CYBERSECURITY LAW, STANDARDS AND REGULATIONS

INSTRUCTOR COURSE DELIVERY – V2

COURSE OUTLINE

1st Semester

1
Introduction to Cybersecurity Law

Overview of cyber crimes and offenses

2
Basic Elements of Criminal Law

Judicial branches, cybercrime enforcement and jurisdiction

3
US Cybersecurity Law

US cyber laws, history of dispute resolution and data breach lawsuits

4
Legal Doctrine

Duties of care, failure to act or warn and reasonable person doctrine

5
Procedural Law

Rules of criminal procedure and state computer crime laws

COURSE OUTLINE - CONTINUED

1st Semester

6
Data Privacy Law
Common law of privacy, privacy laws, data breach laws and data breach legislation

7
Personal Liability & Privacy
Personal liability, D&O insurance and preemptive liability

8
Data Encryption Law
Cryptology overview, state and international cryptology law

2nd Semester

9
Digital Forensics Law
Preservation orders, digital evidence and chain of custody

10
Acts, Standards & Regulations
Domestic, international and industry standards

COURSE OUTLINE - CONTINUED

2nd Semester

11
Cybersecurity Law Program

Models, architecture and staffing

12
Cyber Liability Insurance

Coverage categories, policy restrictions and claim processes

13
Compliance Auditing

Audit types, critical audit matters and standards

14
Cyberlaw Developments

Future of cybersecurity law, and impact of technology

15
International Cyber & Privacy Law

Foreign policy, treaties and trade agreements

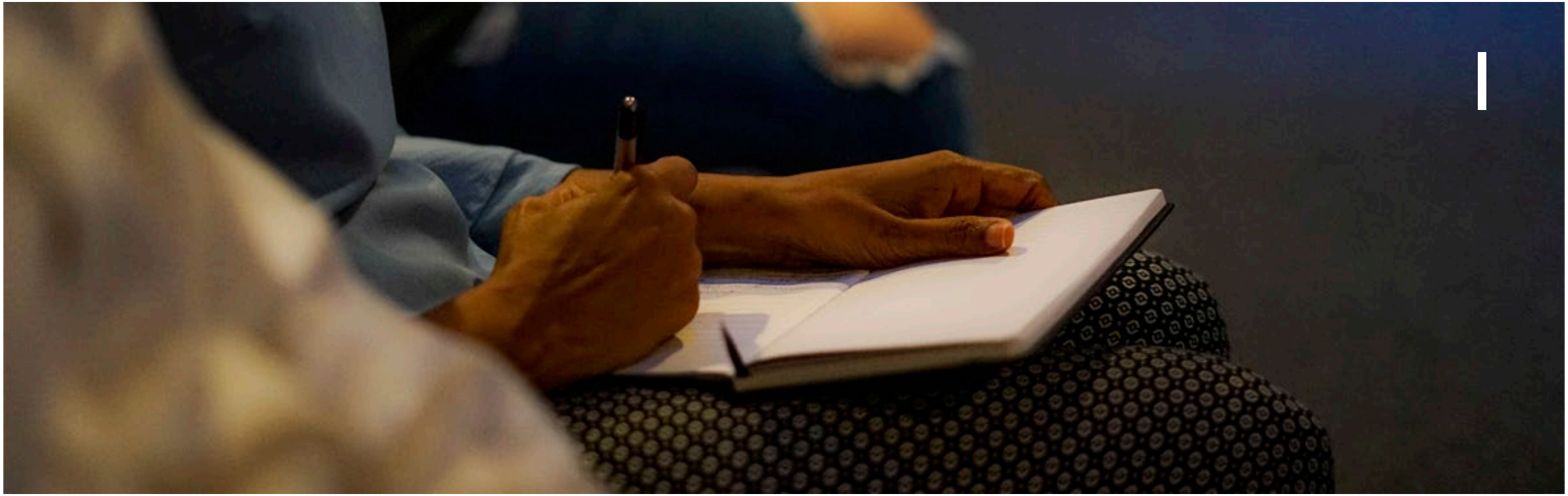
COURSE OUTLINE - CONTINUED

2nd Semester

16

Team Projects Presentations

Cybersecurity law and course team assignment



LESSON 1: INTRODUCTION TO CYBERSECURITY LAW

WEEK 1 LESSON PLAN:
INTRODUCTION TO CYBERSECURITY LAW

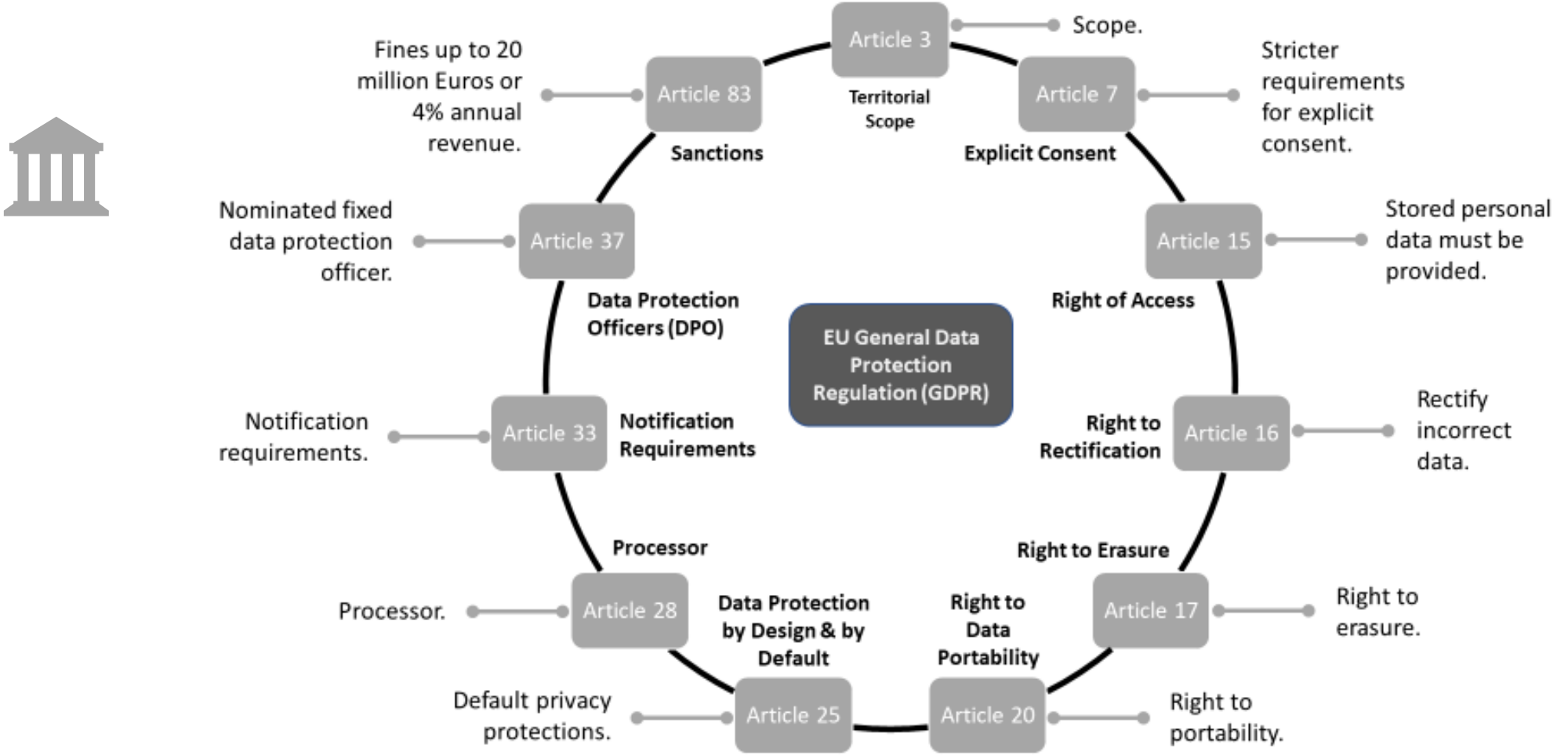
We will cover these topics:

- Course introduction
- Infamous cybercrimes
- Cybercrime taxonomy
- Civil vs. criminal cybersecurity offenses
- Definition of cybercrime
- Cybercrime categories

LESSON 1 LEARNING OBJECTIVES

- Understand the evolution of cybercrime.
- Understand the differences between bad actor- and technology-centric cybercrimes.
- Understand the difference between civil and criminal cyber offensives.
- Understand the definition of cybercrime.
- Understand the categories of cybercrime.
- Know where to integrate cybercrime offenses within an incident response plan.

