

Cybersecurity Law and Policy

Prepared by Dr. Kamal Alieyan

Lecture 2



Introduction to Cyberethics

Lecture 2

Prepared by
Dr. Kamal Alieyan

Outline



- **Ethics In Cybersecurity**
- **Important Ethical Issues In Cybersecurity**
- **Some Ethical Issues Affecting Cybersecurity**
- **The Curious Case Of Black Hats, White Hats And Gray Hats**
- **Ethical Challenges Faced By Cybersecurity Professionals**

Chapter

02

Ethics in Cybersecurity (1/11)

- As we know **Cybersecurity Ethics** is different from **Cyberethics**.
- While **Cyberethics** is more or less concerned with the entire Cyberspace, **Cybersecurity Ethics** is more or less concerned with the security aspect of it.
- **Cybersecurity** practices are concerned with safeguarding data in computer systems and networks (software and hardware).
- The data that is being kept safe may be sensitive and might hold economic value.

Chapter

02

Ethics in Cybersecurity (2/11)

- **Cybersecurity** practices aim to protect confidentiality, integrity, availability (authentication, non-repudiation).
- While **cyberspace** sees users from all respects that communicate with devices and networks, cybersecurity is of utmost importance to cybersecurity professionals.
- Therefore, protection of information is critical as the data might belong to other people.

Chapter

02

Ethics in Cybersecurity (3/11)

For example:

- Safeguarding healthcare data is the job of a cybersecurity professional.
- Thus, a patient's privacy, health, and failure is somehow related to cybersecurity professionals.
- Further, the well-being of patients' families and caregivers may be shielded by the practices of a cybersecurity professional.

Chapter

02

Ethics in Cybersecurity (4/11)

- With the increasing complexity and the underlying challenges in securing online data and systems across a continuously growing landscape of cloud computing services, Wi-Fi-enabled mobile devices, and ‘smart’ objects.
- **The ethical responsibility** to protect data that belongs to others is borne by cybersecurity professionals is a significantly heavy burden.
- Let us take a few examples to analyze the importance of best cybersecurity practices:

Chapter

02

Ethics in Cybersecurity (5/11)

- James is a hard-working employee who works in the finance industry.
- A phishing email opened by him for a bank infects the company network with malware.
- The malware targets customer profiles and authorizes all transactions.

Chapter

02

Ethics in Cybersecurity (6/11)

- Lee and John had been working late at night on an operating system when they identified a vulnerability, which causes execution of malicious code and switches on the camera and voice recorder without the knowledge of the user.
- As they agree on informing the manufacturer the next day and posting the bug on their blog, they are approached by a rival of the phone company, who lures them with money if they do not expose the vulnerability.

Chapter

02

Ethics in Cybersecurity (7/11)

- 
- A company is offering a brand-new Porsche to the 500th caller. Derek, a teenage hacker, takes control of the phone network and effectively blocks calls so that he could be the 500th caller.
 - A massive network outage caused by a virus blocked access to weather updates, following which the Wilson family was stuck in the snowstorm for hours.

Chapter

02

Ethics in Cybersecurity (8/11)

- Pam is a history teacher who teaches sophomores straight from the presentation slides.
- These slides are saved in her email folder.
- A group of students who do not pay attention in her class and got bad grades for the midterm decided to hack her email.
- When she opened her folder the next day, she was shocked to see her picture replaced with a dinosaur and the slides having pictures of cartoons.

Chapter

02

Ethics in Cybersecurity (9/11)

- Which of these hypothetical cases are concerned with ethical questions in cybersecurity? The answer is all of them.
- We observe that in the most cases, the lives of people are impacted by cybersecurity professionals.
- In many cases, cybersecurity best practices may have prevented or limited the harm.
- Thus, cybersecurity professionals are challenged ethically on multiple levels.

Chapter

02

Ethics in Cybersecurity (10/11)

A cybersecurity professional has to deal with several ethical questions on a daily basis. They are sometimes technical as:

1. Which security techniques may be more effective, and what resources do they require?
2. How can network intruders be kept away from the system?
3. What levels and types of security risks are tolerable?
4. How can the users and other affected stakeholders be warned of such risks?

Chapter

02

Ethics in Cybersecurity (11/11)

In many situations, the questions may not be technical as:

1. How to justify the act of exposing others to a breach or greater risk for their own personal profit?
2. How to balance competing duties to the employer?
3. What levels of care must be taken to perform the role responsibly?

