ISA 419: Data Driven Security

Fadel M. Megahed

Endres Associate Professor
Department of Information Systems and Analytics
Farmer School of Business
Miami University
🖂 fmegahed@miamioh.edu
? by appointment @ 2004 FSB

Spring 2022

Learning Objectives for Today's Class

Main Learning Outcomes for Today's Class

- **Define information security (infoSec), its main goals, and how it fits within a firm's overall security protocols**
- **Describe the three main steps in information security**
- **Explain why prevention as a sole security measure is deemed to fail**
- **Describe course objectives & structure**
- **Assess your ability to explore a somewhat simple infoSec dataset**

Outline

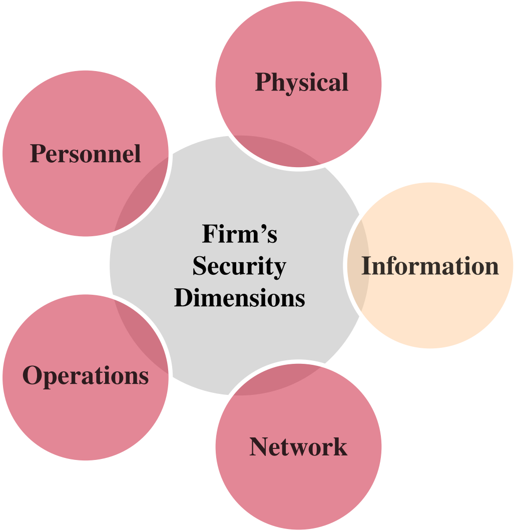
1. **An Overview of Cyber/Information Security**
2. **Course Expectations & Overview**
3. **Self-Assessment of Ability to Explore a Sample InfoSec Dataset**
4. **Recap and Things to Do**

What is security?

Definition

- According to the Merriam-Webster Dictionary [1], security can be defined as: "the quality or state of being secure: such as freedom from danger."
- In other words, the overall objective is to protect against adversaries who would do harm whether it is intentional or not [2].
- For example, national security is a "multilayered system that protects the sovereignty of a state, its assets, its resources, and its people." [2, p. 8]

What is security? A firm's perspective



What is cyber/information security?

While some researchers distinguish between them [3], in this course, we will use both terms interchangeably. Possible definitions for cyber/information security include:

Definition

- **According to the Merriam-Webster Dictionary [4], cyber security can be defined as: "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"**
- **According to the SANS Institute [5], "information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption."**

Information Security Goals: CIA [1]

Confidentiality, Integrity, and Availability (CIA)

- **Confidentiality: Preventing unauthorized reading/disclosure of information.**
- **Integrity: Preventing unauthorized modification of information.**
- **Availability: Preventing unauthorized withholding of information/ resources.**

Information Security Goals: CIA [2]

Suppose that I would like to start an online banking business, named Miami University Online Bank (MUOB). Assume that we have:

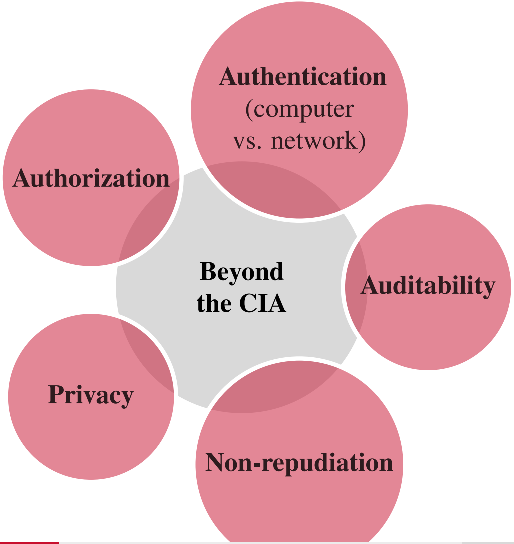
Figure: Fadel (Owner)

Figure: John (Customer)

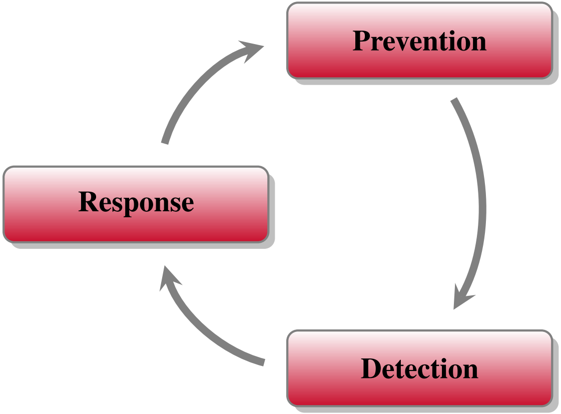
Figure: Hans (Bad Guy)

Question: How can you explain to me the CIA principles in the context of MUOB?

Information Security Goals: Beyond the CIA Principles



A Taxonomy of Information Security (Defense) Measures



Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

Risk Management Controls as Preliminary Preventive Measures

Risk Management Controls

- **Administrative:** Includes the development and deployment of policies and procedures; for example:
  - Password policies
  - Principal of least privilege (POLP)
- **Physical:** In addition to securing a firm's premises through doors/locks/etc., typical risk management controls utilize the:
  - Principal of separation of duties

Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

Risk Management Controls as Preliminary Preventive Measures

Risk Management Controls

- **Administrative:** Includes the development and deployment of policies and procedures; for example:
  - Password policies
  - Principal of least privilege (POLP)
- **Physical:** In addition to securing a firm's premises through doors/locks/etc., typical risk management controls utilize the:
  - Principal of separation of duties

Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

Risk Management Controls as Preliminary Preventive Measures

Risk Management Controls

- **Administrative: Includes the development and deployment of policies and procedures; for example:**
  - **Password policies**
  - **Principal of least privilege (POLP)**
- **Physical: In addition to securing a firm's premises through doors/locks/etc., typical risk management controls utilize the:**
  - **Principal of separation of duties**

Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

Risk Management Controls as Preliminary Preventive Measures

Risk Management Controls

- **Administrative:** Includes the development and deployment of policies and procedures; for example:
  - Password policies
  - Principal of least privilege (POLP)
- **Physical:** In addition to securing a firm's premises through doors/locks/etc., typical risk management controls utilize the:
  - Principal of separation of duties

Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

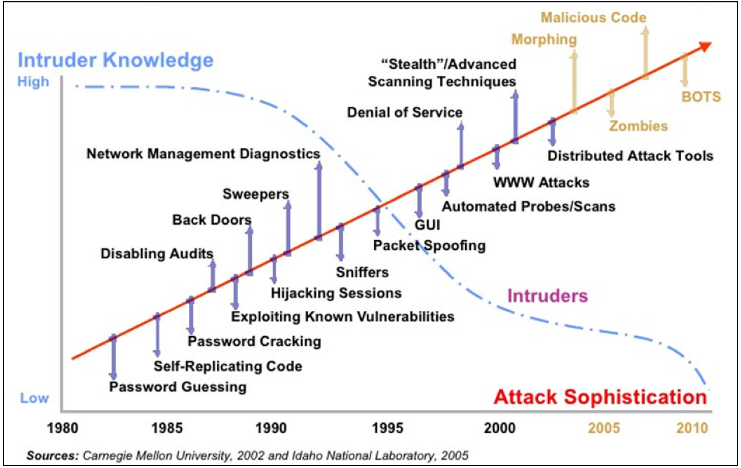
Other Preventive Measures

Other Important Preventive Measures

- **Protocols:** For example, the reliance on secure socket layer (SSL) to authenticate the web source
- **Host-based protections:** secure operating systems and/or patching
- **Access Control:** Through identification (username), authentication (over a computer/ network), and authorization (file permissions, need-to-know principle)
- **Firewalls:** to control inter-network traffic (e.g., from/to internet)
- **Security by design:** code reviews, unit testing, defense in depth, and principle of least privilege

Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

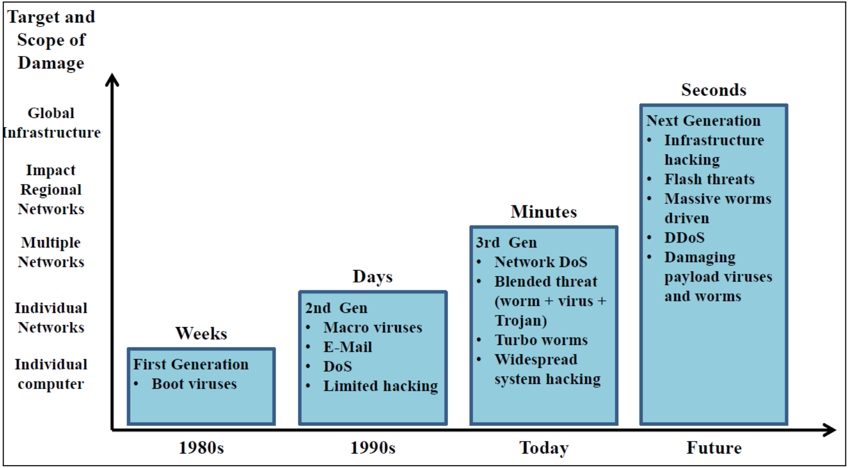
Failure of Prevention: Attacking Constantly Getting Easier



Sources: Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005

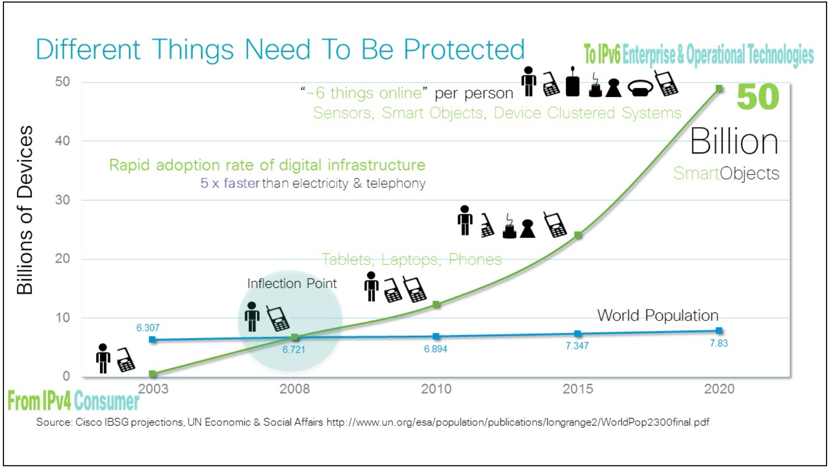
Source: Figure 1-1 in Pacheco Ramirez's PhD Dissertation [6], University of Arizona.

Failure of Prevention: Attacking Constantly Getting Faster



Source: Figure 1-2 in Pacheco Ramirez's PhD Dissertation [6], University of Arizona.

Failure of Prevention: Attackers Having More Options due to IoT



Source: Figure 1 in Cisco's *Securing the Internet of Things: A Proposed Framework* [6].

Failure of Prevention: Possible Root-Causes

Inherent weaknesses in increasingly complex systems

- Poor design affecting software and hardware
- Poor implementation due to security being an afterthought, lack of personnel experience, & poor system configuration
- Poor management, i.e. inadequate policies/ procedures
- Trade-offs between security and usability
- Humans using computer/network systems; We are the weakest link in any system

Vulnerabilities

- Back doors
- Denial of Service
- Exploits
- Social engineering

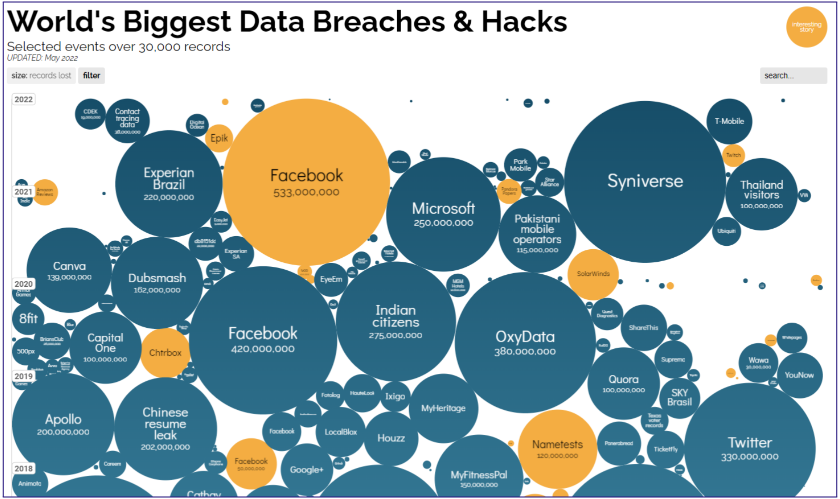
Source: Adapted from CS 259D, Stanford University, https://web.stanford.edu/class/cs259d/lectures/Session1.pdf

Class Activity: Failure of Prevention - Have you been pwned?

The purpose of this class activity is to investigate how many of your web accounts have been breached. This activity consists of the following steps:

- **Go to: https://haveibeenpwned.com/**
- **Insert the email you use most online (e.g., in my case it is my gmail) into the search bar and then click on "pwned?"**
- **Record the number of breaches that you were pwned in, using the code shown in class for the website: www.menti.com**
- **Outside of class: Address the breaches by changing your password for these sites, opting into 2-factor authentication, and changing the passwords in other websites (if you re-used this password).**

Failure of Prevention: World’s Biggest Data Breaches & Hacks



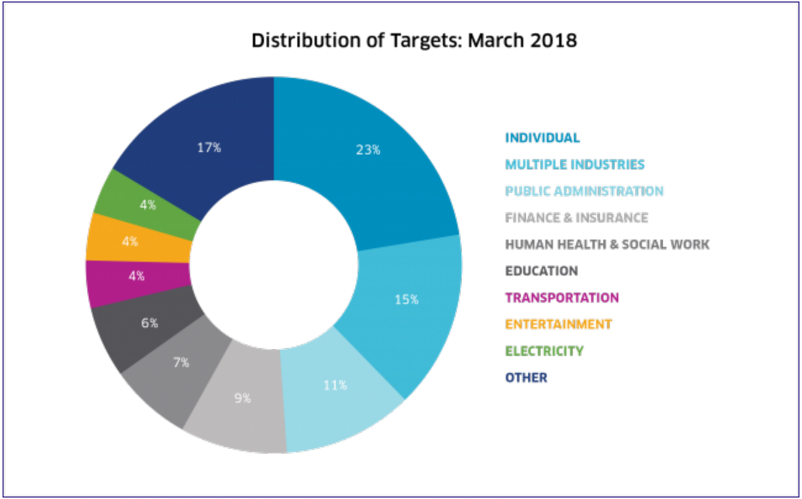
World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: May 2022

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Failure of Prevention: Most Targeted Industries



Source: https://www.nasdaq.com/articles/cybersecurity-industry-report-investment-case-2018-06-25

Detective Security [1]

> *Detection of a system compromise is extremely critical. With the ever increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. There is no full proof "silver bullet" security solution. A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm. The most important element of this strategy is timely detection and notification of a compromise. Intrusion detection systems (IDS) are utilized for this purpose. Sans Institute [7, p. 4]*

Note: You are expected to read P. 1-6 in [7]. Refer to the References Slides for detailed information.