3.3.4 GENERAL DATA PROTECTION REGULATION (GDPR)



3.4.1 INJURY VS. NO-INJURY CLASS ACTION LAWSUITS

- 2013 Neiman Marcus Group case precedent.
- Rules of civil procedure.
- 2015 Appeal of original finding of no harm.
- Prove standing:
  - Injury-in-fact
  - Causation
  - Redressability

3.7 DATA DISPOSAL LAWS

Stage	Summary
Data creation	Prevent data alteration during creation.
Data use	Prevent data misuse and handling when used.
Data transmission	Prevent data interception and alteration.
Data processing	Prevent data alteration when transformed by processing.
Data storage	Prevent theft, destruction, or errors when backed up.
Data archival	Prevent theft, destruction, loss, or errors when archived.
Data disposal	Prevent reconstitution; ensure total destruction.

3.8 ELECTRONIC WIRETAP LAWS

- Electronic Communications Privacy Act.
- One-party consent.
- Buse use exception.

4.2 CRYPTOGRAPHY LAW

- Cryptology shapes privacy, free speech, and human rights.
- Encrypting data subject to various laws and regulations.
- Encryption of data is fundamental data protection control.
- Many types of encryption technologies.

4.2.1.1 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

- ITAR 22 – CFR 120-130.
- Controls import and export of defense-related articles and services.
- Violations can exceed $1 million

4.2.4.1 DIGITAL SEARCH WARRANTS

- Search warrants generally required.
- Probable cause.
- Digitally describing device to be searched difficult.
- Searching encrypted devices problematic.

4.3.1 STATE ENCRYPTION SAFE HARBOR PROVISION

- All states as well as Guam, Puerto Rico, and the Virgin Islands have incorporated a safe harbor provisions within their data breach statutes.
- Data breach disclosures required when:
  - When data is unencrypted
  - When data is unredacted
  - When data is encrypted, but the key is disclosed
  - Does not meet NIST standards
  - Does not use 128-bit or higher encryption

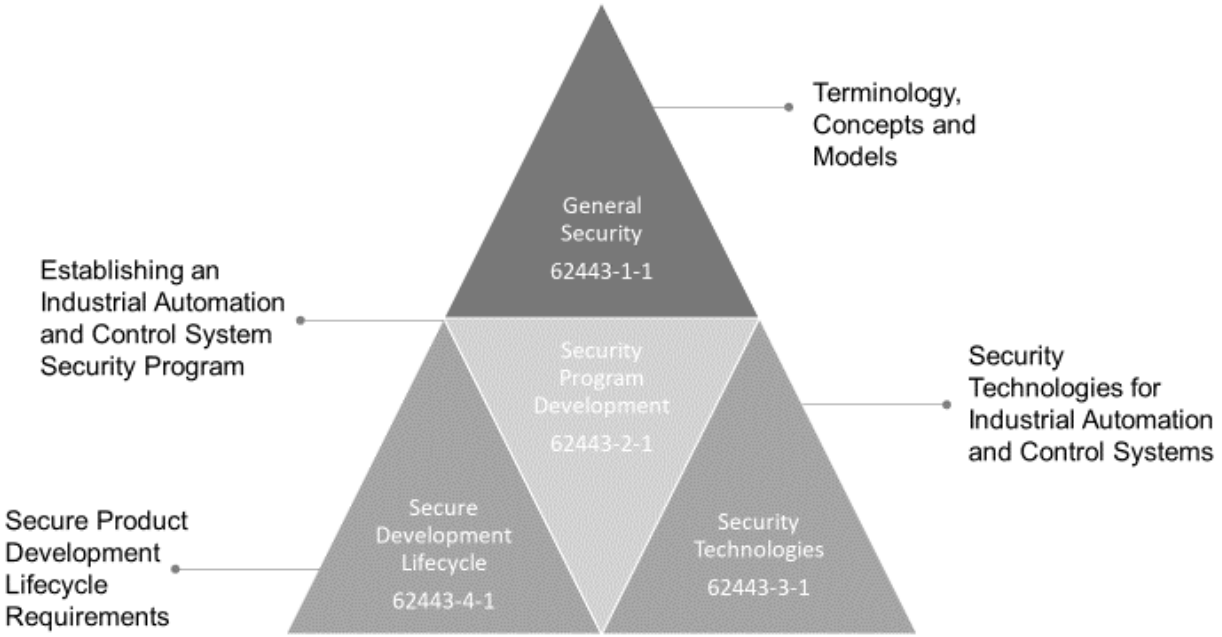
4.8.2 DIGITAL BEST EVIDENCE RULE

- US Federal Rules of Evidence
- Original and best one can produce.
- The following are the types of digital evidence admissible in court:
  - Computer stored/generated documents.
  - Email.
  - Social network communications and postings.
  - Text messages.
  - Website data.

