



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA5034

Data Security and Compliance

Week 3 :Legal, Ethical, and Professional Issues in Information Security

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Explain why we need laws
- Explore the importance of the ethics

Key Concepts

- Why laws, ethics, and professionalism matter in data security.
- Today: Key legal rules, ethical choices, and your role as a pro.
- Hook: “Ever wonder why hacking’s illegal—or when it’s not?”

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain behavior and are enforced by the state.
- Ethics: regulate and define socially acceptable behaviour.
- Cultural mores: fixed moral attitudes or customs of a particular group.
- Laws carry the authority of a governing authority; ethics do not.
- Liability: the legal obligation of an entity extending beyond criminal or contract law; includes the legal obligation to make restitution.
- Restitution: the legal obligation to compensate an injured party for wrongs committed.

Legal Frameworks

UK Data Protection Act 2018

- Implements GDPR in the UK—rules for personal data.
- Key points: Consent, rights (e.g., access, deletion), fines up to £17M.
- Example: Social media firm fined for mishandling user info.

Computer Misuse Act 1990

- Makes unauthorised access (hacking) illegal.
- Penalties: Up to 7 years in prison.
- Scenario: Student hacks university grades—legal trouble!

Other Key Laws

- Cyber Essentials (UK gov scheme)—basic security standards.
- PECR 2003—rules on email/spam privacy.

General Data Protection Regulation (GDPR)

- Strictly controls how personal data of European Union (EU) citizens is collected, stored, used, and retired
- Affects non–EU organisations that do business with EU citizens
- Challenging requirement is the “right to be forgotten”

Ethical Issues

What's Ethics in Security?

- Right vs. wrong beyond laws—moral choices.
- Example: Should you report a flaw that could harm users?

Understanding Ethics

- Ethics involves determining what is right and wrong beyond legal requirements.
- It encompasses moral principles guiding our behaviour and decisions in various situations.
- **Moral Choices**
 - Ethical decisions often require balancing different values and interests.
 - Examples: ensuring user safety vs. protecting proprietary information

Privacy vs. Security

- Dilemma: Monitoring employees to catch leaks—fair or invasive?
- Case: Retail chain tracks staff keystrokes—ethical?

Black Hat vs. White Hat

- **Black Hat Hackers**

- *Illegal Activities*: Engaging in cybercrimes like stealing data, spreading malware, and causing harm.
- *Selfish Motives*: Driven by personal gain, whether financial or reputational, often at the expense of others.

- **White Hat Hackers**

- *Legal Activities*: Conducting authorised penetration testing to identify and fix security vulnerabilities.
- *Helpful Intentions*: Aiming to improve security and protect organisations and users from potential threats.

- **Ethical Dilemma**

- *Question*: Is "ethical hacking" truly ethical?
- *Considerations*: Balancing the benefits of finding and fixing security flaws with the potential risks and implications.
- *Example*: Where do we draw the line between legal, ethical behaviour and actions that might be perceived as intrusive or harmful?

Reporting Vulnerabilities

- Should you disclose a security flaw that could potentially harm users?
- Ethical considerations: user protection, transparency, and the potential impact on the organisation.

Data Breach Responsibility

- Scenario: You find a breach—tell the boss or the public first?
- Ethics: Transparency vs. company loyalty.

Different Perspectives on Ethical Hacking

- Proponents
 - Improves Security: Identifies vulnerabilities before malicious hackers can exploit them.
 - Legal: Follows rules and guidelines.
 - Protective Motives: Aims to defend organisations and users.
- Sceptics
 - Privacy Issues: May intrude on privacy.
 - Risk of Misuse: Hackers might misuse knowledge.
 - Ethical Ambiguity: Questions if hacking is ever fully justifiable.
- Neutral
 - Context Matters: Ethics depend on context and intention.
 - Balanced Approach: Considers both security needs and ethical implications.

The Ten Commandments of Computer Ethics (Computer Ethics Institute)

1. Thou shalt not use a computer to harm other people
2. Thou shalt not interfere with other people's computer work
3. Thou shalt not snoop around in other people's computer files
4. Thou shalt not use a computer to steal
5. Thou shalt not use a computer to bear false witness
6. Thou shalt not copy or use proprietary software for which you have not paid
7. Thou shalt not use other people's computer resources without authorization or proper compensation
8. Thou shalt not appropriate other people's intellectual output
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans
(Source: Computer Professionals for Social Responsibility)

Professional Issues

Your Role as a Security Professional

- Protect data, follow laws, act ethically.
- Skills: Technical + communication + judgment.

Association of Computing Machinery (ACM)

- Established in 1947 as “the world’s first educational and scientific computing society.”
- Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others’ privacy, and respecting others’ intellectual property and copyrights.

International Information Systems Security Certification Consortium, Inc. (ISC)2

- The code of ethics put forth by (ISC)2 is primarily designed for information security professionals who have earned one of their certifications
- This code includes four mandatory canons:
 - Protect society, the commonwealth, and the infrastructure
 - Act honourably, honestly, justly, responsibly, and legally
 - Provide diligent and competent service to principals
 - Advance and protect the profession
- Example Rule: “Don’t misuse client data”

Real-World Challenges

- Pressure to cut corners (e.g., weak passwords for deadlines).
- Whistleblowing: Report illegal acts or stay quiet?

Career Impact

- Fines, jail, or job loss for breaking laws/ethics.
- Example: IT admin jailed for selling customer data.

Compliance

Organisational Liability and the Need for Counsel

- Jurisdiction: court's right to hear a case if the wrong was committed in its territory or involved its citizenry.
- Long-arm jurisdiction: application of laws to those residing outside a court's normal jurisdiction; usually granted when a person acts illegally within the jurisdiction and leaves.
- Due care: the legal standard requiring a prudent organization to act legally and ethically and know the consequences of actions.
- Due diligence: the legal standard requiring a prudent organization to maintain the standard of due care and ensure actions are effective.

Compliance Is the Law (1 of 2)

- Organizations collect sensitive data called personally identifiable information (PII), which includes:
 - First, middle, and last name
 - Home mailing address
 - Social Security number (SSN)
 - Driver's license number
 - Financial account data
 - Health data and biometric data
 - Authentication credentials

Compliance law obligations

- Review compliance law requirements
- Designate a compliance officer
- Develop policies and standards
- Identify and prioritise compliance gaps
- Implement security controls
- Deliver annual security awareness training

Why Laws Matter in Information Security

- **Protect Data**
 - *Ensure confidentiality, integrity, and availability of information.*
 - *Safeguard personal and sensitive data from unauthorised access and misuse.*
 - *Example: GDPR mandates stringent data protection measures to secure user information.*
- **Punish Breaches**
 - *Hold individuals and organisations accountable for security violations.*
 - *Impose fines, sanctions, and legal actions to deter non-compliance.*
 - *Example: In 2018, British airways were fined a £20M fine due to a significant data breach.*
- **Guide Organisations**
 - *Provide a legal framework for information security practices.*
 - *Help organisations develop policies, procedures, and strategies to protect assets.*
 - *Example: ISO/IEC 27001 sets international standards for information security management systems.*

References

- Slides are devised from the recommended books:
 - Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 7th Edition.
- Some of the slides are devised from my own notes



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk