CYBERSECURITY LAW, STANDARDS AND REGULATIONS

INSTRUCTOR COURSE DELIVERY

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.

LECTURE: COURSE INTRODUCTION

- This course is a study of cybersecurity law, regulations and standards from a layman's perspective. The best practices necessary to design, deploy and manage a cybersecurity law program are presented.
  - View cybersecurity law from a Chief Information Security Officer's (CISO) perspective.
  - Acquire a working knowledge of domestic and international cybersecurity laws, regulations and standards.
  - Understand how criminal and civil law procedure works.
  - Create strategies to mount a legal defense against data breach lawsuits.
  - Write papers, research case studies and collaborate on labs to reinforce learning through practical exercises.

LECTURE: EVOLUTION OF CYBERCRIME – 1ST DIGITAL CRIME

Roswell Steffen

Source: AP Wire Photo

Union Dime Savings Bank of New York

Source: NYC.gov

Origin of two-week vacation fraud control in financial firms.

Digital Embezzlement

- March 23, 1973
- 41-year-old Chief Teller
- $1.5 million embezzled
- Computerized bank account siphoning program
- Three-year embezzlement scheme
- 25 employees conducted investigation
- Charged with grand larceny and forgery

Source: New York Times

Source: The New York Archive

LECTURE: DID YOU KNOW?

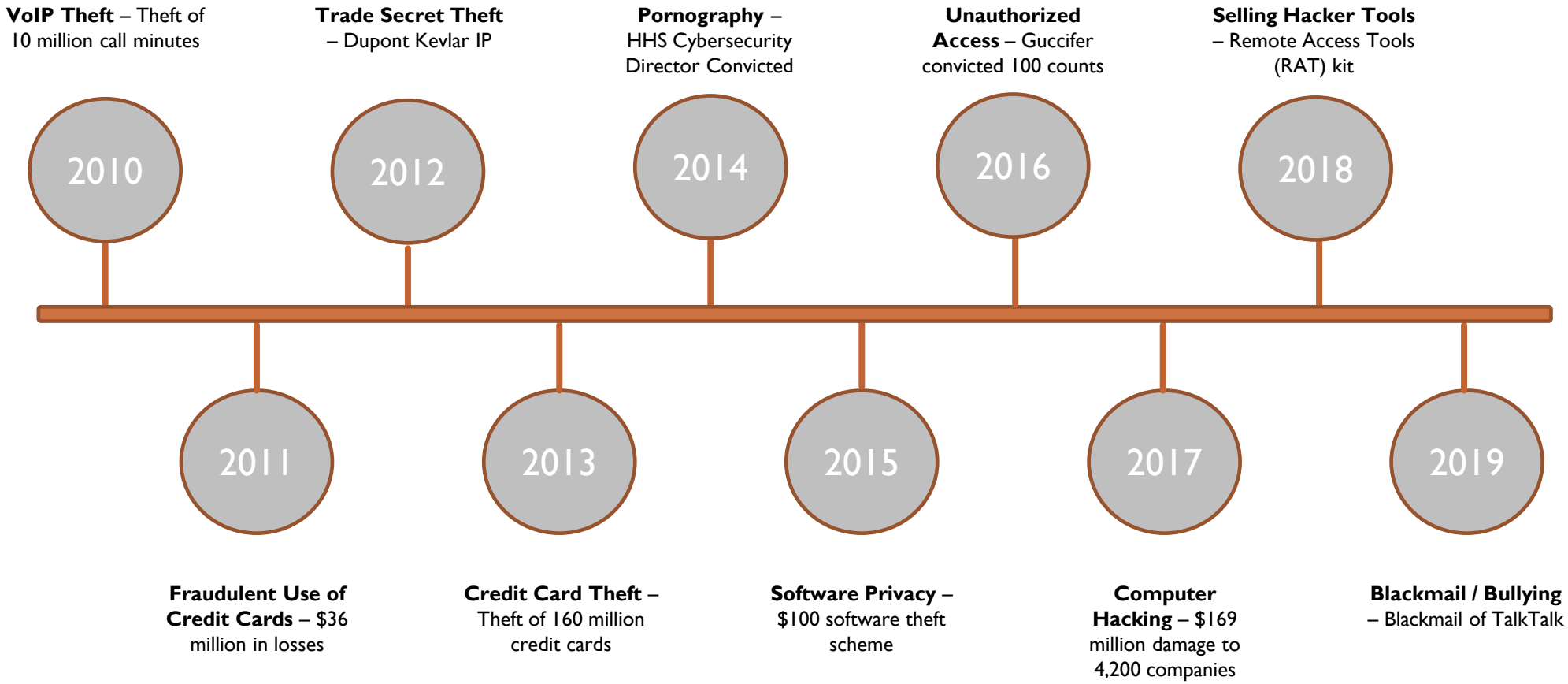
Roman Valerevich Seleznev

Track2

- Arrested July 5, 2014
- $169 million in damages
- Convicted of wire fraud, intentional damage to protected computers and identity theft
- Sentenced to 27 years
- 12-year hacking career
- Arrested wile on vacation

- August 2019
- CapitalOne sued GitHub in class action lawsuit
- Failed in duty to warn regarding hosting of personal data for three months

LECTURE: TEN YEARS OF MAJOR COMPUTER CRIMES



LECTURE: CYBERCRIME TAXONOMY

Bad Actor-Centric	Technology-Centric
Advance Fee Fraud	Cyber Vandalism
Cyber Activism	Data Theft
Cyber Bullying	Distributed Denial of Service (DDoS)
Cyber Blackmail	Exploit Kit Sales
Cyber Espionage	Hacking
Cyber Revenge	Identity Theft
Cybersquatting	Malware
Cyber Stalking	Phishing Attacks
Cyber Terrorism	Prohibited or Illegal Content
Romance Scam	Ransomware
Social Engineering	Scareware
Theft of Service	Spamming

LECTURE: CIVIL VS. CYBERSECURITY OFFENSES

- Criminal cases
  - Insiders or external bad actors committing an illegal cyber offense.
- Civil cases
  - External parties suing a company for harm caused by a cyberattack.

LECTURE: PLAINTIFFS VS. DEFENDANTS

- Plaintiff
  - Claims an entity failed to fulfill a legal duty:
    - Duty to act
    - Duty to protect
    - Duty to warn
- Defendant
  - Defend against a lawsuit:
    - Derivative lawsuits
    - Shareholder lawsuits

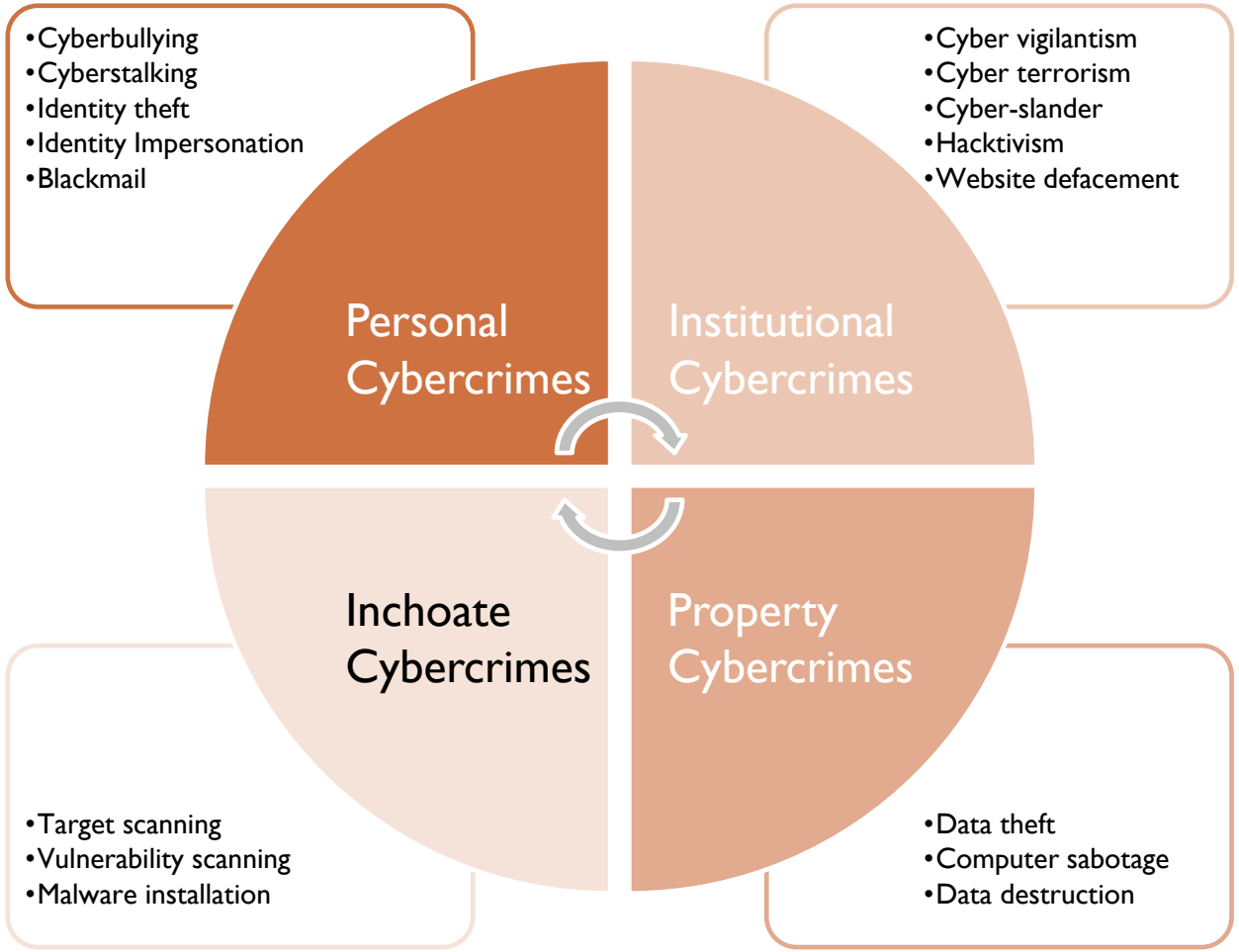
LECTURE: CYBERCRIME DEFINITION

- No universal definition of cybercrime exits.
- Cybercrime, cyber-crime or cyber crime?
- Cybercrime falls into two categories:
  - Everyday crimes committed using computers and networks
    - Theft, embezzlement, terrorist threats, etc.
  - Crimes perpetrated specifically using technology
    - Distributed Denial of Service (DDoS) attack, hacking, ransomware, etc.
- Clear concise definition of cybercrime required to guide cybersecurity programs.

LECTURE: CYBERCRIME DEFINITION

Cybercrime is a criminal act in which computer-based equipment, automated services, or communications mechanism is either the object or the means of perpetrating legal or regulatory restricted or prohibited offenses.

LECTURE: PRIMARY CYBERCRIME CATEGORIES



LESSON 1 ASSIGNMENTS

- **Reading:** Chapter 1- Introduction to Cybersecurity Law: Pages 9 to 20.
- **Case Study:** Research real-life examples of the four primary categories of cybercrimes. Report on the victim, crime and outcome.
- **Lab:** Pair up in teams to create a cybercrime taxonomy replacing the event categories with bad actor- and technology-centric examples.

END OF LESSON 1