National Institute of Standards and Technology
U.S. Department of Commerce

Small Business Information / Cybersecurity Workshop

Computer Security Division, Information Technology Laboratory

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Presenter

Kelley Dempsey, CISSP, CAP, CEH, CHFI

Computer Security Division/Information Technology Laboratory

National Institute of Standards and Technology (NIST)

Gaithersburg, MD

kelley.dempsey@nist.gov

301-975-2827

NISTIR 7621: Small Business Information Security: The Fundamentals

http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Now is a good time to put your mobile devices into "silent" or "vibrate" mode to limit distractions for other attendees. Thanks!

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 ?

- **28 million small businesses**
- **Represent 99.7% of all U.S. employer firms**
- **49% of the private workforce**
- **37% of small businesses have fewer than 20 employees**
- **33% total export value**

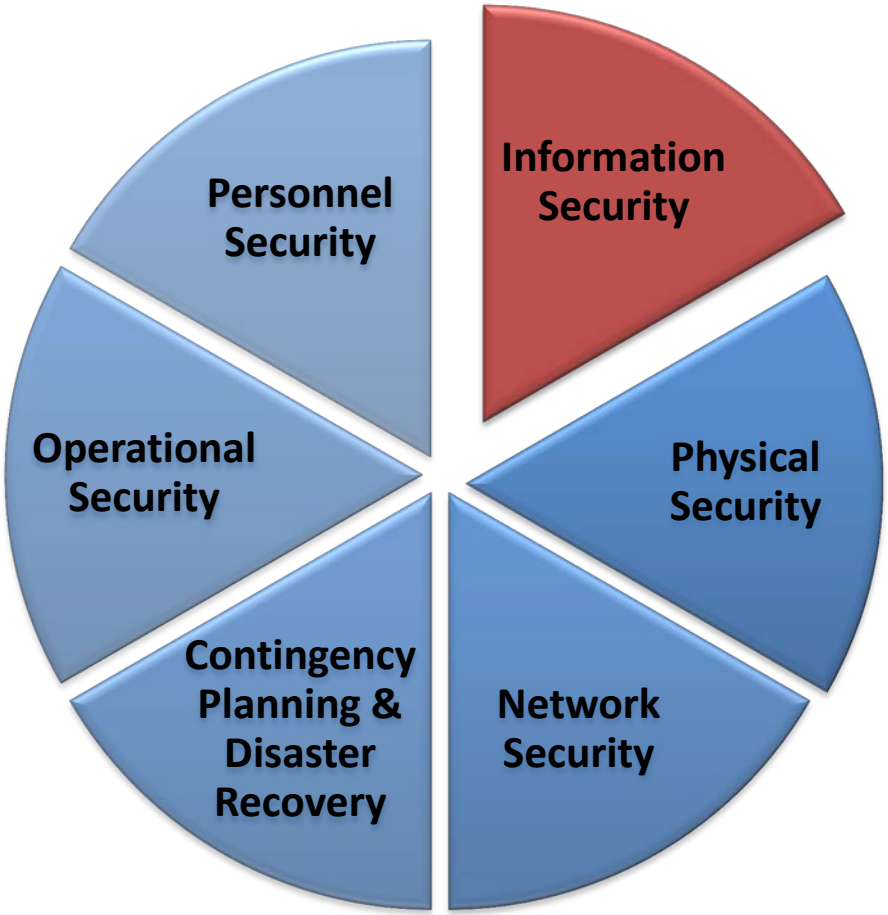
*Source: “2014 Small Business Profiles for the States and Territories”, the U.S. Small Business Administration, Office of Advocacy (Small Business -> less than 500 employees)

Promote

- Awareness of the importance of and the need for cybersecurity
- Understanding of cybersecurity threats, vulnerabilities, and corrective measures
- Target Audience – Small Businesses (not IT or Cybersecurity)

Comprehensive Security Program

Defense in Depth – use of multiple security countermeasures to protect information



Agenda – *You Will Learn*

- **What is Information/Cybersecurity?**
- **Why do we need Information/Cybersecurity?**
  - IC3 Cybercrime Statistics*
- **Where can we start?**
  - Practical steps to protect your business
- **Technologies & Recommendations**
- **When you need help – what can you do?**

*Internet Crime Complaint Center: http://www.ic3.gov/default.aspx

WHAT IS **INFORMATION**/CYBERSECURITY?

What is Information/cybersecurity?

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.

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks.

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

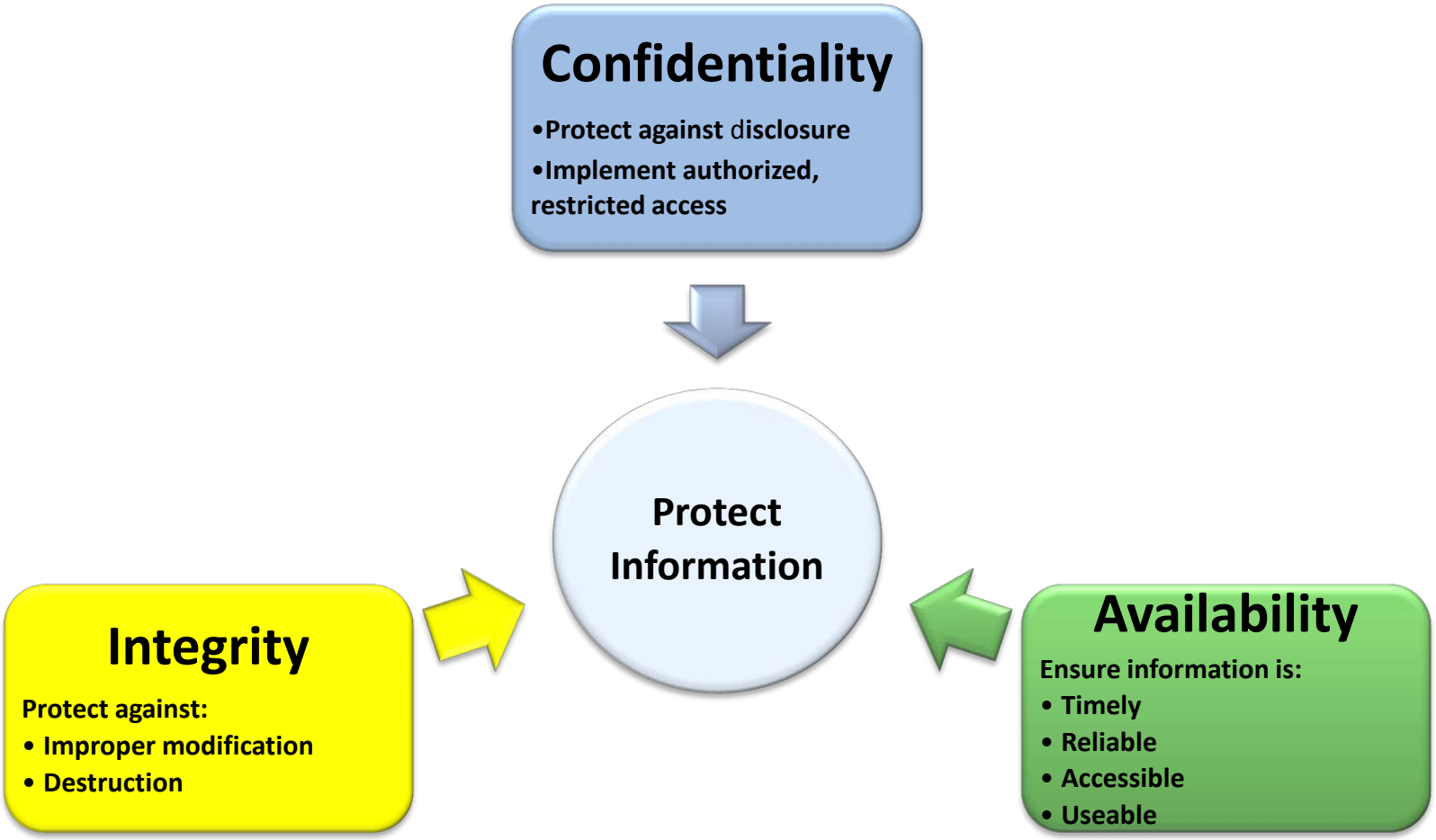
What is Information and an Information System?

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

- **Information System**

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

Security Objectives



Why Do We Need Cybersecurity?

(IC3 – FBI Web Page)

Total complaints received: 289,874

Total Loss: $525,441,110.00

Average dollar loss: $4,573.00

(https://www.ic3.gov/media/annualreport/2012_IC3Report.pdf)

Making the Right Investment!

How much time and money should you invest?

Yes, an investment is required to implement cybersecurity.

But what is the 'right' amount?

Can you spend too little? Can you spend too much? (yes!!)

Cost Benefit/Avoidance Analysis

Potential Loss

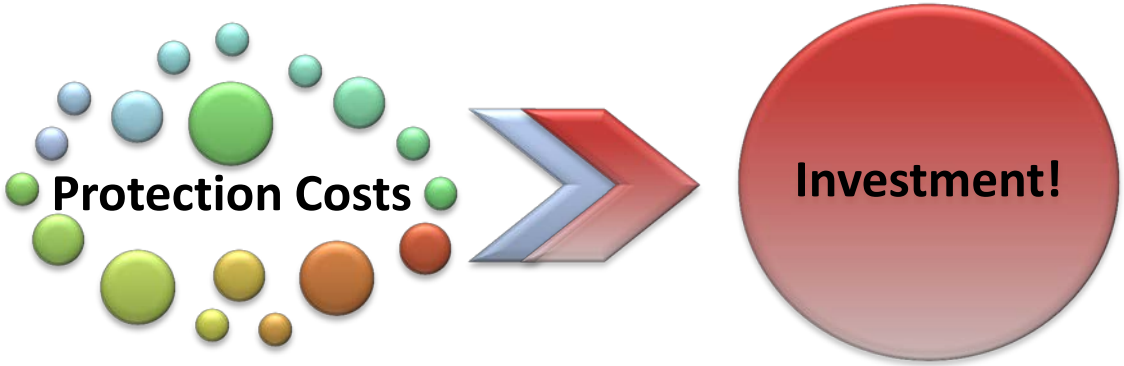
versus

Protection Costs

Making The Right Investment

Providing good information security is evidence of

- Sound management
- Sound customer service
- Sound legal protection
- Sound economics



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 increases your profit, too!>

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 expect their data will be kept safe and accounted for by you

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

(Remember – you are the custodian of the data entrusted to your care – you are NOT the owner of that data)

Sound Legal Protection

Taking steps to ensure that your customer or employee data does not fall into the wrong hands (i.e., demonstrating due diligence) provides protection against liability

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!
- Your personal assets!

WHERE CAN WE START?

Where Can We Start?

Take control by doing the following:

1. Analysis – What information do we use?
2. Assessment – What cost for not securing data?
3. Plan – Protection needs of our data?
4. Implement – Policies, Procedures, Risk Assessment, Mitigation Actions (Best Practices)

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?
- Do you know who has access to your sensitive business information?

Exercise 1: Identify and Prioritize 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 types of information used in your business in order of importance (priority) to the business.

Priority	Type of Information	Where is it stored?	Who has access?
1			
2			
3			
4			
5			

How much would it cost:

- If business information is stolen or obtained by unauthorized parties? (confidentiality)
- To be without some business information? (availability)
- To re-create this information? (availability)
- If the accuracy or completeness of business information cannot be trusted? (integrity)

Exercise 2: Estimate Costs/Values

Exercise 2: Estimated costs if business information is compromised (Loss of Confidentiality, Integrity, and/or Availability)

	Info type one released (C)	Info type one modified (I)	Info type one missing (A)	Info type two released (C)	Info type two modified (I)	Info type two missing (A)
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						

What kind of protection does your information need?

3 objectives (or goals) of security

- Protect Confidentiality
- Protect Integrity
- Protect 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 Information	Where is it stored?	Who has access?	C	I	A
1						
2						
3						
4						
5						

Where Can We Start? - Implement

- **Security Policies (using exercises 1 -3)**
- **Security Procedures**
- **Risk Assessment**
- **Mitigation actions (best practices)**

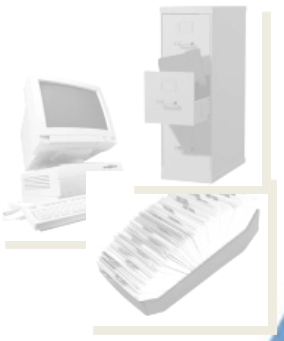
INFORMATION SECURITY POLICY

A security policy states, in writing, requirements for protecting business information. A security policy specifies:

- The information you care about (exercise 1)
- How the information is to be protected

Policy issues to consider (not all inclusive):

- Acceptable use [of information technology] policy
- Training and awareness policy
- Physical security policy
- Logical access policy
- Password policy
- Personnel security policy
- Contingency planning policy
- Etc.



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.
- Passwords are not to be shared with anyone!
- All computer users will read and sign an access and use agreement
- Information Types A, B, C, D, E, and F will be backed up regularly in accordance with their determined priority/criticality.

- For samples, go to http://csrc.nist.gov/groups/SMA/fasp/areas.html and select “Policy and Procedures” in the left-hand column
- Search for “Cybersecurity policy” in any internet search engine

INFORMATION SECURITY PROCEDURES

Best Practices: Security Procedures

- **Procedures implement policies**
- **Procedures specify who, what, when, where, how, how often (with respect to the policies)**
- **Procedures, once written, must be socialized within the organization and then followed:**
  - Good idea to include policy and procedure information in employee training
  - Check periodically to see if procedures are being followed

Example Procedure Supporting a Policy

Policy: All computer users will have their own account and password.

Procedure:

1. Supervisor completes/signs account creation request form for new user and sends it to the system administrator [Note that the account request form would be part of the procedure];
2. System administrator creates new account with unique identifier;
3. System administrator assigns a temporary password to new account ;
4. System administrator notifies the new user of the unique account identifier and temporary password;
5. New user logs into the new account and is prompted to immediately change the password;
6. System administrator reviews user accounts monthly.

To whom is this procedure directed? Who needs to see it?

Tailor procedures to the intended user, for example:

- All employees who use computers in their work
- Help desk staff
- System administrators
- Managers/executives
- System maintenance staff
- Out-sourced/contract staff
- Etc.

Create, then follow your procedures!

HOW DO I ASSESS RISK?

To assess/determine risk, identify:

- ❑Threats
- ❑Vulnerabilities
- ❑Likelihoods
- ❑Impacts

These are the four factors that determine risk.

For more information on formal security risk assessment, see NIST SP 800-30, http://csrc.nist.gov/publications/PubsSPs.html

A threat acts on a vulnerability and creates risk with determinable likelihood and negative impact (consequence)

Threat: Phishing e-mail asking for sensitive info

Vulnerability: Staff has not been trained to identify and ignore phishing e-mails

Risk: How likely is it to occur? What are the consequences if it does? Information is compromised, lawsuits, customers go elsewhere.

To assess/determine risk, identify:

- **Threats**
- Vulnerabilities
- Likelihoods/Impacts/Risks

What is a Threat?

- **A threat is a circumstance or event (source) with the potential to adversely impact business assets**
- **A threat may be a:**
  - Hostile cyber or physical attack
  - Human error (inadvertent)
  - Failure of business-controlled resources (e.g., hardware, software, environmental controls)
  - Natural or man-made disaster or accident

Threat Consequences from Hostile Cyber or Physical Attack

- Destruction of information when information systems are accessed by hacking
- Theft of information or computer hardware
- Website defacement
- Installation of malicious programs (malware) onto information systems or individual computers/devices

What are they after?

- **Access to business information**
- **Access to your money**
- **Personally Identifiable Information (PII)**
  - Your own
  - Your employees'
  - Your customers'
- **To use personal or business computers in a botnet**
- **Any other assets on your computer**

Hostile Attack Types

- Spoofing
- Snooping
- Social engineering
- Increasing the level of system privileges (after gaining unauthorized access)
- Ransomware
- Malware (Malicious code – viruses, worms, etc.)
- Insider threats
- Theft of information (data) and resources

More Hostile Attack Types

- **Identity Theft** - steal & misuse your identity ($$$)
- **Phishing** - Email tricking YOU or your employees into giving personal or business/customer information (a form of social engineering)
- **Spear Phishing** - Email with specific company details and targeted at specific employees to deceive you/the target into responding
- **SPAM** - Unsolicited and unwanted Email
- **Compromised web pages** - invisible code planted on legitimate web pages that attempts to install malware on personal or business computer(s)

Hostile Attacks - Theft of data and resources

- **Stealing personal and business-related information/computer files (electronic and physical)**
- **Accessing information system accounts (to steal information)**
- **Stealing laptops and computers (physical theft)**
- **Intercepting your emails or internet transactions**
- **Mobile devices left unguarded – can/will be stolen (keep track of mobile devices, keep secure)**

Hostile Attacks - Malicious codes and viruses

- Find and send files over Internet
- Find and delete or steal critical personal or business data
- Lock up computer(s)
- 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

ZEUS Malware:

- In the form of a Trojan Horse
- Spread [mainly] through phishing and drive-by downloads
- Often used to steal account credentials (banks,etc.)
- Often installs CryptoLocker ransomware
- Has often been modified to carry out many other types of malicious and criminal acts
- Uses stealth techniques to hide itself/support its botnet

Insider threats: Hostile Attacks/Human Error

- **Malicious actions (hostile attack type of threat)**
  - Stealing information for competitors
  - Revenge for perceived mistreatment
  - Abuse of system privileges
- **Unintentional damage (human error type of threat)**

Natural/Man-Made Disaster & Business Resource Threats

- **Disasters**
  - Fire (natural or man-made)
  - Flooding (natural or man-made, e.g, from burst pipes)
  - Hurricane, tornado, earthquake (natural, locality-based)

- **Business Resource Threats**
  - Equipment (hardware) failure
  - Network/communications failure
  - Application (software) failure
  - Lack of protections (e.g., no fire protection in place)

To assess/determine risk, identify:

- ☑ Threats
- ❑ **Vulnerabilities**
- ❑ Likelihoods/Impacts/Risks

Where are you vulnerable to the threats?

- Outdated and/or unlicensed hardware and software
- Ineffective/nonexistent policies
- Ineffective/nonexistent procedures
- Lazy oversight/Lack of training
- Loose enforcement

(Note: NISTIR 7621 lists 20 actions that must be taken for reasonably effective information security – failure to do any of them is a Vulnerability. http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf)

To assess/determine risk, identify:

- ☑ Threats
- ☑ Vulnerabilities
- ❑ **Likelihoods/Impacts/Risks**

Potential Likelihood

- **Example 1: Your business is vulnerable to phishing attacks (threat) because no training has been provided. Likelihood: High**
- **Example 2: Your business is less vulnerable to exploits related to software flaws because a strong patch management policy and procedure are in place and followed closely by the system administrator. Likelihood: Low to Moderate**

Potential Impact (Consequences/Loss)

- Embarrassment (credibility/reputation)
- Repair costs (& down time)
- Misinformation or worse (misled customers)
- Loss of personal assets
- Loss of business (traditional and eCommerce)
- Out of Business!

Potential Likelihood

- **Example 1: What if proprietary business information is stolen via a phishing attack? Impact: High**
- **Example 2: What if, in spite of regular patching and scanning, a new software flaw-based exploit allows the theft of a hashed password list? NOTE: A strong password policy is in place. Impact: Low to Moderate**

- **Example 1: Proprietary business information could be stolen via a phishing attack.**
  Likelihood: High Impact: High RISK: HIGH
- **Example 2: A hashed password list could be stolen via software flaw-based exploit.**
  Likelihood: Moderate Impact: Low
  RISK: LOW to MODERATE

What do we do once we know the risks?

- Mitigate the risk
- Accept the risk (if it is low enough, but keep an eye on it)
- Reject the risk (let's just not do that!)
- Share/Transfer the risk (may reduce the risk to your business)

Knowing where you need protection:

- Computers (desktops, laptops, servers, mobile devices – yes, mobile devices are computers)
- Network (cabling, firewalls, routers, switches, wireless routers and access points)
- Software (do you have proprietary software?)
- Operations (who is minding the door?)
- Business processes (policies and procedures)

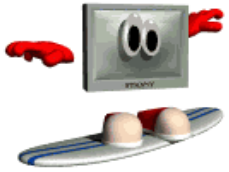
Accepting Risk - How much risk can I live with?

- Risks cannot be completely eliminated
- If the impact would be high and the likelihood would be high, risk is high and your tolerance is low
- If the impact would be minor and the likelihood would be low, the risk may be acceptable
- If the risk is still too high after all mitigation efforts have been done, commercial cyber insurance may be used to "share" the risk/exposure

INFORMATION SECURITY BEST PRACTICES

Implementing secure:

- Internet/network practices
- E-mail practices
- Desktop/laptop/server practices
- Personnel practices
- Data backup practices
- Physical security practices
- And more!



- **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!
  - Click on links in a Facebook/Linked-In message or posting
- **Do:**
  - Protect passwords, credit card numbers, and private information in web browsers (use SSL or other encryption)
  - Implement firewalls, proxy servers, and secure router configurations

Secure E-Mail Practices

- **Be careful:**
  - opening attachments – verify origin
- **Do not:**
  - reply to unsolicited emails
  - click on links in an email – jokes and cat videos are NOT worth it!

Do:

- Use STRONG passwords (NEVER share!)
- 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 – files or entire HDD (especially for laptops/mobile)
- Enable security event logging

Do:

- Confirm identities of people and organizations
- Accompany all vendors, repair persons, visitors, etc.
- Give only enough information to answer questions
- Check references, education, etc., for possible hires
- Conduct background checks! (yours?)
- Control employee entrance and exit
- Control employee terminations/departures
- Include security policy/procedures in employee training

Implement Backup Procedures

- **Ability to restore data to what existed before:**
  - virus/malicious code problems
  - theft or destruction
  - data integrity problems
  - equipment failures
  - natural/man-made disasters
- **Policy and procedure define how often to conduct backups and move them to off-site storage (backup weekly, store off-site monthly?)**
- **TEST YOUR BACKUPS!! Do a test restore on a regular basis (as defined in backup procedures)!**

Backing Up Data in the Cloud

If you wish to use a cloud service provider to back up your data, do your due diligence!

- What security protections has the provider implemented? If the provider is not forthcoming, move on!
- Encrypt your data before putting it into the cloud!
- What will happen to your data if the provider goes out of business?

Facilities

- Locks
- Anonymity
- Alarms
- Lighting
- Fences
- Guards/electronic surveillance
- Floor-to-ceiling walls

Implement Procedural Security

- **Keys**
  - Document key holders
  - Mark keys “Do Not Copy”
- **Protect company directories and contact information** (why help social engineers?)
- **Control passwords**

Implement Password Security

- **At least 12 characters long (16 is better!)**
- **No names, birth dates, or personal info**
- **No dictionary words or patterns**
- **At least one**
  - Upper case
  - Lower case
  - Numeric
  - Special character
- **Change every 3 to 6 months**
- **Replace vendor default passwords**

Malicious code/Malware = viruses, spyware, trojans, worms, etc.

- Company-wide detection tools
  - Include employee's home systems
  - Include mobile devices
- Company-wide process (install, configure, update)
- Assign responsibility in writing
- Up-to-date malware signatures

Management Includes:

- Defining roles and responsibilities
- Committing necessary resources
- Enforcing policies and procedures (enact penalties for not following policies and procedures!)
- Demonstrating importance of IS by example

Remember!

Managers are responsible for protecting company data!!

(Remember the sign – The Buck Stops Here!!)

Staff Security 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”
  - Indicate acknowledgement/understanding of security policies and procedures with a signature
- **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!

Implement Wireless Security

- 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 acceptable level of encryption to use for your wireless network!!
- Change default encryption keys; Change often
- Change the Wireless Access Point (WAP) administrator password!

Implement Secure Destruction

- **When computers are replaced**
  - destroy all information on the old computer's hard disks and/or non-volatile memory
  - Don't forget printers and copiers that have hard disks and/or non-volatile memory
- **When discarding removable media (diskettes, CDs/DVDs, tapes, USB sticks, etc.)**
  - destroy information on the media
  - destroy the media itself

NIST SP 800-88, Guidelines for Media Sanitization

TECHNOLOGIES AND RECOMMENDATIONS

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
  - accountability for data changes

Ways To Authenticate (Authentication Factors)

- **Something you:**
  - **Know** – Password or PIN
  - **Have** – Key or token
  - **Are** – fingerprint, iris scan, facial scan
  - **Do** – write, voice, type
- **Consider multifactor authentication (if risk warrants it)**

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 or individual files/folders)**
  - Whole disk: Bitlocker comes with Windows Vista, Win 7, Win 8; File Vault comes with Mac OS X; Many 3rd party vendors (Symantec, PGP, SensiGuard, SecureIT, SafeBit, etc., $30-150 and up)
  - Individual files/folders - Windows EFS (Encrypting File System); Many 3rd party vendors (FolderLock, CryptoForge, etc.)

What about the Cloud?

- Many cloud providers – Amazon, HP, IBM, Microsoft, Google, Lockheed Martin, etc.
- Most providers offer cloud services to secure data.
- Get details from the cloud provider about their security practices; if they won't provide details, look for another provider.
- Encrypt your data before putting it into a cloud!

Basic Security Tips (Review)

- Use anti-virus software (computers and mobile devices) – Windows offers free Security Essentials or Defender
- Update operating system and applications (patches and new versions)
- Install a firewall (or multiple firewalls, 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 BACKUPS!

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 and 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

Contact the local FBI office

- and/or your State or Local Fusion Center (DHS)

File a complaint with the "Internet Crime Complaint Center" at www.ic3.gov

Other Security Resources

- **NIST Guidance: http://csrc.nist.gov/publications**
- **http://www.nist.gov/nice**
  - –National Initiative For Cybersecurity Education
  - –Cybercrime Case Studies – http://krebsonsecurity.com/category/smallbizvictims/
- **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

Kelley Dempsey

Computer Security Division

Information Technology Laboratory MS8930

National Institute of Standards and Technology

Gaithersburg, MD 20899-8930

301-975-2827

kelley.dempsey@nist.gov

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