National Institute of Standards and Technology

# Small Business Information Security Workshop

Computer Security Division, Information Technology Laboratory

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

## Presenter

# *Richard Kissel*, CISSP, CISM

**Computer Security Division**

**Information Technology Laboratory**

**National Institute of Standards and Technology**

# Small Business Outreach: Partnership





**The support given by SBA, NIST and FBI to this activity does not constitute an express or implied endorsement of any cosponsor's or participant's opinions, products or services. All SBA, NIST and FBI programs are extended to the public on a nondiscriminatory basis.**

# The NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

# How Important Are Small Businesses ?

- **26.8 million small businesses**
- **Represent 99.7% of all U.S. employer firms**
- **78.5% of all businesses did not have employees**
- **Most of small business(89.9%) have fewer than 20 employees**

*Source: “2011 Small Business Profiles for the States and Territories”, the U.S. Small Business Administration, Office of Advocacy

# Goal

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

# Comprehensive Security

## Agenda – *You Will Learn*

- **What is Information Security?**
  - How your data is vulnerable
- **Why do we need Information security?**
  - What you can lose through an information security incident
- **Where can we start?**
  - Practical steps to protect your business
- **How-tos**
  - Tools and techniques

# What is Information Security?

# What is Information Security?

**The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability**

*Source: “Glossary of Key Information Security Terms”, NIST IR 7298

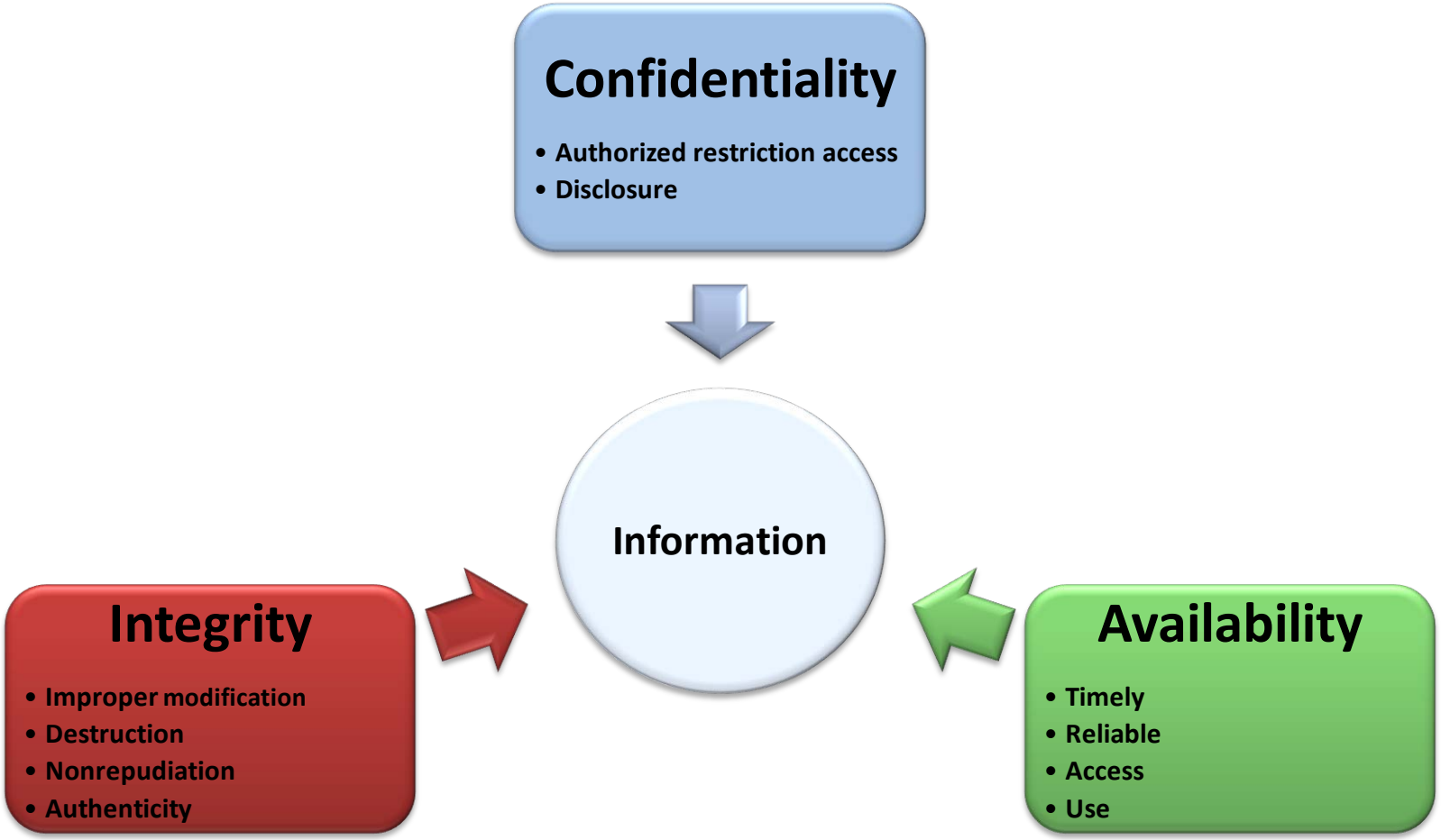
# What is Information and Information System?

