record Access is customized by:
  - Governing laws and regulations
  - Industry practices
  - Business operations and culture
- Creates relationship between authenticated record users, records and authorized operations
  - Specific record access criteria



Electronic Records Definition

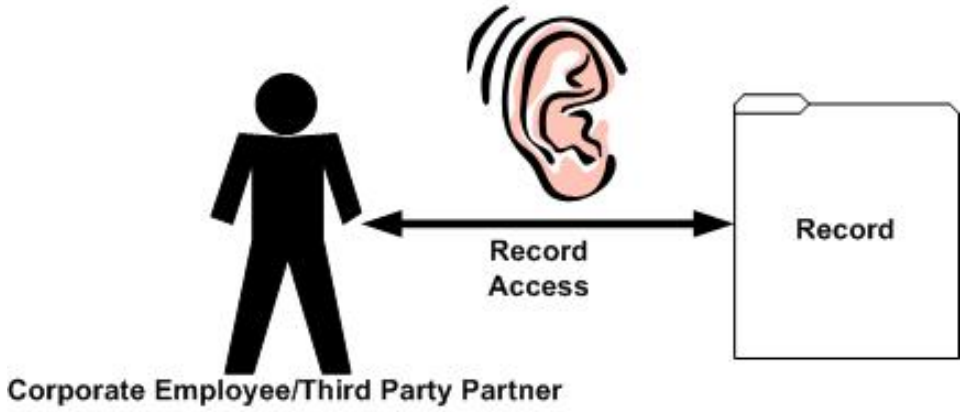
- Records relationship is characterized by:
  - Confidential access
  - Authorized electronic record operations
  - Record integrity
  - Auditing
- Principle of Least Privilege
  - Each user is authorized for the least amount of records
  - Each record is restricted to the smallest group of users
- Security violations exploit relationship vulnerabilities
  - Computer Network Infrastructure
  - Record authentication/authorization
  - User Lifecycles
  - Privilege implementation

Electronic Records Security – Threat Agents

- Internal Staff
  - Proximity to records
  - Malicious/Accidental
  - Statistically, the greatest security threat
- 3rd Party Partners
  - Access to specific organizational resources under specific conditions
  - Violates access resources and conditions
- Hackers
  - Malicious intent
  - Connected over Internet/Intranet
  - Can include external parties, internal employees, …

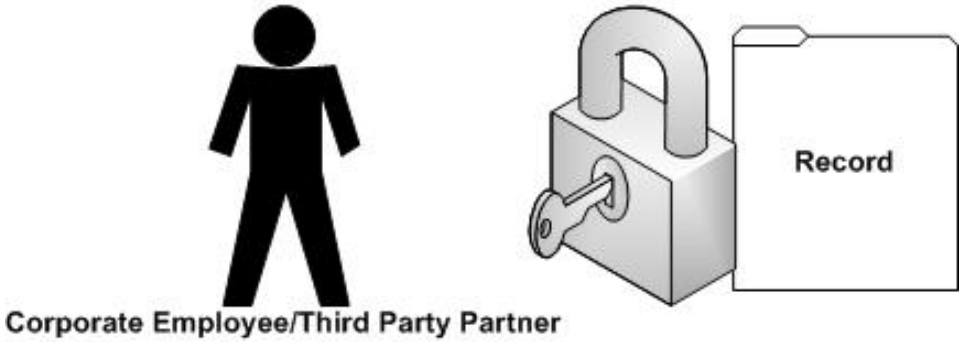
Electronic Records Security – Threat Types

- Passive Attacks
  - Unauthorized Record Disclosure
    - Disclosure of confidential information via email, IM
    - Improper protections/practices for laptops and desktops
  - Eavesdropping
    - Viewing records while they are transmitted, or stored on desktops/laptops, …

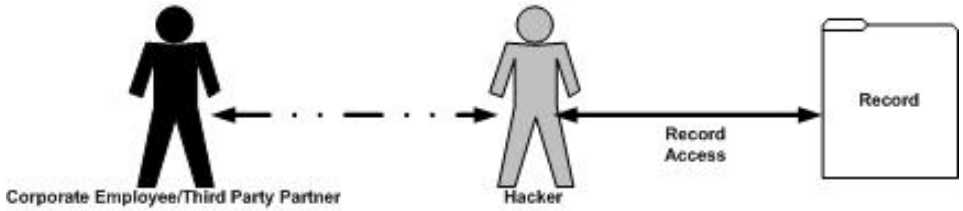


Record Security Violations - Types

- Active Attacks
  - Abuse of User Privileges
    - User manipulates record access controls to obtain records classified above their privilege level

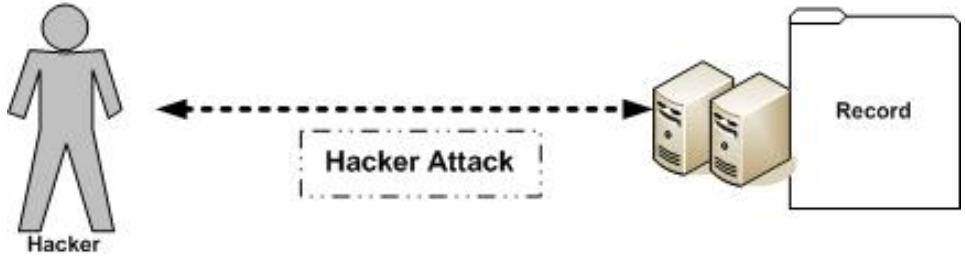


  - Credential Stealing
    - Obtaining records by ”cracking” valid user’s authentication credentials



Record Security Violations - Types

- Malware
  - Hackers gain record access and/or disrupt organizational computer infrastructure through distributing viruses, worms, trojans



- These and other threat types are used in combination to control an organization's computer infrastructure, and violate record privacy and security

Electronic Record Security

- Everyone is a target
  - Hacker attacks can range from random to focused
  - Small businesses are as likely to be targeted as large corporations
- AntiVirus and Firewall controls are not sufficient
  - Does not protect against disclosure violations
  - Stops “known” threats
  - Can be circumvented
- Application Access Controls
  - Can be circumvented
  - Lower level attacks can exploit server weaknesses

Effective record security requires an ongoing security management process

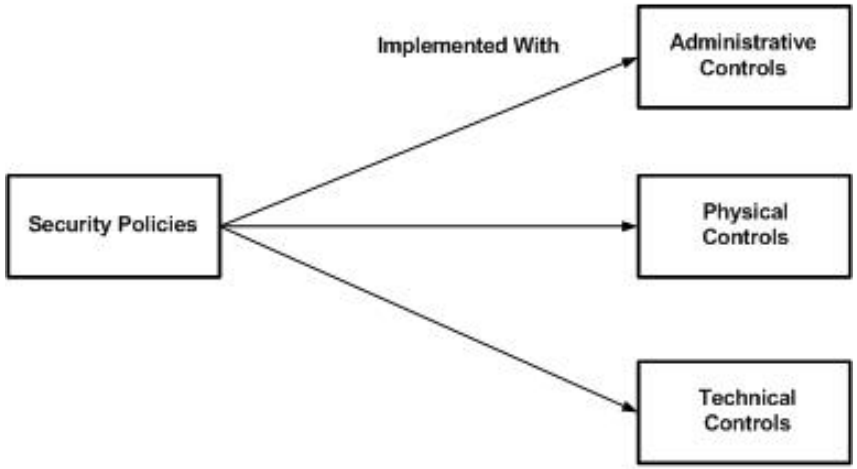
Security Management Principles

Establish and maintain confidence that Information Systems and Record Lifecycles are correct and productive

- Record Confidentiality
  - The required level of Information Systems secrecy is enforced at each stage of record lifecycle. Unauthorized record disclosure is prevented
- Record Integrity
  - Assurance of Information Systems record accuracy and reliability
- Record Availability
  - Adequate Information Systems capacity and performance to capture, store, manage, deliver, and preserve records

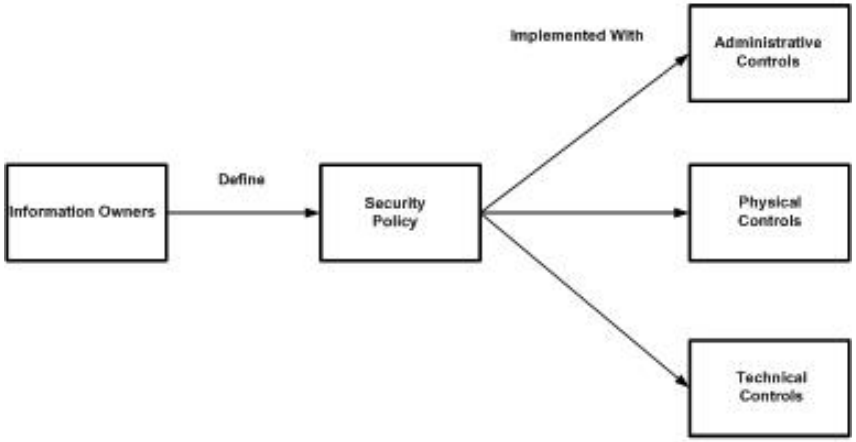
Security Management Concepts

- Security Policy – documents data protection for essential business records and operations. References laws, rules, and practices for regulating how an organization manages, protects, and distributes sensitive information.
- Administrative, Technical, and Physical Controls implement the Security Policy



Security Management Concepts

- Information Owners – responsible for determining how records and operations should be protected
- Information Owners include CxOs, IT personnel, business operations and Record Managers

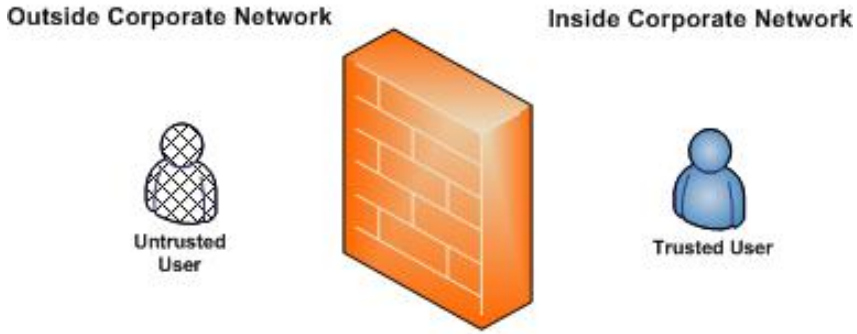


Security Management Concepts

- Administrative Controls
  - Policies
  - Procedures
  - Education
- Physical Controls
  - Facility Protections
  - Security Guards
  - Environmental Controls/Alarms
- Technical Controls
  - Access Controls (passwords, biometrics, …)
  - Encryption
  - Security Devices (firewalls, antivirus protection, …)

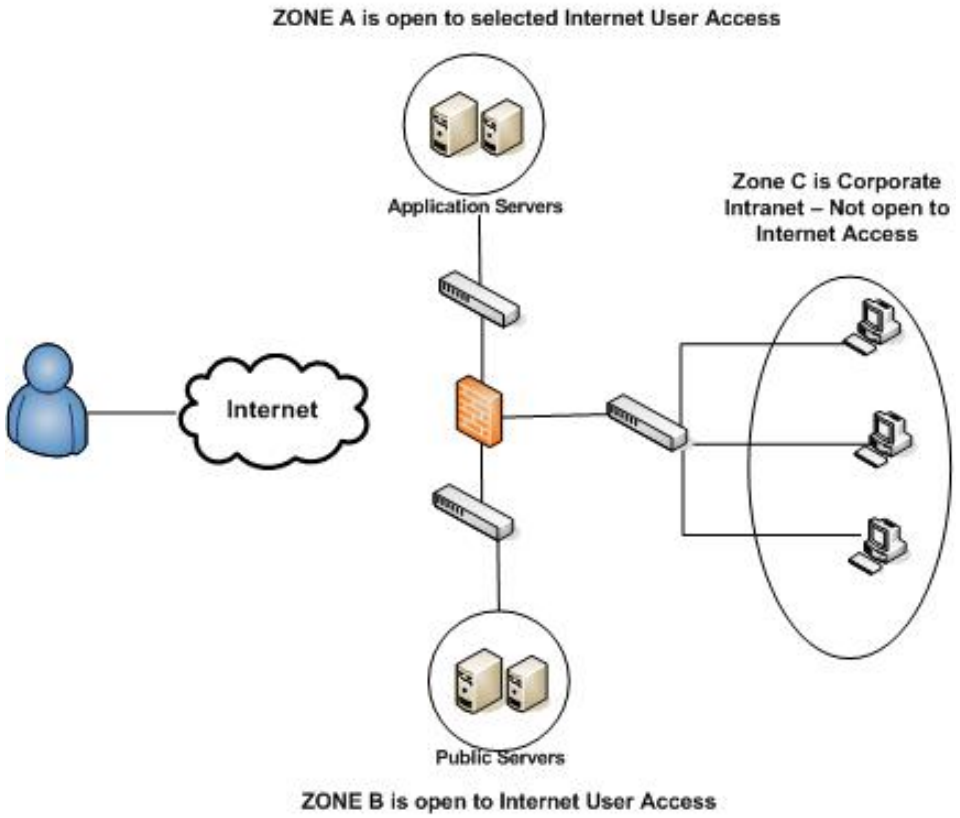
Security Management - Layers

- Security Management controls protect organizational resources through combining overlapping layers of security
- Perimeter
  - Trust users within the corporate network. Distrust users outside of the corporate network
  - Data transmission into the perimeter is restricted



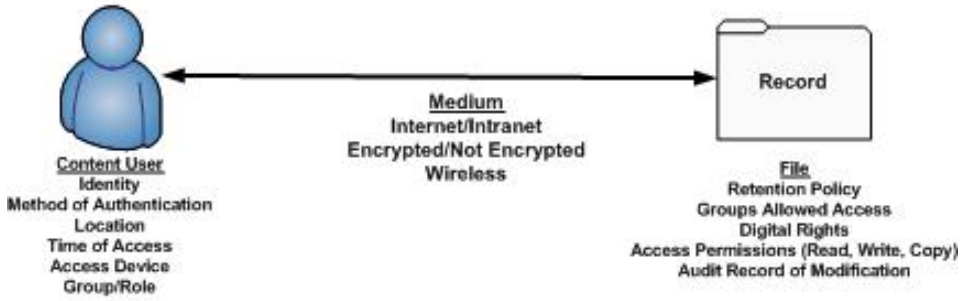
Security Management - Layers

- Zone Security
  - Corporate Network is subdivided into groups of trusted users
- Core Security
  - Access to Desktops, Servers, other devices is limited to specific users



Security Management – Layers

- Content Security
  - Creates context for record access, including:
    - User status
    - Transmission Medium
    - Record Lifecycle
    - Auditing of record access and operations
  - Defined criteria for authorized record access, including security protections
  - Driven by business policy, and technical concerns



Security Management - Process

- The Security Management process consists of:
  - Risk Assessment
    - Identify Information Systems security vulnerabilities
    - Security policy gaps
  - Implementation of Security Controls
    - Administrative, Physical, and Technical
  - Monitoring and Testing
    - Validate control implementation
  - Auditing and Improvement
    - Evaluate control effectiveness
    - Investigate security improvement opportunities

Security Management - Process

- Security Management Success Factors
  - Security policy reflects business objectives
    - Implementation approach consistent with organizational culture
  - Management must provide both consistent participation and support
    - Partnership between Information Owners and IT
  - Commitment towards identifying and managing risk
  - Education and training
    - Development Of Human firewalls
  - Auditing system to evaluate performance

Security Management – Risk Analysis

- Inventory of organization hardware, software applications and configurations
- Review Security Policy
  - Determine if policy reflects current business operations, compliance needs and technology
- Evaluate Security Policy against Controls
  - Employee job changes
  - Third party contractor termination
  - Client record requests
  - Record Lifecycle changes
  - Mobile workers
  - Wireless network connections
- Identify Gaps between documented policies and results

Security Management – Risk Analysis

- Rank risk by organizational impact
- Risk Handling
  - Accept Risk
  - Transfer Risk (insurance)
  - Reduce Risk (implement controls)
- Develop solutions
  - Information owners investigate risk elements
  - Define solution criteria and alternatives
  - Prototype and select solution strategy

Security Management – Implementation

- Layered Security model
  - Isolate security breaches
  - Provide multiple defenses against security threats
- Update Security policy
  - Incorporate new security model
  - Review with Information Owners
- Auditing
  - Controls to track security incidents
  - Document how to recognize security threats
  - Incident reporting procedures
- Education
  - User education and training is essential

Security Management

- Test and Monitor
  - Test control implementation
    - Validate vendor claims
  - Measure control performance
  - Investigate security incidents
- Audit and Measure
  - Schedule regular Information Owner meeting
    - Conduct vulnerability testing
  - Identify new record management issues
    - Changes to network infrastructure
    - Changes to business operations/culture
  - Identify security improvements

Security Management – Summary

- Sustained Record Security and Record Privacy is the result of:
  - Strong partnership between Information Owners and IT
  - Definition of authorized record access policies
  - Understanding of record access scenarios
  - Implementation and maintenance of relevant controls
  - Continuous follow-up

Security Management – Resources

- Description of common Information Technology terms and acronyms
  - http://www.webopedia.com
- The SANS Security Policy Project
  - http://www.sans.org/resources/policies
- Schneier on Security
  - http://www.schneier.com/blog/
- Security Fix
  - http://blog.washingtonpost.com/securityfix/
- Stay Safe Online
  - http://www.staysafeonline.info
- The Practical Guide to HIPAA Privacy and Security Compliance - Kevin Beaver and Rebecca Herold

Thompson Network Consulting

- Thompson Network Consulting provides organizations with solutions for protecting their confidential electronic records from unauthorized access and manipulation.

Please contact Thompson Network Consulting at:

DarylThompson@thompsnet.com

708.214.7544

www.thompsnet.com