

Ethics in Cyber Security



Dr David Douglas

Senior Lecturer

Central Washington University

IT Management



Introduction

“Cyber Security - the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access.”

Ethics within Cyber Security is paramount when looking at the totality of the work done within the Cyber Security world

Why Cybersecurity Ethics Matter

- Technology is pervasive in modern society.
- Ethical behavior is crucial for maintaining trust and security in the digital realm for cyber security professionals.
- Current trend of attacks presents unique challenges

Ethical Frameworks and Principles

- Deontology, utilitarianism, and virtue ethics.
- Our ethical beliefs guide decision-making in cybersecurity.
- Ethical principles in cybersecurity (confidentiality, integrity, availability, and accountability) inform ethical behavior.

Privacy and Data Protection

- Individual Privacy Rights
- Ethical challenges related to data breaches, surveillance, and the collection and use of personal data
- Privacy scandals and controversies highlight the relevance of this topic

Hacking and Unauthorized Access

- What is hacking and the difference between ethical (white hat) and malicious (black hat) hacking.
- Ethical considerations regarding unauthorized access to computer systems and networks.
- Ethical hacking initiatives illustrate the positive impact of ethical behavior.

Vulnerability Disclosure

- Responsible vulnerability disclosure and its importance in cybersecurity.
- Ethical considerations involved in disclosing security vulnerabilities.
- Bug bounty programs as an example of incentivizing ethical behavior in vulnerability disclosure.

Cyber Warfare/Nation State Actors

- Cyberwarfare and its ethical implications.
- Ethical dilemmas related to state-sponsored hacking and offensive cyber operations.
- Importance of international cooperation and agreements to address these ethical challenges.

Social Engineering & Manipulation

- Social engineering and its role in cyberattacks.
- Ethical considerations related to manipulating individuals for malicious purposes.
- Importance of raising awareness about social engineering tactics and obtaining informed consent in interactions involving personal data.

Cybersecurity Professionals' Responsibilities

- Ethical responsibilities of cybersecurity professionals.
- Importance of professional integrity, confidentiality, and honesty.
- Ethical dilemma of whistle-blowing and the balance between loyalty to employers and the public interest.

Conclusion

- Importance of ethical behavior in cybersecurity for protecting individuals, organizations, and society.
- Reflect on how you can apply ethical principles in your future careers in cybersecurity.

Q & A