4.8.6 FOURTH AMENDMENT RIGHTS & DIGITAL EVIDENCE

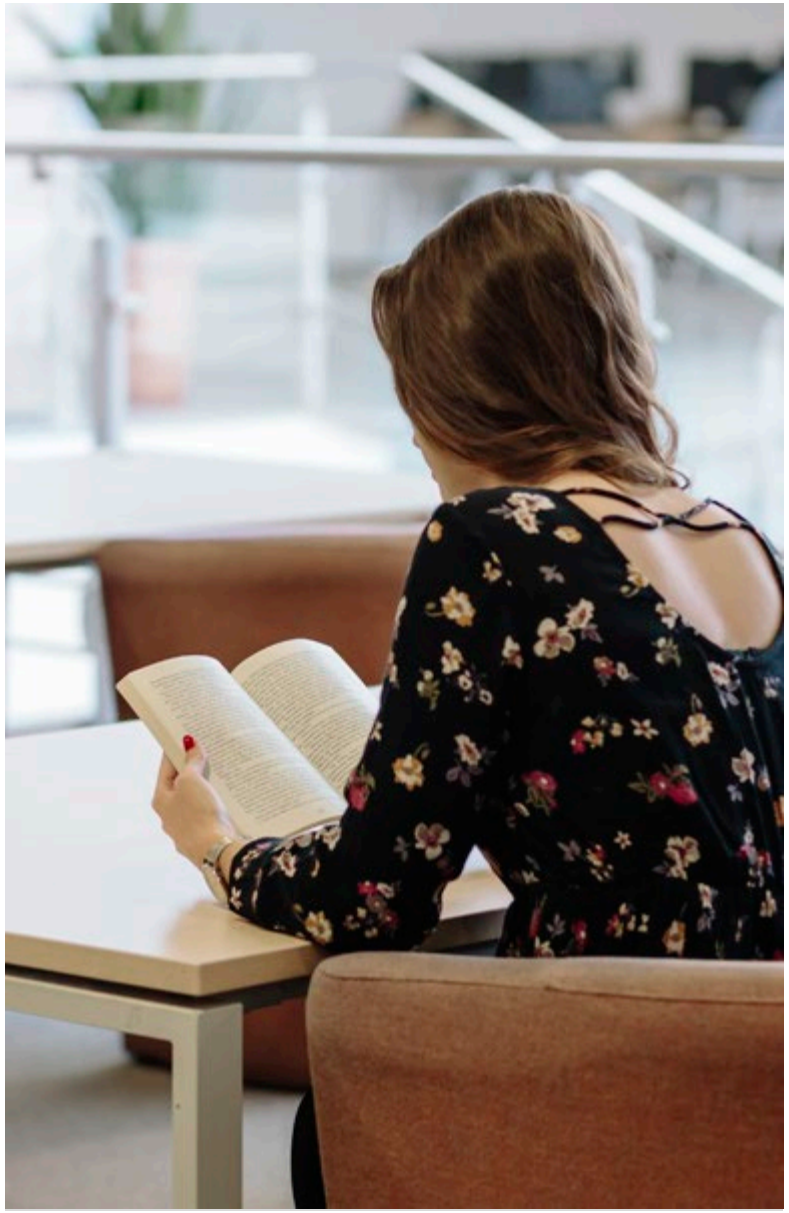
- United States v. Ganias.
- How long can digital evidence be held?
- What purpose can the evidence be used?

