NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Welcome!

Presenter

Richard Kissel, CISSP, CISM

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

Goal

- **Promote:**
  - Awareness of the importance of and the need for IT security
  - Understanding of IT security vulnerabilities and corrective measures

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

You Will Learn

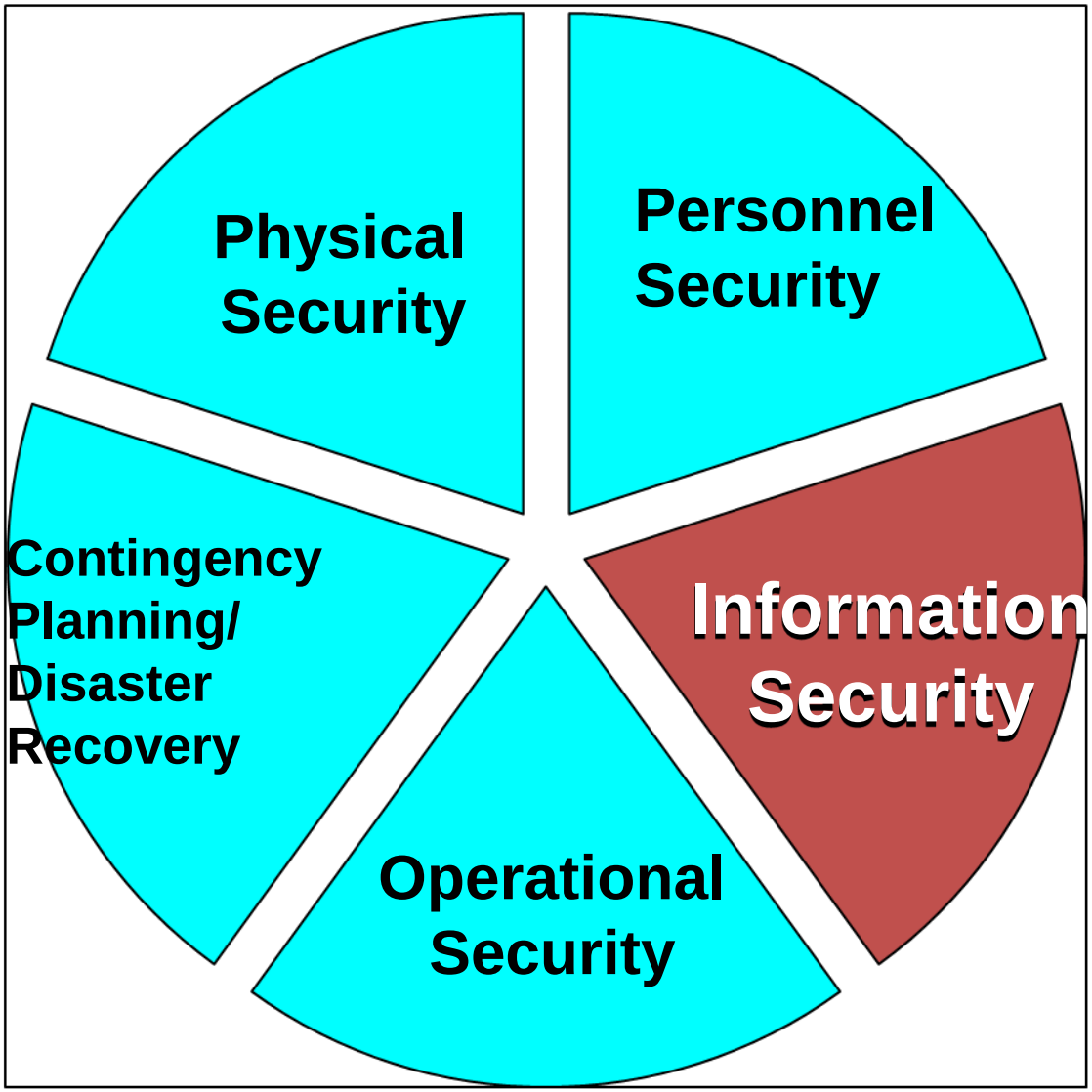
- How your data is vulnerable
- What you can lose through an information security incident
- Practical steps to protect your business
- How to evaluate tools and techniques based on your needs

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

General information

Comprehensive Security



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

What is Information Security?