IMPORTANT ETHICAL ISSUES IN CYBERSECURITY (1/3)

- As humans, we also look out for respectful and fair treatment by others, entertainment, education, meaningful work, and opportunities for leisure, and creative and political expression, among other things.
- Each of these fundamental interests can be significantly impacted by Cybersecurity practices.

IMPORTANT ETHICAL ISSUES IN CYBERSECURITY (2/3)

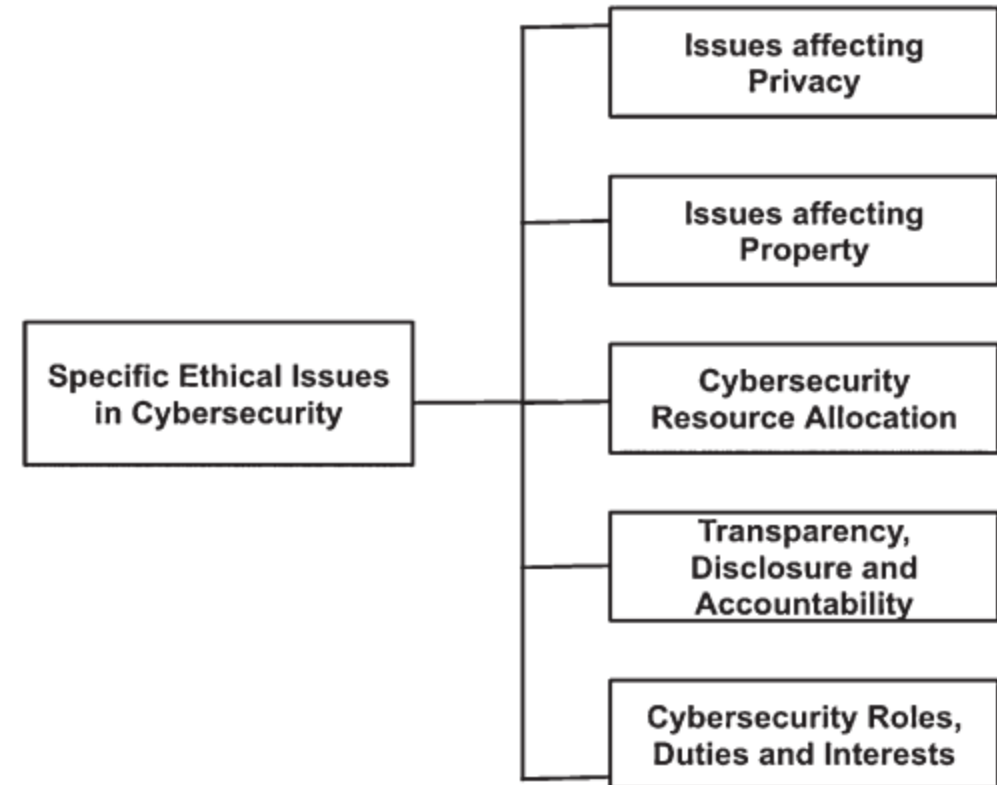
- Therefore, it is right to say that cybersecurity has a much stronger need of holding onto ethics than other technical practices like the engineering of bridges. Making unethical design choices for building bridges may lead to destruction of bodily integrity and health.
- Such damage may have an impact on society and can make it harder for people to flourish. In the realm of cyberspace, unethical choices with respect to cybersecurity may cause different kinds of harm.

IMPORTANT ETHICAL ISSUES IN CYBERSECURITY (3/3)

- Cybersecurity failures have an economic impact on our lives, also damage our reputation, savings, or liberty.
- Firms that are affected by security breaches or health records that are sabotaged are some examples which leave our physical bodies intact yet put us at risk of losing our reputations and privacy.
- Hence, there is a need to introduce effective cybersecurity practices.
- These practices are capable of generating a vast range of benefits for society, some of which include stable infrastructure, diminished social and economic anxiety, and better investment and innovation.

SOME ETHICAL ISSUES AFFECTING CYBERSECURITY (1/7)

- ETHICAL ISSUES AFFECTING PRIVACY
- ETHICAL ISSUES AFFECTING PROPERTY
- CYBERSECURITY RESOURCE ALLOCATION
- TRANSPARENCY, DISCLOSURE, AND ACCOUNTABILITY
- CYBERSECURITY ROLES, DUTIES, AND INTERESTS



SOME ETHICAL ISSUES AFFECTING CYBERSECURITY (2/7)***ETHICAL ISSUES AFFECTING PRIVACY***

Common cyber threats include:

- Identity theft, wherein, PII may be stolen and used to impersonate victims. For example, Using credit card information to make unauthorized purchases.
- Social engineering, in which the adversary uses deception techniques for manipulating individuals into disclosing confidential or personal information to be used for conducting fraud.
- Hacking and other network intrusions are popular techniques for obtaining sensitive information about individuals and their activities. Such information can be used for extortion purposes, and other forms of unethical illegal manipulation.

SOME ETHICAL ISSUES AFFECTING CYBERSECURITY (3/7)***ETHICAL ISSUES AFFECTING PROPERTY***

- It is possible to target property through cyberattacks which may affect intellectual property (IP) and lead to accessing sensitive information like trade secrets, obtain bank account numbers and passwords, and may also cause damage to organization's property. Such harms to property are often targeted by profit-seeking criminal enterprises, by politically-motivated groups, nation-states, detectives, intelligence agents of foreign nations, or by script kiddies and hackers who are seeking to demonstrate their own skills, abilities, and destructive powers.
- Property may not have any ethical value. Hence, any damage to these properties may be termed as an unethical issue in the cybersecurity domain, even if they may not be punishable by law.

SOME ETHICAL ISSUES AFFECTING CYBERSECURITY (4/7)***ETHICAL ISSUES AFFECTING PROPERTY***

- Sometimes, unauthorized destruction of property may be argued to be ethical if it is in the interest of the nation.
- In 2010, the nation-state used the Stuxnet worm to disrupt Iranian centrifuges being used for enriching uranium.
- Sometimes, defenders of a network that has been vandalized by a cyberattack, assert an ethical right to 'hack back' in ways that intend to damage the systems of the cyber attacker, so that no further damage may be caused.
- These situations also generate significant ethical concerns. The release of Stuxnet affected thousands of other computers that were not a part of the Iranian nuclear program.

SOME ETHICAL ISSUES AFFECTING CYBERSECURITY (5/7)***ETHICAL ISSUES AFFECTING PROPERTY***

- Hacking back may be risky for innocent parties as its effects are unknown. Moreover, spoofing strategies in the past have also led to the misidentification of systems responsible for attacks.
- Even though all these arguments are valid, cybersecurity professionals must have a default ethical obligation to protect their organization's networks, or those of their clients, from any and all property-targeting intrusions and attacks.

CYBERSECURITY RESOURCE ALLOCATION

- Cybersecurity operations consume time, money, and expertise.
- System resources bear considerable cost and cybersecurity operations incorporate several operations like power efficiency, data storage capacity, system usability/reliability, and speeds related to network and downloading.
- While cybersecurity operations lead to such high costs, not adopting effective cybersecurity measures may lead to excessive damage and even higher costs.

SOME ETHICAL ISSUES AFFECTING CYBERSECURITY (7/7)

TRANSPARENCY, DISCLOSURE, AND ACCOUNTABILITY

- Ethical issues in cybersecurity practices are linked to transparency, disclosure, and accountability.
- A significant part of cybersecurity is concerned with ***risk management***. And because of that, since risks also have an impact over people in cyberspace, the default ethical duty to disclose the risks when known is necessary. This ensures that the people who might be affected due to the risks can be better prepared.
- In a situation where an organization discovers a critical vulnerability, the customers/clients are informed about the vulnerability in a timely manner so that a patch may be installed or other defensive measures may be taken.

White Hats: Or ethical hackers, are referred to as the good guys in the hacking world. They are concerned with getting into computer networks and systems in order to test or evaluate its security systems.

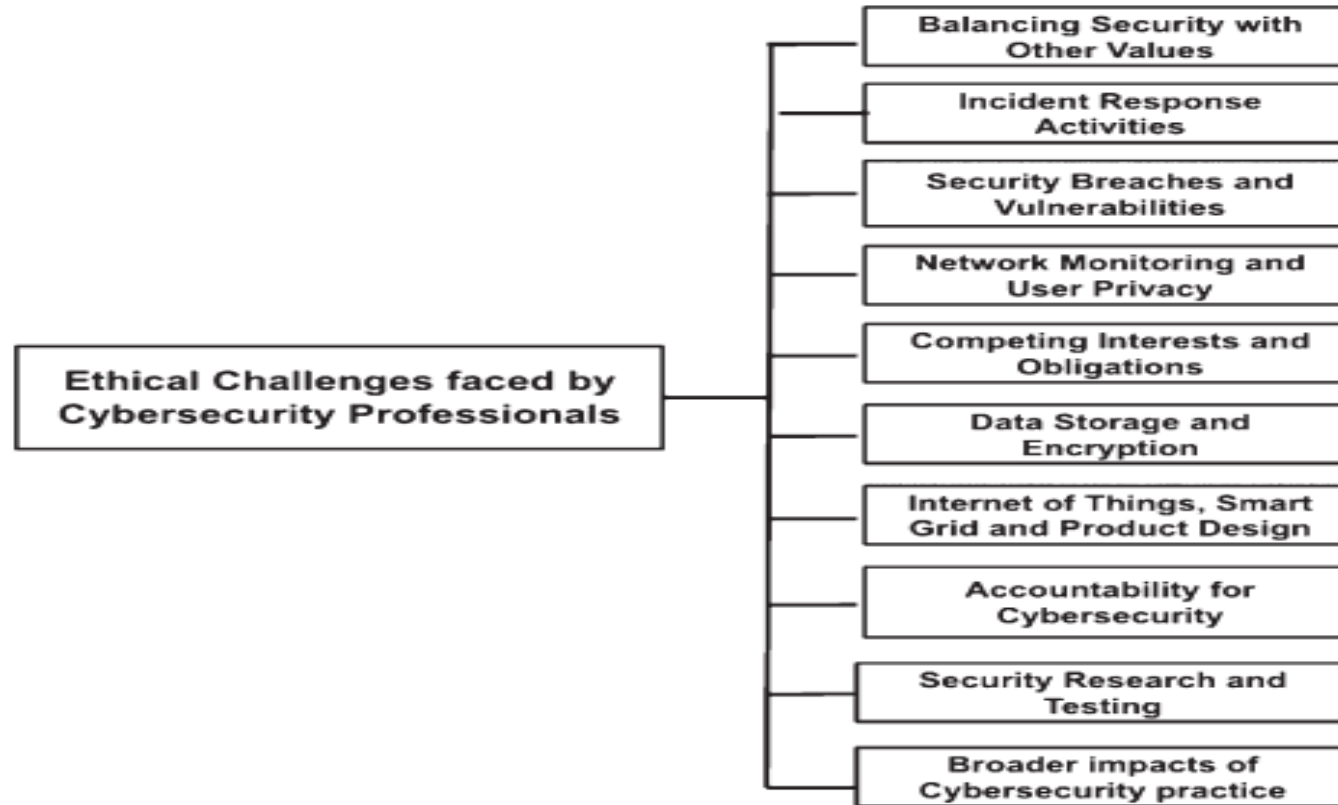
Black Hats: These are commonly known as crackers; these are the bad guys in the hacking world. They hack into computer networks and systems with malicious or criminal intent.

- **Gray Hats:** These are computer security experts who often violate laws or typical ethical standards. While they breach security standards like black hats, they do not have any malicious intent.
- **Green Hats:** These hackers are usually newcomers who work on improving their skills to get better. They often idolize well-known black hats. This is because they are serious about elevating themselves to the real world of hacking.

- **Red Hats:** These are also known as the vigilantes of the hacking world. This is because much of their work is about living and playing by their own rules.
- Although they do want to halt black hats just like white hats, their approach is different. White hats hunt for loopholes and try to build a stronger wall.

- **Blue Hats:** These hackers can be malicious but usually, target a person or company. They launch attacks in order to seek retribution for some type of offense. Novice blue hats start out as Script Kiddies.

ETHICAL CHALLENGES FACED BY CYBERSECURITY PROFESSIONALS(1/3)



ETHICAL CHALLENGES FACED BY CYBERSECURITY PROFESSIONALS(2/3)

- Ethical challenges in balancing security with other values .
- Ethical challenges in incident response (IR) activities.
- Ethical challenges in security breaches and vulnerabilities .
- Ethical challenges in network monitoring and user privacy.
- Ethical challenges with competing interests and obligations

ETHICAL CHALLENGES FACED BY CYBERSECURITY PROFESSIONALS(2/3)

- Ethical challenges in data storage and encryption.
- Ethical challenges in internet of things (IoT), smart grid, and product design.
- Ethical challenges with accountability for cybersecurity.
- Ethical challenges in security research and testing.
- Understanding broader impacts of cybersecurity practice



Thank You