ACS-2821-001
Information Security in Business

The Growing Importance of IT Security

ACS-2821-001 – Slides Used In The Course

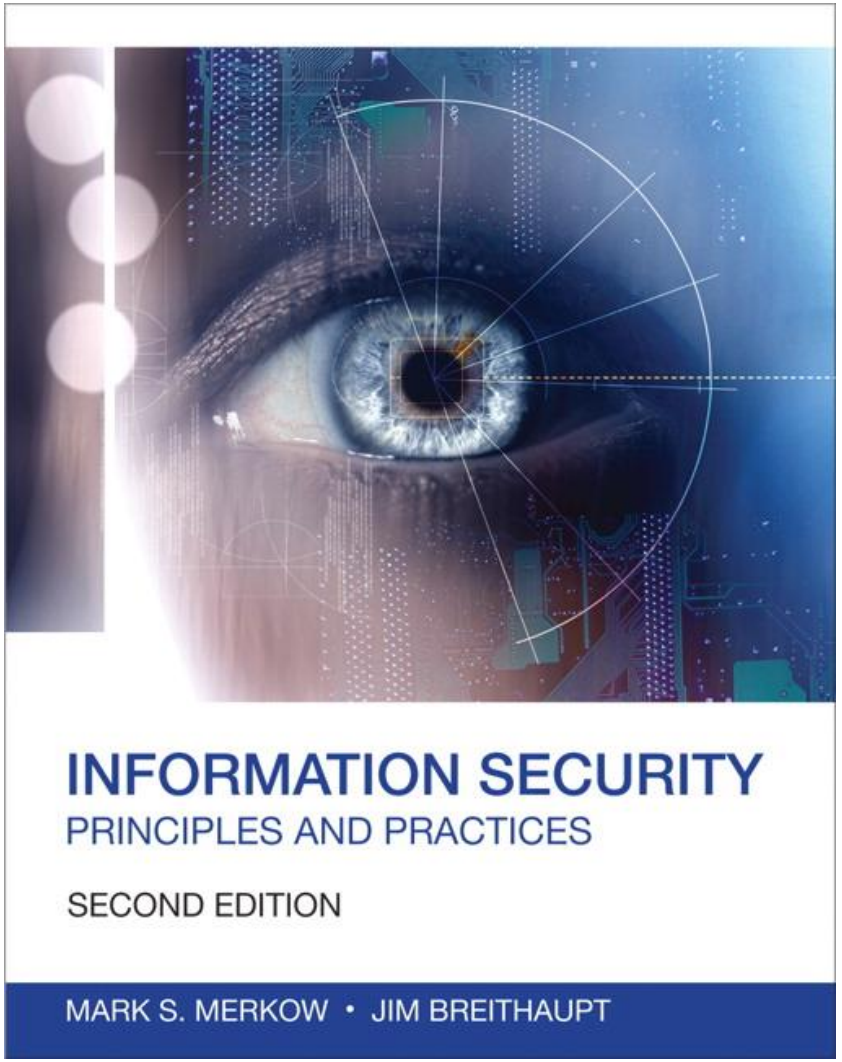
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Recognize the growing importance of information security
- Comprehend information security in the context of the mission of a business

The Growing Importance of IT Security

- Increased services to both vendors and employees create worlds of possibilities in satisfying customer needs, but …
- They also create risks to the confidentiality, integrity, and availability of confidential or sensitive data