- Tools and techniques that protect an organization's:

What is Information Security?

- Tools and techniques that protect an organization's:

Invoices

Email

PAYROLL

Employee Databases

Client Information

Electronic Commerce

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Aspects of Information Security

- Confidentiality
- Integrity
- Availability

What Should You Do About It?

- **Your organization's information:**
  - Is as vital as equipment, staff, and buildings
  - Requires the same protection
  - Has become more vulnerable with the use of Computers, Networks and Wireless Connectivity

- **Take control of your information security with:**
  - Analysis (Security Policies & Risk Assessments)
  - People
  - Procedures & Best Practices
  - Technology

How much time and money should you invest?

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Making the Right Investment

Cost Benefit/Avoidance Analysis

Potential Loss

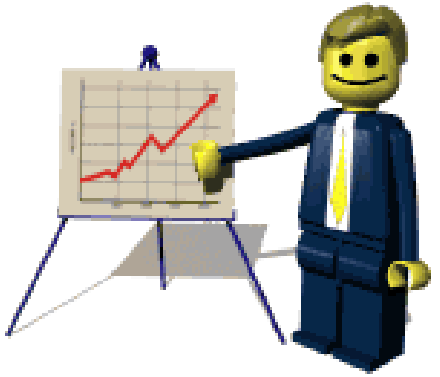
versus

Protection Costs

Making the Right Investment

- **Providing good Information Security is evidence of:**
  - Sound management
  - Sound customer service
  - Sound legal protection
  - Sound economics

Let's talk about these.



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Sound Management

- Protecting information and systems makes good business sense. It reduces your risk and allows you to do more business in a safer environment.
- And it gives you a competitive advantage!

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Sound Customer Service

- Customers want their private information protected and respected
- Customers need to have confidence in you to continue doing business with you
- Customers expectations for their data safety need to be accounted for by you

(Just as you have your expectations of how those that you trade with will protect YOUR information)

Sound Legal Protection

- Privacy/Information Security:
- Taking steps to ensure that your customer/employee data does not fall into the wrong hands provides protection against liability

Sound Economics

- **Cost avoidance analysis for security: What are you risking by not protecting your information and systems?**
  - Decreased productivity
  - Increased labor costs
  - Legal liability
  - Loss of confidence
  - Adverse reputation
  - Your Business!

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Sound Economics

- Consider the information you depend on to operate your business or organization.
- Do you know what you need to run your business?
- Do you know which types of information are the most important?

Exercise 1 – Identifying and Prioritizing Your Organization's Information Types

1. Think about the information used in your business.
2. Enter into the table below the five highest priority types of information used in your business.

Priority	Type of Info.	Who has access?	On which system?
1			
2			
3			
4			
5			

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Exercise 2: Estimated costs from bad things happening to your sensitive business data

	Data type one released	Data type one modified	Data type one missing	Data type two released	Data type two modified	Data type two missing
Cost of revelation						
Cost to verify information						
Cost of lost availability						
Cost of lost work						
Legal costs						
Loss of confidence costs						
Cost to repair problem						
Fines & Penalties						
Other costs – notification, etc						

Exercise 3 – Identifying the protection needs of your important business Information Types

What kind of protection does your important information need?

Priority	Type of Info.	Who has access?	On which system?	C	I	A
1						
2						
3						
4						
5						

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

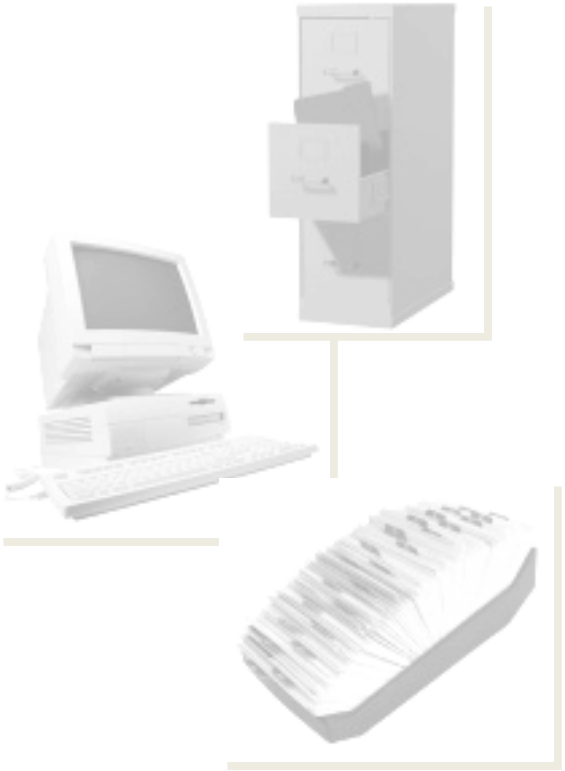
Defining Your Needs Analysis

A Security Policy defines:

- What information you care about
- How you need to protect it
- 1st – Inventory and Prioritize your information
- 2nd - Confidentiality, Integrity, Availability

Consider:

- What happens if this particular information falls into someone else's hands?
- How much would it cost me to be without this information?
- How much would it cost me to re-create this information?
- What happens if I can't trust the accuracy of completeness of my information?
- Other factors: reputation, integrity



Example Policy Statements

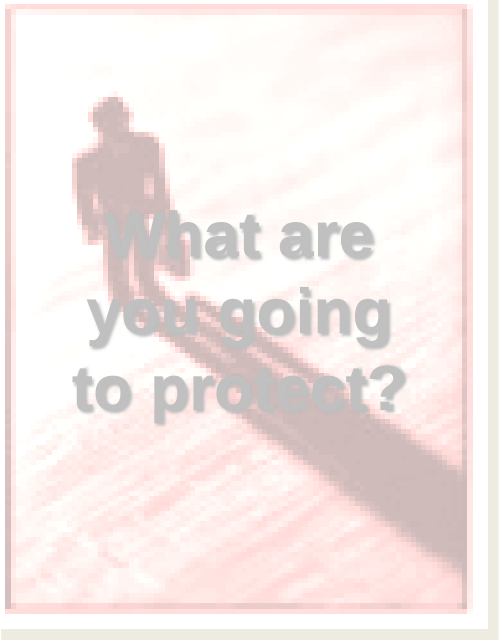
- “All employee personnel data will be protected from viewing or changing by unauthorized persons.”
- “All computer users will have their own account and password.”

(For samples, go to

csrc.nist.gov/groups/SMA/fasp/areas.html

and select “Policy and Procedures” in the left-hand column)

