

# Security of E-Records or Ignorance is Risk

Earl C. Rich, CRM

# How Is Security Defined?

- Electronic Security is defined as:
  - Protection resulting from all measures designed to deny to unauthorized persons information of value.
  - Precautions taken to guard against crime, attack, sabotage, espionage, etc...

# What Needs to Be Secured?

## ❖ Assets of an organization

Employees

Equipment

Records

Business information

Information systems

Raw data

Facilities

# What Are The Challenges?

- Hackers, crackers, script-kiddies (not the geeky teenager)
- Uneducated staff
- Litigation response
- Disgruntled employees
- E-mail
- Portable Devices
- Physical location
- Virus attacks
- Environmental threats to systems

# Hackers...

## External

- Does not have authorized access to computer system
- Is mistakenly stereotyped as geeky teenager
- Is far more advanced in today's world
- Utilizes sophisticated software to identify system's security weaknesses
- Is capable of attacking thousands of computers at a time

## External/Outsider Threat



# Uneducated Staff

Reacting to  
Social Engineering



- ❖ Fall prey to social engineering
- ❖ Open any and all emails – phishing
- ❖ Exchange files via portable devices
- ❖ Leave passwords on sticky notes around the office
- ❖ Use “Mom” for a password... use “password” for a password

# Unhappy Worker Bees

Normally trusted staff can be affected by issues that make them take harmful actions.

- ❖ Stress due to personal situations
- ❖ Frustration with management/policy
- ❖ Overworked and unappreciated
- ❖ Office politics gone awry
- ❖ Underpaid

# Virus Attacks

- Virus – malicious software written intentionally to enter a computer without the user's permission or knowledge
- Types of common viruses:
  - Resident, Direct Action, Overwrite, Boot, Macro, Directory, Polymorphic, File Infectors, Companion, FAT

# More Viruses & Attacks

- Worm – a segment of self-replicating code
- Trojan Horse – backdoor opening into a PC
- Logic Bomb – remains hidden until it is triggered when certain conditions are met
- Vulnerability Scanner – a tool to quickly check for networked computer weaknesses
- Spoofing – involves a program, system, or website successfully masquerading as another by falsifying data
- Packet Sniffer – an application that captures data
- Key Logger (hardware & software) – is a tool designed to record every keystroke on an affected machine for later retrieval

# Portable Devices & Wireless Access



PDA



Laptop



Smart phone



Memory Card



USB drive

Removable Media:

Need we say more!!!!

# Email – Incoming and Outgoing

- Easy mass distribution of corrupted files
- Simple way to steal confidential and proprietary information
- Opening attachments with viruses/Trojan horses
- Re-directional / Referential pixels imbedded into e-mails as a means of verifying e-mail addresses



# Physical Location

- It's 2 AM do you know where your electronic records are?

On the cloud?

In India?

In the server in the back room that is 2 feet above sea level?

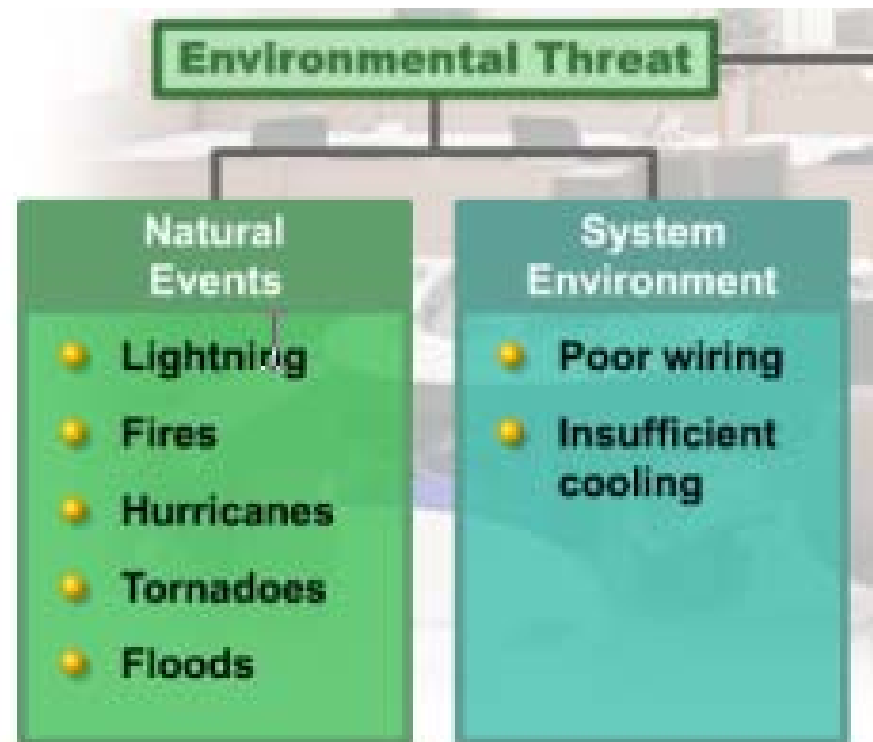
On a disk in Bob's desk?

