OTHM Level-4 Diploma

Diploma in Information and Technology

Cyber Security

Lesson Three

U Tin Naing Htwe
Senior Lecturer(ICT)
Optimum Institute

Today's Lesson

Cyber Security

Cyber Security

1. Understand the fundamentals of cyber security.
2. Understand cyber security protection methods.
3. Understand how to manage a cyber security attack.

1. “ Understand the fundamentals of cyber security ”

1.1 Define the term ‘cyber security’.

1.2 Explain how cyber security risks are managed in an organisation.

1.3 Describe the laws and regulations associated with cyber security.

1.4 Summarise the historical development of cyber security.

1.5 Explain the impact cyber security has on individuals and organisations.

1.6 Explain how to keep up to date with the latest cyber security information.

Part 1

1.3 Describe the laws and regulations associated with cyber security.

Web Sites References and Citations

1. National Institute of Standards and Technology **https://www.nist.gov/cybersecurity**
2. National Cyber Security Centre **https://www.ncsc.gov.uk/**
3. IT Governance **https://www.itgovernance.co.uk/**
4. Information Commissioner's Office **https://ico.org.uk/**
5. National Crime Agency (crime threats, cybercrime) **https://nationalcrimeagency.gov.uk/**
6. Interpol crime areas, cybercrime **https://www.interpol.int/**


SURFACE WEB
- Publicly available websites
- Search engines
DEEP WEB
- Medical information
- Legal documents
- Scientific reports
- Subscription info
- Various databases
- Government Intel
- Company specific repositories
DARK WEB
- Illegal websites and information
- Tor-encrypted websites
- Websites that sell drugs
- Private communication forums

Dark web intelligence

- Dark Web Intelligence is used to proactively fight fraud and has proven to substantially reduce losses.

The Surface Web

encompasses everyday internet browsing and is available to the general public.

Examples

- Google
- Yahoo
- Bing
- FireFox
- Wikipedia
- News sources

The Deep Web

protects private accounts and information not meant for public viewing.

Examples

- Academic information
- Medical records
- Legal documents
- Government reports
- Private databases
- Subscription platforms

The Dark Web

is an extension of the deep web, operating on encrypted internet connections.

Examples

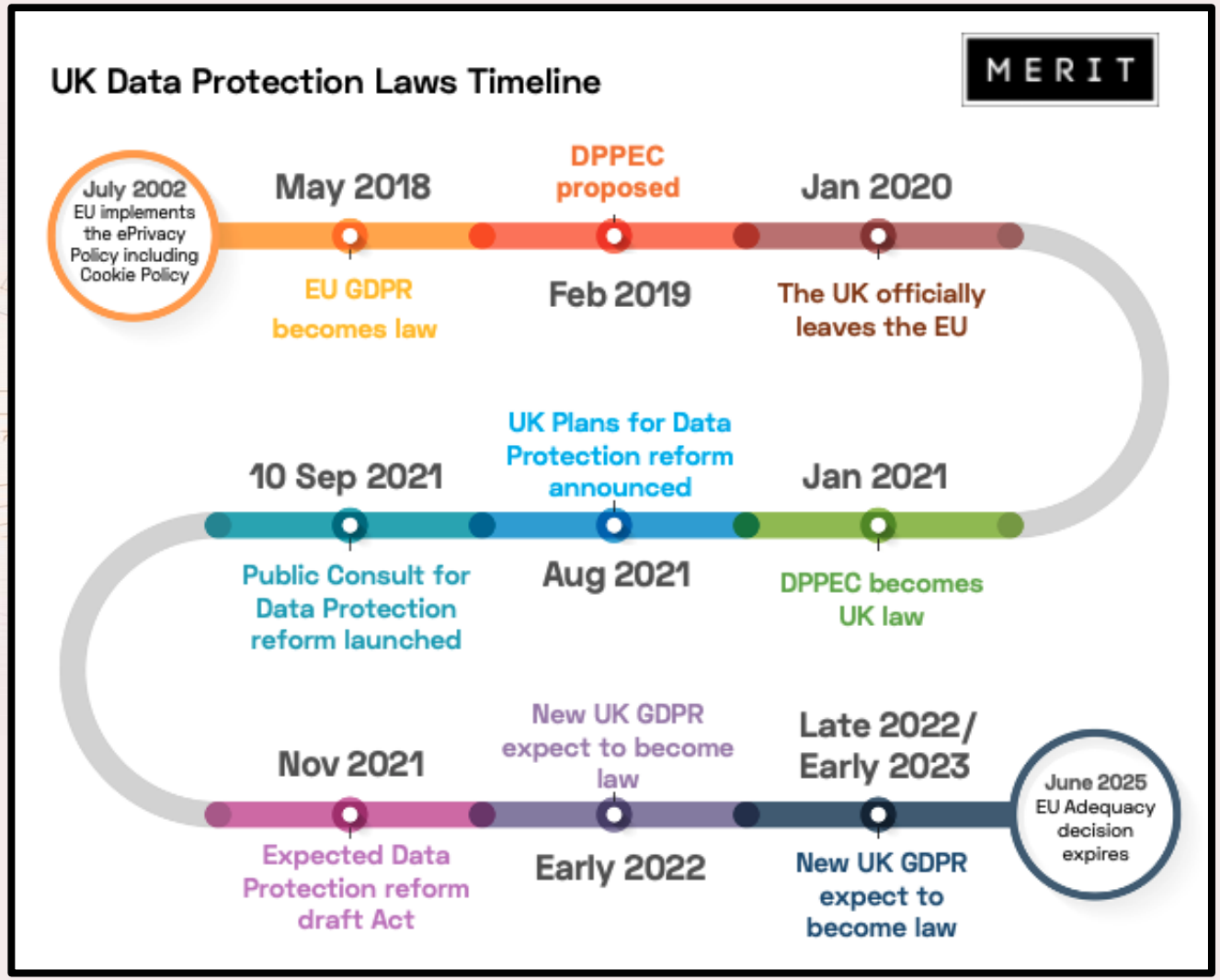
- Drug trafficking
- Cryptocurrency scams
- Illegal activities
- Political protests
- Private communication
- Tor encrypted sites

