Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 13 : Case Studies and Global Perspectives

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 14 : 04-08/01/2026

Instructor: Prof. Dr. Qaysar Salih Mahdi

Introduction

. Introduction Overview

Cybersecurity has evolved from being a technical discipline into a global ethical and legal issue. As digital systems connect nations, cultures, and economies, new moral and legal questions arise about privacy, data ownership, cybercrime, and responsible digital behavior.

Definition:

Cybersecurity ethics refers to the moral principles that guide the responsible use and protection of digital systems, data, and networks.

Cybersecurity law refers to the legal frameworks that define acceptable conduct, accountability, and sanctions for violations in cyberspace.

By the end of this lecture, students should be able to:

1.Understand key ethical theories applied to cybersecurity decisions.

2.Compare international cybersecurity laws and frameworks.

3.Analyze global case studies to identify ethical and legal dilemmas.

4.Propose responsible actions for cybersecurity professionals.

2. Importance of Studying Global Perspectives

Diverse Legal Systems

Different countries have varying laws — for instance, the EU's GDPR emphasizes privacy, while the U.S. focuses on data breach notification and corporate accountability.

Ethical Conflicts:

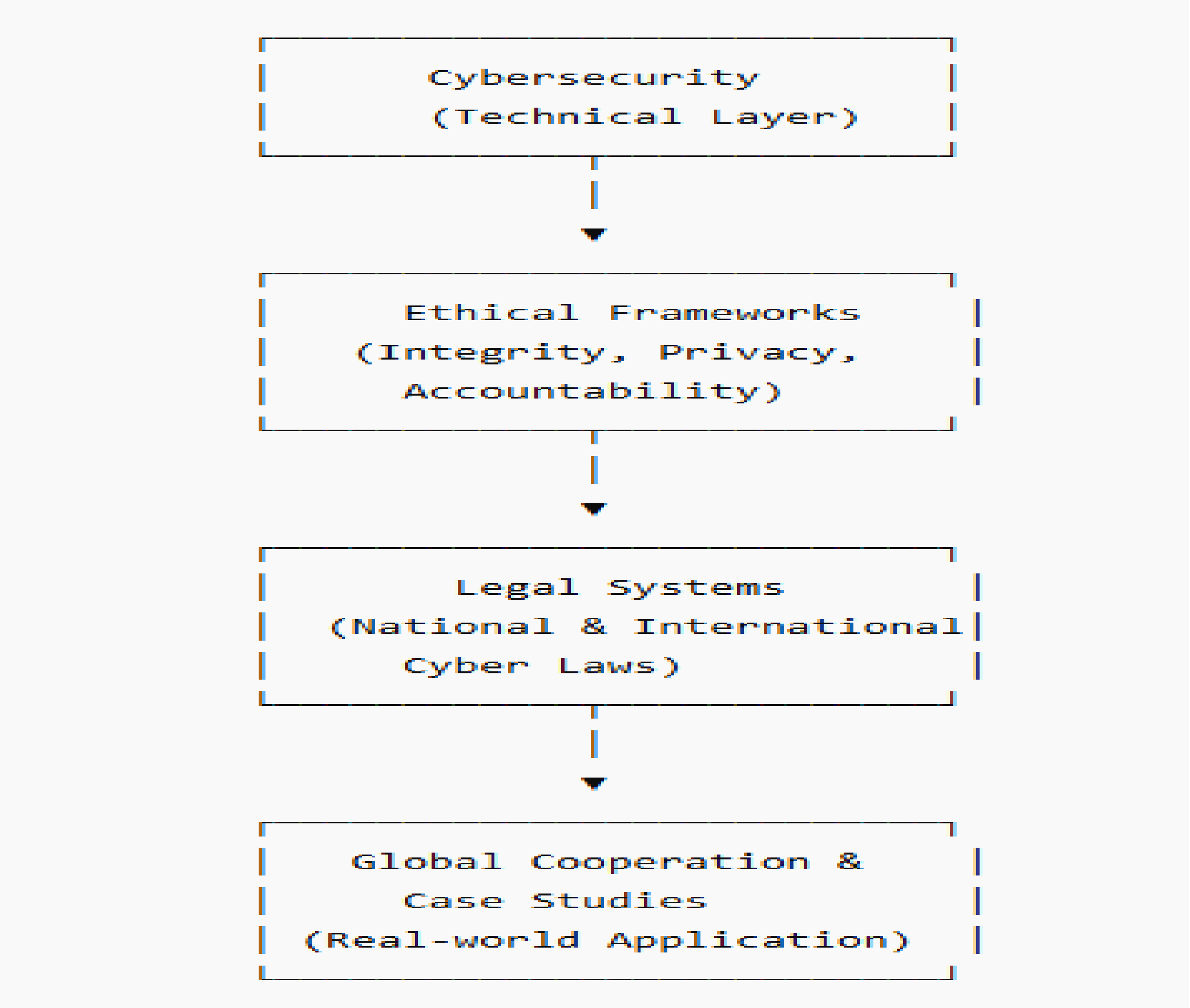
Ethical standards may vary across cultures — what is acceptable data collection in one country may be considered a violation in another.

Global Collaboration:

International treaties like the Budapest Convention on Cybercrime show how nations cooperate to fight cyber threats ethically and legally.

Real-World Impact:
Understanding past case studies (e.g., WannaCry, Facebook–Cambridge Analytica, SolarWinds) helps students connect ethical theories to real decisions.

Below is a conceptual diagram showing how Cybersecurity Ethics and Law interact on a global level:



```
┌──────────────────────────────┐
│        Cybersecurity         │
│      (Technical Layer)       │
└──────────────────────────────┘
               │
               │
               ▼
┌──────────────────────────────┐
│     Ethical Frameworks        │
│  (Integrity, Privacy,         │
│    Accountability)            │
└──────────────────────────────┘
               │
               │
               ▼
┌──────────────────────────────┐
│       Legal Systems           │
│ (National & International│
│    Cyber Laws)                │
└──────────────────────────────┘
               │
               │
               ▼
┌──────────────────────────────┐
│   Global Cooperation &        │
│     Case Studies              │
│ (Real-world Application)      │
└──────────────────────────────┘
```

Cybersecurity incidents are commonplace today. With news making headlines every alternate day, incidents ranging from data theft, security breaches, and digital frauds like phishing, the list is endless. Technological advancements and explosion of the internet usage have further widened the scope for cybersecurity attacks. Threats are getting more and more sophisticated and more evolved and dangerous threats are surfacing.

This blog explores the top 10 real-world case studies on cybersecurity incidents to give a broad understanding of how the threat landscape is evolving and what threats could reach you or your business/organization in today's digitally advanced ecosystem.

Equifax Data Breach (2017)

One of the biggest data breaches globally is the massive breach in 2017 where hackers exploited the web application of Equifax, a multinational consumer credit reporting agency. The incident witnessed a loss of personal data of 147 million consumers approximately. It caused severe damage to the credit bureau both financially and reputation-wise. This massive breach was possible as Equifax made the blunder of not correcting a vulnerability in their web application Apache Struts causing the compromise of personal IDs and data to malicious actors who can use this information even for future thefts. Hackers were able to access about 209,000 credit card details and social security numbers of the British and Canadian clients.

Case studies in a cyber security incident like Equifax shed light on the dire need to keep the company's applications/ software updated and to regularly perform ethical hacking to keep their vulnerability in check. It highlights the importance of efficient vulnerability management and implements strong solutions and measures to prevent such breaches from occurri

Personal data of 147 million consumers exposed

Cause: Exploited vulnerability in Apache Struts web application

Impact: Identity theft, financial loss, reputational damage

Risk Equation: $R = T \times V \times I$

Practical Exercise: $T=0.8$, $V=0.9$, $I=0.95$ → Compute R

Solution: $R = 0.8 \times 0.9 \times 0.95 \approx 0.684$ → High risk

https://www.birchwoodu.org/top-10-real-world-case-studies-on-cyber-security-incidents/

WannaCry Ransomware

Another infamous cybersecurity attack that impacted worldwide, is the WannaCry Ransomware that caused massive destruction and chaos, infecting Windows computer systems worldwide, and impacting over 230,000 computers in over 150 countries in 2017. The hackers took advantage of the vulnerability in the Windows named EternalBlue. Although Microsoft released a security patch before the attack to solve the vulnerability, many users had failed to install it. This attack disrupted operations across various institutions like Hospitals, Government agencies and businesses at the global level. As a response mechanism, a "Kill Switch" was discovered by a security researcher, however, many had already made payment of the ransom to the hackers to restore their computers, with the hackers estimated to have made billions of dollars.

Again, case studies on incidents like this demonstrate the need for installing any new updated version of cybersecurity measures and to keep one's system updated regularl

Colonial Pipeline Ransomware (2021)

Major US fuel pipeline disrupted by ransomware

Cause: Compromised VPN credentials, insufficient network segmentation

Impact: Fuel shortages, emergency response, $4.4M ransom paid

Exercise: Propose immediate mitigation strategies

Solution: Isolate infected systems, implement MFA, restore backups, monitor network traffic

Facebook (Meta) API Scrape Incident

In May 2025, Facebook (Meta) experienced another data scraping incident where hackers collected over 1.2 billion records from a public API that was not properly restricted. Although the data was not directly stolen through a hack, it was gathered using the automated bots, which exploited Meta's API loopholes. This incident proved that you can't always blame direct hacking for privacy breaches, but system design flaws can also cause them. Social media platforms face growing pressure to control data access and prevent scraping at this scale.

WhatsApp Spyware Incident

In 2025, WhatsApp users were targeted by a new zero-click software attack on Graphite. This spyware allowed hackers to access messages and files without the user clicking any links. It is worth noting that victims were mainly journalists, political activists, and human rights workers. The attack revealed how spying tools are evolving and becoming more challenging to detect. Meta quickly released a patch and encouraged users to update their apps. This case proved that even well-known communication tools are not necessarily safe, and regular updates remain one of the simplest yet most impactful ways to stay protected.

Ransomware Trends

Increasing frequency and sophistication globally

Double-extortion: encrypt data and threaten public disclosure

Attack Probability Equation: $P_a = 1 - e^{-\lambda t}$

Exercise: $\lambda = 0.2$/month, $t = 3$ months → P_a ?

Solution: $P_a = 1 - e^{-0.6} \approx 0.451$ (~45%)

Lessons Learned

Patch management is critical (Equifax)

Network segmentation & MFA prevent lateral movement (Colonial Pipeline)

Backup and recovery plans reduce ransomware impact

Employee training and phishing awareness are essential

Global Perspectives

Cybersecurity regulations vary: GDPR (EU), CCPA (US), NIS Directive

International collaboration for threat intelligence sharing is crucial

Emerging threats require proactive risk assessment and global awareness

Quiz and Exercises

1. Main vulnerability exploited in Equifax breach? Answer: Unpatched web applicati

2. Mitigation strategy to reduce Colonial Pipeline impact? Answer: Network segmen

3. Compute risk: T = 0.6, V = 0.7, I = 0.9 → R = 0.378 (Medium risk)

4. Probability of ransomware attack: λ = 0.15/month, t = 4 months → P_a = 1 - e^-0.

Conclusion

Real-world case studies highlight vulnerabilities, mitigation strategies, and ethical considerations

Risk assessment, incident response, and proactive cybersecurity measures are crucial

Global collaboration and adherence to regulations reduce overall cyber risk

References

Wikipedia: Equifax data breach

Wikipedia: Colonial Pipeline cyberattack

ENISA reports on ransomware attacks

Thank you for your listening