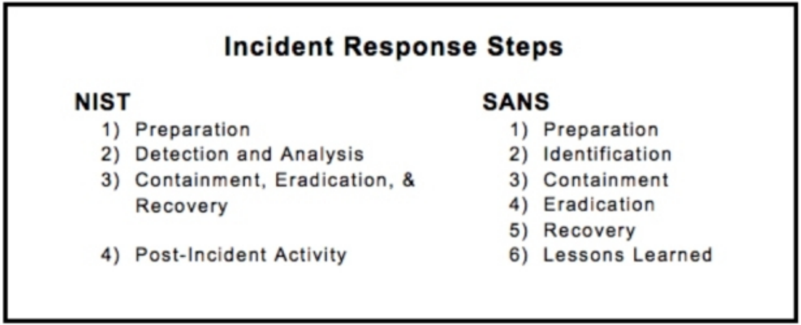
Detective Security [2]

> ***As previously indicated, intrusion detection is much more than an alarm. Although it is an alarm, it's an alarm with brains. Imagine a fire alarm that had the capability of detecting a fire, distinguish the type of fire, pinpoint its source and path, alert the building occupants and fire department, and forward intelligence to the firehouse prior to their response. All this and even having the capability of distinguishing normal activity such as bad cooking. A properly configured intrusion detection system is such a device. An alarm with brains. Sans Institute [7, p. 4]***

Note: You are expected to read P. 1-6 in [7]. Refer to the References Slides for detailed information.

Response: What to do in case of detecting a security breach?

There are two popular/similar frameworks for incident response:



Incident Response Steps

NIST

1) Preparation
2) Detection and Analysis
3) Containment, Eradication, & Recovery
4) Post-Incident Activity

SANS

1) Preparation
2) Identification
3) Containment
4) Eradication
5) Recovery
6) Lessons Learned

Source: First figure in the AT&T Cybersecurity blog post by Elisha Girken [8].

Outline

1. An Overview of Cyber/Information Security
2. **Course Expectations & Overview**
3. Self-Assessment of Ability to Explore a Sample InfoSec Dataset
4. Recap and Things to Do

Course Overview [1]

Traditionally, information technology (IT) security was a job that entailed using a few tools, solutions and best practices that focused on attack prevention and protect a company's sensitive information and network assets. However, these solutions are no longer sufficient. The businesses are transitioning to a new era, where cybersecurity is enhanced and almost requires data-driven analytical solutions. The primarily goals of data-driven security are to: (a) discover malicious patterns from the data-lakes of logs produced by security software, and (b) develop automated tools that can assist in the surveillance of security-related data. This course covers various analytic applications in information/cyber security including: user behavior analysis, network and host intrusion detection, web security, phishing detection, and emerging issues in Industrial Internet of Things (IIoT) security. Note that the course is designed to be very applied, involving a large amount of programming to examine real datasets.

Course Overview [2]

