ISA 419: Data-Driven Security

01: Introduction to Cybersecurity

Fadel M. Megahed, PhD

Professor
Farmer School of Business
Miami University

@FadelMegahed
fmegahed
fmegahed@miamioh.edu
Automated Scheduler for Office Hours

Spring 2025

Learning Objectives 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: prevention, detection, and response.
- Explain why **prevention as a sole security measure is deemed to fail**.
- Describe **course structure**, **goals**, and **overview**.

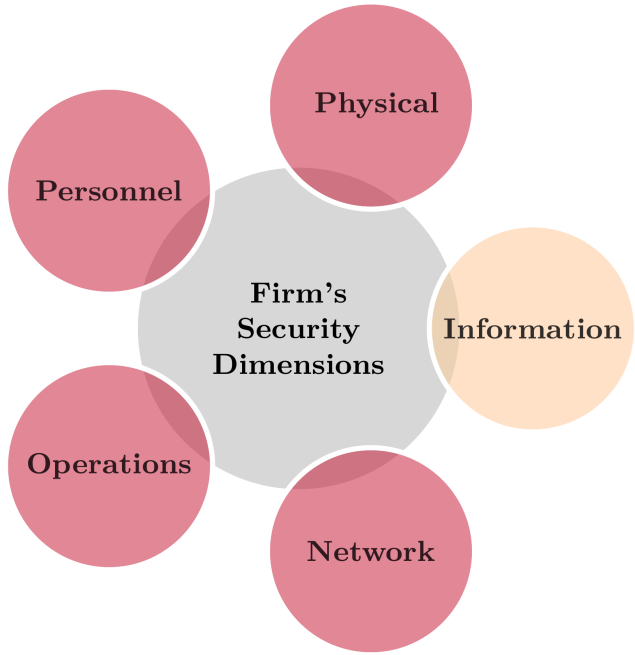
Information Security & its Main Goals

What is Security?

Some Working Definitions

- According to the Merriam-Webster Dictionary, **security** can be defined as: **"the quality or state of being secure: such as freedom from danger."**
- I.e., the objective is to **protect against adversaries who would do harm whether it is intentional or not.**
- For example, **national security** is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people." (Whitman and Mattford, 2022, p. 8)

Security in Modern Organizations



Integrating InfoSec within the Broader Spectrum of Firm's Security Dimensions

What is Cyber/Information Security?

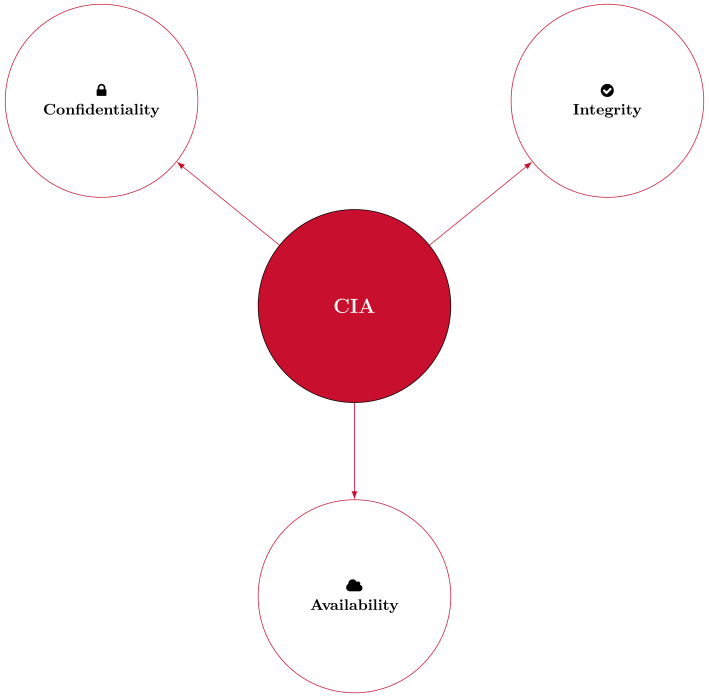
While some researchers distinguish between them, in this course, we will use both terms **interchangeably**. Possible **definitions for cyber/information security include:**

- **According to the Merriam-Webster Dictionary, 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, "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

The CIA Triad:

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



The Interconnected Core of Cybersecurity: CIA Principles in Focus.