Analysis: Defining Your Needs



Security Policies

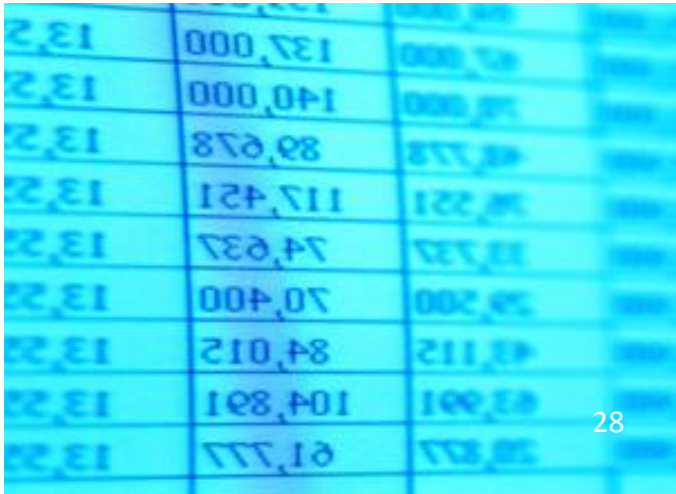
Risk Assessment

Security Risk Assessment

- **Identify:**
  - Threats
  - Vulnerabilities
  - Risks

Most Threats Have a Human at Their Origin

- **Accessing/destroying company information**
  - Stealing your computer
  - Defacing your website
  - Putting malicious programs onto your system
  - Hacking into your system



Threats <discuss each page>

- Spoofing
- Snooping
- Social engineering
- Abuse of system privileges
- Ransomware
- Insider threats – malicious actions, unintentional, non-business use

Other Threats

- Identity Theft – steal & misuse your identity $$$
- Pfishing - Email Tricking YOU into giving personal information (think Identity Theft).
- Spear Pfishing - Email with specific company details to deceive you into responding.
- SPAM - Unsolicited and Unwanted Email.
- Compromised web pages – with invisible code which will attempt to download spyware to your computer.

Security Risk Assessment

- **Identify:**
  - Threats
  - Vulnerabilities
  - Risks

Common Vulnerabilities

- **Where are you vulnerable to the threats?**
  - Computer hardware and software

  (outdated, patched, secure location?, legal SW?)
  - Poor/missing policies/procedures
  - Poor oversight/enforcement

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Security Risk Assessment

- **Identify:**
  - Threats
  - Vulnerabilities
  - Risks

- **A Threat, acting on a**
- **Vulnerability-produces**
- **A RISK (and probable**
- **Consequences)**

- **How much risk can I live with?**
  - No risk can be completely eliminated.
  - If the consequence is high (and the probability is high), your tolerance is low.
  - If the consequence is minor, more risk may be acceptable.
  - If the risk is still too high after all mitigation efforts have been done, use commercial cyber insurance to “share” the risk/exposure.

Outcome of Risk Assesment

- **Knowing where you need protection:**
  - Computers
  - Network
  - Software
  - Operations
  - Business processes

- **A rational sense of what to do, and the justification to do it!**

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Best Practices, Procedures and People

10/4/2011

Best Practices: Procedures

- **Start with:**
  - Security Policy

  (Remember – Procedures Implement Policies)

Best Practices: Procedures

- **Determine who will need procedures.**
  - All employees who use computers in their work
  - Help Desk/system administrators
  - Managers/executives using specialized software
  - System maintenance
  - IT Out-Sourcing
  - Software Applications
- **Create, then follow your procedures!**