- **Information**
  - Email
  - Invoices
  - Payroll
  - Employee Data
  - Client Data
  - Etc.

- **Information System**

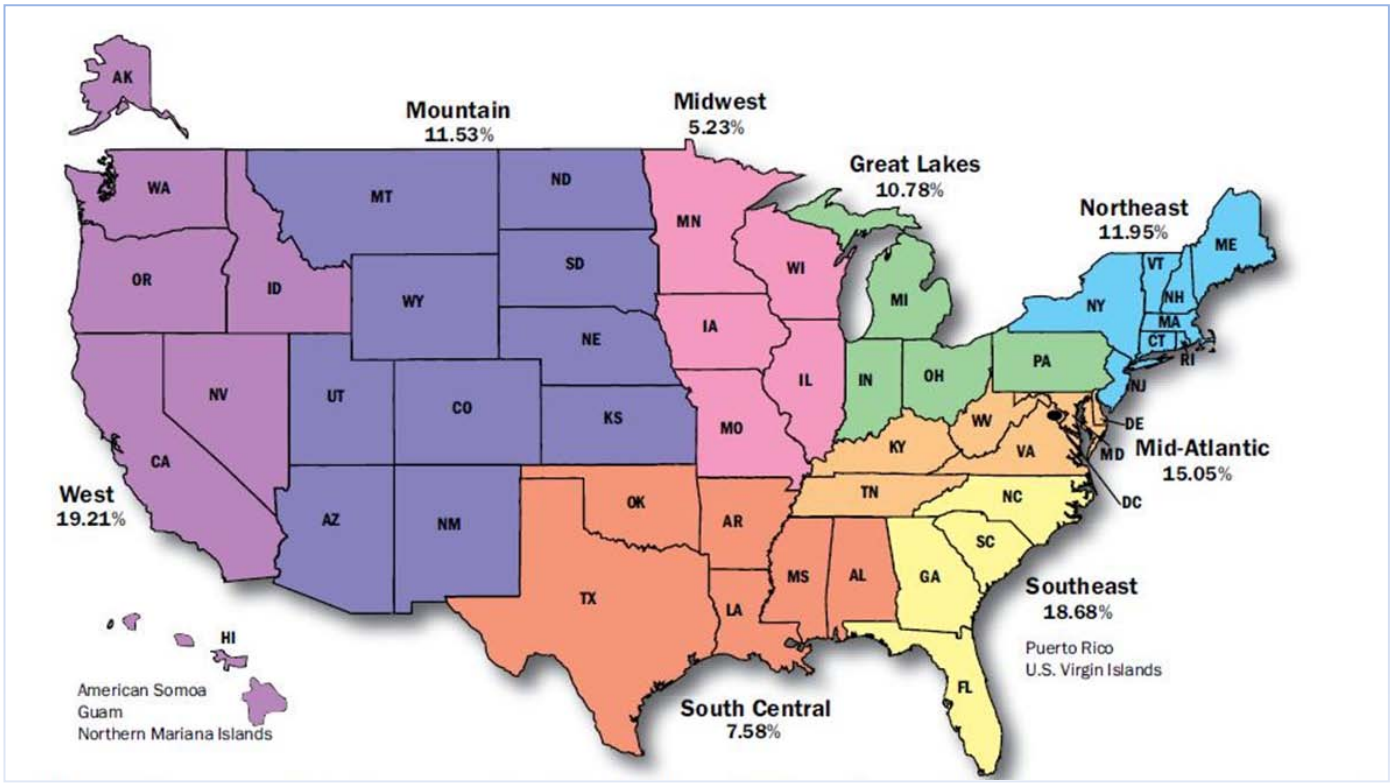
  : any integrated set of information technology and people's activities for collecting , storing, processing and delivering information

# Aspects of Information Security



# Why Do We Need Information Security?

- **Threats Landscape**
  - Internet Crime Complaint Center (www.ic3.gov)
    - 303,809 complaints in 2010




*Source: "2010 Internet Crime Report", IC3

# Top 10 Internet Crime Types with Dollar Loss

| Top 10 Internet Crime Types | | |
|---|---|---|
| 1 | Non-delivery Payment/Merchandise | 21.1% |
| 2 | Identity Theft | 16.6% |
| 3 | Auction Fraud | 10.1% |
| 4 | Credit Card Fraud | 9.3% |
| 5 | Miscellaneous | 7.7% |
| 6 | Computer Crimes | 6.1% |
| 7 | Advance Fee Fraud | 4.1% |
| 8 | Spam | 4.0% |
| 9 | Overpayment Fraud | 3.6% |
| 10 | FBI-related Scams | 3.4% |

- **Total dollar loss**
  - $559.7 million(in 2009)

*Source: “2010 Internet Crime Report”, IC3

# Who Are the Bad Guys?

- Experimenter and Vandals
- Hactivists
- Cybercriminals
- Information Warriors

# Their Common Target?

- **Your**
  - Information
  - Information System
  - Network

## What are they after?

- Access to your and your client information
- Access to your money
- Your PII
- To connect or include you on a botnet
- To connect or use your information for political reasons

# Common Security Attacks Today

- Theft of data and resources
- Denial-of-Service (DoS) attacks
- Malicious codes and viruses
- Insider threats

## Theft of data and resources

- Stealing your computer files (printing, copying, etc.)
- Accessing your computer accounts
- Stealing your laptops and computers
- Intercepting your emails or internet transactions

## Denial-of-Service attacks

- **Attacking your computer or website**
  - Locks up equipment
  - Crashes your systems
- **Result**
  - Stops/slows work/workflow
  - Prevents email communications
  - Shuts down eCommerce

## Malicious codes and viruses

- Send itself over Internet
- Find and send your files over Internet
- Find and delete your critical data
- Lock up your computer or system
- Hide in program or documents
- Make copies of itself
- Install on your system and record your keystrokes to send to a central collection point – out there

# Insider threats

- **Malicious actions**
- **Unintentional damage**
- **Non-business use of computers (a denial of service of person/computer)**

## Potential Consequences/Loss

- Embarrassment (credibility)
- Repair costs (& down time)
- Misinformation or worse (misled customers)
- Loss of (eCommerce) business
- Out of Business!

# Making the Right Investment!

# Cost Benefit/Avoidance Analysis

**Potential Loss**

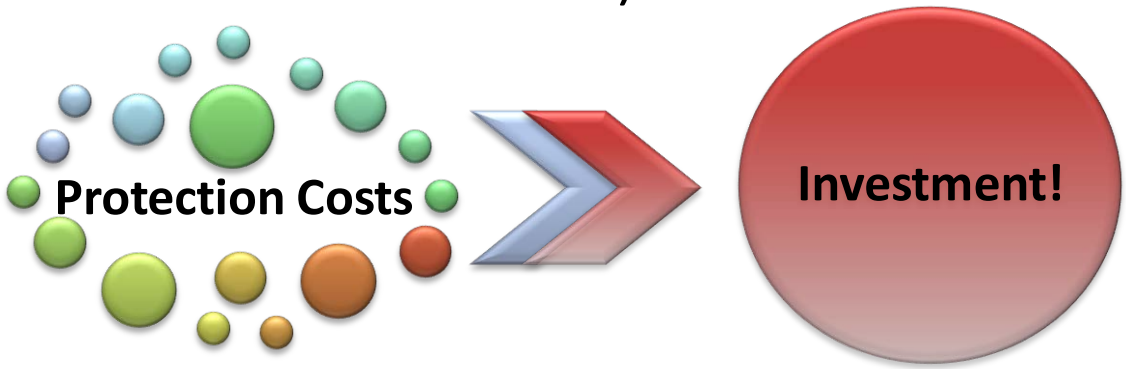
**versus**

**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 chat about each of these)



# 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.

## 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

- **Privacy/Information Security:**

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

- **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!

# Where Can We Start?

## What Should You Do About It?

- **Take control of your information security with:**
  1. Analysis
  2. Assessment
  3. Plan
  4. Implement: Information security controls
     - Policy, Procedures, Practices
     - SW/HW security controls

**How much time and money should you invest?**

## Where Can We Start? – Analysis!

- Do you know what information you need to run your business?
- Do you know where the information is?
- Do you know which types of information are the most important?

**Exercise 1: Identifying and Prioritizing Information**

# 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 | | | |

## Where can we start? - Assessment

- **How much would it cost to me;**
  - If particular information falls into someone else's hand?
  - To be without this information?
  - To re-create this information?
  - If I can't trust the accuracy of completeness of this information?

**Exercise 2: Estimate Costs/Values**

# 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 | | | | | | |

## Where can we start – Plan

- **What kind of protection does your information need?**
  - **3 aspects of security**
    - Confidentiality
    - Integrity
    - Availability

**Exercise 3: Identify the protection needs**

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

What kind of protection does your important information need?

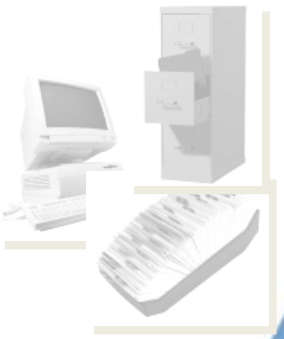
| Priority | Type of Info. | Who has access? | On which system? | C | I | A |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |

## Where Can We Start? - Implement

- Security Policy (using exercise 1-3)
- Information Security Procedures
- Best Practices for IS
- SW/HW  security controls

- **A Security Policy defines:**
  - What information you care about?
  - How you need to protect it
  - Inventory and prioritize your information
  - Ensure confidentiality, integrity and availability

- **Consider:**
  - What happens if this particular information falls into someone else's hand?
  - How much would it coast 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 this 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
  http://csrc.nist.gov/groups/SMA/fasp/areas.html
  and select “Policy and Procedures” in the left-hand column

# Business Information Security Management

## Risk Assessment


Security Policies


Risk Assessment

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

# Most Threats Have a Human at Their Origin

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

## Other Threats

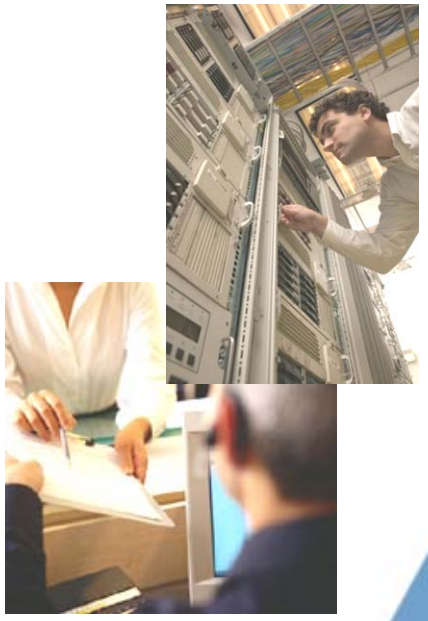
- **Spoofing**
- **Snooping**
- **Social engineering**
- **Abuse of system privileges**
- **Ransomware**
- **Insider threats**
  - malicious actions, unintentional, non-business use

# 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**
  - invisible code which will attempt to download spyware to your computer

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

- **Where are you vulnerable to the threats?**
  - Computer hardware and software
  - Poor policies
  - Missing procedures
  - Lazy oversight
  - Loose enforcement



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

A **Threat**

acting on a **Vulnerability**

produces a **RISK** and probable bad 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

# Risk Mitigation – *Flaky Example!*



# Risk Mitigation


**Reduce threat:**

**Move to New England**



**Reduce threat:**

**Teach people that stealing is not nice**

# Risk Mitigation


**Reduce vulnerability:**

**Strengthen and reinforce home**



**Reduce vulnerability:**

**Keep the computer in a locked room**

# Risk Mitigation


**Reduce the consequence:**

**Leave home before the tornado arrives and take all your stuff with you**



**Reduce consequence:**

**Limit valuable information on the computer(s) (or, encrypt all data on the computer(s))**

## Outcome of Risk Assessment

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

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

# Best Practices
# Procedures and People

- **Start with:**
  - Security Policy

**Remember! Procedures implement Policies**

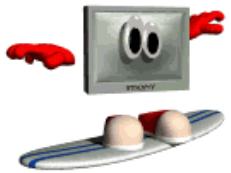
- **Determine who will need procedures:**
  - All employees who use computers in their work
  - Help desk
  - System administrators
  - Managers/executives using specialized software
  - System maintenance
  - IT Out-sourcing

**Create, then follow your procedures!**

- **Enforcing safe**
  - Internet practices
  - E-mail practices
  - Desktop practices
  - Personal 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 websites 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
  - 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!**

- **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)

- **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 Technologies

## Identification/Authentication

- **Identification**
  - Identifies the user to the system/network
- **Authentication**
  - Verifies that the user is who they say they are

**If you cannot identify and authenticate individuals**

**– you don't have access control for your important data**

**– or accountability for data changes**

## Way To Authenticate

- **Something you:**
  - Know – Password or PIN
  - Have – Key or token
  - Are – fingerprint, iris scan, facial scan
  - Do – write, voice, type

## 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 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

**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

## 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

- **http://www.nist.gov/nice**
  - –National Initiative For Cybersecurity Education
- **http://stopthinkconnect.org**
  - –Stop.Think.Connect
- **http://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
- **http://iase.disa.mil**
  - –Information Assurance Support Environment, Defense Information Systems Agency

## *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!**