Class Activity: Explaining the CIA Triad

07:00

Activity | Your Solution

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

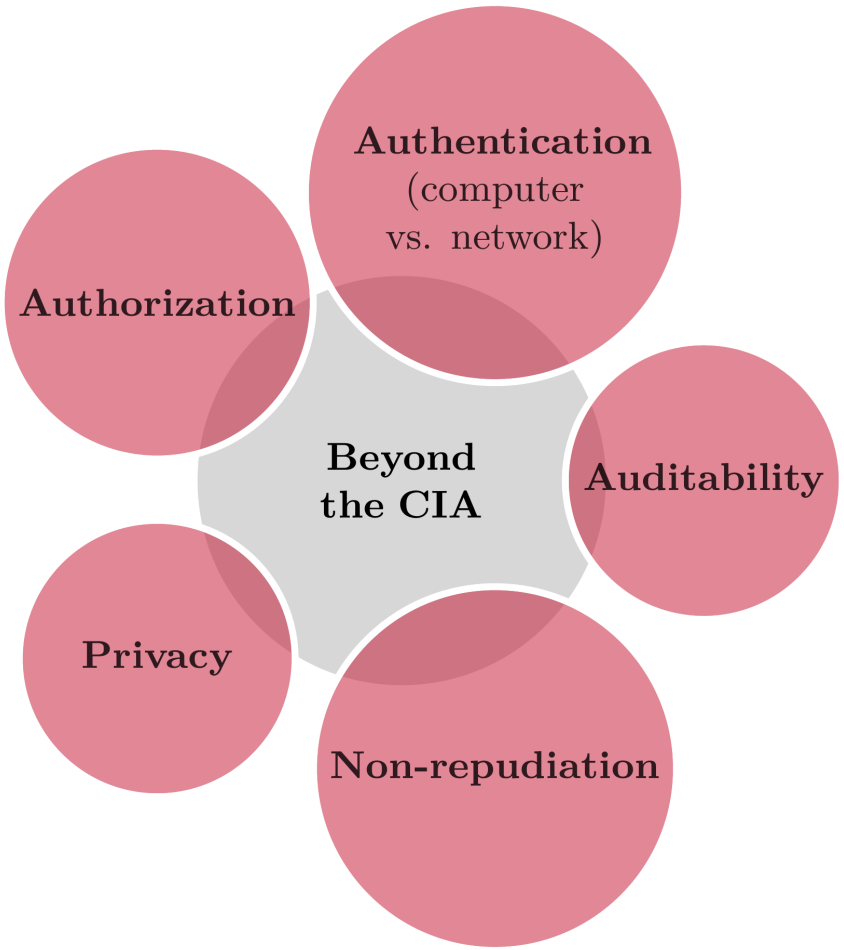
Fadel (Owner)

John McClane (Client)

Hans Gruber (Bad Guy)

Your task: "Think-Pair-Share activity" Reflect individually, then discuss with your partner to finalize your explanation of the CIA principles in the MUOB context. Write it down in 2nd panel.

Beyond the CIA: Other InfoSec Objectives



Risk Management Controls

Effective cybersecurity **begins** with implementing diverse risk management controls, each targeting specific security aspects:

- **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

Protocols, Host-Based Protections, and Other Key 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

Class Activity: Have you been Pwned?

02:00

- 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 count of breaches that you were pwned in.
- Anonymously, report the count of your breaches on the survey site (you will need to include the access code shown in class).
- **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).

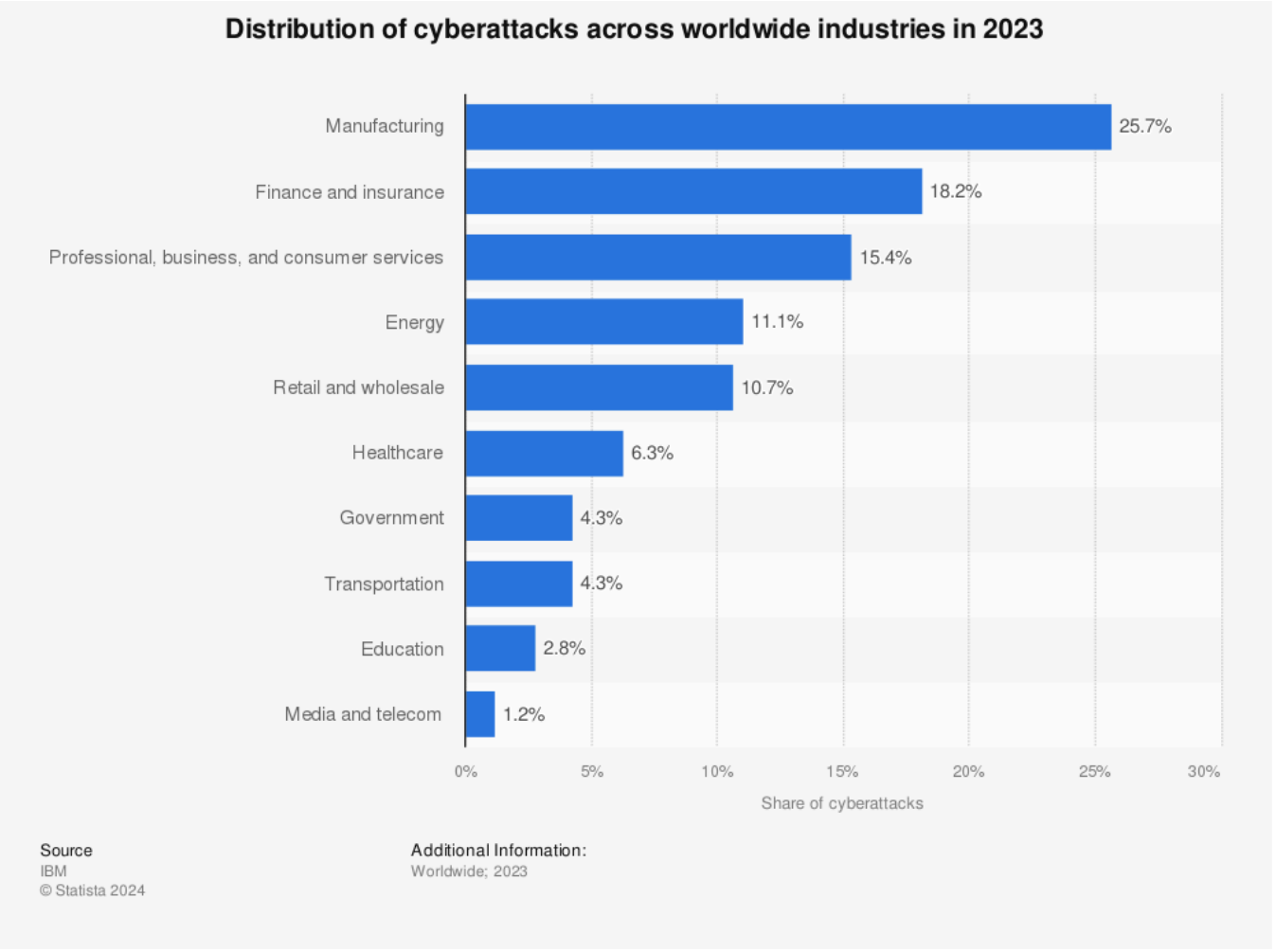
Class Activity: Have you been Pwned? (Cont.)

ıny data breaches have you been involved in, per https://haveibeenpwned.com/ ?

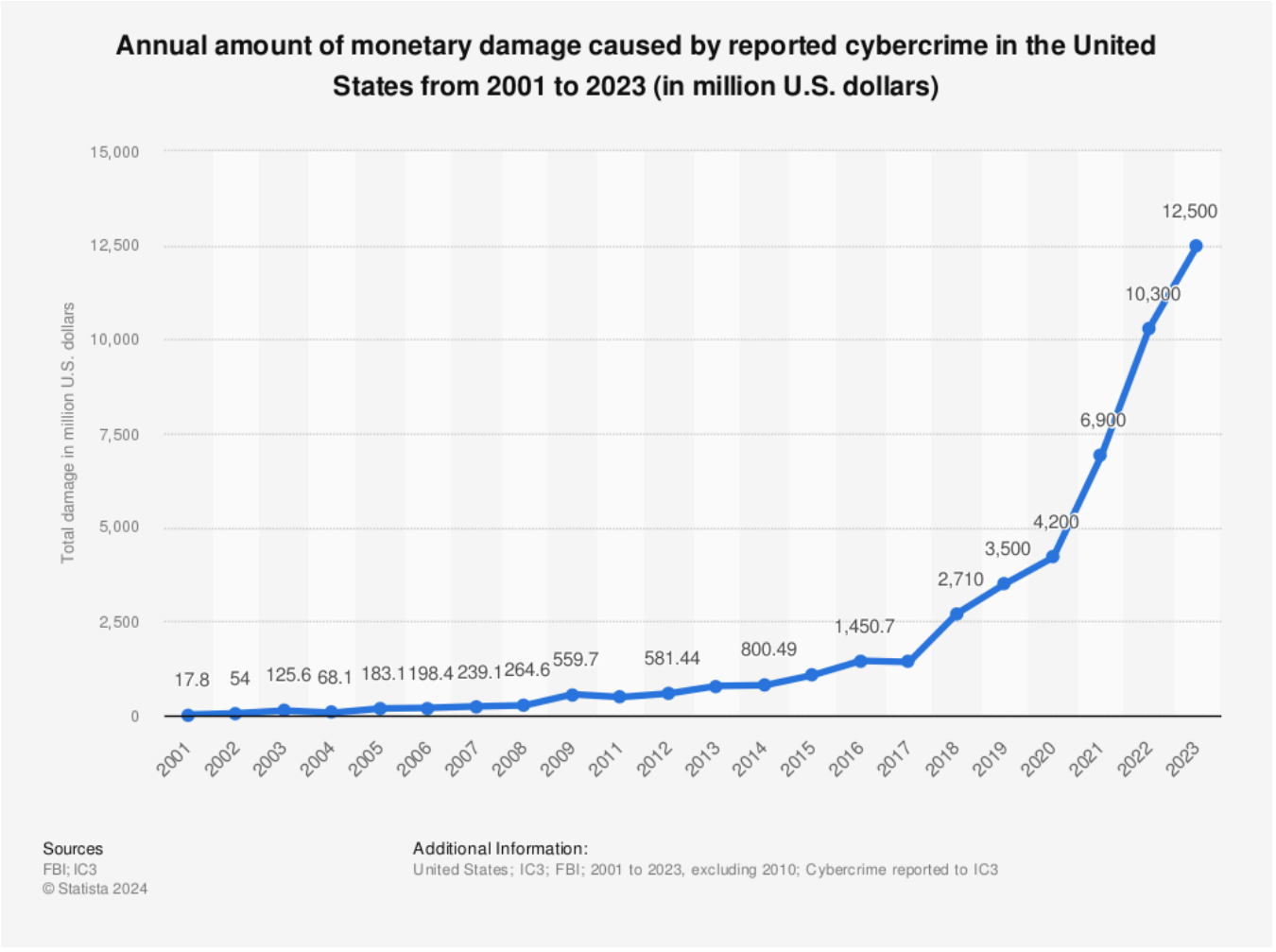
Prevention as a Sole Security Measure is Deemed to Fail