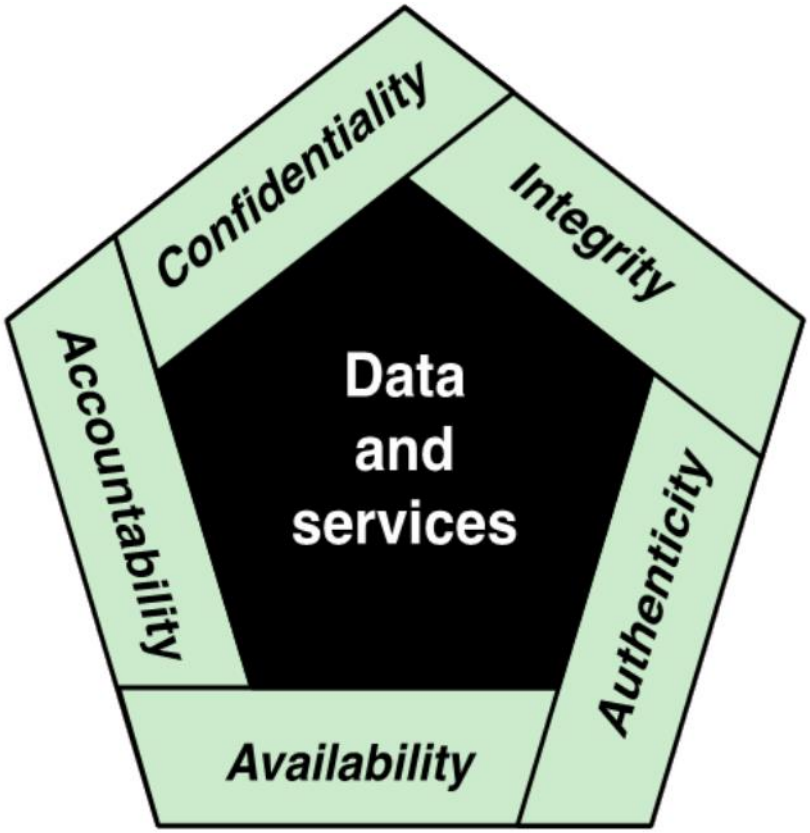
Information Security Definition

The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms , May 2013) defines the term computer security as follows:

> *" Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated."*

Information Security Objectives – C.I.A. Triad

Information Security Objectives – C.I.A. Triad Extended



Contextualizing Information Security

THE UNIVERSITY OF WINNIPEG

- Information security draws upon the best practices and experiences from multiple domains including:
  - Compliance, policies, and standards
  - Administration, auditing, access controls, and permission controls
  - Intrusion detection and prevention and incident response
  - Software development security
  - Physical security
  - Operations control
  - Public key infrastructure and key management
  - Business continuity and disaster recovery
  - Security testing
  - Antivirus solutions
  - Training and awareness
  - The list goes on…

THE UNIVERSITY OF WINNIPEG

Information security

Protection of information, regardless of format, including:

- Paper documents
- Digital and intellectual property
- Verbal or visual communications

Cybersecurity

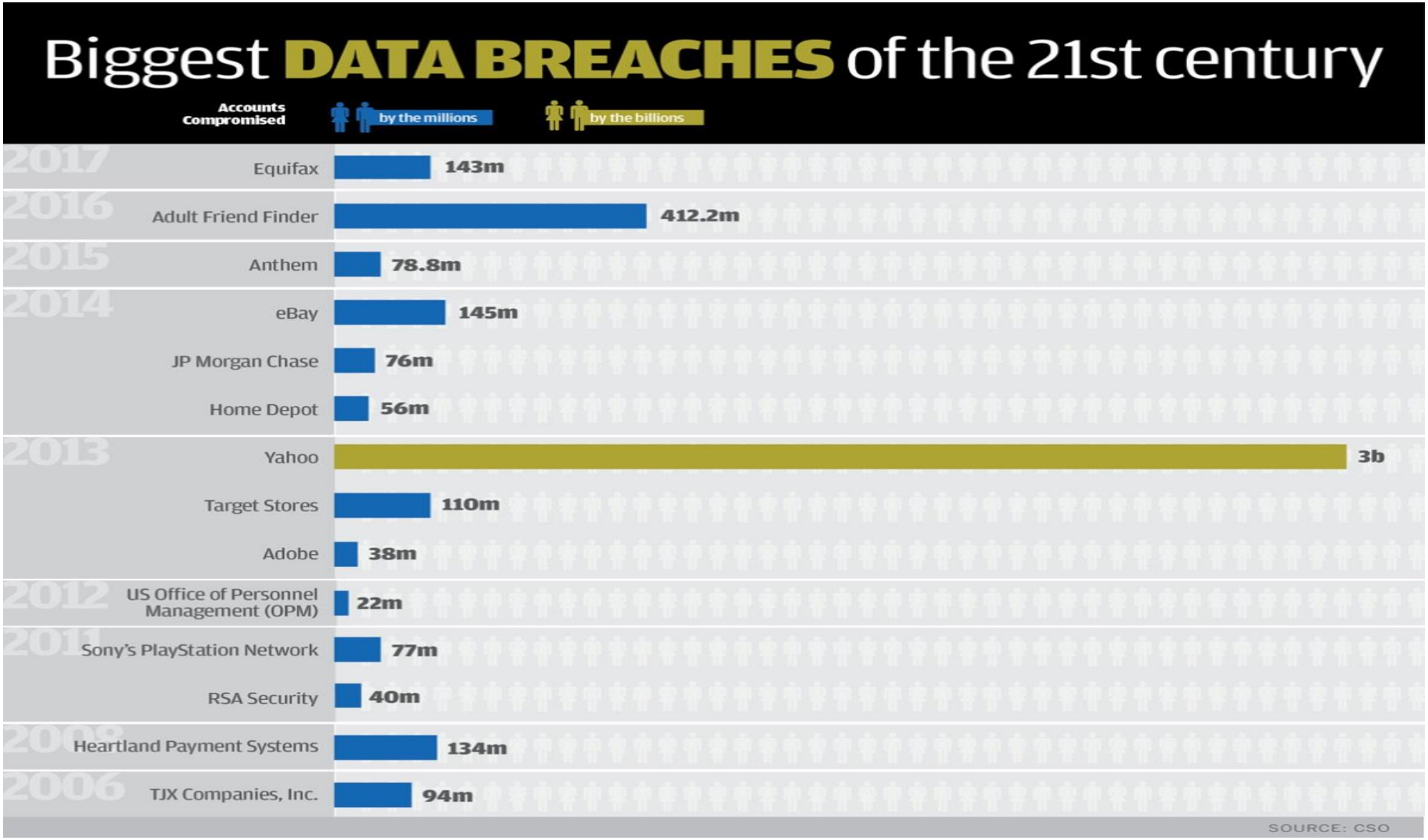
Protection of digital assets, including:

- Network hardware
- Software
- Information processed and stored in isolated or networked systems

Information Security Must Meet the Needs of Business

- To support business operations an Information Security Specialist must understand:
  - Nature of the business and business goals
  - The organization risk tolerance and appetite
  - What security mission, vision and strategy
  - Industry alignment and security trends
  - Compliance requirements and regulations
  - Business Mergers, acquisitions and partnerships
  - Business's outsourcing of services or providers

Data Breaches of the 21st Century



Yahoo Data Breach – 2013 – 3 Billion User Accounts

- September 2016, announced the biggest data breach in history
  - likely by “a state-sponsored actor”.
  - in negotiations to sell itself to Verizon.
- Compromised real names, email addresses, dates of birth and telephone numbers of 500 million users.
  - "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm were safe.
- Later, in December, it buried that earlier record with the disclosure that a breach in 2013,
  - different group of hackers had compromised 1 billion accounts.
  - names, dates of birth, email addresses and passwords.
  - security questions and answers were also compromised.
- October of 2017, revised that estimate to 3 billion user accounts.
- Knocked an estimated $350 million off Yahoo’s sale price.
- Verizon paid $4.48 billion for Yahoo’s core Internet business.
- Both companies had to share regulatory and legal liabilities from the breaches.
- Yahoo, founded in 1994, had once been valued at $100 billion.

Marriott International - 2014-2018 - 500 million customers

- November 2018, Marriott International announced approximately 500 million customers had been stolen data.
- The breach actually occurred on systems supporting Starwood hotel brands starting in 2014.
- The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.
  - For some of the victims, only name and contact information were compromised.
  - Attackers took some combination of contact info, passport number, Starwood Preferred Guest numbers, travel information, and other personal information.
  - Credit card numbers and expiration dates of more than 100 million customers were stolen
    - Credit card numbers were encrypted.
- The breach was attributed to a Chinese intelligence group
  - To gather data on US citizens
- If true, this would be the largest known breach of personal data conducted by a nation-state.

Adult Friend Finder – 2016 - 412.2 million accounts

- The FriendFinder Network was breached sometime in mid-October 2016
  - websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com.
  - Hackers collected 20 years of data on six databases.
    - names, email addresses and passwords.
- Most of the passwords were protected only by the weak SHA-1 hashing algorithm.
  - 99 percent of them had been cracked by the time LeakedSource.com published its the entire data set on November 14.
- CSO Online's Steve Ragan reported at the time that
  "a researcher who goes by 1x0123 on Twitter and by Revolver in other circles posted screenshots taken on Adult Friend Finder (that) show a Local File Inclusion vulnerability (LFI) being triggered."
- The vulnerability was discovered in a module on the production servers used by Adult Friend Finder.
- AFF Vice President Diana Ballou issued a statement saying
  "We did identify and fix a vulnerability that was related to the ability to access source code through an injection vulnerability."

eBay – 2014 - 145 million users compromised

- The online auction giant reported a cyberattack in May 2014.
- Exposing names, addresses, dates of birth and encrypted passwords of all of its 145 million users.
- The hackers got into the company network using the credentials of three corporate employees.
  - Had inside access for 229 days, during which time they were able to make their way to the user database.
- The company asked its customers to change their passwords.
- Fortunately, financial information, such as credit card numbers, was stored separately and was not compromised.
- The company was criticized for lack of communication informing users and poor implementation of the password-renewal process.
- CEO John Donahue said the breach resulted in a decline in user activity, but had little impact on the bottom line.
- Q2 revenue was up 13 percent and earnings up 6 percent, in line with analyst expectations.

