

# Security Breaches and Investigation

# Agenda

- Current and expected security breach trends
- Types of security breaches
- Information security laws
- Private industry security compliance requirements
- Security breach laws
- Actions taken and security breach response guidelines
- Law enforcement involvement
- Business and legal implications of security breaches
- Security breach handling methodology
  - Prevention
  - Detection
  - Containment
  - Investigation (manual and digital)
  - Resolution and reporting
- Live digital security breach and investigation demonstration

## What is a Security Breach?

- Acts that bypass existing security policies, procedures and controls of an organization.
- Security breaches focus on the compromise of data that can create a reasonable risk of harm.

## Current and Expected Security Breach Trends

Financial losses from security breaches have increased from the previous years.

The highest dollar amount losses were related to the following types of security attacks:

- Financial fraud
- Customer and proprietary data
- Outsider system penetration

## Current and Expected Security Breach Trends

- More of the perpetrators of security breaches and computer crime cases are motivated by monetary gain.
- The use of targeted attacks is increasing. This type of attack is also more difficult to detect.
- The development and use of malicious software is increasingly more sophisticated.
- New types of security threats are emerging.

## Current and Expected Security Breach Trends

- The protection provided by existing technologies (e.g., virus software, firewalls) are increasingly less capable of controlling security breaches.
- Insider abuse of network system access is increasing.
- The theft of laptops and mobile devices is increasing.

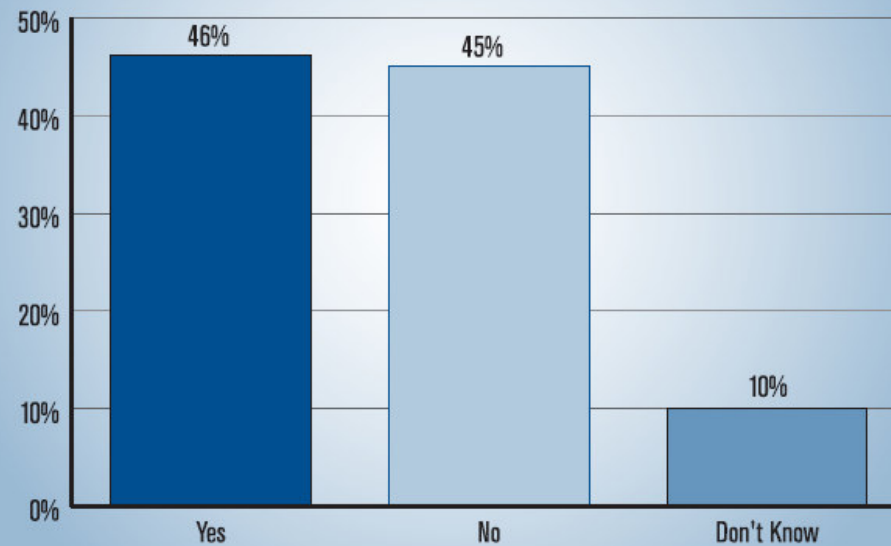
# Current and Expected Security Breach Trends

- The number of organizations that are reporting security breaches to law enforcement is increasing.
- The majority of the organizations assign a small portion of their IT budget to security measures that can assist controlling security breaches.

# Current and Expected Security Breach Trends

**Figure 11. Did Your Organization Experience a Security Incident in the Past 12 Months?**

By Percent of Respondents  
(Numbers do not add up to 100% due to rounding.)



CSI 2007 Computer Crime and Security Survey  
Source: Computer Security Institute

2007: 487 Respondents

## Type of Security Breaches

| TYPE OF ATTACK  | 2007 | TYPE OF ATTACK   | 2007 |
|---|------|--|------|
| ■ Insider abuse of Net access   | 59%  | ■ Financial fraud  | 12%  |
| ● Virus   | 52%  | ☆ Password sniffing**                                      | 10%  |
| ◇ Laptop / mobile device theft  | 50%  | ■ Web site defacement*                                     | 10%  |
| ★ Phishing where your organization was fraudulently represented as sender** | 26%  | △ Misuse of public Web application*                        | 9%   |
| ☆ Instant messaging misuse**  | 25%  | ◆ Theft of proprietary information (intellectual property) | 8%   |
| ■ Denial of service   | 25%  | △ Exploit of the organization's DNS server**               | 6%   |
| ▲ Unauthorized access to information  | 25%  | ▲ Telecom fraud  | 5%   |
| ● Bots within the organization**  | 21%  | ● Sabotage   | 4%   |
| ★ Theft of customer / employee data**                                       | 17%  |  |      |
| ◆ Abuse of wireless network*  | 17%  |  |      |
| ○ System penetration  | 13%  |  |      |

\*Added in 2004 survey  
\*\*Added in 2007 survey

CSI 2007 Computer Crime and Security Survey  
Source: Computer Security Institute

2007: 436 Respondents

Insider abuses of the network access increased from 42% to 59%

Laptop and mobile device theft increased from 47% to 50%

Viruses decreased from 65% to 52%

Unauthorized access to information decreased from 32% to 25%

# Information Security Laws

## Federal Law

### Gramm-Leach-Bliley Act (GLBA)

Applies to “financial institutions” as defined by the law, that is, institutions “significantly engaged” in “financial activities.”

Applies not only to banks, securities firms, and insurance companies, but also to other institutions providing many other types of financial products and services to consumers.

# Information Security Laws

## Federal Law

### Gramm-Leach-Bliley Act (GLBA)

The law is enforced by several regulatory agencies such as the FDIC, the OCC, OTS, and the Federal Reserve.

Non-traditional financial institutions, for example universities, that are covered by the GLBA are regulated by the FTC.

Each regulatory agency has issued regulations and guidance under the GLBA.

# Information Security Laws

## Federal Law

### Gramm-Leach-Bliley Act (GLBA)

Financial institutions are required to follow standards set forth by the regulatory agencies to protect the security, confidentiality and integrity of non-public customer information through administrative, technical and physical safeguards.

Prohibits financial institutions from sharing any information that is non-public with nonaffiliated third parties.

# Information Security Laws

## Federal Law

### Gramm-Leach-Bliley Act (GLBA)

The security program should address monitoring systems and procedures to detect actual and attempted attacks or intrusions into information systems that contain non-public customer information.

The security program should include a response program that specifies the actions to be taken when the institution detects that unauthorized individuals have gained access to information systems that contain customer information.

The response should include reporting to regulatory and law enforcement agencies.

# Information Security Laws

## Federal Law

### Health Insurance Portability and Accountability Act (HIPAA)

This law applies to certain entities that handle confidential medical information. The law requires the preservation of the security, integrity and privacy of confidential medical information.

HIPAA is enforced by the U.S. Department of Health and Human Services (HHS). HHS has issued regulations that require covered entities to ensure the protection of patient information through administrative, technical and physical safeguards.

HIPAA regulations provide a framework for how security should be managed for any facility that creates, accesses, shares or disposes of patient information.

# Information Security Laws

## Federal Law

### Fair and Accurate Credit Transaction Act (FACT Act)

In 2003 the United States Congress reacted to the increasing problem of identity theft by amending the Fair Credit Reporting Act with sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act).

# Information Security Laws

## Federal Law

### Fair and Accurate Credit Transaction Act (FACT Act)

In November of 2007 several Federal agencies issued their joint final rules and guidelines concerning “Identity Theft Red Flags and Address Discrepancies.”

The agencies include the OCC, Board of Governors of the Federal Reserve System, FDIC, OTS, NCUA, and the FTC.

The joint final rules and guidelines became effective on January 1, 2008.

The mandatory compliance date for these final rules is November 1, 2008.

# Information Security Laws

## Federal Law

### Fair and Accurate Credit Transaction Act (FACT Act)

The new regulations impact financial institutions and creditors such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies that offer or maintain one or more covered accounts.

# Information Security Laws

## Federal Law

### Fair and Accurate Credit Transaction Act (FACT Act)

The new rules and guidelines require the following primary components:

Development, implementation and enforcement of an Identity Theft Prevention Program

Performance of on-going and comprehensive risk assessments

Development of specific policies, procedures and practices to combat identity theft issues

Training for entity personnel

Management and oversight of the Program

Oversight of service providers

# Information Security Laws

## Federal Law

### Federal Trade Commission Act (FTC Act)

Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”

The FTC guards against deception by enforcing companies’ privacy promises (implicit or express) regarding collection, use, and security of consumers’ personal information.

The FTC also has used its authority to challenge information security practices that cause substantial consumer injury.

# Private Industry Security Compliance Requirements

## Payment Card Industry Data Security Standard (PCI-DSS)

Visa Int'l, MasterCard Worldwide, American Express, Discover Financial Services, and JCB formed the PCI SCC.

It is an independent industry standards body providing oversight of the development and management of Payment Cards Industry Security Standards on a global basis.

Ensure cardholder data safeguarding.

Standardize protection against fraudulent activities.