On a laptop that was stolen while Bob was at a conference?

# Environmental Threats

Welcome to central Florida... SLOSH Central!!!

Have you talked to IT about disaster recovery of records?



# Headlines

- VA will pay \$20 million to settle lawsuit over stolen laptop's data

Class action law suit – names, dates of birth and Social Security numbers of about 26.5 million active duty troops and veterans

# Data Breaches On The Rise

- The 2008 Data Breach Investigations Report released by the Verizon Business Risk Team compiled data from more than 500 forensics cases the team handled from 2004 to 2007, comprising more than 230 million breached records. Although some of the breaches were attributed to malicious activity, human error contributed to 62 percent of the cases.

# Assess the Risks

- Risk analysis is the key to security
- Understand your organization's mission
- Know where the records & data & information live, and their formats
- Have content owners been trained?
- Who has what responsibility for the security of the records?

# Your Mission

- Determine the following and develop a plan of action:
- What is being created?
- How is it being treated?
- Where are your vital records and who has access to them?
- Are your organization's data secure?

# Data Mapping

- Know what records exist within your organization
- What medium is being used to store them?
- What production applications create/maintain them?
- Where they live physically?
- What formats are being used?
- Who owns the content?
- Who has access to what data/records?
- How are the records secured?

# DOD 5015.2 Compliant Systems

- Kid tested, NARA approved!
- Controls access to documents
- Tracks internal access attempts to information
- Provides document revision control
- Robust auditing capabilities
- Encrypts source data to eliminate back-end database access

# Technology Is Not The Silver Bullet

- Technology cannot prevent an employee from faxing off something inappropriate.
- No form of technology can keep employees from either inadvertently or maliciously destroying physical records
- Technology can be used to encrypt information and records.
- People need to be trained, this is a people problem, not a technology problem.

# People Training

- Does Management understand the issues surrounding e-records security?
- Have the people who work with records been trained?
- Does IT understand the risks associated with lax security?

# Solutions

- Create an organizational wide policy on the security of electronic records
- Build a strong partnership with your IT staff
- Learn about end of life data security

# Responsibility Mapping

- Who really has the responsibility for the security of the data, records, and information within your organization?
- Is it a shared responsibility?
- Do the people understand they also have a responsibility for the security of e-records?
- Does IT understand their role in the security of e-records?

# Data Destruction

- Hard drive erasure
- CD/Optical media destruction – beyond forensic recovery
- Use of NAID certified destruction technology

National Association for Information Destruction  
<http://www.naidonline.org/>

# Conclusion

- You cannot sit back and do nothing to secure electronic records
  - Requires proactive steps
  - Risk analysis
  - Data mapping
  - Responsibility mapping
  - Training for creators, recipients, and custodians of the records

# Questions?

Earl C. Rich, CRM

SWFWMD – Document Services Manager

Office: 352-796-7211 ext. 4052

Cell: 352-279-2472