THEORIES OF ETHICS – CYBER SECURITY

Lecturer: Mark Gillan

© EXTENDED CLASSROOM

MORAL PRINCIPLES

- Ethics, the moral principles that govern a person's behaviour or the conducting of an activity, plays a crucial role in the field of cybersecurity.
- Cybersecurity professionals often face complex ethical dilemmas that require careful consideration and decision-making.
- Understanding various ethical theories can help them navigate these challenges and make sound judgements.

© EXTENDED CLASSROOM

UTILITARIANISM

- Focuses on maximising overall happiness or minimising overall suffering.
- For the greater good.
- Not so good for minorities.
- In cybersecurity, a utilitarian approach might prioritize actions that protect the greatest number of people, even if it means sacrificing the privacy of a few.
- **Example**: Implementing a security measure that could potentially compromise the privacy of some individuals but significantly reduces the risk of a large-scale data breach.

© Extended Classroom

DEONTOLOGY

- Emphasises adherence to moral rules and duties, regardless of the consequences.
- Strict adherence to rights and wrongs, no half measures, black or white with no grey areas.
- With Deontology, if my hairstyle is rotten, you would tell me, irrespective of hurt feelings or not being nice. It disregards the consequences of the moral rules and duties.
- In cybersecurity, a deontological approach might prioritise protecting individual rights and respecting privacy, even if it means sacrificing some level of security.
- **Example:** Refusing to install surveillance software on employees' devices, even if it could potentially prevent cyberattacks.

© Extended Classroom

SOCIAL CONTRACT THEORY

- Emphasises the importance of social contracts and agreements between individuals.
- In cybersecurity, a social contract theory approach might prioritise upholding the terms of service agreements and respecting user privacy.
- **Example:** Designing systems that are transparent and accountable to users, allowing them to understand how their data is being used and protected.

© Extended Classroom

RIGHTS-BASED ETHICS

- Focuses on protecting individual rights, such as the right to privacy, free speech, and due process.
- In cybersecurity, a rights-based ethics approach might prioritise protecting user data and preventing unauthorised access to personal information.
- **Example:** Implementing strong data protection measures and responding promptly to data breaches.

© Extended Classroom

DUE CONSIDERATION OF THEORIES

- Cybersecurity professionals must consider these ethical theories when making decisions that impact individuals, organisations, and society as a whole.
- By understanding the different ethical perspectives, professionals can possibly make informed choices that align with their values and promote responsible cybersecurity practices.
- Additionally, cybersecurity professionals should be aware of the ethical implications of emerging technologies
- Such as artificial intelligence and machine learning.
- As these technologies become more sophisticated, they raise new ethical questions about bias, transparency, and accountability.

© EXTENDED CLASSROOM

STAY INFORMED

- Cybersecurity professionals must stay informed about these developments and ensure that they are used ethically and responsibly.
- By incorporating ethical considerations into their work, cybersecurity professionals can help build a more secure and just digital world.

© EXTENDED CLASSROOM