

Security in Records Management



Presented by: Kevin Blue

BSBAMIS, CCNP, CCDP, CCNA, CCDA, MCSE,
Security+, NNCDS, NNCSS, NNCAS, MCP +I, A+

Introduction

- **Kevin Blue**
- **Certifications**
 - BSBAMIS, A+, MCP+I, MCSE, CNA, CCNP, CCDP, CCNA, CCDA, NNCSS, NNCAS, NNCDS, Security+.
- **Been in the IT industry about 15 years and security about 8 years.**

Agenda

- **What is Security**
- **Security Program**
- **Securing Data**
- **Common Practices and Standards**
- **Conclusion**
- **Questions**

What is Security?

- Definition of Security
 - The security of a system is the extent of protection against some unwanted occurrence such as the invasion of privacy, theft, and the corruption of information or physical damage.
- Comes in many forms
 - Physical Security
 - Information Security
 - Network Security
 - Security Practices

Physical Security

- Typically these are:
 - Fences
 - Lighting
 - Fire Detection and Suppression
 - Safes
 - Locked Doors and Windows
 - Alarm and Surveillance Systems

Physical Security (cont.)

- Fences
 - Work as a preventative and deterrent mechanism.
 - Most serious is 8FT tall with strands of barded wire.
 - Typically the fence is 6 to 7 feet.

Physical Security (cont.)

- Lighting
 - Provide safety for critical sections of the building
 - Helps to monitor and maintain a safe and controlled work environment for staff and data.

Physical Security (cont.)

- Fire Detection and Suppression
 - Come in many forms
 - Sprinkler system
 - Smoke activated
 - Optical
 - Heat Activated
 - Flame Activated
 - Important to have some sort of detection and suppression system near document storage.

Physical Security (cont.)

- Safes
 - Storage of backup tapes and important documents
 - Two hour UL Classified proven fire protection, and water- resistant safe is preferred.
 - UL and MET marks both indicate that the product has met the minimum requirements of the applicable safety standards.

Physical Security (cont.)

- Locks and Facility Access
 - All critical information should stay behind locked doors.
 - Most document rooms should have security codes, master locks, or card readers to allow access.
 - Intruders typically perform piggybacking to enter facilities.

Physical Security (cont.)

- Alarms and Surveillance
 - All document rooms should have surveillance of some kind.
 - Guard
 - Camera + recorder
 - All document rooms should have an alarm in case of intrusion of person without presenting the correct credentials.

Questions



Any questions on Physical Security?

Security Program

- Based on management requirement
- Defines all relevant policies, procedures, standards, software and personnel, to protect the company. Example is a security policy or an acceptable use policy.
- Defines information life-cycle: creation, maintenance, storage (or retention), and recorded disposal.

Securing Data

- Many ways to secure data:
 - Encryption and Cryptography
 - Virus protection
 - Password protection
 - Protection against attacks
 - Storage Vaults
 - Backups

Securing Data (cont.)

- **Encrypting Data and Cryptography**
 - Is taking the data that was created by a user/users and hiding it within other data.
 - Transforms plain text or documents to unreadable documents.
 - Remember the old crypto decoder you may have gotten from ovaltine:
 - 1=A 2=P 3=L 4=E
 - 12234 = Decoded would equal APPLE

Securing Data (cont.)

- Virus Protection
 - Definition of a virus
 - Small application or string of code that infects applications.
 - Come in many forms
 - Viruses
 - Worms
 - Trojan horse
 - Logic Bombs

Securing Data (cont.)

- Some preventative measures
 - Scan all documents with a virus protection software
 - McAfee Anti-virus
 - Norton Anti-virus
 - Do not open emails or documents unless you know who they are from or what the document is.

Securing Data (cont.)

- Password Protection
 - Critical data should **always** be password protected.
 - Passwords should be at least 8 characters in length
 - Passwords should always be alphanumeric and special characters. (if applications will accept special characters)
 - Example
 - **K3v1NbLu3**

Securing Data (cont.)

- Protection Against Attacks
- Attacks come in many different forms
 - Viruses
 - Man in the middle
 - Shoulder surfing
 - Social Engineering

Securing Data (cont.)

- Protection Against Attacks (cont.)
 - Always require user name and password authentication to access documents or files.
 - Always have the most up to date virus definitions for protection against viruses.
 - Never open files, documents, or emails unless you know what they are and where they came from.

Securing Data (cont.)

- Some other ways to protect against attacks
 - Firewalls
 - VLANs (Virtual local area networks)
 - IP Management
 - IDS (Intrusion Detection Systems)
 - System Change Management
 - Routing Authentication

Securing Data (cont.)

- Storage

- All data should be stored on non-volatile media.

- CD

- Laser Fichie

- Optical

- Tape


- All data should be stored in area that has physical security along with data security.

- All backups should be kept off site.

Securing Data (cont.)

- Backups
 - Depending on how critical the data backups should be run either daily or weekly
 - All data backups should be kept off site.
 - These are the following types of backup:
 - Hardware backup
 - Software backup

Common Practices & Standards

- Data Integrity
 - Data Confidentiality
 - Data Availability
 - Standards
- 

Common Practices & Standards

- **Data Integrity**
 - The assurance of accuracy and reliability of information
 - Unauthorized modification of data is prevented
 - For example
 - Data corruption can occur by users filling out information incorrectly.

Common Practices & Standards

- Data Confidentiality
 - “Need-to-know” basis
 - Ensure that the necessary security is in place to prevent unauthorized users from accessing data.
 - Can be provided by just password protects of documents to encrypting documents that require key codes to open.

Common Practices & Standards

- **Data Availability**
 - Reliable and timely access to data to authorized individuals.
 - Avoiding single points of failure.
 - Always keep backups of critical data.
 - Keep critical data in a HVAC-controlled environment.

Common Practices & Standards

- Standards (Regulations)
 - HIPPA
 - Gramm-Leach-Bliley Act
 - Electronic Data Security Act of 1997
 - CIPA – Children’s Internet Protection Act
 - FERPA – Family Educational Rights and Privacy Act

Common Practices & Standards

- **HIPPA**
 - Health Insurance Portability and Accountability Act
 - This the standard for the medical community and how they store, transmit, use personal data.

Common Practices & Standards

- Gramm-Leach-Bliley Act
 - Applies to all banks
 - They have to develop a privacy notice
 - The notice states that the customer has the option to disclose personnel information.
 - Also all banks most have a security programs in place.

Common Practices & Standards

- **Electronic Data Security Act of 1997**
 - If a company chooses to use some sort of encryption.
 - Encryption Standards are in place that assure individuals can transmit and receive data securely.

Conclusion

- Always practice due care and due diligence when working with critical information or data.
 - Due Diligence – the understanding of the current risk the company faces.
 - Due care – taking responsibility for the activities that take place in a company and protecting that company from possible risk.

Questions

Any questions on what we have covered tonight