

Information and Communication Technology Law

Lecture Title: Implications of IT on legal processes (I)

Lecturer: Alexia Valenzia

Date: 7 May 2026



Diploma in Law (Malta)



BOV goes dark after hackers go after €13m

Bank of Valletta says clients' funds are safe

- 2019 incident
- Hackers broke into its systems and moved €13 million into foreign accounts
- Hackers sought to make international transfers to banks in the UK, US, Czech Republic and Hong Kong.
- The transfers were blocked within 30 minutes and the banks alerted.
- Reversing such transactions is no easy feat.



BA, BBC and Boots hit by cyber security breach with contact and bank details exposed

What Happened

In June 2023, British Airways (BA), the BBC, Boots, and Aer Lingus were caught up in a significant cyber security incident that exposed the personal data of employees to hackers.

The breach originated with Zellis, a company providing payroll support services to BA and other major organisations, which suffered a cyber-attack. The incident was caused by a previously unseen vulnerability in a widely used file transfer tool called MOVEit, supplied by Progress Software, which Zellis used to transfer files between and within organisations.

Data Compromised

The personal data of current and former BA staff paid through the UK and Ireland payroll was compromised, including:

- Names
- Contact details (home address and work email)
- Dates of birth
- National Insurance numbers
- Banking details (account number and sort code)
- Pay and reward details
- Other ancillary role-related data

BA, BBC and Boots hit by cyber security breach with contact and bank details exposed

Who Is Behind the Attack

Microsoft and IT specialists attributed the cyber-attack to the notorious Russian ransomware group Clap (also written as C10p), based on its similarity to previous attacks carried out by the group. Clap posted a notice on its darknet site claiming it had exploited vulnerabilities in MOVEit to download data from "hundreds of companies" and warned affected organisations to pay a ransom or face having their data published.

Response Measures

BA reported the incident to the Information Commissioner's Office (ICO) and the UK National Cyber Security Centre (NCSC). BA also set up a free credit and web monitoring package with Experian, available to affected staff for 12 months, and encouraged those affected to monitor their bank accounts for unauthorised activity and change passwords on online accounts.



BA, BBC and Boots hit by cyber security breach with contact and bank details exposed

Legal Implications

Those affected may have claims against BA and/or Zellis and/or Progress Software for failing to take the necessary action to keep their personal data safe, potentially seeking compensation for distress and/or financial losses. Potential legal grounds include breach of the UK General Data Protection Regulation, the Data Protection Act 2018, misuse of private information, breach of confidence, and negligence.

Key Takeaway

This incident serves as a stark reminder of the risks posed by supply chain vulnerabilities — where a third-party service provider's security failure can expose the sensitive data of tens of thousands of employees across multiple major organisations simultaneously.



Cybercrime Statistics

“Globally, 323,972 internet users fell victim to phishing attacks in 2021. This means half of the users who were a victim of cyber crime fell for a phishing attack. This is despite Google’s cyber security measures blocking 99.9% of phishing attempts from reaching users.” AAG, The Latest 2025 Cyber Crime Statistics (Updated April 2025)

“With an average of \$136 lost per phishing attack, this amounts to \$44.2 million stolen by cyber criminals through phishing attacks in 2021”. AAG, The Latest 2025 Cyber Crime Statistics (Updated April 2025)

Europol’s Internet Organised Crime Threat Assessment (IOCTA) (14 September 2023) - Cybercrime is becoming more aggressive and confrontational

<https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>



Cybercrime Prevalence

- Network and information security (NIS) policy making and investment have evolved rapidly, especially since 1999:
 - The 'Millenium Bug' or Y2K which led to a complete inventory of computing inside large organisations, often for the first time since the deployment of PCs in the mid-1980s
 - DoS attacks beginning in 2001 against Yahoo! and eBay
 - Business continuity planning in the wake of the 9/11 attacks



Cyber threats hitting Malta's businesses (2026)

- Malta ranks third in the EU for businesses hit by cybersecurity incidents, with 28.7% of companies experiencing attacks in 2023 (Eurostat, October 2025).
- A PwC Malta honeypot study recorded over six million attacks targeting Maltese infrastructure in just three months, five million of those being DDoS (Distributed Denial of Service) attempts designed to overwhelm systems until they crash. Malta's Police Cyber Crime Unit handled 4,500+ investigations in three years, with 81% of all fraud cases now occurring online. 58% of DDoS attacks target banks, 21% hit government financial websites, and ransomware increasingly targets service providers (29%) and insurers (17%), with average ransoms reaching €250,000.
- Phishing remains the weapon of choice, linked to 95% of all breaches through human error.
- More information on the Eurostat findings read [here](#).



Legal Frameworks Surrounding Cyber Security

Malta does not have a specific law which regulates cybersecurity. Accordingly, several laws govern different aspects of cybersecurity, and such laws include both primary and secondary legislation.

EU:

- NIS Directive – NIS II
- EECC
- GDPR
- DORA
- Cyber Resilience Act



NIS 2 Directive

- Adopted by the European Parliament and the Council on 14 December 2022.
- The review of the NIS Directive was carried out in response to the increased cybersecurity threats resulting from the ever-accelerating digitalisation (especially in the context of the COVID-19 pandemic).
- The NIS 2 Directive is intended to address the limitations of the previous NIS Directive and to make it suitable for current and future needs.
- Among the changes introduced by means of the NIS 2 Directive is the expansion of the scope of application to include new sectors based on their importance in terms of societal and economic activities within the internal market. The added sectors include, but are not limited to, entities operating in the sectors of health, public administration, manufacturing, and social media platforms
- The NIS 2 Directive entered into force on 16 January 2023. As with other Member States, Malta had until 17 October 2024 to transpose the provisions of the NIS 2 Directive into Maltese law. SL 460.41 was published on 8 March 2025



EECC

- The purpose of the European Electronic Communications Code (EECC) Directive was to revise and consolidate the directives forming part of the EU telecommunications regulatory framework, on which the domestic legal system for telecommunications is based.
- Among the objectives of the EECC is to promote the interests of EU citizens by maintaining the security of networks and services. As defined in the EECC itself, 'security of networks and services' refers to the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of those networks and services themselves, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those networks or services.



EECC

- The ECNS Regulations deal with security under Part VII. In particular, the ECNS Regulations are concerned with security incidents and require undertakings providing public electronic communications networks or publicly available electronic communications services, or gateway operators, to take certain measures to appropriately manage the risk involved and to ensure a level of security appropriate to that risk, so that the incidence of security incidents is prevented or minimised. The ECNS Regulations also state that an undertaking providing publicly available electronic communications services over public electronic communications networks must undertake all necessary measures to ensure the maximum availability of such services in the event of a catastrophic network breakdown or circumstances of force majeure.

DORA

- DORA consolidates and upgrades the regulatory framework on digital operational resilience for financial entities with a view to ensure that financial entities have the capability to withstand, respond to, and recover from cyber and other ICT risks and disruptions, which would help preserve the stability and integrity of the EU financial market. DORA lays down requirements concerning the security of network and information systems supporting the business processes of financial entities, including requirements on:
 - ICT risk management;
 - reporting of major ICT-related incidents;
 - testing of ICT systems, controls, and processes;
 - information and intelligence sharing between financial entities; and
 - contracts concluded with ICT third-party service providers.
- DORA has a broad coverage to include nearly all financial entities (with the exception of those listed in Article 2(2) thereof), but the application of certain rules depends on the size and overall risk profile of the financial entity, and the nature, scale, and complexity of its services, activities, and operations. DORA shall become applicable on 17 January 2025.

The Cyber Resilience Act

Diploma in Law (Malta)

Scope:

- products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules

Requirements

- Security requirements
- Vulnerability handling requirements



High risk AI systems

- Conformity with CRA → Deemed in compliance with accuracy and robustness requirement of AI Act

Critical Products

Free movement

- Only if compliance with requirements

Obligations

Manufacturers

- Ensuring compliance with requirements
- Cybersecurity risk assessment
- Documenting relevant cybersecurity aspects
- Reporting

Importers

- Placing on market only if conformity with regulation
- Corrective measures if product is not in conformity

Distributors

- not placing on the market if reason to believe that conformity is not achieved
- Ensuring that corrective measures are taken if necessary

Cyber Resilience Act: Assessment and Enforcement

Conformity

- In specific cases presumed
- Technical documentation
- Conformity assessment

Market Surveillance

- Evaluation if believed that product carries risk

Penalties

- non-compliance with essential requirements: up to 15.000.000€ or 2.5% of annual worldwide turnover
- Non-compliance with other measures: up to 10.000.000€ or 2% of annual worldwide turnover



What Constitutes 'Cybercrime'?

