Information Security: Barbarians at the Gateway (and Just about Everywhere Else)

Dr. Bharti Motwani

Section 19.1: Learning Objectives

1. Recognize that information security breaches are on the rise.
2. Understand the potentially damaging impact of security breaches.
3. Recognize that information security must be made a top organizational priority.

Information is the oil of 21st Century

Got a Bank Account or Credit Card? You've been Hacked (A look at Equifax)

Large Data Breach occurred in **summer 2017 against Equifax .**

Grabbed data of **143 million customers** (Credit card numbers, Social Security numbers and others).

Impacted those **beyond U.S. borders**: 400,000 in U.K and 100,000 in Canada

Equifax confirmed that their high-profile, high-impact data breach was due to an exploit of a vulnerability in an open source component, **Apache Struts product.**

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

A Look at the Target Hack

- Hackers installed malware in Target's security system in **2013** prior to Thanksgiving.
  - Every credit card used in company's **U.S. stores**
  - **40 million credit cards stolen** and additional personal info on **70 million consumers exposed.**
  - Breach was followed by the **firms largest ever decline in transactions, falling profits, lawsuits, and the CEO's dismissal.**
- Target had software **security from FireEye**:
  - **Paid $1.6 million for software**
  - **Warnings were ignored on several occasions**—had the warnings been heeded, the firm could have prevented the data theft.
  - Even worse, the firm's security software has an option to **automatically delete malware as it's detected but Target's security team had turned that function off.**

Source: Light Studio Design/Shutterstock.com

THE

Security must be a top organizational priority

- Firm suffering a security breach can experience **direct financial loss, exposed proprietary information, court costs, damaged reputation.**
- **Loss of $45 billion in more than 2 million** cyber incidents in 2018.
- Good news is **95% percent of attacks were seen as preventable.**
- Annual worldwide cybercrime costs **$600 billion** per year.
- **No text can provide an approach that is 100 percent secure.**
- Important to determine whether firm has **technologies , training, policies and procedures to assess risks**, **lessen the likelihood of damage and respond in the event of a breach.**

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

Section 19.2: Learning Objectives

1. Understand the source and motivation of those initiating information security attacks.
2. Relate examples of various infiltrations in a way that helps raise organizational awareness of threats.

Why Is This Happening? Who Is Doing it? And What's Their Motivation?

- **Data harvesters:** Cybercriminals who infiltrate systems and collect data for **illegal resale**.

- **Cash-out fraudsters:** Criminals that **purchase assets from data harvesters** to be used for illegal financial gain. They might buy goods using stolen credit cards or create false accounts.

- **Extortionist might leverage hacked data to demand payment**
  - U.S. based extortion plot **against state of Virginia threatened to reveal names, SSN and other information stolen from medical records database**.

  - **Victims of French cyber-extortionist group included Domino's, Swiss Banks and a European medical testing firm.**

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

"Hacker": Good or Bad?

- **Hacker:** A term that may be applied to either 1) someone who breaks into a computer, or 2) to a particularly clever programmer.
- **White hat hackers:** Someone who uncovers computer weaknesses without exploiting them.
  - Contribute to improving system security.
  - Share their knowledge in hopes that security will be improved.
- **Black hat hackers:** Computer criminals.
  - Bad guys, also called "crackers."

Why Is This Happening? Who Is Doing it? And What's Their Motivation? (cont'd)

Cyberwarfare has become a legitimate threat.

- **Technology Disruptions by terrorists** might be devastating
- **A 60 minute news program showed by white hat hackers:**
  - Key component in an **oil refinery** force it to overheat and **cause an explosion**
  - **Taking out the key components of U.S Power grid will be devastating**
    - Equipment is expensive
    - Not made in US
    - 3-4 months to replace

- Stuxnet (New era of Cyberwarfare) showed that with computers at the heart of so many systems, **it's now possible to destroy critical infrastructure without firing a shot.**

Why Is This Happening? Who Is Doing it? And What's Their Motivation? (cont'd)

- **Twitter was once brought down, and Facebook** was hobbled as hackers targeted the social networking and blog accounts of **Georgian blogger** (Cyxymu - an outspoken critic).

- **Revenge by Employees: San Francisco city government** lost control of a large portion of its own computer network over ten-day period when an employee refused to share critical passwords.

Is Your Government Spying on You?

- Government surveillance came under scrutiny when a **former CIA (Confidentiality, Integrity and Availability) employee and NSA (National Security Agency) contractor, Edward Snowden, gathered over 1.7 million digital documents** from U.S., British, and Australian agencies and began leaking them to the press.
  - Disclosures revealed several **U.S. government agencies had data-monitoring efforts** far more pervasive than many realized.
  - **XKeyscore**, allows the collection of data on “nearly everything a user does on the Internet.”

Section 19.3: Learning Objectives

1. Recognize the potential entry points for security compromise.
2. Understand infiltration techniques such as social engineering, phishing, malware, website compromises (such as SQL injection), and more.
3. Identify various methods and techniques to thwart infiltration.