Equifax - July 29 2017

- Personal information of 147.9 million consumers
  - including Social Security Numbers, birth dates, addresses, and in some cases drivers' license numbers)
  - 209,000 consumers also had their credit card data exposed.
  - 19,000 Canadian Customers was affected.
- Equifax is one of the largest credit bureaus in the U.S.
- An application vulnerability on one of their websites led to a data breach
- The breach was discovered on July 29, but the company says that it likely started in mid-May.
- The cost - $575 million, and potentially up to $700 million in a global settlement with the US Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) and 50 US states and territories

How much does a data breach cost?

- Data breaches up by 54%, and number of records exposed up by 53%- first half of the year compared to the same period in 2018
- First 6 months of 2019 – 3.813 breaches was reported and 4.1 billion records exposed.
- Eight largest breaches exposed 100 million records each totaling to 3.2 billion records.
- Breaches reported by sectors:
  - Business sector accounted for 67% reported breaches and 84.6% records exposed
  - Medical sector – 14 %
  - Government – 12%
  - Education - 7%

How much does a data breach cost?

From a report done by Deloitte indicated that:

- "Hidden" costs can amount be 90 percent of total business impact on an organization.
- This effect can last for two years or more after the event.

14 business impacts are broken down as:

Above the surface, or well-known cyber incident costs

- Customer breach notifications
- Post-breach customer protection
- Regulatory compliance (fines)
- Public relations/crises communications
- Attorney fees and litigation
- Cybersecurity improvements
- Technical investigations

Below the surface, or hidden or less visible costs

- Insurance premium increases
- Increased cost to raise debt
- Operational disruption
- Lost value of customer relationships
- Value of lost contract revenue
- Devaluation of trade name
- Loss of intellectual property (IP)

How Much Does a Data Breach Cost? An Example

- A healthcare organization suffers a data breach
- A laptop was stolen that containing 2.8 million of personal health information (PHI) records from the company's healthcare analytics software vendor.
- Total cost of the breach was determined to be $1,679 million.

Above the surface

- Customer breach notifications = six months, at a cost of $10 million (0.6 percent of the total)
- Post-breach customer protection = three years, at a cost of $21 million (1.25 percent of the total)
- Regulatory compliance = $2 million over a two-year period (0.12 percent of the total)
- Public relations/crisis communications = $1 million over the first year (0.06 percent of the total)
- Attorney fees and litigation = five years at a cost of $10 million (0.6 percent of the total)
- Cybersecurity improvements = $14 million during the first year (0.83 percent of the total)
- Technical investigations = six weeks at a cost of $1 million (0.06 percent of the total)

Beneath the surface

- Insurance premium costs = $40 million over three years (2.38 percent of the total)
- Increased cost to raise debt = $60 million (3.57 percent of the total)
- Operational disruption = $30 million (1.79 percent of the total)
- Lost value of customer relationships = $430 million over a three year period (25.61 percent of the total)
- Value of lost contract revenue = $830 million over three years (49.43 percent of the total)
- Devaluation of trade name = $230 million loss over five years (13.7 percent of the total)
- Loss of intellectual property = No dollar value was affixed here

13 Data Breach Predictions For 2019

THE UNIVERSITY OF WINNIPEG

1. Biometric hacking will rise
2. A cyber attack on a car will kill someone
3. Attackers will hold the internet hostage using DDoS attack
4. A DevOps doomsday breach is upon us
5. API breaches will become the most costly
6. A top cloud vendor will be breached
7. A significant breach will be launched through a printer
8. An attack on a major wireless carrier will affect both iPhones and Android
9. Terrorists will use off-the-shelf crimeware to launch cyber attacks
10. Financial institutions will continue to be attack targets, with a few twists
11. Cybercriminals will pose as gamers to breach online gaming systems
12. A third-party compromise will shut down critical infrastructure
13. More nation-state technology and know-how will trickle down to cyber criminals, leading to more sophisticated attacks

Summary

- Networked systems remain vulnerable to attacks from within and outside an organization
- The explosive growth of e-commerce and the pervasive personal and business uses of the Internet
- The principles, approaches, and concepts in INFOSEC should work together to provide the harmonious mix of risk and reward that modern business demands

ACS-2821-001 – Questions?

Sources and References Used in the Slides

Articles reference in this slide are from:

CSO Online (https://www.csoonline.com/).

- The 18 biggest data breaches of the 21st century
- How much does a data breach cost? Here's where the money goes.
- 13 data breach predictions for 2019

Deloitte Advisory

- Beneath the Surface of a Cyberattack

CmputerWeekly.com

- 2019 set to be another record year for data breaches