- There is no official definition of 'cybercrime' however, it is widely understood as being the facilitation of traditional criminal activity (be it organised or otherwise) through the use of computer systems.
- More novel means of computer crime may only be committed through digital means (such as DDoS attacks), which only came about as computer systems became more advanced, facilitating the scale and speed at which such crimes may be carried out.
- Malta is a signatory to the Budapest Convention on Cybercrime (Council of Europe Cybercrime Convention) and has therefore implemented the provisions therein within our Criminal Code (Chapter 9, Laws of Malta).



Types of Cybercrime

- using botnets—networks of devices infected with malware without their users' knowledge—to transmit viruses that gain illicit remote control of the devices, steal passwords and disable antivirus protection
- creating “back doors” on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets
- creating online fora to trade hacking expertise
- bulletproof hosting and creating counter-anti-virus services
- laundering traditional and virtual currencies
- committing online fraud, such as through online payment systems, carding and social engineering
- various forms of online child sexual exploitation, including the distribution online of child sex-abuse materials and the live-streaming of child sexual abuse
- the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services.





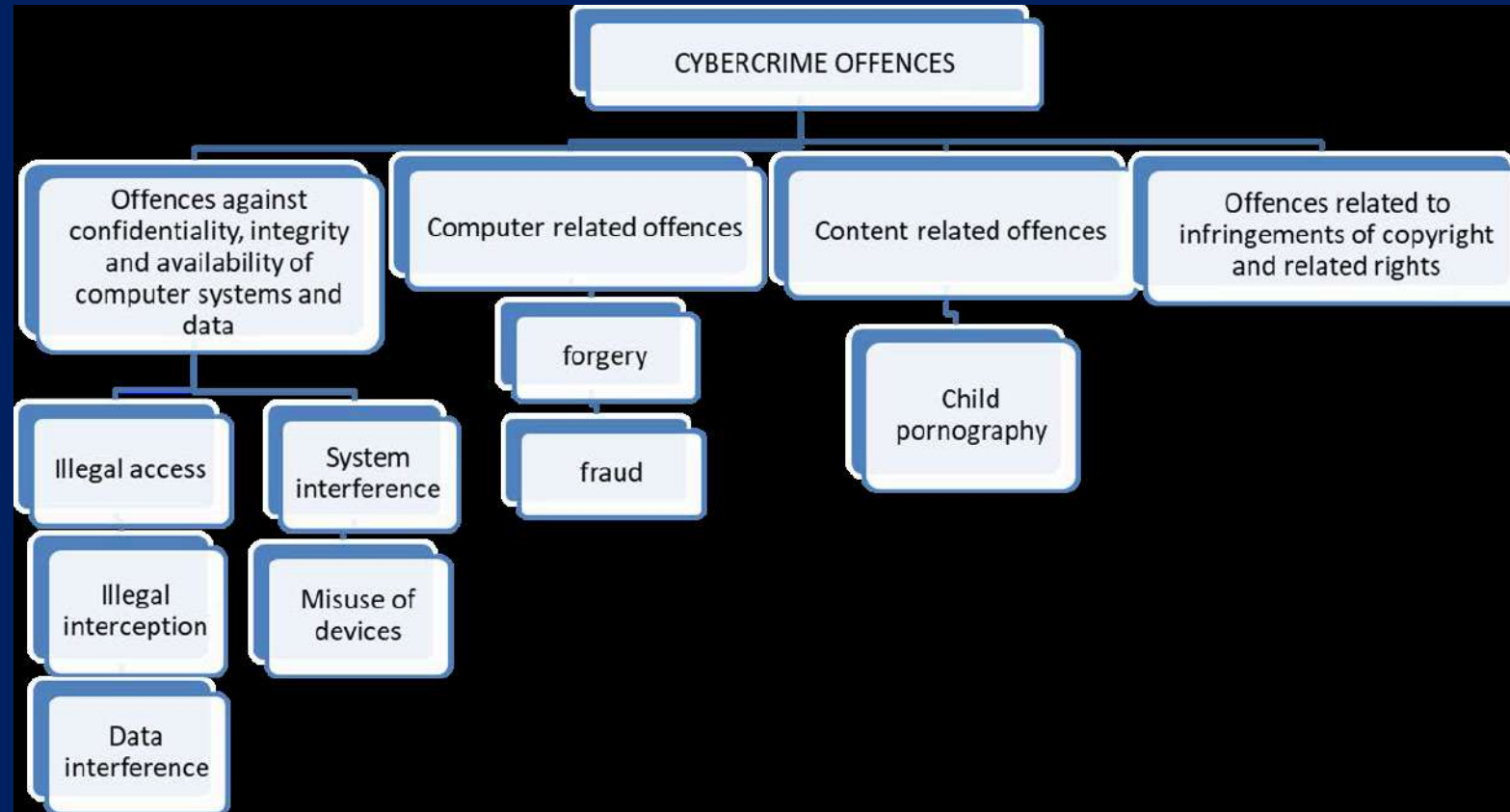
<https://www.youtube.com/watch?v=P6x4GhjDVHY>