What Is Cyber Law and Regulations?

- Cyber law and regulation is any law that applies to the **internet and internet-related technologies**.
- Cyber law is one of the newest areas of the **legal system**.
- This is because internet technology develops at such a **rapid pace**.
- Cyber law provides legal protections to **people using the internet**.
- This includes both **businesses and everyday citizens**.
- Understanding cyber law is of the utmost importance to **anyone who uses the internet**.
- Cyber Law has also been referred to as the "**law of the internet**."
- Cyber laws and regulations **directly and indirectly govern** the various cybersecurity requirements for any given business.

Types of cyber law and regulations

1. Federal Laws
2. Federal Regulations & Guidance
3. State Laws
4. International Laws

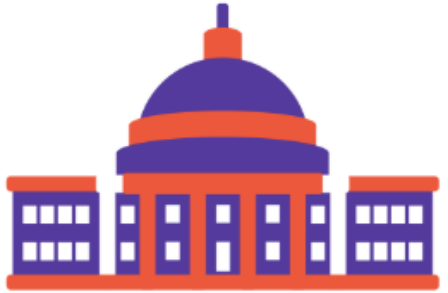


Categories of Cybercrime

Crimes against people

Crimes against property

Crimes against the government



Categories of Cyber Crime

Generally, there are three major categories of cybercrimes that you need to know about. These categories include:

- **Crimes Against People.** While these crimes occur online, they affect the lives of actual people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online related libel or slander.
- **Crimes Against Property.** Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and violations.
- **Crimes Against Government.** When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

What is a cybersecurity standard?

- cybersecurity standard is a **set of guidelines or best practices** that organizations can use to improve their cybersecurity posture.
- Organizations can use cybersecurity standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats.
- Standards can also provide **guidance on how to respond to and recover** from cybersecurity incidents.
- Cybersecurity frameworks are generally applicable to all organizations, regardless of their size, industry, or sector.

https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

https://www.gov.uk/government/organisations/information-commissioner-s-office

Standards of Law and Regulations

- ✓ General Data Protection Regulation (EU) (GDPR)
- ✓ Information Commissioner's Office (ICO) Purpose and Responsibilities
- ✓ Information Security Act
- ✓ Telecommunications Security Act

General Data Protection Regulation (EU) (GDPR)

- The General Data Protection Regulation (GDPR) is a law that governs how organisations process personal data.
- There are now two GDPRs: the **EU GDPR and the UK GDPR**.
- The EU GDPR supersedes the EU Data Protection Directive 1995 and all member state law based on it. It applies to organisations that process or control the processing of EU residents' personal data, wherever the organisations are based.
- The UK version of the EU GDPR is the **UK GDPR**. It is substantially similar to the EU regulation and places similar obligations on data controllers and processors.

https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

Information Commissioner's Office (ICO)

Purpose and Responsibilities

- The ICO **regulates data protection in the UK**.
- We offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.
- We also cooperate with data protection authorities in other countries, including the **European Data Protection Board (EDPB)**, which includes representatives from data protection authorities in each EU member state.

https://ico.org.uk/

Information Security Act

Information communication and technology (ICT) includes any communication device or application and includes: radio, television, cellular phones, computers, network hardware, software, satellite systems, and all of the components associated with those products.

- The EU Cybersecurity Act is the fruit of an initiative started by the European Parliament in 2017 with the goals of permanently establishing an agency to address cybersecurity threats, reducing the complexity for companies to comply with cybersecurity frameworks in each EU member state, and establishing a common cybersecurity certification framework.
- Formal adoption of the EU Cybersecurity Act occurred on March 27, 2019 and resulted in both the formation of the EU Cybersecurity Agency (formerly the ENISA) as a permanent agency and established a **cybersecurity certification framework**.

https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa

Telecommunications Security Act

- The **Telecommunications (Security) Bill** is an proposed Act of the Parliament of the United Kingdom.
- The Bill builds upon and strengthens the Communications Act 2003, in particular the role of **Office of Communications (Ofcom)**, the United Kingdom's Office for Communication, in regards of its role in policing the security of telecommunications and telecom providers.
- The Bill requires the provider of a telecommunications network to ensure that they identify, prepare, and reduce the risk of security compromises.

https://en.wikipedia.org/wiki/Telecommunications_(Security)_Bill

Thank You!

Lesson Three Completed!

U Tin Naing Htwe
Senior Lecturer(ICT)
Optimum Institute