Failure of Prevention: World's Biggest Data Breaches

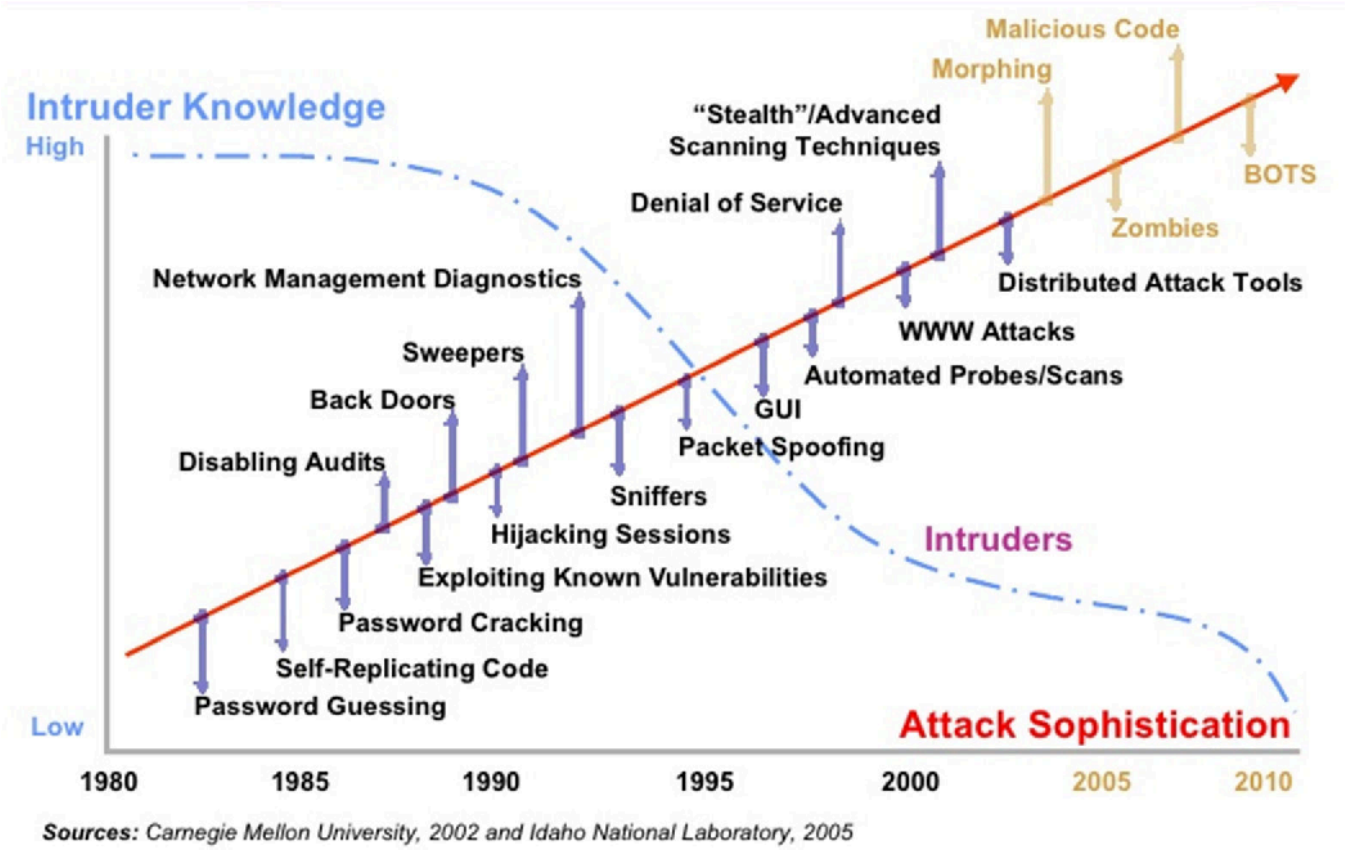
Failure of Prevention: World's Most Targeted Industries



Failure of Prevention: Monetary Damage in the U.S.



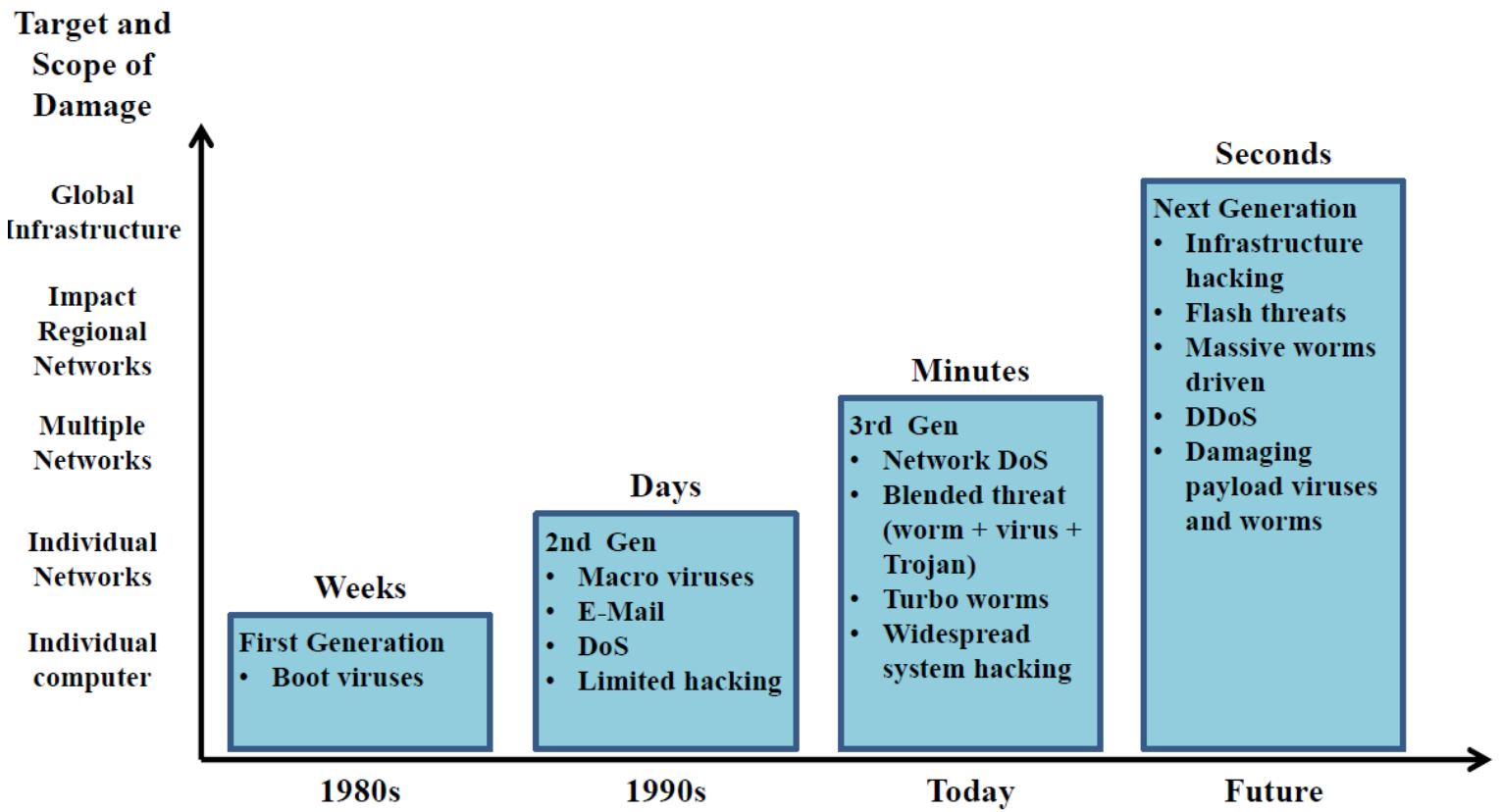
Failure of Prevention: Attacks Constantly Getting Easier



Attack sophistication versus intruder technical knowledge

Source: Ramirez, J. H. P. (2017). An Anomaly Behavior Analysis Methodology for the Internet of Things: Design, Analysis, and Evaluation (Doctoral dissertation, The University of Arizona).

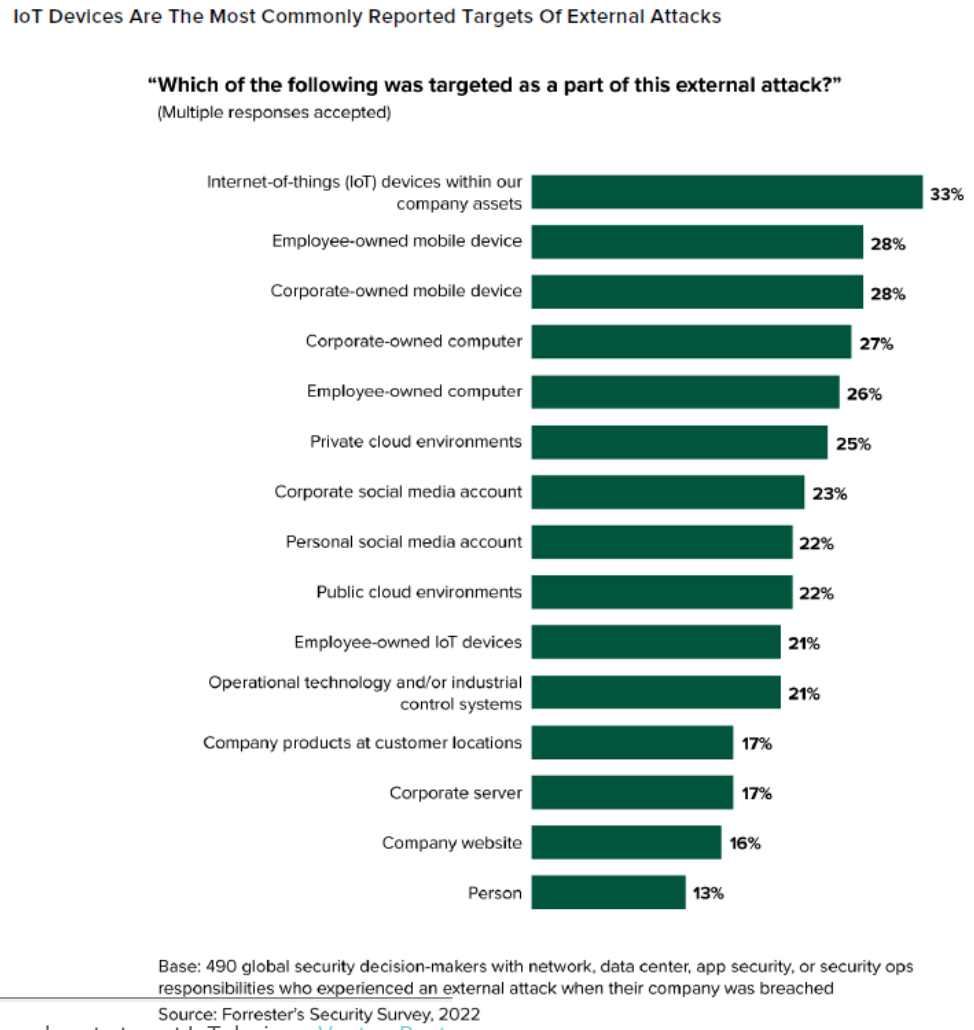
Failure of Prevention: Attacks Constantly Getting Faster



The timeline of cyber-threads scope of damage and impact time

Source: Ramirez, J. H. P. (2017). An Anomaly Behavior Analysis Methodology for the Internet of Things: Design, Analysis, and Evaluation (Doctoral dissertation, The University of Arizona).

Failure of Prevention: Attackers Having More Options



Source: Louis Columbus (2023). Why attackers love to target IoT devices. VentureBeat.

Why is Prevention Not Enough?

- Inherent weaknesses in increasingly more complex systems/networks
  - Poor Design
    - Software and hardware
    - Example: sendmail (race condition vulnerability, buffer overflow, group permission vulnerability, etc.)
  - Poor Implementation
    - Security an afterthought
    - Lack of personnel experience/training
    - Poor system configuration (e.g., default firewall configurations with open insecure ports)
  - Poor Management
    - Inadequate policies/procedures

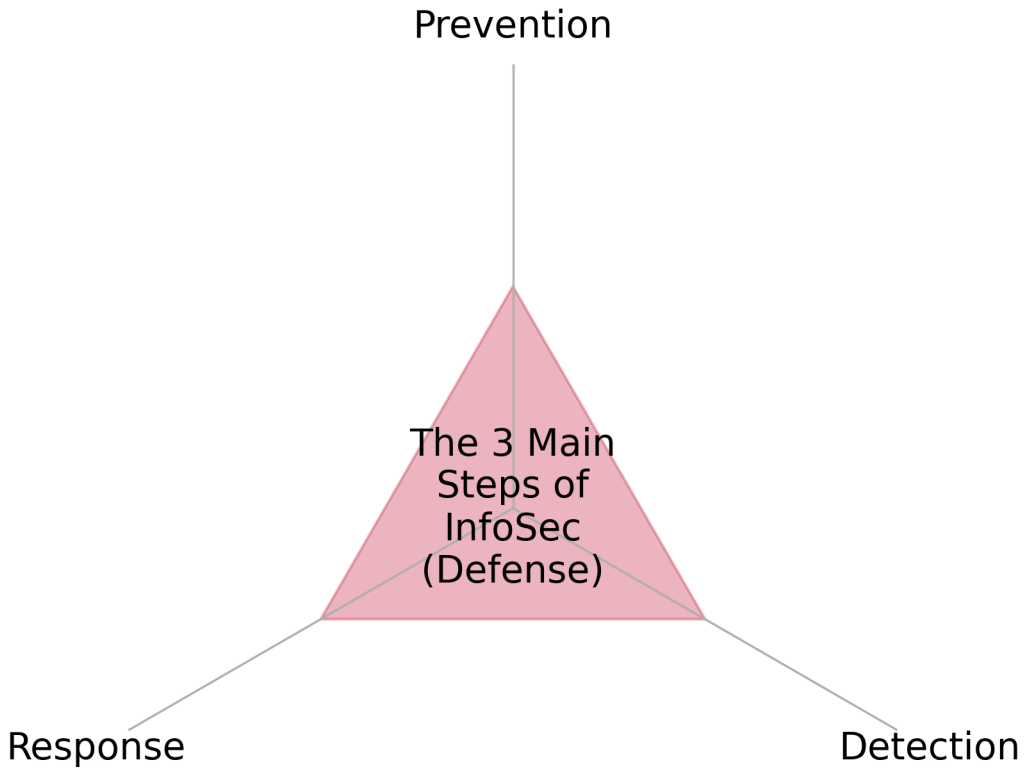
Why is Prevention Not Enough?

- Tradeoff between security and usability
- Cost of prevention

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

The Three Main Steps in Information Security (Defense)

A Taxonomy of Information Security Measures



Course Design, Expectations, and Overview

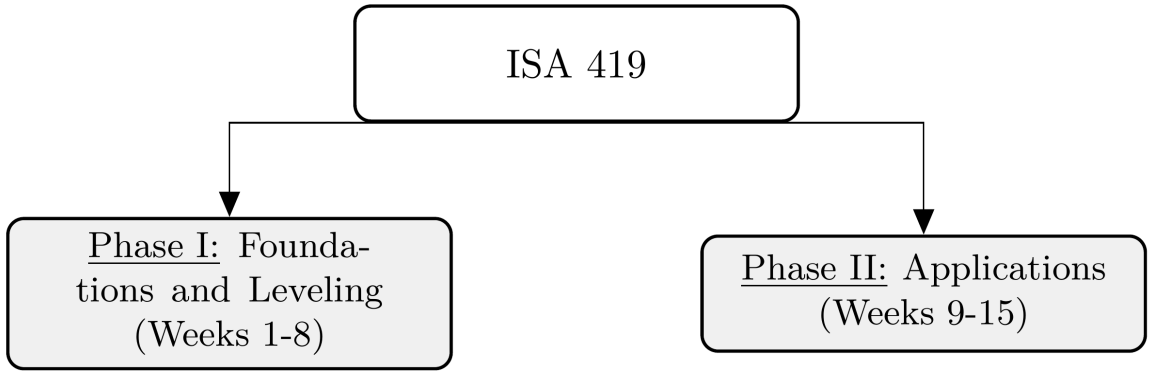
Course Overview

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 always requires data-driven analytical solutions**. The primarily goals of data-driven security are to:

- discover malicious patterns from the data-lakes of logs produced by security software, and
- 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