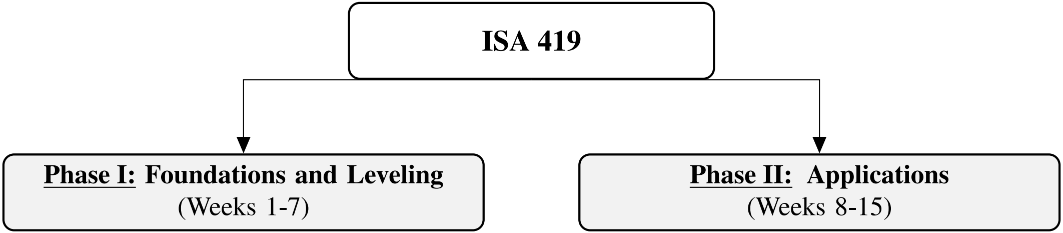


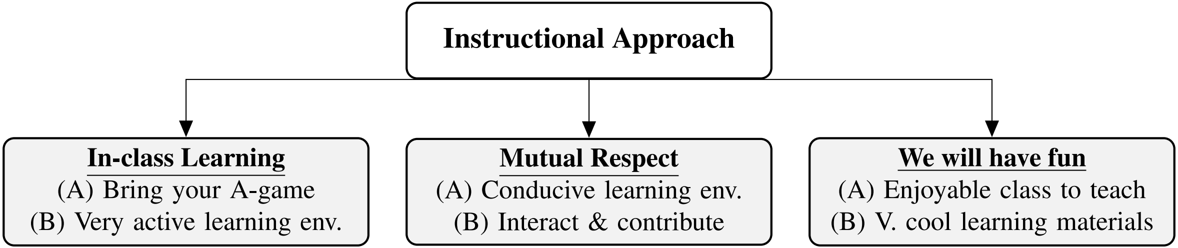
Figure: How the ISA 419 course is organized. See the tentative class schedule for more details.

Course Objectives

Upon completing the course, you will:

- **Describe key cybersecurity concepts including the CIA Triad, access management, incident response and common cybersecurity best practices.**
- **Demonstrate a fundamental understanding of the role of analytical solutions in state-of-the-art cybersecurity solutions.**
- **Understand the uniqueness of cybersecurity datasets, including: the nature of unbalanced data and diversity of data in each class, asymmetrical costs of misclassification and non-stationary inference.**
- **Have a basic understanding of the theory behind some commonly used statistical methodologies and machine learning algorithms in data-driven security.**
- **Use and implement an appropriate modeling paradigm to tackle cybersecurity problems.**

Instructional Approach



Instructional Approach

In-class Learning
(A) Bring your A-game
(B) Very active learning env.

Mutual Respect
(A) Conducive learning env.
(B) Interact & contribute

We will have fun
(A) Enjoyable class to teach
(B) V. cool learning materials

Figure: An overview of the instructional approach for ISA 419.

How will I Evaluate your Learning?

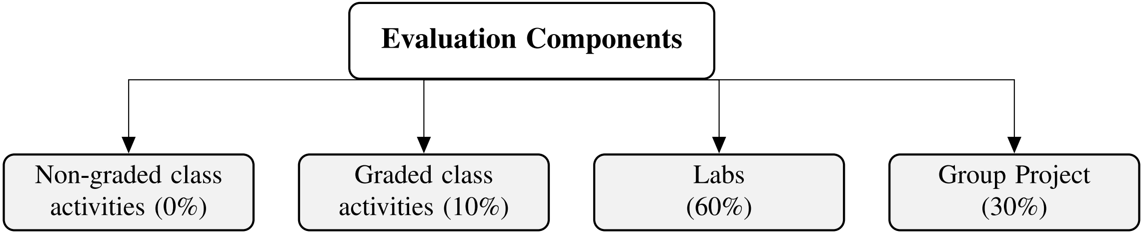

Evaluation Components
Non-graded class activities (0%)
Graded class activities (10%)
Labs (60%)
Group Project (30%)

Figure: An overview of the evaluation components for ISA 419.

Outline

1. An Overview of Cyber/Information Security
2. Course Expectations & Overview
3. **Self-Assessment of Ability to Explore a Sample InfoSec Dataset**
4. Recap and Things to Do

Activity: Explore the Los Alamos National Laboratory's Dataset

In 2014, researchers from the Los Alamos National Laboratory have made available a dataset on "User-Computer Authentication Associations in Time". A brief description of the dataset is available at: https://csr.lanl.gov/data/auth/. In this class activity, you are asked to examine a sample of the data, which can be downloaded from:

- https://www.dropbox.com/s/88ajdyp7hfnvrl2/lanl-auth-dataset-1-03.csv (where you will need to click on the triangle next to open to download the unzipped ".csv" file)