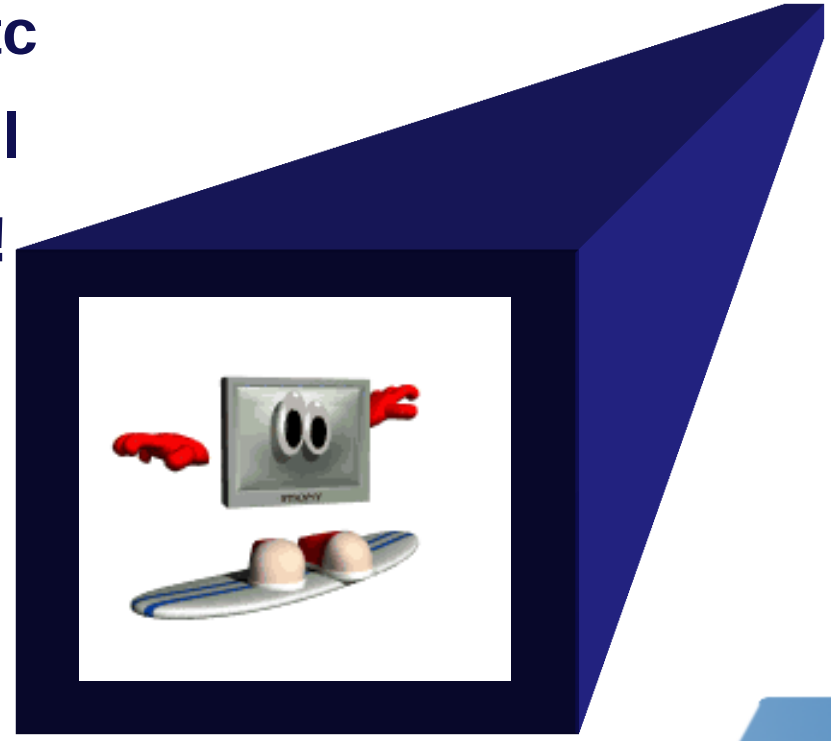
Best Practices: Procedures

- **Enforcing safe**
  - Internet practices
  - E-mail practices
  - Desktop practices
  - Personnel practices

  (will address each of these, in turn)

Do not:

- Download files from unknown sources
- Respond to popup windows requesting you to download drivers, etc
- Allow any web site to install software on your computer!

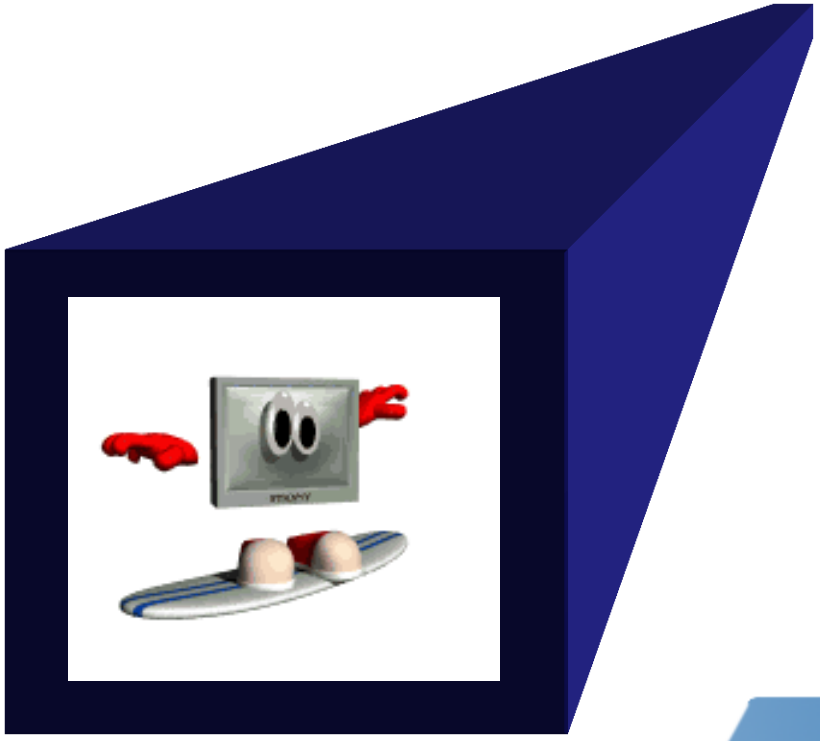


Do:

- Protect passwords, credit card numbers, and private information in web browsers

Safe E-Mail Practices

- Be careful opening attachments
- Do not reply to unsolicited emails
- Do not click on links in an email



Safe Desktop Practices

- **Do:**
  - Use passwords (Don't share yours!)
  - Use separate computer accounts for each user
  - Use screen locking
  - Log on and off
  - Power down your system at the end of the day
  - Seriously consider encrypting sensitive data on your system!