Users/Administrators
- Bad apple
- Social engineering
- Phishing
- Weak or easily compromised passwords
- Careless or uninformed user (insecure "sharing" settings, no encryption, software updates turned off, poor configuration)

Physical Threats
- Dumpster diving
- Eavesdropping (key loggers, cameras, mics, devices mailed or left on premises)
- Destruction of property (terror, disaster)

Network
- Sniffers, compromised relays, and equipment
- DNS redirects
- Weak user authentication/open hotspots

Client Vulnerabilities
- OS holes
- Application weaknesses
- Language in applications
- Applets in applications
- Smart phones and connected automobiles
- Network device/IoT insecurities (Smart speakers, TVs, watches, toys, Internet-linked appliances, and embedded devices)

Computing Hardware
- Removable media (USB, DVD, etc.) insert malware or steal data
- PC/device theft
- Physical access (break into room)

Server Software
- OS holes
- Application weaknesses
- Language in applications
- Applets in applications
- Applications poorly coded (allow for SQL injection, cross-site scripting)
- Unfederated systems (entering one system allows access to others)

User and Administrator Threats

- **Bad apples**
  - **Dishonest employees** who steal secrets, install malware, or hold a firm hostage.
- **Social engineering**
  - **Con games that trick employees into revealing information or performing other tasks that compromise a firm.**
  - Sampling of methods employed in social engineering:
    - Impersonating senior management, investigators, or staff.
    - Identifying a key individual by name or title as a supposed friend.
    - Making claims with confidence and authority.
    - Baiting someone to add, deny, or clarify information that can help an attacker.
    - Using harassment, guilt, or intimidation.
    - Using an attractive individual to charm others into gaining info, favors, or access.
    - Answering bogus surveys.

User and Administrator Threats (cont'd, 2)

- **Passwords**
  - Most users employ inefficient and insecure password systems.
  - Some sites force users to change passwords regularly, but this often results in insecure compromises (users only make minor tweaks).
- **Building a better password:**
  - **Biometrics:** Measure and analyze human body characteristics for identification or authentication.
  - **Multi-factor authentication:** When identity is proven by presenting more than one item for proof of credentials. Password and some other identifier such as code on email/mobile phone, biometric, swipe a card and others

Source:
Bloomicon/Shutterstock.com

Technology Threats (Client and Server Software, Hardware, and Networking)

- **Malware** seeks to compromise a computing system without permission.
- **Methods of infection:**
  - *Viruses:* Infect other software or files.
  - *Worms:* Programs that take advantage of security vulnerability to automatically spread. **Unlike viruses, worms do not require an executable.**
  - *Trojans:* Misleads users of its true intent **by disguising itself as a standard program.**

The Encryption Prescription

Deploying encryption dramatically **lowers the potential damage from lost or stolen laptops, or from hardware recovered from dumpster diving.**

- **Encryption:** Scrambling data using a code, thereby hiding it from those who do not have the unlocking key.
- **key:** Code that unlocks encryption.
- **brute-force attacks: Exhausts all possible password** combinations to break into an account.

Section 19.4: Learning Objectives

1. Identify critical steps to improve your individual and organizational information security.
2. Be a tips, tricks, and techniques advocate, helping make your friends, family, colleagues, and organization more secure.
3. Recognize the major information security issues that organizations face, as well as the resources, methods, and approaches that can help make firms more secure.

Taking Action as a User

- Tips for users:
  - Surf smart.
  - Stay vigilant.
  - Stay updated.
  - Stay armed—install a full suite of security software.
  - Be settings smart—secure home networks and encrypt hard drives.
  - Regularly update passwords.
  - Be disposal smart.
  - Regularly back up your system.
  - Check with your administrator.

Taking Action as an Organization

- **Follow frameworks, standards, and compliance**.
  - ISO27k or ISO 27000 series provides "a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and **improving an Information Security Management System."**
  - **Compliance requirements:** Legal or professionally binding steps that must be taken.
- **Education, audit, and enforcement**
  - Functions of research and development:
    - Understanding emerging threats and updating security techniques.
    - Working on broader governance issues.
  - **Employees should**:
    - Know a firm's policies and be regularly trained.
    - **Understand the penalties for failing to meet their obligations**.
  - Audits include real-time monitoring of usage, announced audits, and surprise spot-checks.

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

Taking Action as an Organization—Technology's Role

- **Patches: Software updates that plug existing holes.**
- **Lock down hardware:**
  - **Prevent unapproved software installation**.
  - Force file saving to hardened, backed-up, and monitored servers.
  - Re-image hard drives of end-user PCs.
  - **Disable boot capability of removable media.**
  - Prevent Wi-Fi use and require VPN encryption for network transmissions.
- **Lock down networks**:
  - **Firewalls:** Control network traffic, block unauthorized traffic.
  - **Intrusion detection systems:** Monitor network use for hacking attempts and take preventive action.
  - **Honeypots:** Tempting, bogus targets meant to lure hackers.
  - **Blacklists:** Deny the entry of specific IP addresses and other entities.
  - **Whitelists:** Permit communication only with approved entities or in an approved manner.


WHEN?
HOW?
WHERE?
WHO?
WHAT?
WHEN?
WHAT?
WHERE?
WHAT?
WHERE?
When?
WHEN?
Where?
When?
WHERE?
ANY
WHERE?
HOW?
WHEN?
What?
QUESTIONS?
What?
When?
When?
Why?
WHEN?
When?
Where?
WHAT?
When?
When?
Why?
HOW?
WHAT?
When?
When?
Why?
WHERE?
Why?
WHERE?
When?
HOW?
HOW?
Why?


TEST