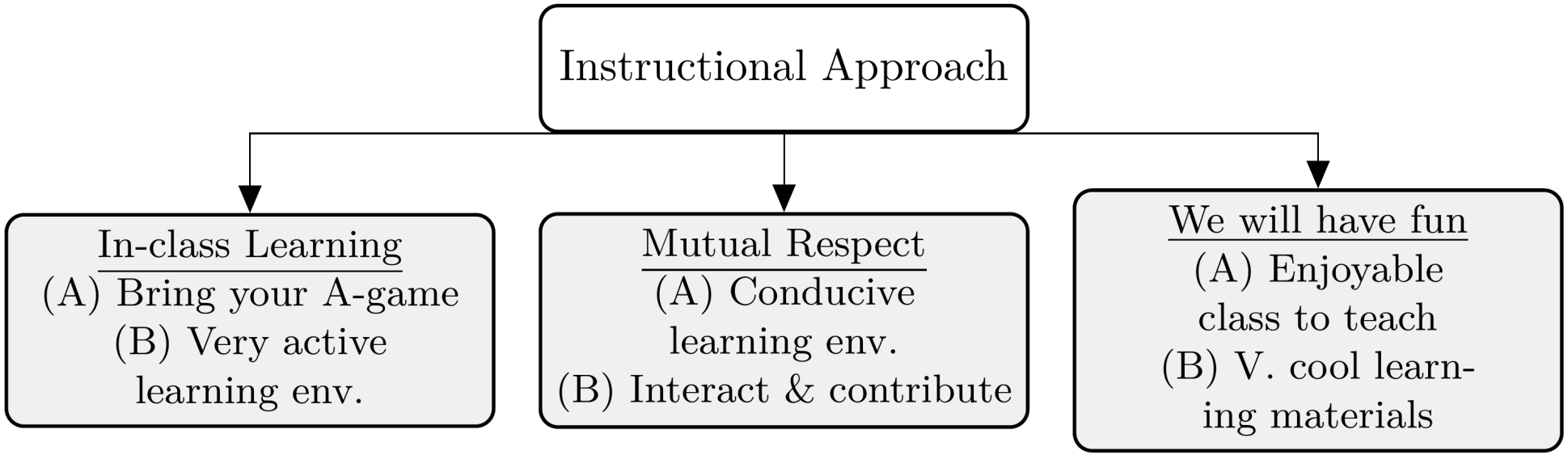
How the ISA 419 course is organized.

Course Objectives

Upon completing the course, you will:

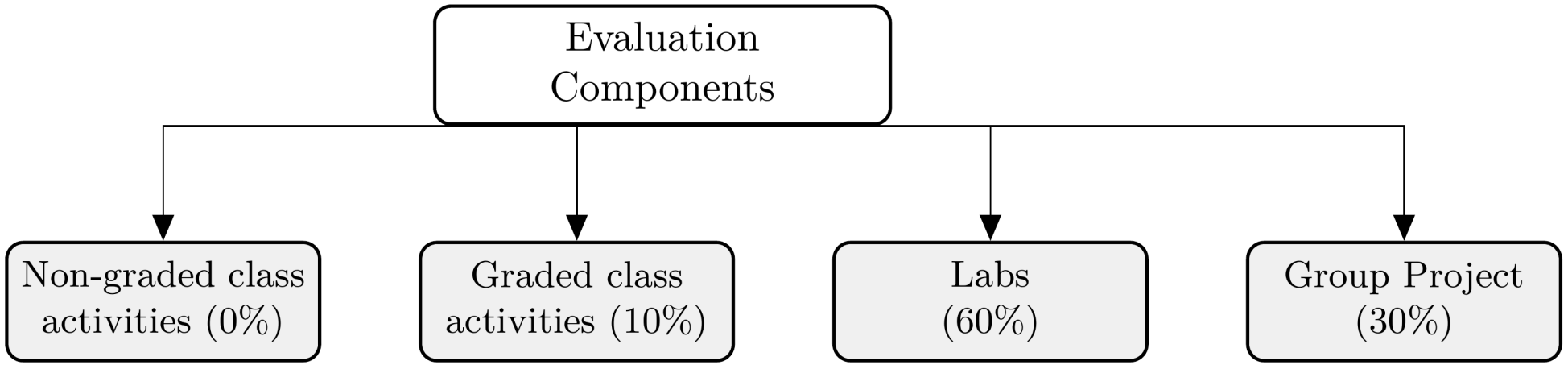
- Describe key cybersecurity concepts, including the CIA Triad, access management, incident response, and common cybersecurity best practices.
- Demonstrate a fundamental understanding of the role of analytical solutions in state-of-the-art cybersecurity solutions.
- Understand the uniqueness of cybersecurity datasets, including the nature of unbalanced data and diversity of data in each class, asymmetrical costs of misclassification, and non-stationary inference.
- Understand 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



An overview of the instructional approach for ISA 419.

How will I Evaluate your Learning?



An overview of the evaluation components for ISA 419.

The Equifax Data Breach: A Case Study

Case Background

Equifax Overview:

- Major credit reporting agency.
- Manages sensitive personal data of millions.

The Breach Discovery:

- Disclosed in September 2017.
- Compromised personal information of 147 million individuals.

Vulnerability Exploited:

- Apache Struts CVE-2017-5638.
- Equifax's system was unpatched.

Case Background (Cont.)