5.17.4 INDUSTRY-SPECIFIC CYBER SECURITY STANDARDS



LESSON 10 ASSIGNMENTS

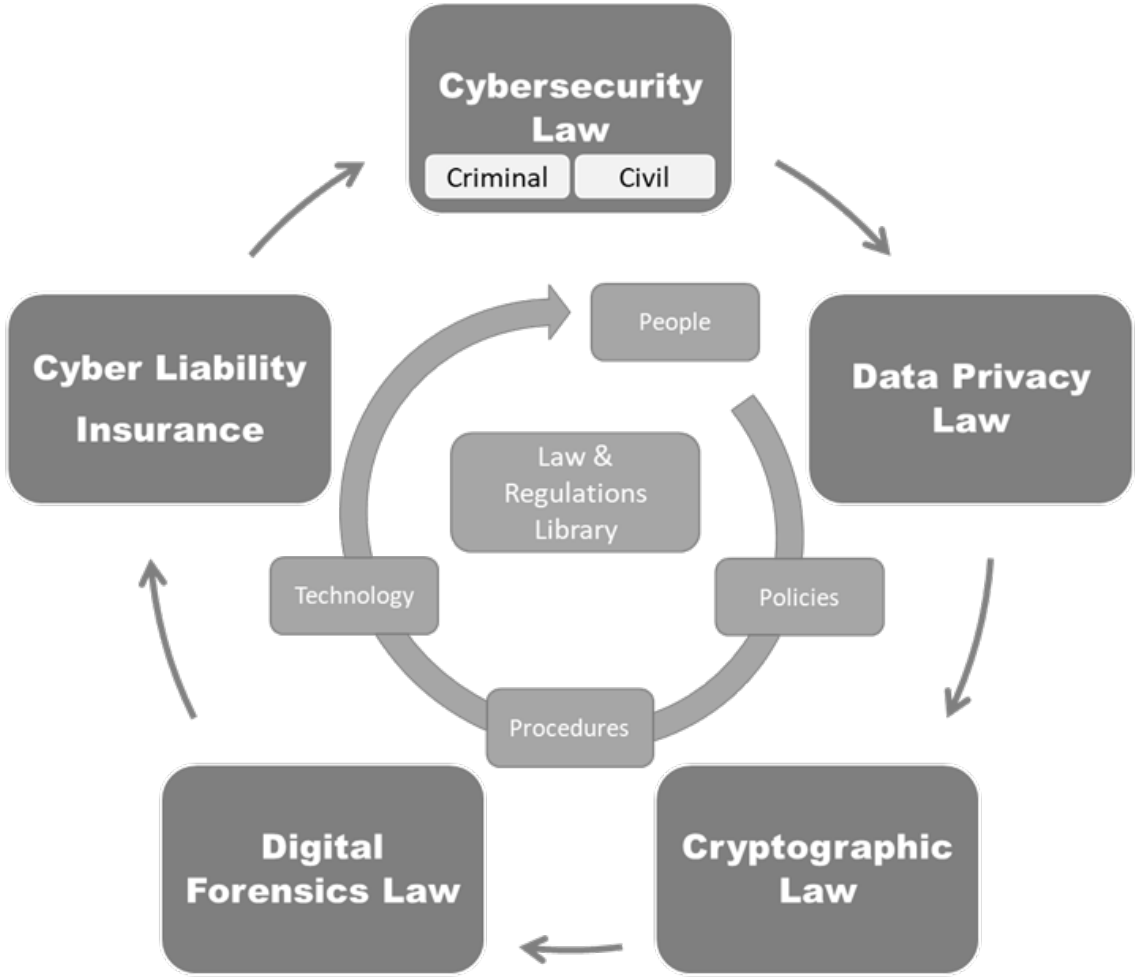
- **Reading:** Assign chapter reading.
- **Case Study:** Assign a case study.
- **Lab:** Define and assign a lab exercise.



6.1 LAW PROGRAM

- It is one thing to have a lot of knowledge about cybersecurity law, but it is another to harness that knowledge into something that is pragmatic and usable. One way to make knowledge actionable is to leverage it into a program. In this case, it is creating a cybersecurity law program for your organization. Think of the program as a plan to accomplish something within a specific structure. The program will provide you with the means to ensure your organization complies with the myriad of laws and regulations as well as abide by the rules of procedure and evidence in the event a company is sued.

6.1.1 MODEL



6.2.5 POLICY CLAIMS

- Average breach claim was $603,900.
- The average payout for crisis services was $307,000.
- The average claim for a large company was $8.8 million.
- Defense: average = $106,000, median = $17,000.
- Settlement: average = $224,000, median = $58,000.
- Regulatory Defense: average = $514,000, median = $84,000.
- Regulatory Fines: average = $18,000, median = $11,000.

6.2.11 SILENT CYBER RISK INSURANCE

- One of the newest issues in cyber risk insurance is "silent cyber risk." This term describes cyber related losses stemming from insurance policies that were not specifically designed to cover cyber risk. For example, an insured leverages their general liability policy to make cyber loss claims.
- These policies were never intended for that purpose. Insurers have come to realize they have substantial unquantified cyber exposures. This exposure is causing insurance companies to quantify their silent exposure. Insurance rating service Moody's announced it will start using its credit-rating expertise to evaluate organizations on their risk to a major impact from a cyberattack.

7.6.7 DATA LOCALIZATION LAWS

- Data localization is a way of storing data within the physical boundaries of a country. For instance, the data which has been generated in China should be stored within the physical boundaries of China. Some countries also demand that the company creating and transmitting this data should have a physical presence within the geographical boundaries. The main reason behind the push in data localization laws has been the increasing concern about how the security and privacy of data will be maintained once it has crossed international borders. Russia began enforcing domestic data storage standards in 2015, forbidding Russian citizens' data to leave the country.