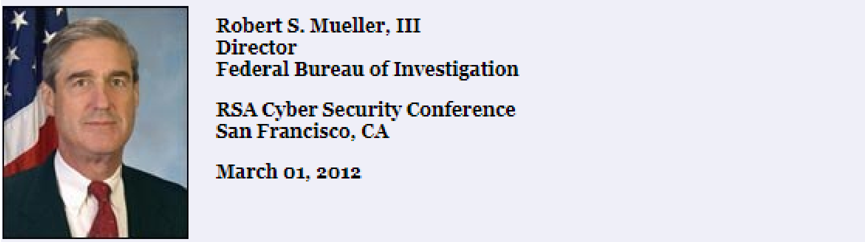
For the data in lines 1.1M-1.2M, please answer the following questions:

- What is the timestamp of observation (i.e. row number) 1,200,000?
- What are the number of unique users for the aforementioned 100,000 observations?
- What is the number of unique computers used by U12 for the aforementioned 100,000 observations?

Outline

1. An Overview of Cyber/Information Security
2. Course Expectations & Overview
3. Self-Assessment of Ability to Explore a Sample InfoSec Dataset
4. **Recap and Things to Do**

The FBI Director's Remarks in the RSA Security Conference



Robert S. Mueller, III
Director
Federal Bureau of Investigation

RSA Cyber Security Conference
San Francisco, CA

March 01, 2012

> *"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."*

Source:
https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Learning Objectives for Today's Class

By the end of the class, you should be able to:

- **Define information security (infoSec), its main goals, and how it fits within a firm's overall security protocols**
- **Describe the three main steps in information security**
- **Explain why prevention as a sole security measure is deemed to fail**
- **Describe course objectives & structure**
- **Assess your ability to explore a somewhat simple infoSec dataset**

Things to Do Before Next Class

Suggested Activities before Next Class

- You should read the Sans Institute's Information Security Process [7].
- You should skim through the NIST Cyber security framework (Sections 1 and 3) available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf or watch the overview video from NIST at: https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview
- To work on your coding/Googling skills, please create a summary table of the number of unique users by day from the dataset that I have shared with you. (i.e. divide the dataset into different days, if there are multiple, and then create a two column table with day and # unique users)

References [1]

[1] Merriam-Webster Dictionary.
Security — Definition of Security by Merriam-Webster.
https://www.merriam-webster.com/dictionary/security, 2020.
[Online, last accessed 1-26-2020].

[2] Michael E Whitman and Herbert J Mattord.
Principles of information security.
Cengage Learning, 2011.

[3] Rossouw Von Solms and Johan Van Niekerk.
From information security to cyber security.
Computers & Security, 38:97–102, 2013.

[4] Merriam-Webster Dictionary.
Security — Definition of Cybersecurity by Merriam-Webster.
https://www.merriam-webster.com/dictionary/cybersecurity, 2020.
[Online, last accessed 1-26-2020].

References [2]

[5] SANS Institute.
SANS Institute — Information Security Resources.
https://www.sans.org/information-security/, 2020.
[Online, last accessed 1-26-2020].

[6] Jesus Horacio Pacheco Ramirez.
An anomaly behavior analysis methodology for the internet of things: Design, analysis, and evaluation.
PhD Dissertation. The University of Arizona.
https://repository.arizona.edu/bitstream/handle/10150/625581/azu_etd_15658_sip1_m.pdf, 2017.
[Online, last accessed 1-26-2020].

[7] James LaPiedra.
The information security process: Prevention, detection and response.
SANS Institute. Global Information Assurance Certification Paper.
https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197, 2002.
[Online, last accessed 1-26-2020].

References [3]

[8] Elisha Girken.
2020 incident response steps for NIST and SANS.
AT&T Cybersecurity.
https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide, 2020.
[Online, last accessed 1-26-2020].

ISA 419: Data Driven Security

Fadel M. Megahed

Endres Associate Professor
Department of Information Systems and Analytics
Farmer School of Business
Miami University
✉ fmegahed@miamioh.edu
? by appointment @ 2004 FSB

Spring 2022