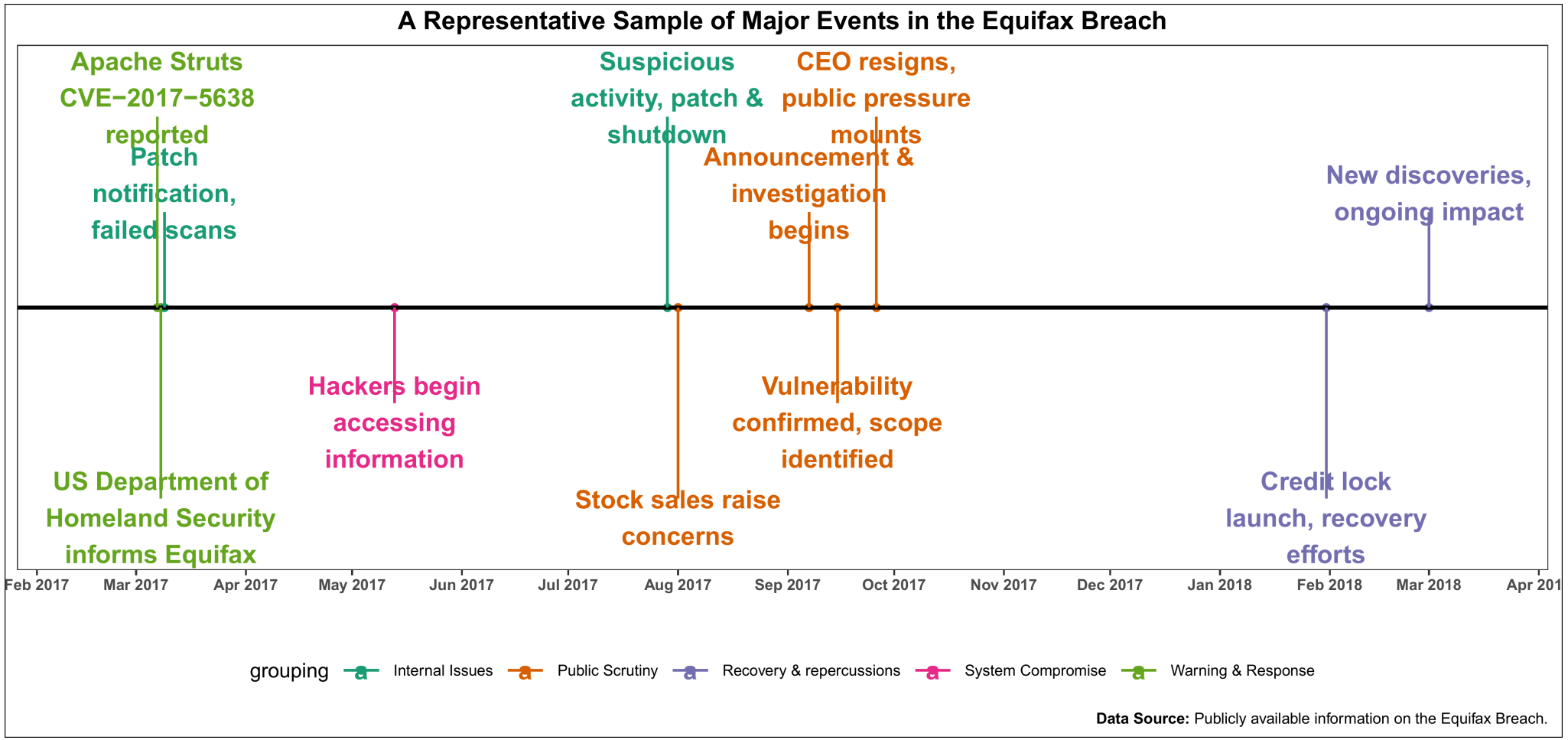
Breach Timeline:

- Apache reported the vulnerability in March 2017.
- Equifax’s systems remained vulnerable for months.
- Unauthorized access occurred from May to July 2017.

Data Compromised:

- Included names, Social Security numbers, birth dates.
- Addresses, and in some cases, driver's license numbers and credit card numbers.

The Detailed Timeline of the Equifax Data Breach



Recap

Summary of Main Points

By now, you should be able to do the following:

- 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: prevention, detection, and response.
- Explain why **prevention as a sole security measure is deemed to fail**.
- Describe **course structure**, **goals**, and **overview**.

📝 Review and Clarification 📝

- **Class Notes**: Take some time to revisit your class notes for key insights and concepts.
- **Zoom Recording**: The recording of today's class will be made available on Canvas approximately 3-4 hours after the session ends.
- **Questions**: Please don't hesitate to ask for clarification on any topics discussed in class. It's crucial not to let questions accumulate.

🎯 Assignment 🎯

In pairs, you are expected to do a deep dive on the case by reading the following sources:

- **Student 1:** should read in detail the CSO Online article.
- **Student 2:** should read in detail the archived artile from the EPIC report
- You are **both** encouraged to explore any hyperlinks within both articles and take notes pertaining to the discussion questions below.

Discussion Questions

- What was the Apache Struts CVE-2017-5638 vulnerability and its associated patch?
- Discuss how the Equifax breach violated the principle of **confidentiality**.
- what was the impact of the breach on Equifax's data **integrity** and service **availability**?
- Evaluate Equifax's response strategy in terms of information security best practices.

Assignment Details and Submission

The assignment should be submitted on Canvas. See the assignment submission page for more details.