# Security Breach Laws

**Most states have enacted security breach laws.**

## **Florida Security Breach Notification Law**

The Florida Statute § 817.5681 requires organizations to notify clients within 45 days of a security breach, if it is reasonably believed that the unencrypted personal information of a Florida resident has been acquired by an unauthorized person.

Failure to do so can result in a fine from \$1,000 per day to a maximum fine of \$500,000.

# Security Breach Laws

## Florida Security Breach Notification Law

The timing of the notice may be delayed upon the request of law enforcement if notification would jeopardize a law enforcement investigation.

Organizations will be deemed to be in compliance with the Florida law if they comply with notification procedures under their federal regulatory agency's guidelines.

# Actions Taken after a Security Attack

- Attempt to identify perpetrator
- Improve their security controls
- Report the security breach to legal counsel
- Report the security breach to law enforcement

# Security Breach Response Guidelines

Institutions should have a sound incident response program.

Take appropriate actions to ensure the contracts with service providers clearly specify the actions that need to be taken to address incidents of unauthorized access including notification to the institution.

Assess the nature and scope of the incident.

Identify the type of data, including customer information, that have been accessed or misused.

## Security Breach Response Guidelines

Notify primary Federal regulator, when applicable, as soon as possible when the organization becomes aware of an incident involving unauthorized access to sensitive customer information.

Notify appropriate law enforcement authorities and filing a timely SAR in situations involving Federal criminal violations.

Take appropriate steps to contain and control the incident as well as prevent further unauthorized access to sensitive information.

## Security Breach Response Guidelines

Preserve relevant records and evidence.

Conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.

Notify customers when warranted even when they use the service of service providers.

# Security Breach Response Guidelines

The institution may limit notification to affected customers.

Customer notification can be delayed if law enforcement determines that release of this information will interfere with a criminal investigation.

Customer notification should be given in a clear and conspicuous manner.

Customer notification should outline the incident, type of information subject to the unauthorized access and the actions taken to protect the information from further unauthorized access.

## Law Enforcement Involvement

| Type of Crime  | Investigative Law Enforcement Agencies   |
|--|--|
| Computer Intrusion (i.e. hacking)  | FBI local office<br>U.S. Secret Service<br>Internet Crime Complaint Center (T2)  |
| Counterfeiting of currency   | U.S. Secret Service  |
| Internet fraud and SPAM  | FBI local office<br>U.S. Secret Service (Financial Crimes Division)<br>Federal Trade Commission (online complaint)<br>Securities and Exchange Commission (online complaint)<br>The Internet Crime Complaint Center |
| Internet harrassment   | FBI local office   |
| Password Trafficking   | FBI local office<br>U.S. Secret Service<br>Internet Crime Complaint Center (T2)  |
| Child Pornography or Exploitation  | FBI local office<br>if imported, U.S. Immigration and Customs Enforcement<br>Internet Crime Complaint Center   |
| Child Exploitation and Internet Fraud matters that have a mail nexus         | U.S. Postal Inspection Service<br>Internet Crime Complaint Center  |
| Internet bomb threats  | FBI local office<br>ATF local office   |
| Trafficking in explosive or incendiary devices or firearms over the Internet | FBI local office<br>ATF local office   |

Law enforcement should be involved when:

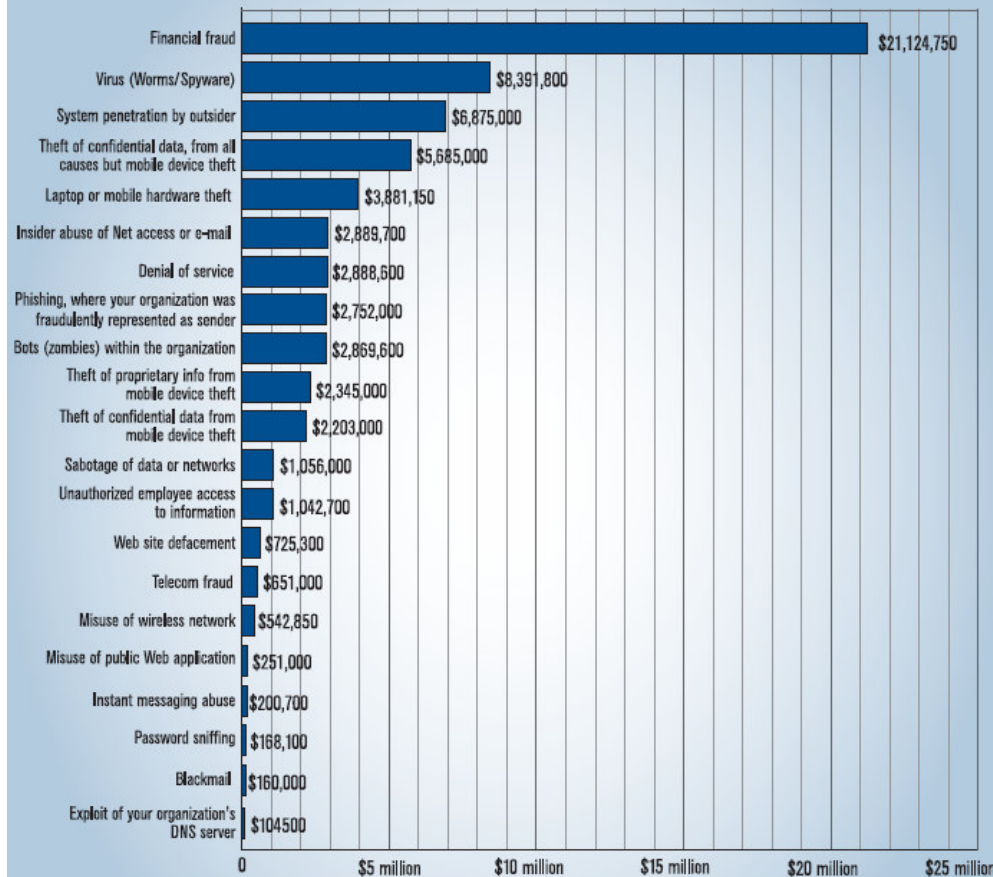
A technological crime was committed.

A traditional crime such as financial fraud was committed.

Source: United States Department of Justice - <http://www.usdoj.gov/criminal/cybercrime/reporting.htm>

# Business and Legal Implications of Security Breaches

**Figure 16. Dollar Amount Losses by Type of Attack**



CSI 2007 Computer Crime and Security Survey  
Source: Computer Security Institute

2007: 194 Respondents

The total financial losses in 2007 was 27% more than during 2006.

## **Business and Legal Implications of Security Breaches (cont.)**

### Business Impact – Florida

A front desk office coordinator at Cleveland Clinic, Weston, Florida, improperly obtained Medicare information and other demographic information about Cleveland Clinic patients and sold the information.

The investigation revealed that the Medicare numbers were later used by medical providers in Miami to fraudulently bill Medicare for services not rendered and equipment not supplied, resulting in a \$7 million fraud to Medicare.

The defendant pled guilty to computer fraud, conspiracy to commit identity theft and conspiracy to wrongfully disclose individually identifiable health information.

## **Business and Legal Implications of Security Breaches (cont.)**

### Business Impact – Florida

A Colombian citizen pled guilty to a 16-count indictment involving a complex computer fraud scheme victimizing over 600 people.

The defendant engaged in a complex series of computer intrusions, aggravated identity thefts and credit card frauds designed to steal money from payroll, bank and other accounts of their victims.

The defendant engaged in a conspiracy that began with illegally installing keystroke logging software on computers located in hotel business centers and internet lounges around the world. This software would collect the personal information of those who used the computers, including passwords and other personal identifying information the victims used to access their bank, payroll, brokerage and other accounts online.

# Business and Legal Implications of Security Breaches (cont.)

## Business Impact – Florida

Law enforcement officials in Florida arrested six individuals suspected of carrying out a fraud scheme built around the misuse of credit card data stolen from retailer TJX Companies.

The expected financial losses and other business implications are significant.

## **Business and Legal Implications of Security Breaches (cont.)**

### Business Impact – California

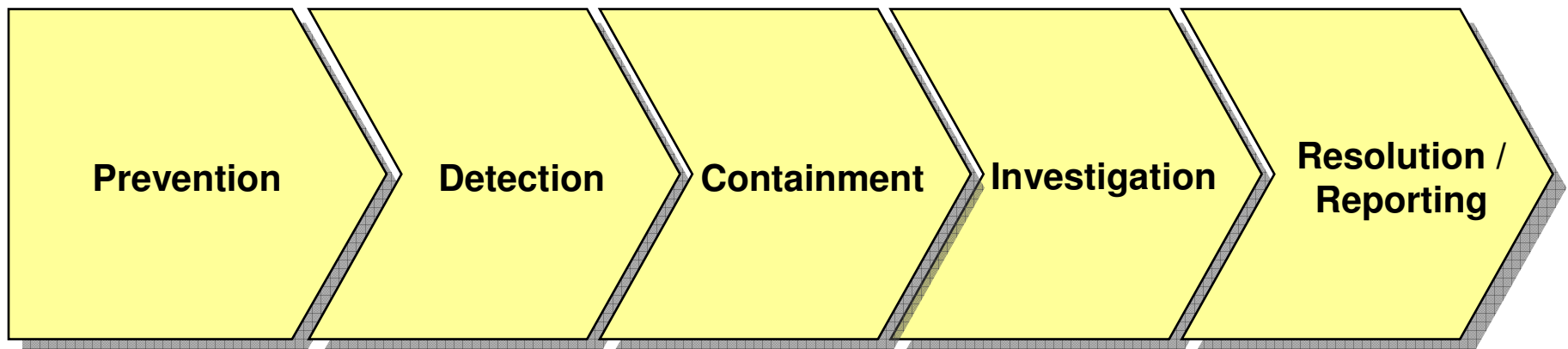
A computer security consultant and several associates developed malicious computer code and distributed that code to vulnerable computers.

The computer security consultant and the others used the illicitly installed code to assemble armies of up to 250,000 infected computers, which they used engage in a variety of identity theft schemes.

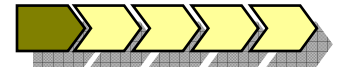
The defendant also used the compromised computers to defraud banks and an advertising company.

# Security Breach Handling Methodology

The overall security breach handling methodology has the following 5 phases:



# Security Breach Handling Methodology Prevention

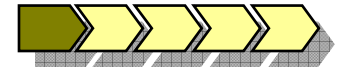


The main goal of this phase is to understand the overall company infrastructure, not only from the informational point of view, but also from the attacker point of view.

## Information View

- The technology, information systems and security infrastructure in place
- Internal and external system users
- Operational and business processes
- The potential areas of exposure for security breaches

# Security Breach Handling Methodology Prevention



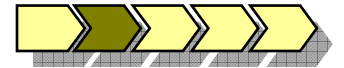
The main goal of this phase is to understand the overall company infrastructure, not only from the informational point of view, but also from the attacker point of view.

## Attacker View

- Security risk assessments
- Security audits
- Security vulnerability and penetration testing
- On-going security monitoring
- Application of patches and updates

# Security Breach Handling Methodology

## Detection



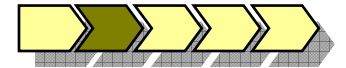
Most important thing!! Define what are acceptable and unacceptable behaviors.

Use of combination of technologies and procedural monitoring controls

- IDS/IPS, firewall, routers, operating systems, databases, applications
- Event log correlation applications
- Employees that are aware and trained to detect, react and report suspicious activities

# Security Breach Handling Methodology

## Detection



- Involve legal counsel
- Notify regulatory bodies as required
- Estimate the scope of the incident
- Document everything that happens
- Handle necessary reporting for regulatory agencies, laws enforcement, SARs and customers

# Security Breach Handling Methodology

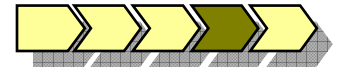
## Containment



The goal of this phase is to limit the extent of the attack and thus the potential damage or loss.

- Apply changes to systems to control the attack
- Define response strategy options
- Establish notification escalation procedures
- Document details, conversations and actions
- Handle necessary reporting for regulatory agencies, laws enforcement, SARs and customers
- Organize a public relations program

# Security Breach Handling Methodology Investigation

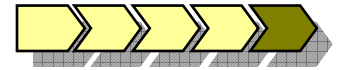


The investigation phase determines who, what, when, where, and how surrounding an incident.

- Plan the investigation approach
- Document details, conversations and actions
- Acquire evidence related to the security breach
- Determine whether to continue with the investigation
- Conduct forensic investigation
- Handle necessary reporting for regulatory agencies, laws enforcement, SARs and customers

# Security breach handling methodology

## Resolution and Reporting



Prepare an incident final report

Handle necessary reporting for regulatory agencies, laws enforcement, SARs and customers

Prepare a forensic report (clear, non-technical, legal document)

Follow-up the incident

- Lessons learned

- Training material for new team members

- Yield information that might be useful for legal proceeding

- Justify an organization's incident response effort (Metrics)



## Demonstration

Financial Institution ABC has a need to perform an investigation on a recent breach of customer data. According to the limited provided information, a large portion of the institution's customers have complained on charges on their credit card accounts, which seem to be due to fraudulent activity.

The institution has communicated that all of its customer data is kept logically in a secure database backed by a very secure and controlled infrastructure. Additionally, external monitoring agents have not reported anything out of the ordinary.

ABC has hired ERM to further investigate the incident.

# Questions