What is Cybercrime from a legal perspective?

- The Budapest Convention classifies cybercrime into 4 categories:
 1. Offences against confidentiality, integrity and availability of computer data and systems
 2. Computer-related offences
 3. Content-related offences
 4. Offences related to infringements of copyright



The Budapest Convention on Cybercrime



European Commission – Legal Aspects of Digital Forensics

Criminal Offences Under Maltese Law

- The old legal maxim “actus non facit reum, nisi mens sit rea” means that the criminal act alone does not amount to guilt, it must also be accompanied by a ‘guilty mind’.
- The general principle within the field of Criminal Law is that **three** distinct elements must co-exist for there to be a crime:
 1. The Legal Element
 2. The Material Element
 3. The Mental Element

The Legal Element

- “*Nullum crimen sine lege*” means that an action may only be deemed as a criminal offence if it is prohibited by a specific law.
- Prior to the amendments relating to computer misuse & extreme/child pornography within our Criminal Code, attributing a particular crime to an offence was tedious and challenging as our law did not cater for (now) illegal activity conducted through digital means.
- Previously, there was a valid (legal) argument to be made that an offence could not be committed as Maltese Law did not define an action (such as hacking) as a criminal offence.



The Material & Mental Elements

- The Material element is the “*actus reus*”, which means the commission of an offence by the person to be held liable.
- In certain cases, a purposeful omission could also give rise to criminal liability, provided that the other formalities are present.
- The Mental element is the “*mens rea*” or the ‘guilty mind’ with which the act is done. This is a procedural necessity and cases are dismissed typically on this basis, as it is particularly difficult to prove a persons’ malintent.

Various Forms of Cybercrime

- Computer Fraud
- Phishing
- Hacking
- DDoS
- Malware
- Trojans and other viruses
- Ransomware
- Sexploitation
- Cyberterrorism
- Child Pornography
- Infringement of intellectual property rights

Computer Misuse

- Malta's Criminal Code (Chapter 9, Laws of Malta) regulates computer misuse through Articles 337B-337H
- Based on the UK Computer Misuse Act and the Budapest Cybercrime Convention
- Drafted and defined broadly to account for 'all' scenarios



Computer Misuse

- Definitions
- Unlawful access to, or use of, information
- Misuse of hardware
- Commission of an offence outside Malta
- Offences and Penalties
- Search and Seizure



Interpretation – Art. 337B(1)

- "**computer**" means an **electronic device** that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, **software** and communication facilities that are connected or related to a computer in a **computer system** or **computer network**;
- "**computer network**" means the interconnection of communication lines and circuits with a computer through a **remote device** or a **complex** consisting of two or more **interconnected** computers;
- "**computer output** " or "**output**" means a statement or a **representation of data** whether in written, printed, pictorial, screen display, photographic or other film, graphical, acoustic or other form produced by a computer



Interpretation – Art. 337B(1)

- **"computer software" or "software"** means a computer program, procedure or associated documentation used in the operation of a computer system
- **"computer supplies"** means punched cards, paper tape, magnetic tape, disk packs, diskettes, CD-roms, computer output, including paper and microform and any storage media, electronic or otherwise
- **"computer system"** means a set of related computer equipment, hardware or software



Interpretation – Art. 337B(1)

- "**function**" includes logic, control, arithmetic, deletion, storage, retrieval and communication of data or telecommunication to, from or within a computer;
- "**supporting documentation**" means any documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.



Unlawful access to, or use of, information – Art. 337C

A person who without authorisation does any of the following acts shall be guilty of an offence

- a) **uses** a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;
- b) **outputs** any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;
- c) **copies** any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
- d) **prevents or hinders access** to any data, software or supporting documentation;
- e) **hinders or impairs** the operation of any system, software or the integrity or reliability of any data.



Unlawful access to, or use of, information – Art. 337C

- f) **hinders or interrupts** the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;
- g) **takes possession** of or makes use of any data, software or supporting documentation;
- h) **installs, moves, alters, erases, destroys**, varies or adds to any data, software or supporting documentation;
- i) **discloses** a password or any other means of access, access code or other access information to any unauthorised person;
- j) **uses another person's** access code, password, user name, electronic mail address or other means of access or identification information in a computer;
- k) **discloses** any data, software or supporting documentation unless this is required in the course of his duties or by any other law;



Unlawful access to, or use of, information – Art. 337C

- l) **intercepts** by technical means, non-public transmissions of data, to, from or within an information system or a computer system, including electromagnetic emissions from an information system or a computer system carrying such computer data;
- m) **produces, sells, procures for use, imports, distributes, possesses or otherwise makes available** a device, including a computer program, designed or adapted primarily for the purpose of committing any of the acts in paragraphs (a) to (k) or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.



What does acting without authorisation mean? Article 33C(2)

A person is deemed to be acting without authorisation if he is not duly authorised by an entitled person.

... but what is an entitled person?

A person is deemed to be entitled if the person himself is entitled to control the activities defined in (a) – (k) or in article 4(a) or 4(b) of this Sub-Title.



Misuse of Hardware – Art. 337D

Any person who, **without authorisation**, does any of the following acts shall be guilty of an offence:

- a) **modifies** computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.
- b) **takes possession** of, damages or destroys a computer, computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network or impairs the operation of any of the aforesaid.

Commission of an offence outside Malta – Art. 337E

- If any act is committed outside Malta which, had it been committed in Malta, would have constituted an offence against the provisions of this Sub-title, it shall, if the commission affects any computer, software, data or supporting documentation which is situated in Malta or is in any way linked or connected to a computer in Malta, be deemed to have been committed in Malta.
- Notwithstanding sub-article (1), if the offence is committed partially outside Malta and which had it been committed in Malta constituted an offence contrary to the provisions of this Sub-title, said offence shall be deemed to have been committed in Malta.



Offences and Penalties – Art. 337F

1. Fine not exceeding €23,293.73, or imprisonment not exceeding **four** years, or **both** such fine and imprisonment.
2. When such offence is directed towards the Government or a public authority or hinders/hampers any public service or utility, the penalty shall be a fine ranging from €500 to €150,000 or imprisonment ranging from **three** months to **ten** years, or both such fine and imprisonment.

Subsequent offences shall be fined at a minimum of €5,000.



Offences and Penalties – Art. 337F

3. The increased penalty range shall also apply when committed by an employee to the prejudice of their employer.
4. If a person produces any material or acts in preparation or furtherance of an offence, the same punishment for that offence shall be awarded.
5. Accomplices or any person who aids or abets the commission of an offence shall be equally liable.
6. The burden of proof lies on the party alleging authorisation and this burden shall not be considered to have been discharged with the mere uncorroborated testimony of the person charged (hence further proof is required).



Misuse of electronic communication networks or apparatus to transmit misleading information or spread false news

Added in 2025 (ACT No. XXXVII of 2025)

Article 337B

"**electronic communication apparatus**" means any equipment or machinery howsoever so described;

"**electronic communication network**" means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and where applicable switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit-switched and packet-switched, including Internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, irrespective of the type of information conveyed.



Misuse of electronic communication networks to transmit misleading information or spread false news

Article 337I:

Whosoever, knowingly with intent to cause harm, shall engage in actions that impact the integrity of electronic communications or with intent to spread false news shall use an electronic mail address or website domain likely to deceive the recipient as to the identity of the person transmitting the information or news or otherwise make use of an electronic communication network or apparatus for any of the purposes mentioned above, shall be guilty of an offence and shall on conviction, be liable to imprisonment for a term not exceeding two years, or to a fine (multa) not exceeding €10,000 or both such imprisonment and fine.

Search, Seizure & Retention – Arts. 337G & 355P

- **337G:** The Minister may, for the purposes of this Sub-title, by regulations prescribe:
 - a) the manner in which the Police may search computers, computer systems or computer supplies and seize data or software stored therein;
 - b) procedures and methods for handling evidence that is in an electronic form.

355P: The Police, when **lawfully** on any premises, may seize anything which is on the premises if they have **reasonable grounds** for believing that it has been obtained in consequence of the commission of an offence or that it is evidence in relation to an offence...and that it is necessary to seize it to prevent it being concealed, lost, damaged, altered or destroyed.

Computer Data & Retention – Arts. 355Q & 355S

- 355Q: The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.
- 355S: (1) Anything which has been lawfully seized by the Police may be retained so long as is necessary in all the circumstances.
- (2) Without prejudice to the generality of the aforesaid, anything lawfully seized by the Police under this Code may be retained for use as evidence at the trial or for forensic examination or any other aspect of the investigation, or in order to establish the thing's lawful owner.
- (3) The Commissioner shall provide for the proper custody of anything seized.





The Role of Local and Inter-state IT Crime Authorities



The Maltese Cybercrime Unit

- The Cyber Crime Unit is a specialised section within the Malta Police Force set up in 2003. It primarily provides technical assistance in the detection and investigations of crime where the computer is either the target or the means used.
- Not limited to criminal acts associated with technology, but extends to investigations of more traditional offences such as fraud, threats and other serious crimes.
- Also assists in the analysis of digital evidence seized in connection with investigations as well as in identifying persons who are committing crimes over the internet.
- Works closely with a number of international organisations and law enforcement agencies.



EUROPOL and EC3

- The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU.
- At operational level, EC3 focuses on the following types of cybercrimes: **cyber-dependent crime, child sexual exploitation and payment fraud.**
- The support provided also extends to tackling criminality on the dark web and alternative platforms.



J-CAT

- The Joint Cybercrime Action Taskforce (J-CAT) was launched in September 2014. Located at Europol's European Cybercrime Centre (EC3), it helps fight cybercrime within and outside the EU.
- Intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint **identification, prioritisation, preparation, initiation** and **execution of cross-border investigations** and operations by its partners.
- J-CAT Members include EU and Non-EU States, and their tasks includes:
 - selecting the most relevant proposals;
 - sharing, collecting and enriching data on the cases in question;
 - developing an action plan, which is led by the country that submitted the selected proposal;
 - going through all the necessary steps to ensure the case is ready to become a target of law enforcement action — a process that involves consulting with judicial authorities, the identification of the required resources, and the allocation of responsibilities.



Combatting Cybercrime

- Legislation enacted as a deterrent to commit the offence with proportionate punishments depending on the severity of the crime. The issue with this is that laws merely act as a deterrent and defendant may use certain procedural technicalities to delay the judgment or have it dismissed.
- There is also the principle of 'innocent until proven guilty' within criminal law, which means that all elements of the criminal offence must be proven by the alleging party. This causes delays to any sentence being adjudicated upon, particularly due to the compilation of 'best evidence'.
- Legislation imposing industry standard certification (particularly for cybersecurity) is one way of combatting the 'hands-on' attacks such as hacking, which relates to the physical and virtual infrastructure implemented by organisations.
- Educating the public to safeguard their digital identity and minimise their digital fingerprint could combat against cybercrime such as ransomware, malware, fraud and identity theft, as attackers typically target older or less educated individuals who would not be as tech-savvy.



Combatting Cybercrime

- Increased collaboration and information sharing between supervisory authorities may dampen the effect and longevity of any crimes as assailants will be found more effectively.
- Jurisdictional issues may be remedied through multi-lateral agreements between contracting states, setting a definite jurisdictional framework and defining which Court will have jurisdiction, so as to speed up the litigation process in cross-border situations.



Legal Challenges

- Identifying which activities can be considered illegal (*"Nullum crimen sine lege"*).
- Enacting criminal law relating to computers and the Internet.
- Identifying the offenders and victims of the crimes.
- Enforcement, particularly focused on **preservation of evidence, jurisdiction** and the **international aspect** of the crimes.
- Concept of "adequate punishment" and how to quantify damages in the digital age.

Case Studies



Woman conditionally discharged over computer misuse

Investigation revealed she had started to download clients' data but stopped, deleted the information and did not share it

- February 2026
- The police received a criminal report from Blexr, an iGaming company based in Sliema, in February 2025, in which they were informed that a woman had allegedly accessed company files containing confidential information on the company's clients and downloaded them.
- In January 20, 2025, the company offered the woman a severance package, and she said she would consider it. The woman was also informed that access to her work laptop would be blocked. Later during the day, the company noticed that Bugeja accessed the files from her mobile phone and was checking and downloading them.



Woman conditionally discharged over computer misuse

Investigation revealed she had started to download clients' data but stopped, deleted the information and did not share it

- She then sent in her resignation and informed the company that she had accepted the severance package. The next day, she went to hand back her work laptop when she was confronted about the data, which was allegedly exported from the company files, and the woman said she had deleted the data.
- The company still proceeded to file a criminal complaint since it could not ensure whether the data had been deleted or not, and this was sensitive information. The woman did not get her severance package.
- When she was arraigned, the woman admitted to a raft of computer misuse charges on January 27, 2026.

Woman conditionally discharged over computer misuse

Investigation revealed she had started to download clients' data but stopped, deleted the information and did not share it

- In its considerations, the court took into account that the woman admitted at a very early stage and was a first-time offender. It also considered that the woman collaborated fully with the police.
- From the testimony of the police inspector, it emerged that the woman began exporting the data but stopped.
- No company data was found on her device, and no data was shared with third parties.
- It also observed that despite the woman and the company having agreed on a termination package, this incident was used to not give her the benefit. It considered that the woman was in stable employment.

Woman conditionally discharged over computer misuse

Investigation revealed she had started to download clients' data but stopped, deleted the information and did not share it

- While the charges carried up to 10 years' imprisonment, the law allows for the accused to be conditionally discharged. The court held that in this case, it did not feel justice would be done if handed a severe punishment.
- The woman was found guilty by her own admission and was conditionally discharged for three years, during which she shall not breach any condition; failing to do so will result in a sentence.
- The court did not award any compensation to the company, remarking that it had already gained by withholding the severance package.

Gaming company spent €330,000 on investigation after engineer accessed source code illegally

Man pleads guilty to computer misuse charges after gaining access to gaming company's source code

- An engineer who admitted to gaining unauthorised access to the source code of a leading iGaming company fully cooperated with an internal investigation that cost the company €330,000 to resolve.
- The accused was arraigned on 18 February 2026 and he pleaded guilty to charges of computer misuse after gaining access to its source code.
- Police from the Cyber Crime Unit were informed about the offence after the company's lawyer filed a report alleging computer misuse that negatively impacted the its operations. Although the engineer was abroad at the time the report was filed, he was arrested at the airport upon his return, and his electronic devices were seized.
- A representative of the gaming company testified in court that the firm had to spend €330,000 on security remediation measures after the former employee accessed its source code without authorisation.
- The source code forms the foundation of the company's entire operation.
- The court heard that the breach required a team of 14 individuals working around the clock to determine exactly what had occurred within the system. The process also involved changing employee access credentials, which required the assistance of external specialists.



Gaming company spent €330,000 on investigation after engineer accessed source code illegally

Man pleads guilty to computer misuse charges are gaining access to gaming company's source code

- The company representative outlined the potential damage such a leak could have caused, explaining that in the wrong hands, access to source code could allow hackers to steal company funds or fully replicate its business model.
- Serious concerns were also raised regarding employee safety, as similar leaks in the industry abroad have, in some cases, led to incidents of kidnapping.
- An Inspector from the Cyber Crime Unit confirmed that the accused fully cooperated throughout the investigation.
- While the accused admitted to the charges, cross-examination revealed that there is currently no evidence that any company data was shared with third parties.
- The accused remains on bail under a personal guarantee of €50,000 and a deposit of €500.
- His identity, as well as that of the company, is protected by a court order due to the sensitive nature of the case.



Any Questions?





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES