COMPUTER SECURITY

. . . .is Good Business

Welcome!

8/14/2008

Presenter

Richard Kissel, CISSP, CISM

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

Partners in this Outreach

U.S. Small Business Administration

(National Headquarters and District Offices)

Federal Bureau of Investigation-InfraGard

National Institute of Standards and Technology

Supported by:

National Cyber Security Alliance

The NIST Mission

To develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Goal

Promote:

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

You Will Learn

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

Seminar Agenda

Computer Security is Good Business

Open/Welcome (8:00 am/1:00pm) (we operate on an –ish schedule!)

1. **Making the Right Investment (8:15 am/1:15pm)**

Learn how to define information security (IS) for your organization and demonstrate the necessity of IS in your operations. Hear examples of the most common types of threats to information security and understand how to do a cost-benefits analysis to determine the extent to which your organization should proactively address known threats.

2. **Defining Your Information Security Needs (9:00 am/2:00pm)**

Learn to create a security policy that supports your organization's mission. Understand the fundamentals of risk assessment and risk mitigation.

Break – 9:45-10:00am/2:45-3:00pm

3. **Common Information Security Practices (10:00am/3:00pm)**

Internet, E-mail, Desktop, Personnel – learn common Best Practices and procedures and operate more securely. (Focus on procedures.)

4. **Mechanisms and Technologies of Information Security (11:00am/4:00pm)**

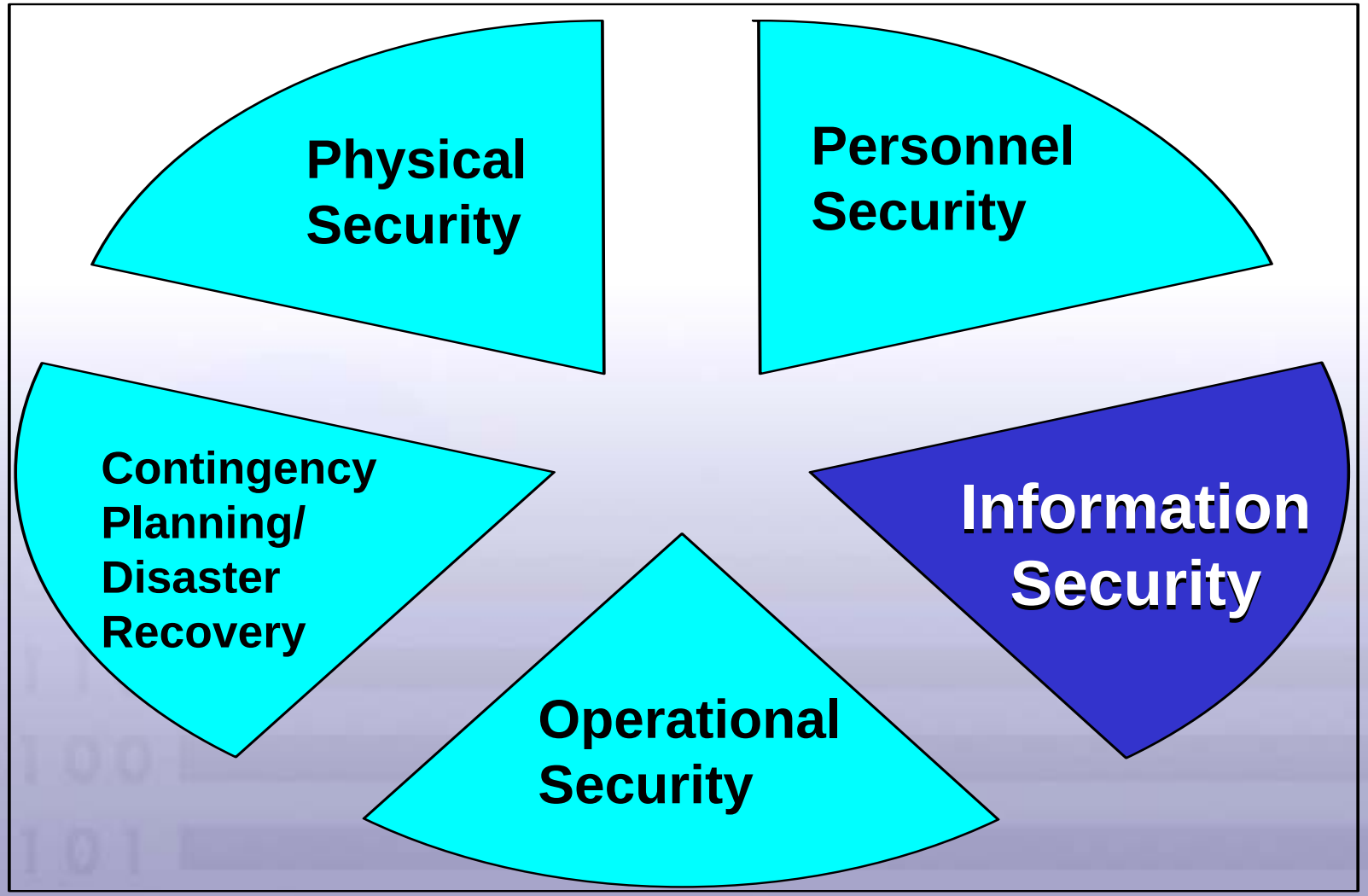
Hear an overview of current technologies used in reducing IS vulnerabilities and learn of NIST (and other) resources available to your organization.

COMPUTER SECURITY

. . . .is Good Business

General Information

Comprehensive Security



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

Characteristics of InfoSec

- Confidentiality
- Integrity
- Availability

Today's Security Issues

Computer Security Institute Survey*:

- **46% reported security breaches.**
  - 26% more than 10 incidents
  - 23% didn't know if or how many
- **59% reported employee Internet abuse**
- **52% detected computer viruses**

*2007

Today's Security Issues (Cont)

Computer Security Institute Survey:

- **Attacks results**
  - Financial losses - $66.9Million (2007)
  - Average loss per business/year $345K
  - FBI-2005 $67Billion total loss estimate

Not Just Big Guys

34%
Small Businesses/Organizations

Web Defacement and Break-In

Large and small organizations

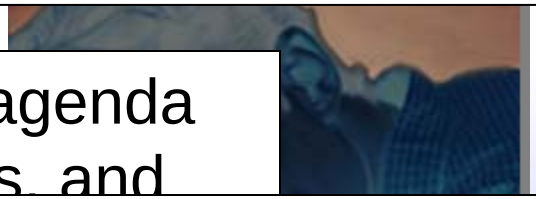
- A “Big Bank” to a small electronics store
- In 2007, 40% reported one to five web defacements
- In 2007, 56% did not know how many times their web servers had been defaced

Who are the bad guys?

Amateurs Through Experts:

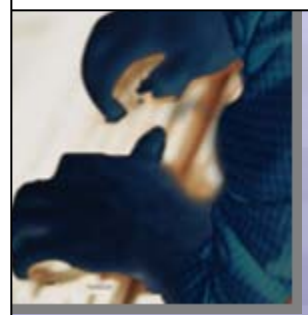
- **Experimenters and Vandals**
- **Hacktivists**
- **Cybercrimina**
- **Information warr**

Impress their peers and leave their mark



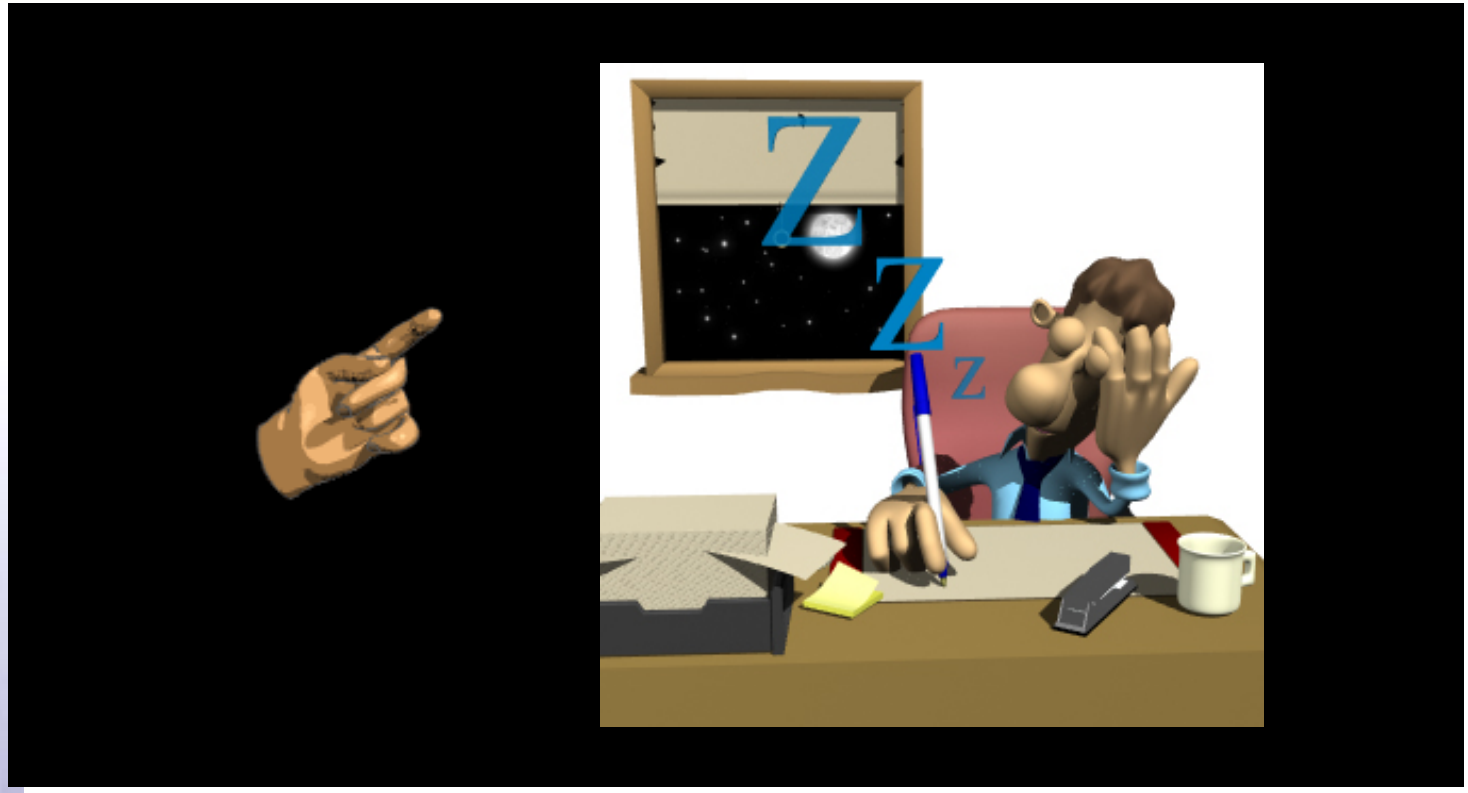
Personal or political agenda to destroy, embarrass, and blac

Steal your customers' credit cards and account information – perhaps s.



State-supported professionals who want to disrupt the Internet, soften up a potential target or gain control of power grids, Oil/gas pipelines/terminals, etc.

Their common target?



You/Your Information

Potential Consequences

- Embarrassment
- Repair costs
- Misinformation or worse
- Loss of (eCommerce) business

Three Common Attacks Today

- Theft of data and resources
- Denial-of-service attacks
- Malicious codes and viruses
- Insider Threats

(Let's look at each of these)

Theft of Data and Resources

- Stealing your computer files
- Accessing your computer accounts
- Stealing your laptops and computers
- Intercepting your e-mail

Denial-of-Service Attacks

Attacking your computer or website

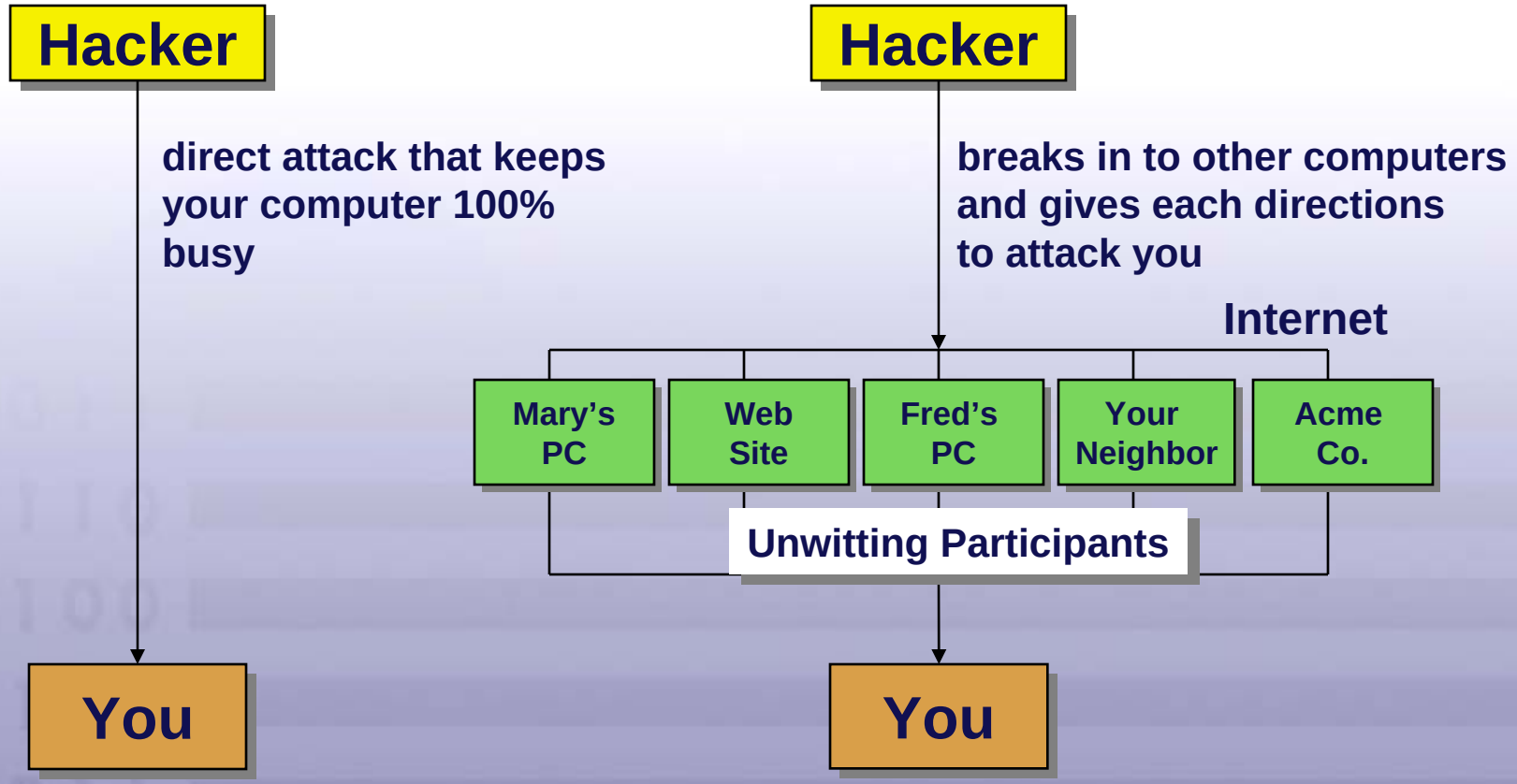
- **Locks up equipment**
- **Crashes your systems**

Results

- **Stops/slows work workflow**
- **Prevents e-mail communications**
- **Shuts down eCommerce**

Denial-of-Service Attacks

Methods



Malicious Code

- Sends itself over Internet
- Sends your files over Internet
- Deletes your data
- Locks up your computer or system
- Hides in program or documents
- Copies itself

Insider Threats

- Malicious actions
- Unintentional damage
- Non-business use of computers

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 and Networks

Take control of your information security with:

- Analysis
- People
- Policies & Procedures
- Technology

How much time and money should you invest?

COMPUTER SECURITY

. . . .is Good Business

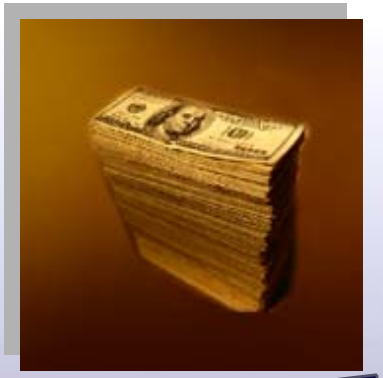
Making the Right Investment

Cost Benefit Analysis

Potential Loss

versus

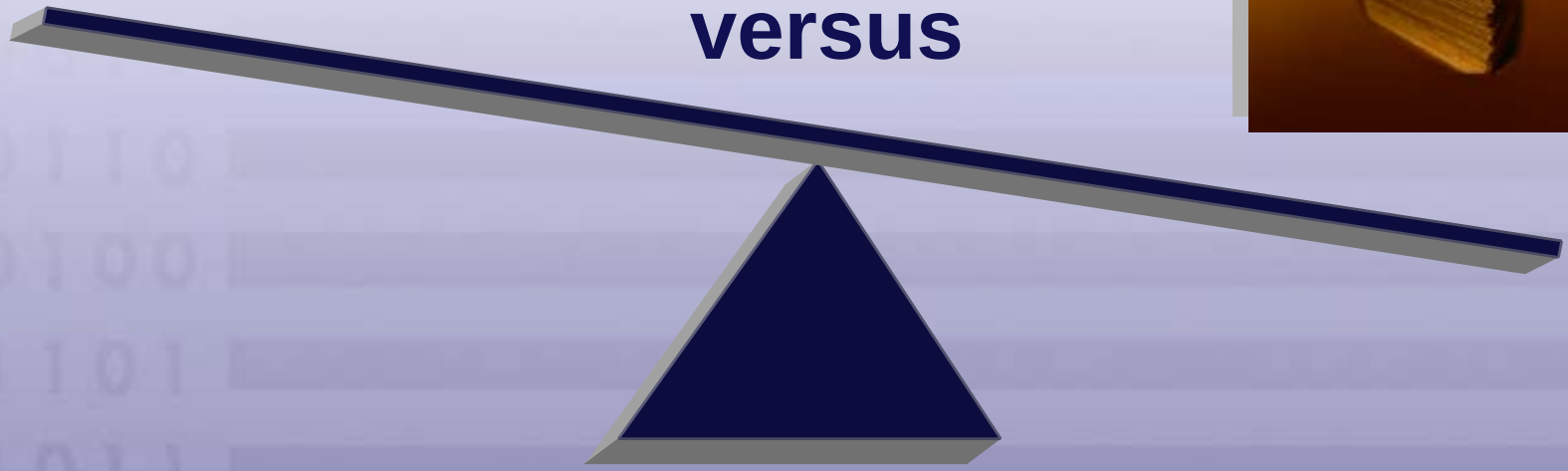
Protection Costs



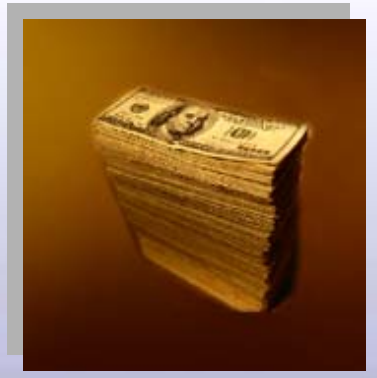
Cost Benefit Analysis

Potential Loss

versus



Protection Costs

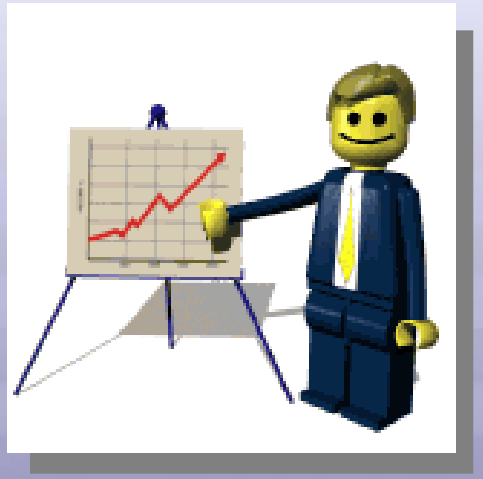


Making the Right Investment

Information Security is:

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

Let's talk about these.



Sound Management

The business case for Information Security should:

- **Support your organization's mission**
- **Be cost-effective (but it does cost!)**
- **Be integral to your management plan**

Sound Customer Service

- Customers want their private information protected and respected
- Customers need to have confidence in placing orders with you
- Customers desires for their data 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:

Ensuring that your customer/employee data does not fall into the wrong hands

Sound Economics

Cost benefit analysis for security: What are you risking?

- Decreased productivity
- Increased labor costs
- Legal liability
- Loss of confidence
- Adverse reputation

Sound Economics

Information Security is Good Business!	Medical Information Released	Medical Information Modified	Credit Card Information Stolen	Accounting System Shut Down or Compromised
Cost of Revelation				
Cost of Loss/ Recreation				
Cost of Availability				
Lost Work				
Legal				
Confidence				
Repair				

Sound Economics

Information Security is Good Business!	Medical Information Released	Medical Information Modified	Credit Card Information Stolen	Accounting System Shut Down or Compromised
Cost of Revelation	$-Contract	NA	$-Contract $-Client $-Value stream	NA
Cost of Loss/ Recreation	NA	Life $$$ Threatening	NA	$- Hours to rebuild or decipher
Cost of Availability	NA	NA	NA	$-Rework $-Delayed or lost income
Lost Work	$-Hours to "close the gate" and reassure clients/employees	$-Hours to reassure clients/employees	$-Hours to reassure clients/employees	$-Hours with clients
Legal	$$$-Liability based on business procedures/practices			NA
Confidence	$$$- Future Business			
Repair	$-Security			

Your Investment Pays Off

An investment in information security is an investment in:

- Sound Management
- Sound Customer Service
- Sound Legal Protection
- Sound Economics

Information security is good business!

INFORMATION SECURITY

...is good Business

Survival Tools & Techniques

Defining Your Needs

Analysis

8/14/2008

Security Policies

A Security Policy defines:

- What information you care about
- How you need to protect it
- 1st – Inventory and Prioritize your information

Security Policies

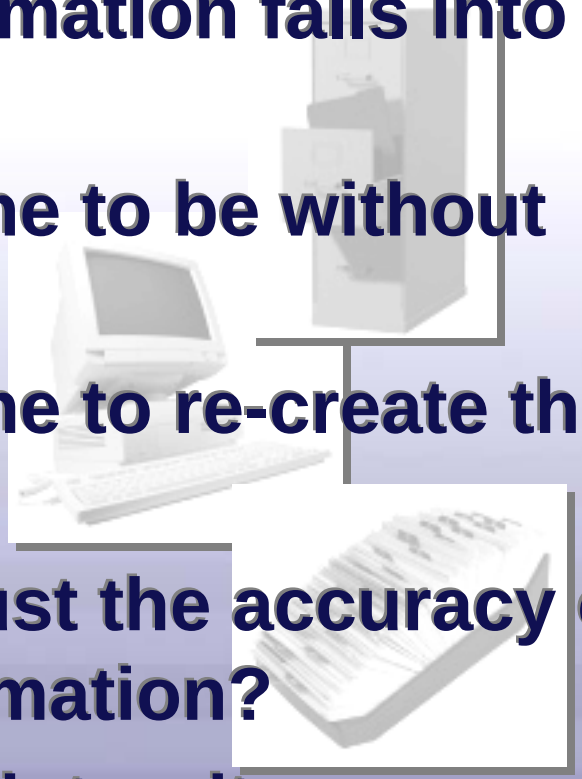
A Security Policy defines:

- **What information you care about**
- **How you need to protect it**
  - Confidentiality
  - Integrity
  - Availability

Security Policies

Consider :

- What happens if this 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



What You Care About

What	Type of Protection		
Assets	Confidentiality	Integrity	Availability
Patient files	√	√	√
Time Records		√	
Tax Records	√	√	
Payroll	√	√	√

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

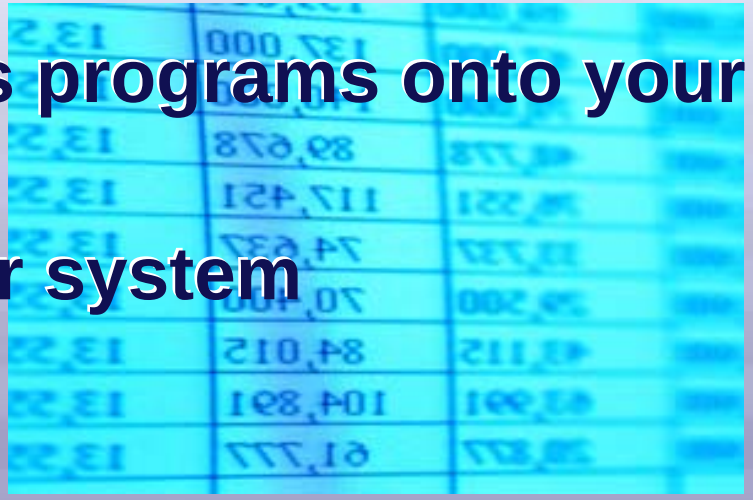
Identify:

- **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**



Other Threats <discuss>

- Spoofing
- Snooping
- Social engineering
- Abuse of system privileges

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.
- Pfarming -Redirecting Your Web Page Requests to Phony (but Authentic looking) Web Pages.
- SPAM - Unsolicited and Unwanted Email.
- SPIT - Spam over Internet Telephony (VOIP).
- Compromised web pages – with invisible code which will attempt to download spyware to your computer.

Other Threats

- Ransomware – a specialized malicious program which encrypts your valuable information and you are offered the opportunity to get the unencryption key – for a price!
- Zero-day exploits – Vulnerabilities discovered and exploited before anti-malware companies have the opportunity to create and distribute the capability to find and correct the vulnerability.

Security Risk Assessment

Identify:

- Threats
- **Vulnerabilities**
- Risks

Common InfoSec Vulnerabilities

Where are you vulnerable to the threats?

- **Computer hardware and software**
- **Poor/missing procedures**
- **Poor oversight/enforcement**

Security Risk Assessment

Identify:

- Threats
- Vulnerabilities
- **Risks**

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

Risk Management

How much risk can I live with?

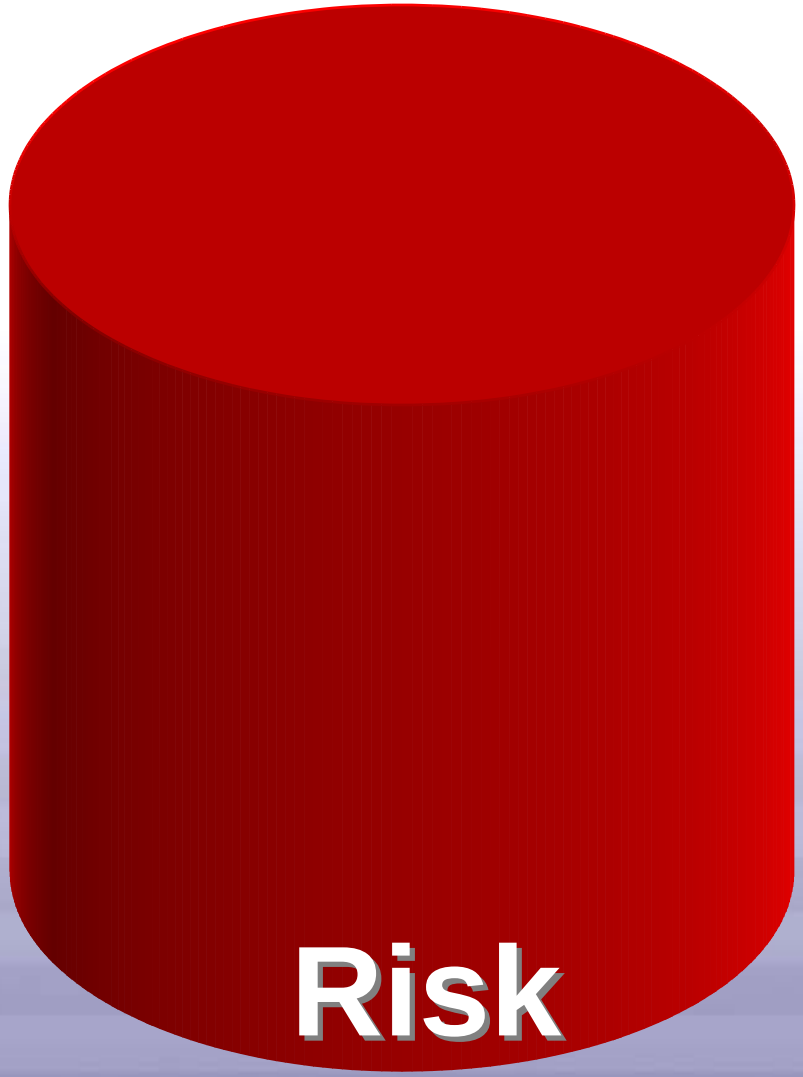
- No risk can be completely eliminated.
- If the consequence is high (& the probability is high), your tolerance is low.
- If the consequence is minor, more risk

Risk Management

How much risk can I live with?

- If the risk is still too high after all mitigation efforts have been done, use commercial 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 that computer in a locked room

Risk Mitigation

Reduce consequence:

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

Reduce consequence:

Put no valuable information on that computer (or, encrypt all data on the computer).

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!

INFORMATION SECURITY

...is good Business

Survival Tools & Techniques

Best Practices: Procedures and People

8/14/2008

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
- System maintenance
- IT Out-Sourcing
- Software Applications

Create, then follow your procedures!

Best Practices: Procedures

Enforcing safe

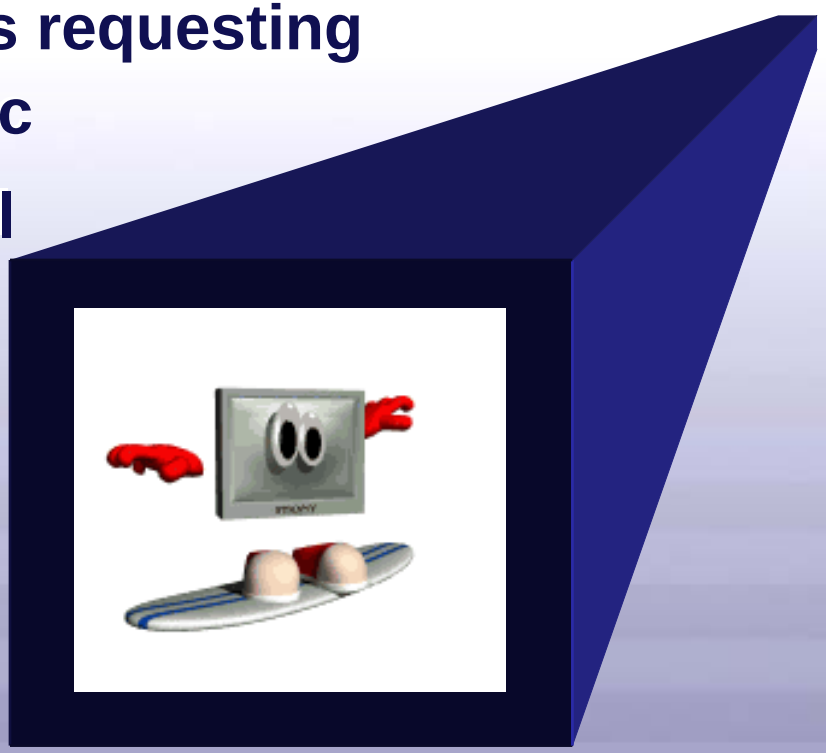
- Internet practices
- E-mail practices
- Desktop practices
- Personnel practices

(will address each of these, in turn)

Safe Internet Practices

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!

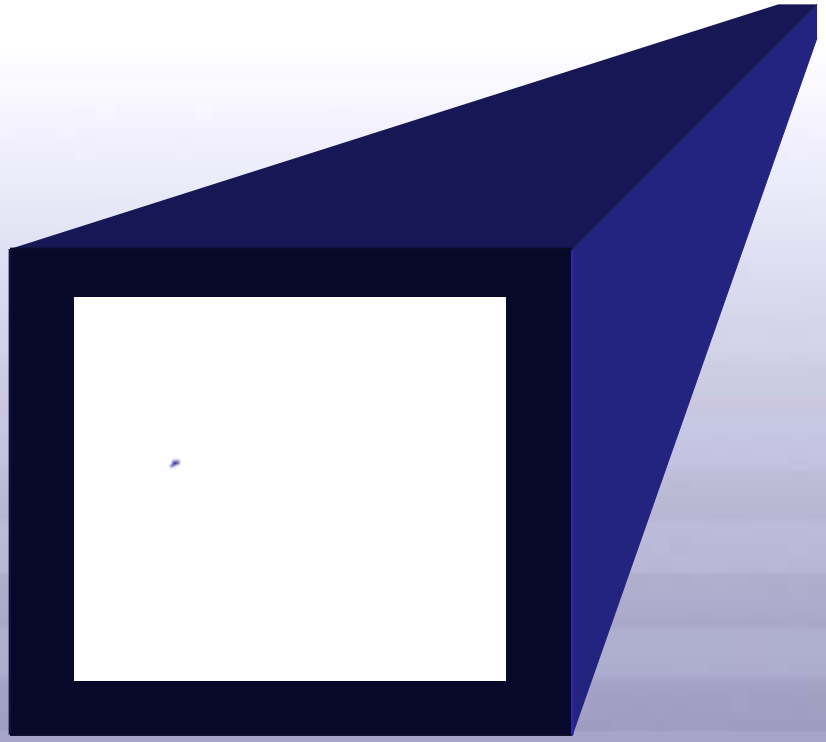


Do:

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

Safe E-Mail Practices

- Be careful opening attachments
- Make sure your e-mail software is properly configured
- 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 computer accounts
- 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**
- **Properly dispose of sensitive information**

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 RESTORE AT LEAST ONCE A MONTH!

Implement Physical Security

Facilities

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

Implement Personnel Security

- **Conduct background checks.**
- **Control employee entrance and exit.**
- **Control employee departures.**

Implement Procedural Security

- Document keys holders.
- Protect company directories and contact information.
- Control passwords.

Password Control

Make it difficult:

- To guess someone's password
- For password cracking tools to work
- To use compromised passwords

Password Control *(continued)*

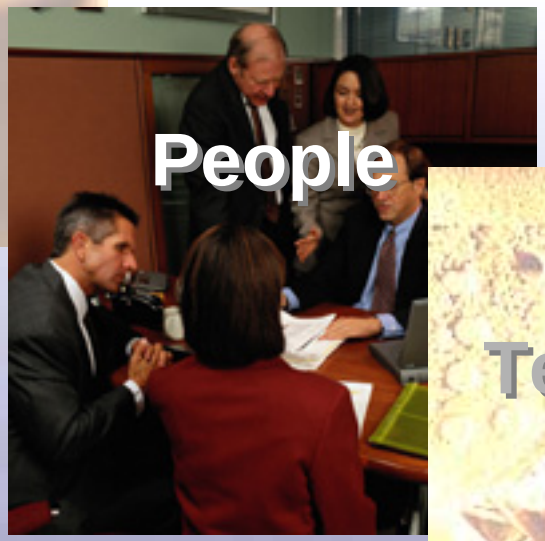
- **At least 8 characters long**
- **No names or birth dates**
- **At least one:**
  - Upper case
  - Lower case
  - Numeric
  - Special character
- **Change every 45-60 days.**

Virus Control

Viruses

- Company-wide detection tool
- Company-wide process
- Assign responsibility in writing
- Up-to-date virus definitions
- Include employee's home systems (many people take work home and telework)

Information Security Solutions



Management: A Vital Role

Includes:

- **Defining roles and responsibility**
- **Committing necessary resources**
- **Enforcing policies and procedures**
- **Being involved**
- **(Remember: Managers are Responsible for Information Security!!)**

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:

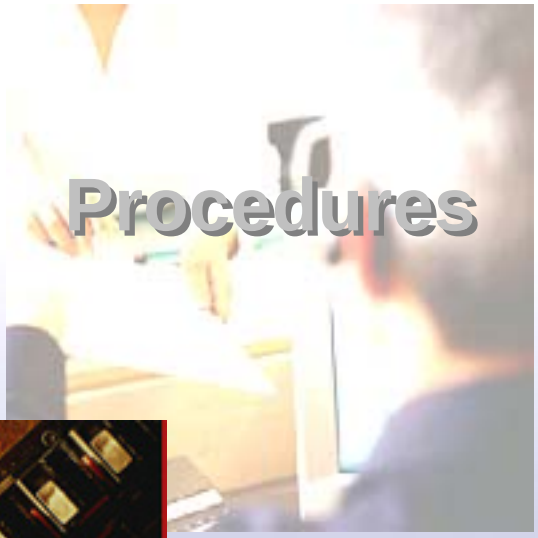
- **Pamphlets, posters, newsletters, videos**
- **Rewards for good security**
- **Periodic re-training – because people forget**

Training: Focus

- **Why InfoSec is important to the organization**
- **What the organization's InfoSec policy is**
- **What InfoSec procedures the staff is expected to follow**

It helps to focus training on the individual roles that employees have.

Best Practices: Elements



INFORMATION SECURITY

...is good Business

Survival Tools & Techniques

Information Security: Mechanisms and Technologies

8/14/2008

Security Technologies

Technology and products to:

- **Identify and authorize people**
- **Monitor computer use**
- **Protect you from Internet threats**
- **Protect you from malicious code**
- **Protect your data**

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)

Ways To Authenticate

Something you:

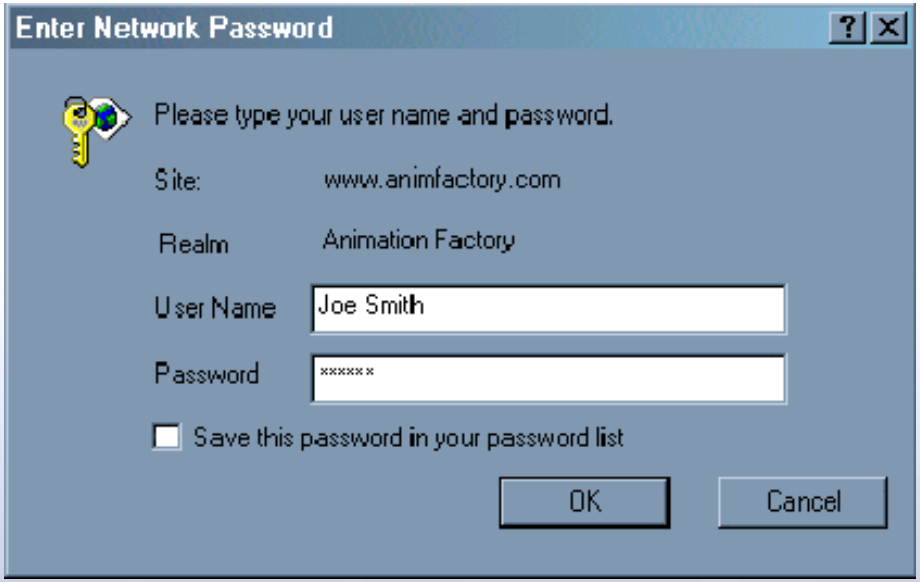
- **Know**
- **Have**
- **Are**
- **Do**

(examples follow)

Ways To Authenticate

Something you:

- **Know**
- Have
- Are
- Do



- Password
- PIN

Ways To Authenticate

Something you:

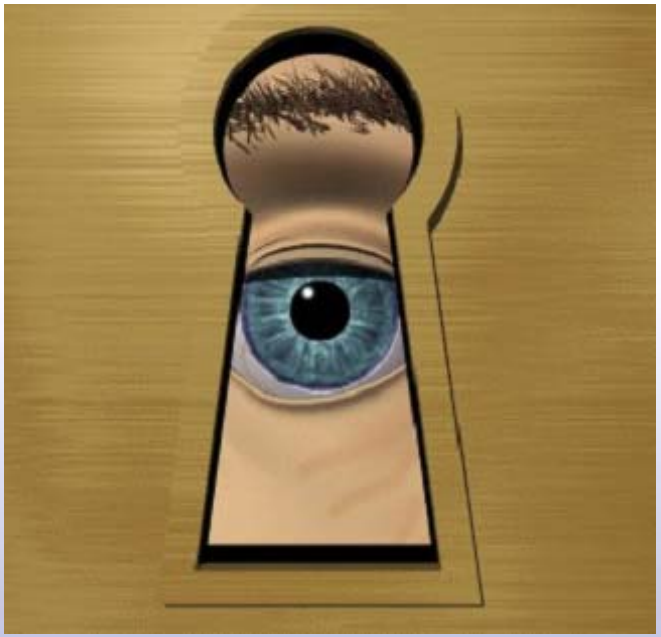
- Know
- **Have**
- Are
- Do

- Card
- Token
- Key

Ways To Authenticate

Something you:

- Know
- Have
- **Are**
- Do



- Fingerprint
- Face
- Retina or iris pattern

Ways To Authenticate

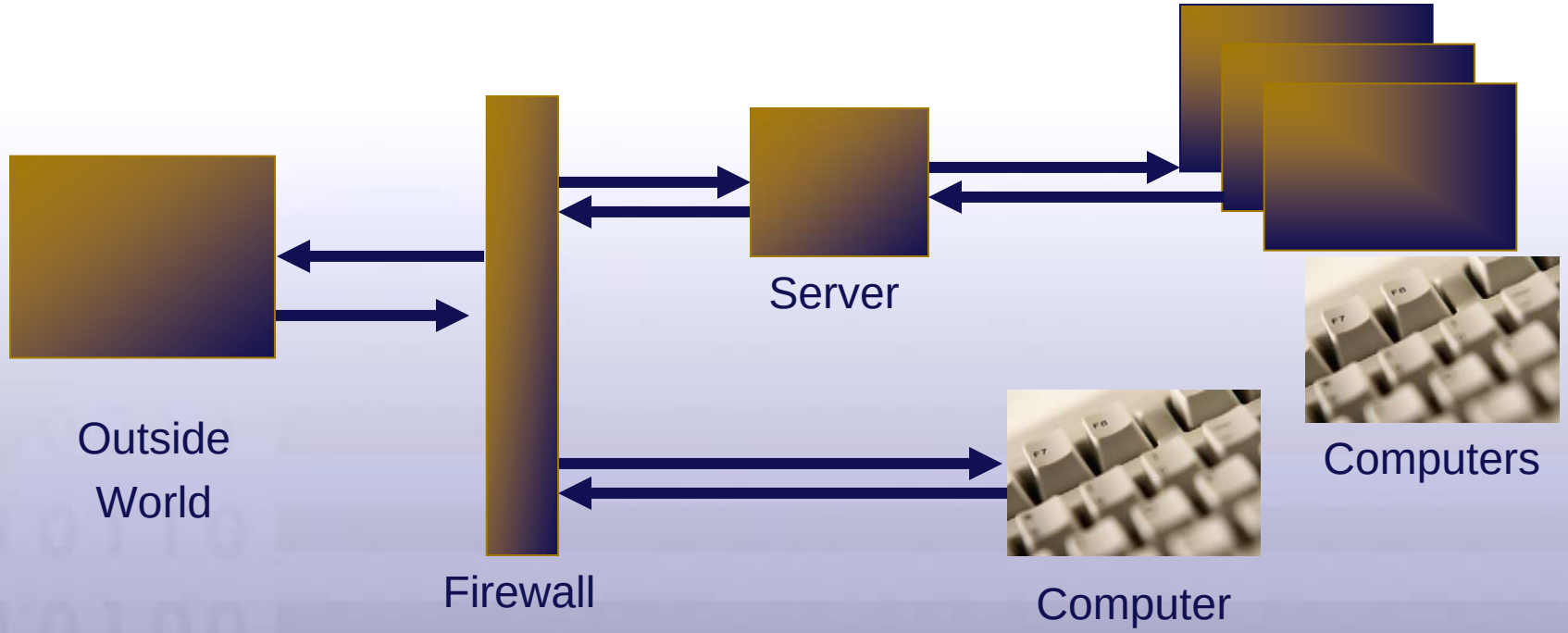
Something you:

- Know
- Have
- Are
- **Do**

- Signature
- Voice pattern
- Key stroke pattern

Firewalls (WAP? Where?)

Firewall: *Device or software, between computer and the outside world, that all traffic goes through*



SP 800-41 Guidelines on Firewalls and Firewall Policy

Other Technologies

- Data content filters (inbound/outbound/stored)
- Email filters
- Web filters
- 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, Linus – www.truecrypt.org – PGP, www.pgpi.org Pretty Good Privacy)

Basic Security Tips (Review)

- Use anti-virus software
- Update operating system and applications
- Install a firewall
- 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 RESTORE FILES)

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.

Wireless Security Precautions

- **Treat wireless network as an “Internet”**
- **Use hardware address (MAC) access control**
- **Change the default identifiers (SSIDs)**
- **Don’t Use WEP (Wired Equivalent Privacy)**
- **WPA (WiFi Protected Access) is minimum encryption to use for your wireless!!**
- **Change default keys; Change often**
- **Change your Admin password!**

SP 800-48 *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*

Other Security Resources

www.staysafeonline.info Nat. Cyber Security Alliance
For small business, home users.

www.asbdc-us.org Security Guide for Small Biz

iase.disa.mil Information Assurance Support
Free training materials, security configuration guides

www.isalliance.org Common sense infosec guides
(for Senior Managers, Home Users, Small Biz)

irtsectraining.nih.gov/ Free online-information security training – National Institutes of Health

www.ftc.gov Federal Trade Commission infosec info

Other Security Resources

NIST – eScan Security Assessment Tool

https://cip.nist.gov/sat/

The NIST eScan Security Assessment is a diagnostic tool designed to assess the electronic security infrastructure of a small business and provide an action plan for improving it. This tool will provide you with a set of recommendations to correct your security problems, helping you to develop a more secure model for future eBusiness strategies and positioning.

National Vulnerability Database (NVD) http://Nvd.nist.gov/cvss.cfm

Presenter

Richard Kissel, CISSP, CISM

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

301-975-5017
richard.kissel@nist.gov

http://csrc.nist.gov