Safe Personnel Practices

- **Do:**
  - Confirm identities of people and organizations
  - Accompany all vendors, repair persons
  - Give only enough information to answer questions
  - Conduct background checks. (yours?)
  - Control employee entrance and exit.
  - Control employee terminations/departures.

Implement Backup Procedures

- **Goal is ability to restore systems and data to what existed before any:**
  - Virus/malicious code problems
  - Theft or destruction
  - Data integrity problems
  - Equipment failures

<Done weekly, store copy off-site monthly>

TEST YOUR BACKUPS! DO A TEST RESTORE AT LEAST ONCE A MONTH!

Implement Physical Security

- **Facilities**
  - Locks
  - Anonymity
  - Alarms
  - Guards
  - Floor-to-ceiling walls

Implement Procedural Security

- Document keys holders.
- Protect company directories and contact information. <why help social engineers?>
- Control passwords.

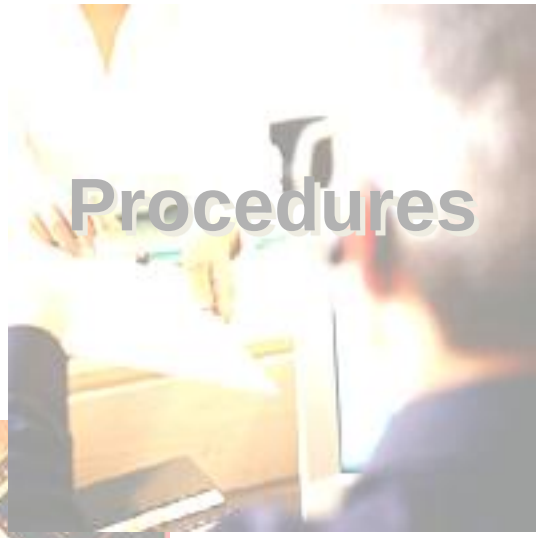
Password Control

- At least 12 characters long
- No names, birth dates or personal info
- At least one:
  - Upper case
  - Lower case
  - Numeric
  - Special character
- Change every 3 to 6 months.

Virus-Malicious Code Control

- **Viruses-Spyware-Trojans-Malware**
- **Company-wide detection tools**
  - Company-wide process
  - Assign responsibility in writing
  - Up-to-date search definitions
  - Include employee's home systems (many people take work home & telework)

Information Security Solutions



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Management: A Vital Role in IS

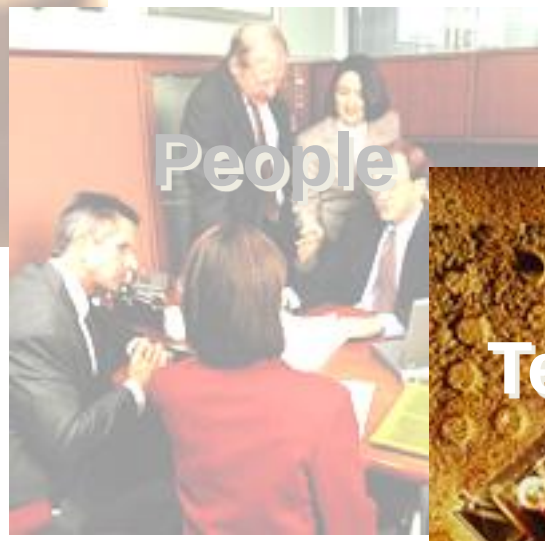
- **Includes:**
  - Defining roles and responsibilities
  - Committing necessary resources
  - Enforcing policies and procedures (there are penalties for not obeying policies!)
  - Being involved
  - (Remember: Managers are responsible for Information Security for their data!!)

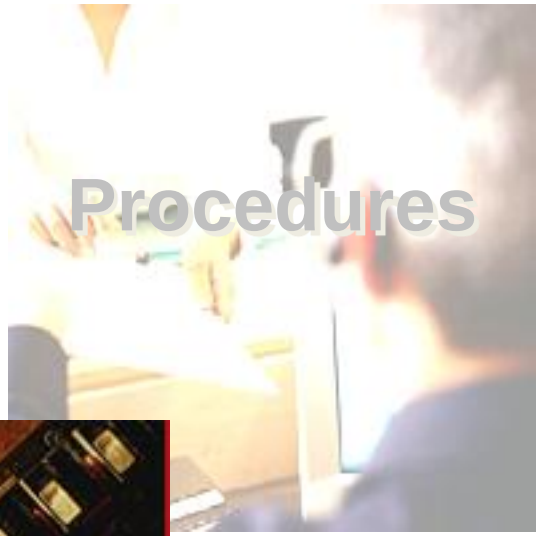
Staff Awareness and Training

- **Begins with the first day at work:**
  - Security policies and procedures
  - Security threats and cautions
  - Basic security “do’s and don’ts”
- **Continues with reminders and tools:**
  - Pamphlets, posters, newsletters, videos
  - Rewards for good security
  - Periodic re-training – because people forget

This is one of the most significant information security weakness in most organizations!

Best Practices: Technology





NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Useful Technologies

- Data content filters (inbound/outbound)
- Email filters
- Web filters (blacklists/whitelists)
- Web content monitor/integrity checker
- Integrated security packages
- Encryption software – whole disk (i.e. Bitlocker comes with Windows Vista, freeware Truecrypt runs on Windows 7/Vista/XP, Mac OSX, Linux – www.truecrypt.org – PGP, www.pgp.com - Pretty Good Privacy – not free)
- (Google “free encryption software” for ideas)

Wireless Security Precautions

- Treat wireless network as an “Internet”
- Use hardware address (MAC) access control
- Change the default identifiers (SSIDs) & don’t broadcast them
- Don’t Use WEP (Wired Equivalent Privacy)
- WPA2 (WiFi Protected Access 2) is the minimum encryption to use for your wireless!!
- Change default encryption keys; Change often
- Change the Wireless Access Point (WAP) Administrator password!

Basic Security Tips (Review)

- Use anti-virus software
- Update operating system and applications
- Install a firewall <multiple, where needed>
- Control access to important company data
- Teach all users “Safe Computing/Internet Skills”
- Ensure that backup copies of important data are made regularly – and stored offsite (NOTE: ENSURE THAT YOU TEST YOUR ABILILITY TO RESTORE FILES FROM YOUR BACKUPS!)

Basic Security Tips (Review)

- When systems are replaced – destroy all information on the old system's hard disks.
- For old floppy disks, tapes, other removable media – destroy information when the media is discarded.
- Keep your operating system and applications updated/patched.

NIST SP 800-88 Guidelines for Media Sanitization

When You Need Help…

Get professional help when you need it.

- 1. Review potential vendor past performance.
- 2. Get list of current customers – call them! (satisfied?, would they hire them again?)
- 3. How long has the company been in business?
- 4. Find out who, specifically, will be assigned to you & what their qualifications are.

When You Need Help – Cybercrime

If you are or think you are the victim of cybercrime, first report it to your local cybercrime unit. (local police, county police/sheriff, state police)

You can contact the local FBI office. (and/or your State or Local Fusion Center)

You can file a complaint with the "Internet Crime Complaint Center" at www.ic3.gov

Other Security Resources

- www.staysafeonline.org National Cyber Security Alliance For small business, home users.
- http://www.ftc.gov/bcp/edu/microsites/idtheft/ Federal Trade Commission – Identity Theft Information

Presenter

Richard Kissel, CISSP, CISM

Computer Security Division

Information Technology Laboratory MS8930

National Institute of Standards and Technology

Gaithersburg, MD 20899-8930

301-975-5017

richard.kissel@nist.gov

http://csrc.nist.gov/groups/SMA/sbc/index.html

Thank you for filling out the Feedback Form (2 sides) – your suggestions help make this a better presentation!

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION