



**Technology**  
**Privacy and Computer**  
**Network Security Risks**

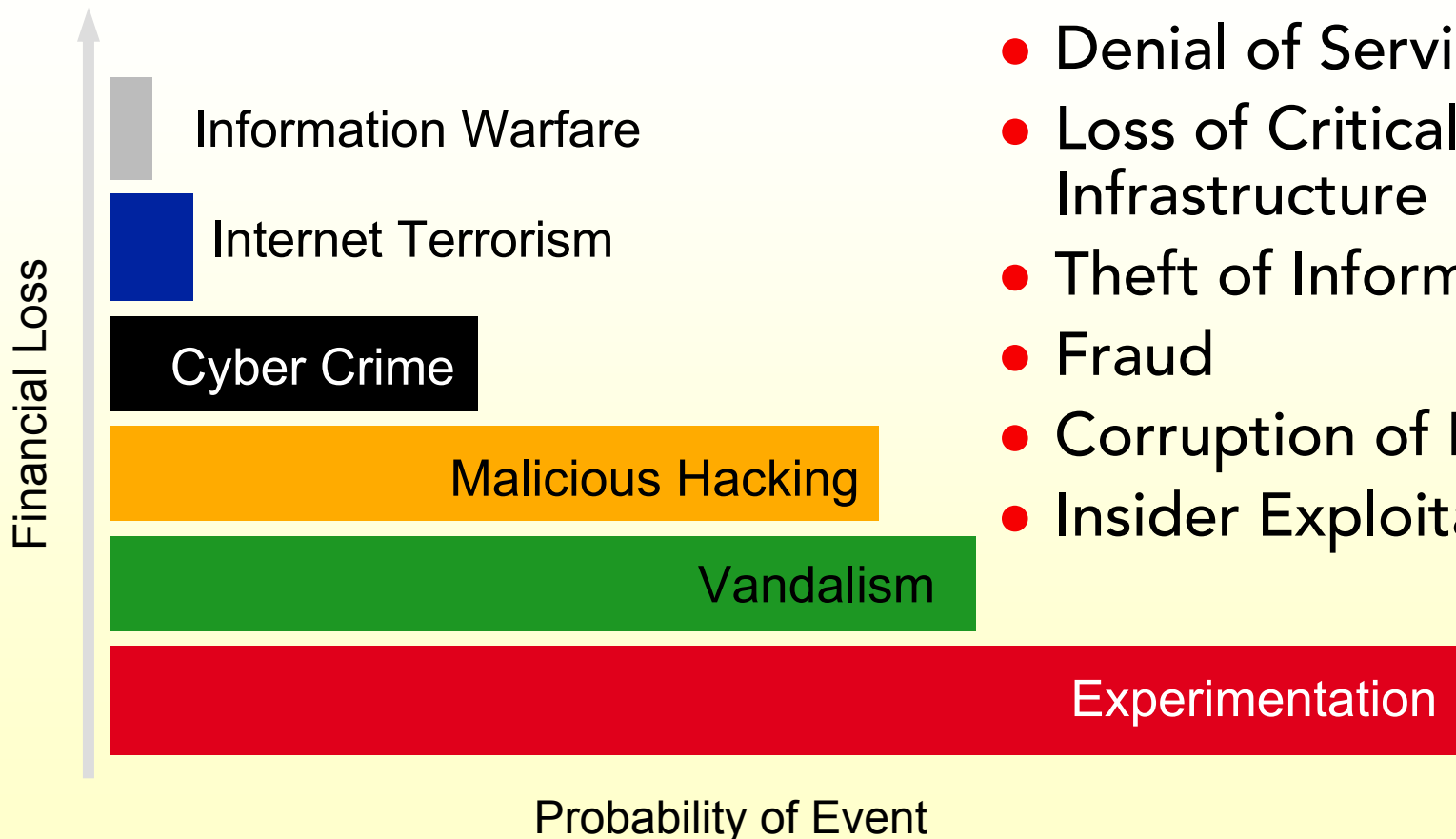
## Learning Objectives

At the end of this class, participants should be able to:

- identify most common network security and privacy liability risks facing businesses today.
- explain risk control techniques appropriate for these risks.
- discuss current insurance policy coverages and exclusions associated with these risks

# Threats to Information Security

A shift in planning assumptions ...



## Methods of Attack:

- Denial of Service
- Loss of Critical Infrastructure
- Theft of Information
- Fraud
- Corruption of Data
- Insider Exploitation

## Information Risks

---

Information risks include threats to:

- information technology systems
- intangible property handled by them

and the consequences of failure of these systems.

## Information Risks *(continued)*

---

3rd party risks - Your responsibility to others: Liability

- Privacy Injury Liability – unauthorized disclosure of sensitive or non-public private information.
- Errors and Omissions – data entry clerks, system operators, and programmers may make errors which contribute directly or indirectly to security breaches.
- Network Security – breach of others' confidential information, inability to access/use, infecting others, damage to others' information, information corruption/ reliability.
- Content Liability - you publish something disparaging or infringing – e.g., plagiarizing content, erroneous advice.

## Information Risks *(continued)*

---

Exposures to loss - 1<sup>st</sup> party risks: What can happen to you:

- Loss of data – cost to recreate data and restore network.
- Loss of business income - loss of income and extra expenses associated with containing damage, stopping attacks and implementing work-arounds.
- Electronic theft – of intangible property or system resources.
- Extortion – cost associated with responding to demands by those threatening to damage or disrupt network or release sensitive or private non-public information harvested from your network.

## Information Risks *(continued)*

---

Hazards which cause these types of losses:

- Virus/Malicious code
- Denial of service attacks
- Hacker attacks / unauthorized access
- Malicious Hardware
- Physical theft of device / media
- Accidental release
- Rogue employees
- Social engineering

## Information Risks *(continued)*

---

### Hazards - Virus/Malicious Code

- Virus - code segment that inserts itself into a program and uses that program's resources to reproduce and spread itself.
- Worms - self-contained, self-replicating program - takes advantage of known vulnerabilities and scans network for other vulnerable machines.
- Trojan Horses - non-replicating programs that appear to be useful, but actually have a hidden malicious purpose.

## **Information Risks** *(continued)*

---

### Hazards - Virus/Malicious Code

Virus/Malicious Code can be utilized for a variety of malicious purposes:

- Forwarding personal information
- Wiping out data
- Installing backdoors
- Performing Denial of Service Attacks

## Information Risks *(continued)*

---

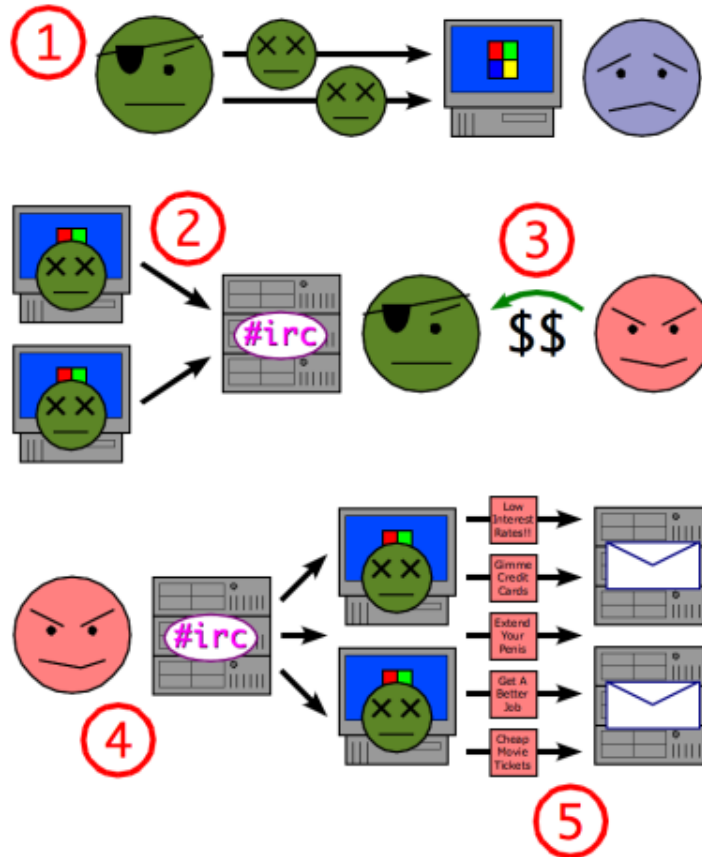
### Hazards – Denial of Service Attacks

Denial of Service Attacks (DoS) - an attacker attempts to prevent legitimate users from accessing information or services.

- The most common type of DoS attack occurs when an attacker floods a network with information:
  - » URL requests
  - » Spam e-mail messages

Distributed Denial of Service Attack (DDoS) attacker uses *backdoors* installed on the systems of others to perform a coordinated attack against a target utilizing these infected machines.

## Information Risks *(continued)*



## **Information Risks** *(continued)*

---

Hazards – Hack – Computer-based intrusion

- Hackers break into computers without authorization.
  - » Can include both insiders and outsiders.
  - » Malicious activities can include theft of information, destruction of data, sabotage.
  - » One of the leading causes of privacy breaches.

## **Information Risks** *(continued)*

---

Hazards – Hardware Hacks & Malicious Hardware

Card Skimmers

Fare cards – RFID

Virus Infected Hardware

Attacks on hardware and embedded systems

## **Information Risks** *(continued)*

---

### Hazards – Physical Theft of Device/Media

- Physical theft of desktop PCs, laptops, PDAs, tapes, disks, USB drives, other devices, and media storing data create significant risks to that data.
  - » Primary risk is that unauthorized parties will have access to sensitive or non-public private information stored on the device or media.

## **Information Risks** *(continued)*

---

### Hazards – Accidental Release

- Accidental release of sensitive or non-public / private information can occur several ways:
  - » accidentally released in electronic form via internet, Web site or e-mail.
  - » equipment or media is discarded that has not been “sanitized.”

## **Information Risks** *(continued)*

---

### Hazards – Rogue Employees

Unauthorized access to or unauthorized use of information and systems by employees can result in:

- compromise of sensitive or private non-public information
- acts of sabotage
  - » planting malicious code, such as logic bombs that destroy programs or data.
  - » compromising the integrity of, or deleting data.

## Information Risks *(continued)*

---

### Hazards – Social Engineering

Social Engineering techniques can be used to manipulate people into performing actions or divulging confidential information – i.e. tricking an individual into revealing his or her password

- Pre-texting
- Phishing, Spear Phishing and Whaling
- Trojan horse
- Quid pro quo

## Privacy Liability Exposure

<b>Number of ID theft/Privacy breaches (Feb 05 thru Feb 07)<sup>1</sup></b>	<b>Incidents 354</b>		<b>Individuals exposed ~102.1MM</b>																																			
<b>Which industries get hit the most?</b>	<u><b>Frequency</b></u>		<u><b>Severity</b></u> <b>(# of Individ. exposed)</b>																																			
<ul style="list-style-type: none"> <li>- Technology?</li> <li>- Government?</li> <li>- Health Care?</li> <li>- Data/Info Services?</li> <li>- Retail?</li> <li>- FI/Banking?</li> <li>- Education?</li> <li>- Telecoms/Media?</li> <li>- Industrial/Manf. ?</li> </ul>	<table border="0"> <tr><td>Education</td><td>33%</td></tr> <tr><td>Government</td><td>24%</td></tr> <tr><td>Health Care</td><td>11%</td></tr> <tr><td>FI/Banking</td><td>8%</td></tr> <tr><td>Retail</td><td>5%</td></tr> <tr><td>Insurance</td><td>5%</td></tr> <tr><td>Industrial/ Manf.</td><td>3%</td></tr> <tr><td>Data/Info Srvcs</td><td>2%</td></tr> <tr><td>Telecom/Media</td><td>2%</td></tr> </table>	Education	33%	Government	24%	Health Care	11%	FI/Banking	8%	Retail	5%	Insurance	5%	Industrial/ Manf.	3%	Data/Info Srvcs	2%	Telecom/Media	2%	<table border="0"> <tr><td>FI/Banking</td><td>48%</td></tr> <tr><td>Government</td><td>34%</td></tr> <tr><td>Retail</td><td>4%</td></tr> <tr><td>Education</td><td>4%</td></tr> <tr><td>Health Care</td><td>2%</td></tr> <tr><td>Insurance</td><td>2%</td></tr> <tr><td>Data/Info Svc</td><td>2%</td></tr> <tr><td>Telecom/Media</td><td>1%</td></tr> <tr><td>Industrial/Manf.</td><td>1%</td></tr> </table>	FI/Banking	48%	Government	34%	Retail	4%	Education	4%	Health Care	2%	Insurance	2%	Data/Info Svc	2%	Telecom/Media	1%	Industrial/Manf.	1%
Education	33%																																					
Government	24%																																					
Health Care	11%																																					
FI/Banking	8%																																					
Retail	5%																																					
Insurance	5%																																					
Industrial/ Manf.	3%																																					
Data/Info Srvcs	2%																																					
Telecom/Media	2%																																					
FI/Banking	48%																																					
Government	34%																																					
Retail	4%																																					
Education	4%																																					
Health Care	2%																																					
Insurance	2%																																					
Data/Info Svc	2%																																					
Telecom/Media	1%																																					
Industrial/Manf.	1%																																					

## Privacy Liability Exposure *(continued)*

Most likely cause of compromise	Incidents 354	Individuals exposed ~102.1MM
	<u>Frequency</u>	<u>Severity</u>
		<u>(# of Individ. exposed)</u>
Accidental Release/Exposure	Phys. Theft 36%	Hacking 47%
Rogue Employee	Hacking 26%	Phys. Theft 37%
Physic Theft of device/medial	Accidental 20%	Lost media 11%
Lost media	Lost media 11%	Employee act 3%
Hacking	Employee act 6%	Accidental 2%
Social Engineering	Social Eng. 1%	Social Eng. <1%

## Some industry specific considerations

---

### Healthcare

Increasingly, Protected Health Information (PHI) theft is linked to benefits and treatment fraud <sup>2</sup>

Breaches by 3rd parties account for between 30 and 40% of all breaches. <sup>3</sup>

Custody of patient financial info – Not just PHI/HIPAA related  
Custody of other's IP; drug discovery, clinical trials, informatics based research

---

### Manufacturing

Network disruption/corruption impacts deliveries and customers' ability to make money

Similar first party Business Income impact  
Custody of other's trade secret ( e.g. proprietary design, process)

---

### Retail

Custody of credit card & transaction info.  
FACTA/other regulatory exposure  
Reliance on network for inventory optimization & Just in Time supply

---

### Accountants

Custody of client private info (NPI)  
Custody of corporate client financial info,  
Custody of others trade secret ( e.g. due diligence for M&A)

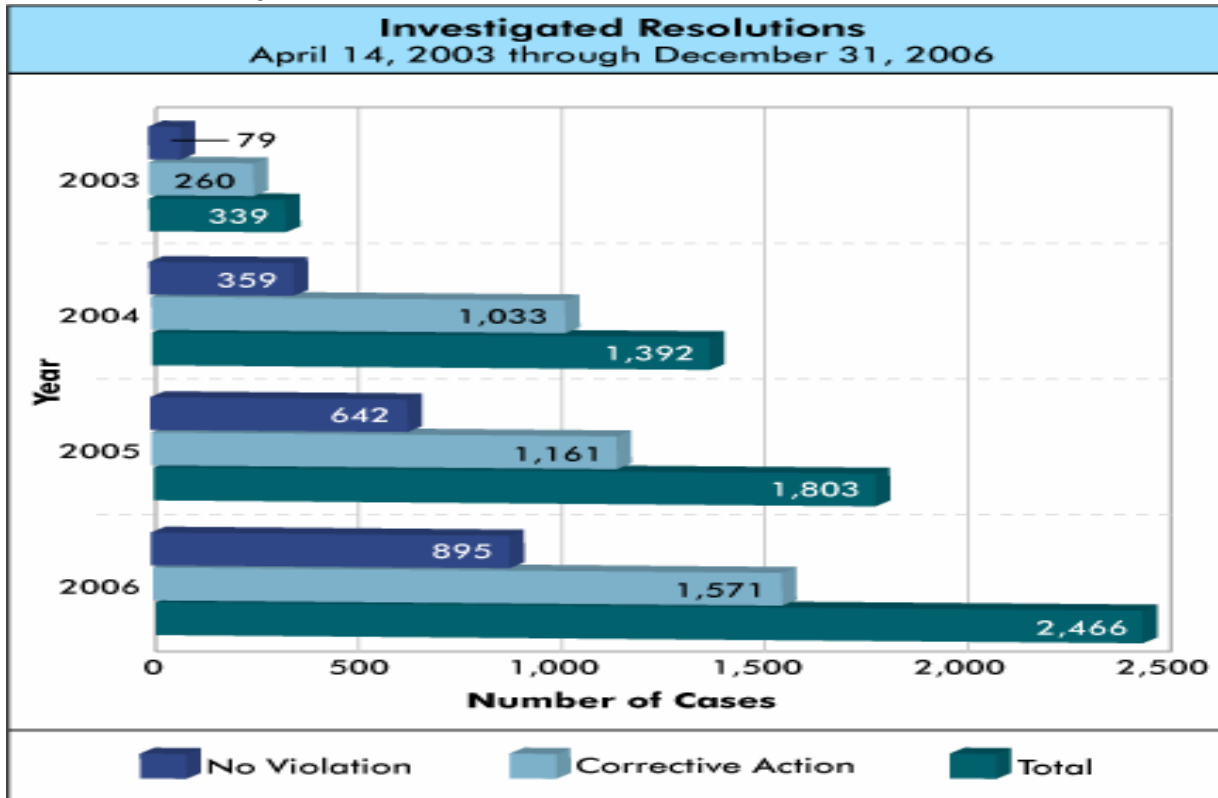
## Legislative and Regulatory Impact on Privacy Exposures

**And what about regulatory impact?**

- **HIPAA**
- **Breach Notification Laws**
- **GLBA**
- **FACTA**
- **State Merchant Laws**
- **FTC enforcement actions**

## Legislative and Regulatory Impact on Privacy Exposures

HHS Office of Civil Rights (OCR) statistics on HIPAA  
Privacy enforcement actions<sup>4</sup>



And HHS has engaged Price Waterhouse Coopers to conduct surprise audits<sup>5</sup>

## Regulatory enforcement trend is toward proactive investigations even without a breach or complaint

---

### Healthcare organizations feeling cyberattacks growing

The other pressure: The surprise HIPAA security audit from the feds

By [Ellen Messmer](#) , NetworkWorld.com , 02/27/2008

Accessed 29 April, 2008<sup>5</sup>

#### The HIPAA surprise audit

----- the specter of government regulatory probes is looming relating to the federal Security and Privacy Rules promulgated under HIPAA.

The U.S. Department of Health and Human Services (HHS), which oversees HIPAA compliance, has contracted with the firm **PricewaterhouseCoopers (PWC) to conduct surprise audits of hospitals this year**, says Gartner analyst Barry Runyon.

"It's complaint-driven," says Runyon, noting that Tony Trenkle, director of the [Centers for Medicare & Medicaid Services](#) at HHS, last month publicly said the first 10 or so reviews will be at hospitals where CMS received complaints about security.

In visiting the healthcare organization, the government regulatory probe will focus on security risks associated with remote access to data and portable storage concerns, with security managers expected to answer a lot of questions.

CMS plans to publish the results of these audits on its Web site but not the organization's name, unless it uncovers major lapses, which could result in fines or other penalties as defined under the HIPAA guidelines. Last month, Atlanta's Piedmont Hospital was revealed by HHS to be the first unannounced HIPAA security audit.

## States are enacting new laws <sup>6</sup>

---

- If you have a breach, the law in 45 States now requires you to notify affected parties.
- **IMPORTANT TO NOTE:** If affected individuals reside in other states or countries, you comply with the law where they reside. Therefore, the law in numerous jurisdictions may apply.
- Some laws establish a deadline for notification: e.g., FL requires notice within 45 days of breach, or **as quickly as 10 days** if the breach involves a contractor/vendor with custody of another business entity's data.
- Some laws, e.g. TX and WY, require you to notify **even if the data was encrypted**.
- Some laws, e.g. CA, give affected parties a right of private action. In some states, they can even recover attorneys' fees. This represents **a statutory exposure to class action litigation**.

## 25 States also now have Merchant laws <sup>7</sup>

CA, DE, FL, GA, IL, IA, KA, MD, MA, MI, MN, NV, OH, OR, PA, RI, TN, VA, DC, WA, WI

Some of these laws ( e.g. CA 1747.08 & 1725):

Restrict what information can be collected at point of sale/return in conjunction with a credit card transaction

Restrict when you can require a credit card in conjunction with other transactions ( e.g. not allowed as condition for acceptance of check payment)

Provide statutory damages for violation ( e.g. up to \$1000 each instance)

Provide for recovery of attorney's fees; another statutory exposure to class action litigation

## FTC enforcement is on the rise too... <sup>8</sup>

Since 2005, the FTC has settled 12 cases against companies for issues ranging from failure to safeguard private information to failure to comply with their own privacy policies.

Not even small "do good" firms escape the FTC's ever increasing reach.

Here's the essence of the consent order -- -

- No future misrepresentation of protective safeguards
- Maintain comprehensive security program
- Design, implement and regularly test safeguards
- **Controls on 3<sup>rd</sup> party custodians – includes contractual provisions**
- Continuous future evaluation of exposures and adjustment of controls in response
- For 20 years : Initial and biennial assessments by qualified independent auditors
- FTC gets to approve audit firms and audit results
- For 5 years: obligation to "self incriminate" --provide FTC with documents ( e.g. internal memoranda) that could indicate potential non- compliance with the consent order
- For 3 years: furnish FTC with full details on assessments
- Upon FTC demand: report in detail on manner and form of compliance with consent order

## **Information Risk Control and Transfer**

- **Risk Assessment – how do you evaluate your organizations' specific exposures?**
- **What controls are appropriate?**
- **How do you handle the residual risk?**

## **Exposure Assessment – Privacy**

---

**Do you know what sensitive or private information is in your custody along with:**

whose info it is,

where it is,

and how to contact individuals if their information is breached?

**It is important to clearly understand how sensitive information flows through your organization.**

## **Exposure Assessment – Privacy**

---

**Inventory information that you have by type and location – database servers, workstations, web servers, file cabinets, records storage facilities, etc. The following questions are useful in tracking the information flow:**

- Who sends sensitive information to the organization? - customers? other businesses? credit card companies? banks?
- How is information received by your organization? Through your website? By email? Snail mail?, Fax?, Courier?, Carrier Pigeon?, Transmitted through point of sale devices?

## Privacy Policy

---

**Privacy policies are needed for any organization handling Nonpublic Personal Information (NPI). Specific regulatory guidelines may apply:**

- **The Gramm-Leach-Bliley Act (GLBA)**– addresses consumer financial privacy
- **Health Insurance Portability and Accountability Act (HIPAA)** – addresses the privacy of personal health care information
- **Children’s Online Privacy Protection Act (COPPA)** – applies to the on-line collection of information from persons under 13 years of age

**In general, a privacy policy details what information you gather from the persons or entities that you do business with, how it is protected and the situations in which this information may be shared with a third party.**

## Privacy Policy

---

**Implement, prominently disclose and honor a privacy policy following the general guidelines provided below:**

- Design your policy with your customers in mind - be clear, direct and easy to understand.
- Say what you mean and mean what you say – basis of FTC privacy actions has been that security measures were overstated. Treat these statements the same as advertising claims you make.
- Call customer attention to any changes in policy.
- Create a culture of compliance – employee training

**Consult your attorney when drafting the specific language of your privacy policy.**

## Information Security Policy

---

### Information Security Policy

- A written statement designed to protect an organization's information assets against accidental or malicious disclosure, modification, or destruction.
  - Security objectives of preserving the confidentiality, integrity and availability of the organization's information assets.
  - Should address network access by employees, contractors or any other person with access to the company's network.
  - Should include signed acknowledgement from all to which the policy applies.

## Information Security Policy

---

Information Security Policy - key elements

- Acceptable use policy for users - password management, guidelines for accessing unprotected programs or files, disciplinary actions for unauthorized and/or unacceptable behaviors, etc.
- Policy statement for privileged (administrative) users – guidelines should be more robust for these users, covering additional areas, such as:
  - authority and conditions for monitoring user activity (e.g., e-mail, network traffic, other actions)
  - causing service disruptions
  - using vulnerability testing tools
  - accessing protected programs or files
  - disciplinary actions for unauthorized and/or unacceptable behaviors

## **Information Security - responsibility and training**

---

- A designated individual or individuals to tie individual security activities together – consider training, CISSP and CISA certifications
- Train users on your organizations privacy and acceptable use policies annually.
- Provide annual security awareness training for all users.
  - Information on how to recognize and report security threats.
  - Periodic alerts and reminders to alert employees to new threats as they emerge and to help maintain vigilance in following procedures

## Confidentiality Controls – access controls

---

- Authenticate the identity of all users prior to allowing network access.
- Define access controls based on “need to know” or “least privilege”
- Sensitive data and NPI should be segregated from non-sensitive data, and access should be restricted based on sensitivity levels.
- Centrally administer access controls w/dual sign-off for changes
- Formal procedures to revoke user access privileges as soon as possible after a change – i.e. “unfriendly” termination

## Confidentiality Controls – audit trails / chain of custody/encryption

---

- Audit trails -individual accountability, event reconstruction, intrusion detection to protect NPI
- “Chain of custody” documentation/accountability for information stored on all types of media
- Checks and balances should be in place to ensure that no person acting alone can export NPI
- NPI in transit, in storage and on removal media should be encrypted

## Confidentiality Controls – removable media

---

- Utilize content filtering to prevent export of NPI on media (e.g., iPods, PDAs, USB drives, etc.)
- For removable media exchanged with others (e.g., to data recovery centers, archival storage facilities, between locations, with vendors) also:
  - identify and track – know what sensitive info is on media or device
  - use chain of custody
  - tamper evident packaging
  - distribute encryption keys separately

## Confidentiality Controls – information retention and destruction

---

- Non-public personal information and others' sensitive information should be retained only for as long as needed.
- Develop and implement specific information retention guidelines for the data handled, stored or transmitted by your organization.
- Use appropriate sanitization methods to remove information from media (and equipment) when no longer needed – De-gauss, destroy, irreversibly erase - **DOD Standard 5220.22-M, NIST 800-88**

## Physical Security

---

- Physical access to information system components is one of the easiest ways for intruders to circumvent system protective measures.
- Social engineering techniques, such as posing as a contractor – have been used to gain access
- **Don't forget** - Physical theft or loss of hardware, laptops or media is the leading cause of privacy breaches

## Physical Security – basic controls

---

- Physical access controls for - areas containing system hardware, wiring, telecom and data lines, back up media and source documents, etc.
- Use substantial floor-to-ceiling physical barriers
- Entry point controls include locks, guards, badges, electronic access controls, etc.
- Visitor controls – sign in, badges, escort, challenge
- All desktops and PCs should be equipped with a time-out feature that locks the device and requires user logon and password entry after a period of inactivity.

## Physical Security – laptops

---

### Laptop Theft Prevention

- Laptop theft prevention policy
- Cable locks/ lockable docking stations
- Travel procedures
  - » Never leave laptops in unattended conference rooms
  - » No storage in automobile
- **Don't forget** – limit/prohibit storage of sensitive data and/or use encryption for all portable devices and media

## Physical Security – Malicious Hardware -Card Skimmers

---

**Implement a daily documented inspection of all point of sale credit card readers for evidence of tampering that might compromise the security of data gathered by these devices. Include the following as a part of this inspection process:**

- An inventory of all such devices at a given location (in store, at each gas pump, etc.).
- Acknowledgement by the employee conducting the inspection of the condition of each device at time of inspection
- Rotation of the responsibility for inspection to different employees as often as practical (limit the possibility of installation by an insider)
- Awareness training of personnel as to common indicators of tampering or covert installation of a card skimmer (additional hardware added near the legitimate card reader, miniature cameras to record pin number, etc.)
- A process to immediately remove devices which may have been compromised from service and elevate to the appropriate level of management for investigation.

## **Network Security Controls**

---

**Virus Controls**

**Perimeter Defenses**

**Configuration Management**

**Logging, monitoring and auditing**

**Security Patch Management**

## Virus Control

---

- Antivirus – Installed on all systems and up to date (automatic where possible). Executables and scripts – filter, anti-virus scan and train employees not to open or download.
- Controls on shared drives and folders – unprotected network shares = virus/worm propagation, DDoS. Disable, or create dedicated password protected directories
- Vendor neutral threat notification – Use CERT National Cyber Alert System, SANS Institute @RISK: The Consensus Security Alert, or similar
- Removal of spyware and parasitic code – run a legitimate product, periodic full system scan

## Perimeter Defenses – firewalls – configuration

- Firewall Environment - A DMZ firewall configuration is recommended to segregate important data assets from unsecured networks such as the internet.
- Firewall Policy - written policy on the determination of firewall rule sets:
  - should be updated as new vulnerabilities arise or network applications change
  - default policy for inbound traffic =block all packets and connections unless the traffic type and connections have been specifically permitted
  - factory “default” configurations should be avoided for all network security devices

## Perimeter Defenses – remote access

---

- All remote access should require user identification and authentication utilizing strong passwords.
- Encryption should be used to provide secure communication between the remote users and your networks. A Virtual Private Network (VPN) is the most common method to provide this protection.
- As part of your security policy, allow access only from other networks meeting your organization's security requirements. Using a VPN does not eliminate the need for normal precautions for off-site computers or networks.

## Perimeter Defenses – wireless access

### Perimeter Defenses – wireless access

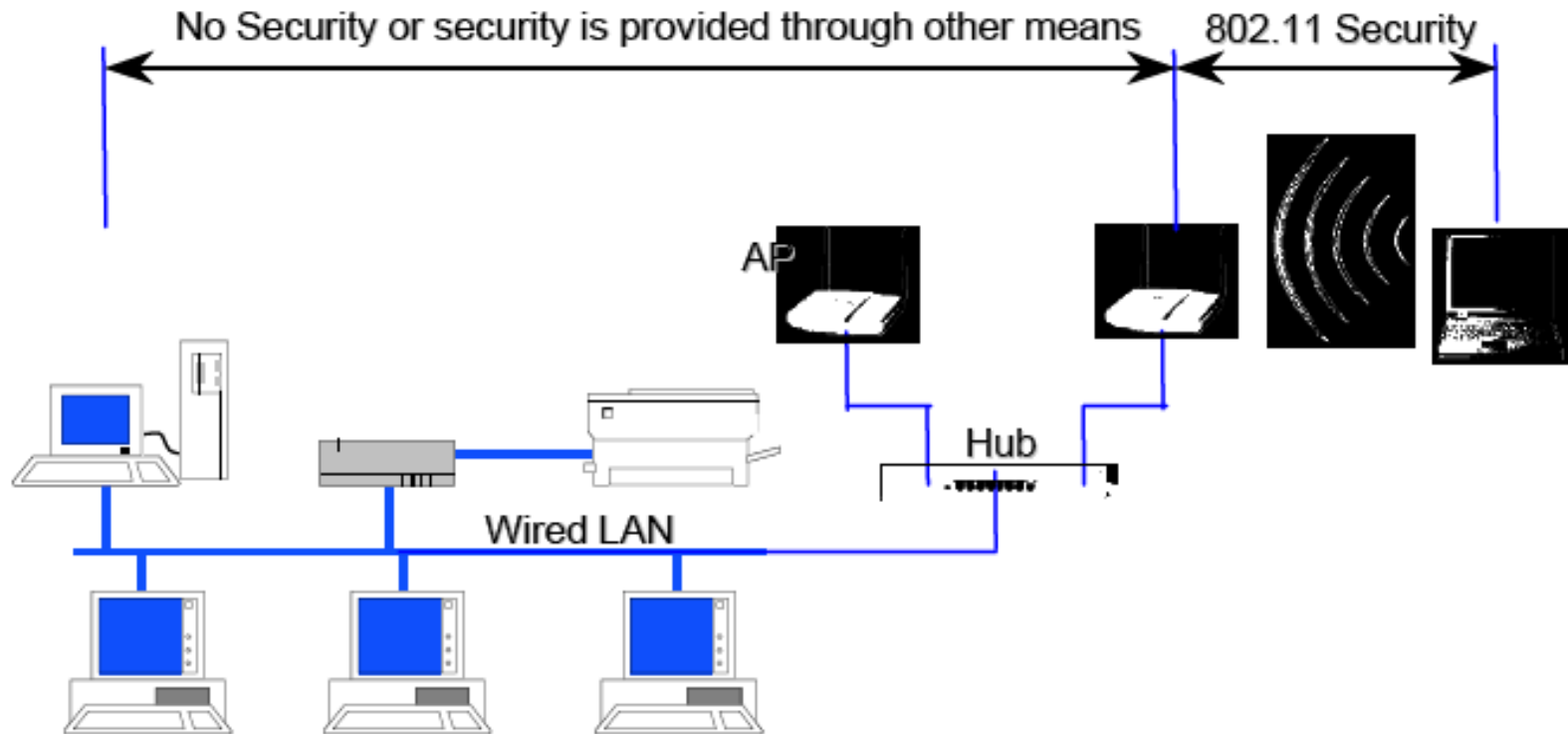


Figure 3-5. Wireless Security of 802.11 in Typical Network

## **Perimeter Defenses – wireless access – security issues**

---

- Radio links easily intercepted
- Original wireless standard (IEEE 802.11b and g) utilized Wired Equivalent Privacy (WEP) - an encryption protocol which is weak and susceptible to widely published attacks.
- Original wireless standards utilized access control and authentication methods vulnerable to man-in-the middle attacks, rouge Access Points and other compromises.

## Perimeter Defenses – wireless access – controls

---

- **Develop a formal security policy regarding use and deployment of wireless technology.**
- **Change WLAN access point Service Set Identifiers (SSIDs) and administrative passwords from factory defaults to unique values for your business.**
- **Disable access point SSID broadcast features and enable MAC address filtering.** Ensure that Access Point access control and authentication schemes are used in which both the Station and Access Point are authenticated and that user access is blocked until authentication is successful.

## **Perimeter Defenses – wireless access – controls**

---

- **Do not depend on WEP (Wired Equivalent Privacy) as a primary means of securing wireless networks. At minimum utilize Wi-Fi Protected Access (WPA).**
  - A Virtual Private Network (VPN) is also an option for securing wireless links.
- **Utilize VPNs for mobile user remote connections to corporate networks from public WLANs or hotspots.**

## Logging, monitoring and auditing

---

**For sensitive information, track and record the identity of those who access or have custody of this information; and record the time at which the access or custody takes place, including:**

- Logging all attempted access to sensitive data
- Logging successful authentication to applications or databases housing sensitive data, along with as much detail of subsequent activity as possible (files accessed, deleting records or fields, printing reports, etc.)
- Maintaining these logs in a tamper evident file and limiting access to these files for separation of duties
- Reviewing logs daily for suspicious activity

## **Configuration Management – key elements**

---

- Configuration management policy and procedures
- Documentation of baseline configuration
- Configuration change control – approval process, separation of duties
- Monitoring configuration changes
- Developers and Development tools should be not be allowed on production systems

## Security Patch Management

---

- Subscribe to patch notification services from vendors for software utilized, review and evaluate at least weekly, preferably daily.
- Test and install critical security patches and upgrades within 24 hours of availability and no later than 30 days for all patches.
- Automatic update of applications whenever possible and appropriate.
- Verification of vulnerability remediation through network and host vulnerability scanning.

## Disaster Recovery / Incident Response - IT continuity plan

Key steps in developing an Information Technology continuity plan

- Conduct a business impact analysis -identify critical IT resources outage impacts, allowable outage times (critical IT resources within 24hrs)
- Identify preventive controls -back up power, fire suppression, redundant air conditioning, etc. The following preventive controls are considered key:
  - » back up network data and configuration files daily
  - » store back-up data in a secure and protected off-site location.
- Develop/document the recovery strategy.
- periodically test and maintain the plan.

## Computer Security Incident Response Plan

---

Implement a response plan that addresses direct (such as hacking), indirect (e.g. virus and malicious code) and denial of service attacks. Test these plans at least annually. The major phases in the incident response process are:

- **Preparation – response policy, reporting and communication procedures**
- **Detection and Analysis – procedures for accurately detecting and assessing possible incidents, detecting when an incident has occurred, and determining the type, extent and magnitude of the problem.**
- **Steps for containment and eradication of the threat and recovery to normal operations**

## Privacy/Confidentiality Breach Response Plan

---

**Develop and implement a plan to respond privacy breaches. Test these plans at least annually. Basic elements of this plan should include:**

- Designated senior member of your staff to coordinate and implement the response plan
- Provision for immediate investigation of the incident
- Steps which should be taken to contain the breach and close off existing vulnerabilities or threats to sensitive information
- Details of who should be notified in the event of a breach. May include law enforcement, insurance carrier, customers, credit bureaus, and other businesses that may be affected by the breach.

## Legal and Contractual Controls

---

### Legal and Contractual Controls

- Contracts / Risk Transfer
- Editorial / Content Control



## Contracts / Risk Transfer

---

Require the following of any third party to which sensitive or non-public personal information is entrusted:

- Signed agreement regarding access to and appropriate use of your information and networks.
- Contractual compliance with your organization's information security standards.
- Compliance with contract requirements should be audited on a regular basis.

## Contracts / Risk Transfer

---

- Assure that written contracts adequately define the parties' responsibilities in regard to insurance and indemnity-appropriate protection for the information risks
- The expertise of attorney conversant with the legal issues relating to the subject matter should be utilized when drafting these agreements.

**Attention to 3<sup>rd</sup> party controls is rapidly increasing in importance:**

- **30-40% of all privacy breaches are attributed to 3<sup>rd</sup> parties<sup>3</sup>**
- **Requirements of recent FTC consent orders include these requirements**

## Editorial / Content Control

---

Web site and other electronic content should be reviewed by legal counsel prior to the public launch of new content to preclude claims of:

- Libel
- Slander
- Privacy invasion – including false light
- Violation of privacy law or regulation
- Intellectual property rights infringement

## Editorial / Content Control

---

- Linking - comply with the site owner's published policy and warn that 3<sup>rd</sup> party privacy policies may differ from your own
- Obtain written permission or rights to use content obtained from 3<sup>rd</sup> parties and credit authors for portions of their work used in your content
- Perform clearance checks on marks and brands displayed on your Web site and obtain written permission to use marks and brands of others.

## Editorial / Content Control

---

Activities which raise risk of content injury claims:

- use of trademarks, brands or proprietary information of others in meta-tags
- “framing” the site content of others on your Web site
- “deep linking” to others’ content
- providing chat rooms, forums, blogs or other services involving the exchange of the content of others

## Editorial / Content Control – terms of use and disclaimers

---

The following should be displayed on all Web sites:

- Terms of Use – rules developed by a qualified attorney to protect intellectual property and govern how the site is used.
- Disclaimers (e.g., no warranty on accuracy, quality, reliability, fitness for a specific purpose, “use at your own risk”) for:
  - » Web site content / information
  - » Advice provided via your Web site
  - » Content provided by others or on sites to which you link
- Privacy policy - must explain the information collected about Web site users, how the information is shared, used, and protected.

## **Information Risk – Insurance Considerations**

### **Potential Gaps in Coverage:**

- Commercial General Liability
- First Party

### **Information Risk Coverage – What to look for:**

- General consideration
- 3<sup>rd</sup> party – Liability – important coverage parts
- First Party – important coverage parts

## **Exposures that may not be addressed by CGL**

---

- **Breach of privacy due to hacking or other "non-publication" related disclosure**
- **Damage to others intangible property (data is not tangible)**
- **Violation of privacy/private occupancy right via invasive, unsolicited content or software ( e.g. SPAM and Spy-ware)**
- **Related non-advertising intellectual property infringement (except patent or trade secret)**
- **Web sites that include editorial content (e.g., medical advice, white papers, blogs) that would fall outside the definition of "advertisement"**
- **Detention by hijacking, re-direction, etc.**
- **Libel, slander, disparagement via e-mail, or other non-advertising electronic utterance**
- **Infringement arising from framing, linking, meta-tag content**
- **Insureds who publish content in other electronically readable non-internet form (e.g., webcasts, DVDs, CD-ROMs)**

## Potential Gaps in First Party Coverage

---

- **Data is not tangible property.**
- **Triggered by named perils - not virus or hacking**
- **Requires “direct” physical loss.**

## Information Risk Coverage – what to look for

---

- **Menu or modular based structure – buy only what you need**
- **Occurrence – first party**
- **Claims made – third party - Wrongful acts triggers**
- **Worldwide coverage**
- **Punitive damages where legally permissible with most favorable venue**
- **Governmental/regulatory actions – where allowed (privacy regulatory defense)**
- **Vicarious liability for wrongful acts of others –**
- **No "Escape Valve" exclusions e.g. "Failure to maintain" – seek very specific criteria**
- **Clear definitions for loss and method for calculating loss**

## Coverage parts – what to look for

---

### 3<sup>rd</sup> Party - Liability

Privacy Injury

Privacy Regulatory  
Proceeding

Public Relations &  
Regulatory Expense

Network Security  
Liability

Content Injury or  
Broad Form Media

### 1<sup>st</sup> Party

Network Extortion

Network loss/damage

Business Interruption &  
Extra Expense

Emergency  
Response Fund

Electronic Theft

## **Privacy Injury Coverage (Private Actions) – what to look for**

---

**Coverage for:**

**All private and corporate confidential information**

**Online and offline** – including the dumpster

**All privacy laws** – **current and future** – **world-wide**

**Removable media** – **on and off-premises**

**rogue employees**

**Any unauthorized use/disclosure**

**Alleged use of spam or spy-ware**

**Emotional distress**

**Triggers: security breach, unauthorized access, and mistakes**

## **Privacy Regulatory Proceeding Coverage (Governmental Actions)– what to look for**

---

**Coverage for:**

**Defense of privacy regulatory actions**

**At full privacy coverage limits (typically)**

**Where permitted by law**

## Public Relations Expense - what to look for

---

**Coverage for:**

**"Duty to notify" compliance cost**

**Credit monitoring cost**

**Public relations expense – repair reputation**

**Remediate regulatory compliance deficiency**

**No deductible – low co-insurance**

**Fast response – 24/7 claim hotline**

## Network Security Coverage - what to look for

---

**Coverage for:**

**Inability to access/use/rely on your network or data**

**Damage to or disruption/infection of others**

## Content Injury Coverage - what to look for

---

### Coverage for:

- **Unintentional:**
  - Libel, slander, disparagement
  - False light
  - Publicity right infringement
  - Infringement of title, slogan, trade name, trademark
  - Copyright infringement (including software)
- **Related unfair trade practice**
- **Covered medium is "any computer readable form" (e.g. internet, web, e-mail, all "Electronic Media" – CD-ROM, Flash, Thumb-drive, tapes, diskettes, etc.)**
- **Not limited to "your advertising" or content prepared by or for you**
- **Covers linking to and/or use of third party content**
- **Broad form is available (print, broadcast media, etc.)**

## 1<sup>st</sup> Party – Network Extortion Coverage - what to look for

---

### Coverage for:

- **Triggers: "Exploit" by an insider or outsider:**
  - Virus/malicious code
  - DOS
  - Hacking
- **Cost to restore network to (substantially) pre-loss condition**
- **Cost to recreate data since (usable) last back-up**
- **Actual loss sustained – generally, extra expense to recover beyond operating expense**

## 1<sup>st</sup> Party – Network Loss or Damage Coverage - what to look for

---

### Coverage for:

- **Triggered by extortionist's demand in exchange for not implementing a threat:**
  - **To damage or disrupt insured network**
  - **To release information harvested by perpetrator**
- **Must involve an act perpetrated via insured's network**
- **Pays if demand is less than cost to prevent or recover, if threat is executed**

## 1<sup>st</sup> Party – Business Interruption and Extra Expense - what to look for

---

### Coverage for:

Loss of **online and offline income** if network dependent

**Insider acts**

**Dependent loss** coverage for network services (not Telco, ISP, Infrastructure)

Extra expense – outside cost or additional expense beyond normal operating cost

Specifically to mitigate loss

Cost of workarounds or short-term measures to expedite recovery

## **1<sup>st</sup> Party – Emergency Response Fund - what to look for**

---

### **Coverage for:**

**No Deductible – low co-insurance**

**Cost to hire an expert security firm or  
rapid response team to:**

- **Stop attacks**
- **Contain damage**
- **Prevent escalating loss**
- **Capture evidence**

## 1<sup>st</sup> Party – E-theft – basic, of services and of intangible property - what to look for

---

### Coverage for:

#### Basic

Theft of **your** money, securities, goods, if theft is via your network

Theft of saleable goods (e.g. retail inventory, supplies, etc.)

#### Services

Theft or diversion of **your** fee-bearing services via your network

#### Intangible Property

Unauthorized access to **your** intellectual property (e.g. **trade secret**)

**Actual economic value of IP asset** – not merely the cost to replace/re-create data.

## Summary

---

Computer attacks are increasing in frequency, severity and efficacy.

A risk management approach combining:

- people
- policies
- technology

Insurance may be implemented.



---

# Questions

## Learning Objectives

Can you:

- identify most common network security and privacy liability risks facing businesses today.
- explain risk control techniques appropriate for these risks.
- discuss current insurance policy coverages and exclusions associated with these risks.

## Information Risk Controls

---

Resources for further information:

Privacy Rights Clearinghouse

<http://www.privacyrights.org/>

United States Computer Emergency Readiness Team

<http://www.us-cert.gov/>

SANS Institute – see resources page – *Reading Room*  
and *The Security Policy Project*

<http://www.sans.org/>

Internet Security Alliance – see *Best Practices*

<http://www.isalliance.org/>

## **Information Risk Controls** *(continued)*

---

National Institute of Standards and Technology  
Computer Security Division's Computer Security  
Resource Center

<http://www.csrc.nist.gov/>

Database of information security professionals certified  
by (ISC)2

[https://www.isc2.org/cgi-  
bin/directory.cgi?displaycategory=503](https://www.isc2.org/cgi-bin/directory.cgi?displaycategory=503)

Information Systems Audit and Control Association

<http://www.isaca.org/>

Netlitigation, Internet Law: News Suits and Discussion

<http://www.netlitigation.com/>

## Data Sources

---

1. Privacy Rights Clearinghouse Chronology of Data Breaches, 2005-2007, viewed February 2007 at <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>.
2. National Committee on Vital Health Statistics Subcommittee on Privacy and Confidentiality. " *Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments*." Testimony of Pam Dixon, Executive Director, World Privacy Forum, San Francisco, California, August 16, 2005.
3. 2007 Annual Study: US Cost of Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, A study summarizing the actual costs incurred by 35 US organizations that lost confidential information and had a regulatory requirement to publicly notify affected individuals, Benchmark research conducted by Ponemon Institute, LLC, November 2007.
4. <http://www.hhs.gov/ocr/privacy/enforcement/numbersglance0407.html>. United States Department of Human and Health Services. Numbers at a Glance
5. "Healthcare organizations feeling cyberattacks growing, The other pressure: The surprise HIPAA security audit from the feds By [Ellen Messmer](#), NetworkWorld.com, 02/27/2008. Accessed 29 April, 2008.
6. State Notification Laws. Scott and Scott LLP, Perkins Coie, Proskauer Rose LLP, CSO Reporting Map last updated: 2/12/2008, <http://www.csoonline.com/read/020108/ammmap/ammmap.html>.
7. Privacy Rights Clearing House, accessed 30 April, 2008, <http://www.privacyrights.org/index.htm>
8. Federal Trade Commission, Privacy Initiatives, Unfairness and Deception, Enforcement cases [http://www.ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html)

The image features the CNA logo, which consists of the letters 'CNA' in a bold, italicized, red sans-serif font. The letters are slanted to the right. The 'C' is a simple, rounded shape. The 'N' is formed by two vertical bars connected at the top and bottom by a diagonal bar. The 'A' is a simple, rounded shape. The entire logo is centered horizontally on a white background. There is a solid grey horizontal bar at the top of the page.

**CNA**