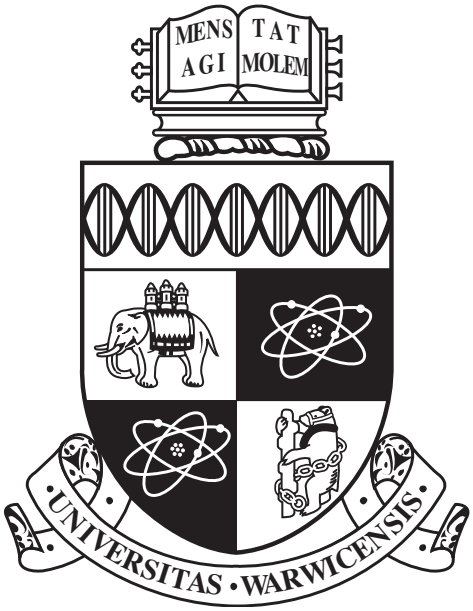
University of Warwick
Department of Computer Science

CS133

Professional Skills



Cem Yilmaz
March 17, 2022

Contents

1 Professional Bodies

1.1 Three features of a profession

Because the definition of a "profession" varies from place to place and dictionary to dictionary, we instead cover what is common between all of them: I.e., the definitions of a profession always have:

- Body of people, i.e, it is a group
- Self-governing i.e., it has its own control over itself
- Entry to profession is controlled i.e., requires a degree

1.2 Professional Bodies

Definition 1.1. Profession - a paid occupation, especially one that involves prolonged training and a formal qualification.

Definition 1.2. Professional body - an organisation with individual members practicing a profession or occupation in which the organisation maintains an oversight of the knowledge, skills, conduct and practice of that profession or occupation.

1.2.1 Engineering Council

The engineering council offers professional qualifications such as:

- CEng, IEng, EngTech which are limited to UK only (awarded through BCS),
- EUR ING (throughout Europe using FEANI)

with BCS (British Computer Society) being a licensed institution of the Engineering Council and it offers:

- CITP (UK only)
- ISEB (a software engineering qualification, highly regarded)

They also have a code of conduct which has four duties:

- Public Interest - regard for public health, privacy, security and well-being of environment and people
- Professional competence and integrity - only perform work/services within professional competence and develop skills and competence on a continuing basis
- Duty to Relevant Authority - carry out responsibilities with care and diligence and avoid conflicts of interest
- Duty to the Profession - Uphold the reputation and seek to improve standards

1.2.2 Science Council

Similarly for science professions, there exists the Science Council and it was incorporated in 2003. It consists of 41 member bodies, including the IMA (Institute of mathematics and its applications). The IMA is a professional institution for scientists in a computing discipline.
Some qualifications include:

- CSci, CSciTech, RSci, RSciTech

1.2.3 Other Councils

The General Medical Council regulates doctors in the United Kingdom. They set standards, hold a register, quality assure education and investigate complaints.
Royal College of Veterinary Surgeons (RCVS)
Royal Institute of British Architects (RIBA)

1.3 Reservation of title and function

Definition 1.3. Reservation of title - name of a profession being restricted to those who are appropriately qualified.

Definition 1.4. Reservation of function - certain activities are restricted to those who have appropriate qualifications or members of particular professional bodies.

2 UK Law

2.1 Fundamentals

The UK government is governed by the parliament which consists of two houses:
House of commons which is an elected lower house which makes the laws
House of lords which is an appointed upper house which scrutinises and revises laws.

2.2 Devolved Government

However things for the UK are not so simple. We consider the following definitions:

Definition 2.1. Crown dependency - a territory that is under the sovereignty of the British Crown but does not form part of the UK. The Crown dependencies are the Channel Islands and the Isle of Man.

Definition 2.2. Devolved parliament - A devolved English parliament is a proposed institution that would give separate decision-making powers to representatives for voters in England. Current devolved parliaments include Scotland and Wales.

Definition 2.3. Devolved assembly - Similar to parliament but instead for an assembly. It gives separate decision-making powers to representatives for voters. Devolved assembly includes Northern Ireland.

2.3 Making a law

A parliament's main job is to create laws. The process is as follows:

1. A bill is passed to the parliament which proposes a new law or a change to an existing law (Bills are introduced by govt or MPs or members of house of lords)
2. The bill is examined by house of commons and house of lords. Each house makes changes and these must be agreed by both houses before it becomes law.
3. There are cases when a bill can be passed without the approval of lords - if the same bill is passed in two successive years or if it is about taxes or public expenditure.

I.e.,

1. First Reading
2. Second Reading
3. Committee Stage
4. Report Stage
5. Third Reading
6. Royal Assent

Definition 2.4. Primary legislation - term used to describe the main laws passed by the legislative bodies of the UK e.g. Acts of the UK Parliament, Scottish Parliament, Welsh Parliament and Northern Ireland Assembly.

Definition 2.5. Secondary legislation - (also called 'subordinate legislation') is delegated legislation made by a person or body under authority contained in primary legislation. Typically, powers to make secondary legislation may be conferred on ministers, on the Crown, or on public bodies.

2.4 EU Law

EU laws take immediate effect when agreed. They are self executing - an example of GDPR.
Furthermore, EU directives must be enacted by the individual countries. Each country makes their own law when directed to do so by the EU.

2.5 UK Legal System

Definition 2.6. Adversarial System - prosecution and defence compete to determine the facts

Definition 2.7. Inquisitorial - getting the truth through enquiry and investigation

The UK system is adversarial.

2.6 Criminal Law and Civil Law

Definition 2.8. Criminal law - there is a presumption of innocence. The prosecution must prove 'beyond reasonable doubt' test that you are guilty. The crown prosecution service decides to move the prosecution forward. The juries decide guilt or innocence whilst the judge decides the penalty.

Definition 2.9. Civil law - the case is decided on a balance of probabilities test and concerns relationships between individuals. E.g., contracts, property, family law etc.

3 Intellectual Property

3.1 Tangible and Intangible

Definition 3.1. Tangible - a thing that is perceptible by touch. E.g., car, house, gas etc.

Definition 3.2. Intangible - unable to be touched; not having physical presence. E.g., software, literature, art etc.

Definition 3.3. Intellectual property - Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. I.e., intangible things

3.2 Copyright v Patents v Trademarks

Copyright, patents and trademarks are all things that relate to law and intellectual property.

3.2.1 Copyright

Copyright is defined as the right to copy/adapt something. This could be one of the following:
Book, journal, article, image, song, software etc.
Work with copyright allows the owner to copy, change, sell, share and rent it to others. More importantly, it can be used to prevent others from doing the same and gaining unfair benefit from your work.
The US favours the copyright holders using the Digital Millennium Copyright Act (DMCA) which protects the copyright
The World Intellectual Property Organisation (WIPO) also exists that regulates the IP.
Lastly, the Anti-counterfeiting Trade agreement (ACTA) came out of secret negotiations in 2011/12 and it criminalises certain classes of IP infringement e.g. downloads of movies, software etc. It puts responsibility to Internet Service Provider (ISP) responsible for users' online use. It has only been ratified in Japan. The EU directive on copyright in 2019 created a law which:

- Requires websites to obtain license from publishers to link to news stories in their sites
- Requires platforms to obtain licenses for content e.g., music videos

In 2014 the copyright went through a change after a result of criticism from a book. It now includes that the following uses of copied materials are permitted:

- Archiving and preserving
- Data analysis e.g. for research

- Research and education as long as the source is acknowledged
- Private use e.g., copying a few pages of a book
- Accessible copies for disabled persons

3.2.2 Trade marks

Trade marks are protected under the Trade Marks act 1994. In the UK, the intellectual property office (IPO) adjudicates on any disputes. Registration of trade marks and designs is advisable, and is checked in disputes. However, there is a great question about how much Trade Marks Act really protects. Copyrighting a domain name works by 'grandfather rights' i.e., registration of domain in good name and there is no conflict of interest you are not infringing the legislation.

3.2.3 Patents

Patent confers to a temporary right to exploit an invention an usually for 20 years. In EU, the patented invention must:

- Be new
- Involve an inventive step
- Be capable of industrial application
- Not be in an excluded area

Excluded areas include:

- Scientific Theories
- Mathematical Methods
- Aesthetic creations - copyright instead
- Presentation of information - copyright instead
- Algorithms and software

A patent must be registered at the IPO. Disclosure before application invalidates a patent, therefore an invention must be kept confidential prior to patenting it. In EU, software are not patentable. However, in the US, this is allowed if the following is true

- Is part of a procedure that is patentable
- Controls a process with physical effect
- Processes real physical data

3.3 Digital Rights Management

In the past deliberate errors were introduced to things such as books to detect copying. Today, software companies try to protect their software etc. by incorporating technology to prevent it:

- Product keys - each purchaser receives a different key
- Limited number of active installations - i.e., max 3
- Presistent online authentication - it continually checks that it is authorised i.e., DRM

3.4 Whistle-Blowing

Confidentiality fails under the following conditions (Public Interest Disclosure Act 1998):

- Criminal offense
- Failure to comply with legal obligation
- Miscarriage of justice
- Environmental damage
- Health and safety
- Concealment of any of the above

3.5 Registration requirement

The following require registration:

- Registered trade marks
- Registered designs
- Patents
- Domain names

And the following are automatically protected:

- Unregistered trade marks
- Unregistered design rights
- Confidential information
- Copyright

4 Data Protection

Data theft can cause damage financially, through fraud or embarrassment.

4.1 Problem

Types of data that can be hacked, accidentally lost or altered. For example through:

- Credit Card theft
- Identity theft
- Sensitive personal information
- Tracking by unauthorised agencies e.g. purchasing behaviour, travel

4.2 TalkTalk

Information commissioners office (ICO) issued a fine of $400,000$ GBP to TalkTalk, a company whose investigation found that an attack last October could have been prevented if TalkTalk had taken basic steps to protect customers' information. The ICO found that the cyber attack between 15 to 21 October 2015 took advantage of the companies' weak systems. The data of 156,959 people was stolen including their numbers, addresses, names, email addresses. In 15,656 cases, the attacker gained access to bank account details and sort codes.

4.3 Facebook

In September 2018, $50m$ Facebook accounts were compromised by an attacker that gave hackers the ability to take over' others' accounts. Users that were affected were notified by facebook and required to log out and log back in. They also stole access tokens - a kind of security key that allows users to log back into the app without having to enter password every time.

4.4 Solution

In 1984, computers stored medical and financial data and then it was realised that potential problems this could occur. As a result, the Council for Europe Convention was introduced which enables discussions between governments on matters of mutual interests. In 1998, the EU Data Protection Directive lead to the 1998 Data protection Act. The GDPR Data Protection Regulation in 2016 forms part of the Data Protection Act. These regular how data is stored and who can access the data.

Definition 4.1. Personal data - data that is stored and processed about a data subject (a real person). GDPR refers to 'any information'

Definition 4.2. Data subject - An 'identified or identifiable natural person'

Definition 4.3. Information Commissioner - a person who makes sure data is correctly supervised under law

Definition 4.4. Processing - anything to do with data, e.g., storage, collection, recording or organising.

Definition 4.5. Controller - can be a person, authority or body that determines the prepose and means of the processing of personal data.

1998 Data Protection Act superseded the 1984 act. The DPA 1998 refers to the accessible records and relevant filing systems e.g. filing cabinets not just computerised data.

4.5 Jurisdiction and Enforcement

The GDPR (General Data Protection Regulation) applies to any organisation anywhere in the world if data is collected relating to any EU resident.The GDPR enforces penalties for violations of obligations and legal justification up to $20m$ euros or 4% of global gross revenue. The GDPR enforces penalties for breaching GDPR for up to $10m$ euroes or up to 4% of global gross revenue.

4.6 Data Protection Officer

The following organisations require data protection officer:

- All entities involved with 'regular and systematic monitoring of data subjects on a large scale'
- All public authorities
- All entities conducting large-scale processing of 'special categories of personal data' e.g., racial/ethnic origin, political beliefs, religious beliefs etc.

4.7 Data Breaches

Data breaches must be reported within 72 hours. Privacy impact assessments must be made (if appropriate) focusing on protecting data subjects' rights.

Definition 4.6. Pseudonymisation - the processing of personal data in such a manner that the personal data cano no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

4.8 7 Data Protection Principles

1. Processing of personal data must be lawful, fair and transparent
2. Purposes of processing of personal data must be specified, explicit and legitimate
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be accurate and kept up to date
5. Personal data must be kept for no longer than is necessary
6. Personal data must be processed in a secure manner
7. The controller is accountable

4.9 Lawfulness of processing

Data can be 'lawfully' processed if:

- Necessary for performance of a contract
- Legal obligations
- 'Vital interests' of a data subject
- Public interest or official authority
- Consent of data subject
- 'Legitimate interests'

However, note that consent to processing must be freely given, should be specific and informed, not be ambiguous and must have 'legitimate interests'

4.10 Exemptions

Exemptions for consentual data include:

- Legal privilege
- Taxation
- Self incrimination
- Immigration
- Journalism
- Research
- Parliamentary privilege
- Employment references
- Exam scripts and marks
- Social work data
- health data

4.11 Right of Access to Data

You have right to access data/information about yourself as a result of GDPR:

- Right of access by the data subject (normally within 1 month)
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object to automated profiling

However, note that you do not have right to view information about yourself that the police has if you are under investigation.

4.12 Profiling

Definition 4.7. Profiling - the activity of collecting information about someone

Certain types of profiling is considered problematic - consider how insurance companies arrive at how much you pay based on your medical data, health, economic situation and reliability. You have a right not to subject to profiling, but it is not yet 100% clear in legal terms. A good example of profiling is personalised advertising.

4.13 Privacy

Issue of privacy is extremely complicated and is complex. For the sake of this module we only consider Regulation of Investigatory Powers Act 2000 (RIPA). It sets up a framework for controlling the lawful interception of computer, telephone and communications. Governments can access data only in certain specified situations such as preventing and detecting crime. They are allowed to monitor and record communications without the consent.

5 Freedom of Information

The freedom of information act 2000 covers all public bodies in the UK e.g., local government, NHS, universities, police, parliament etc. Furthermore it:

- Extends definition of data in Data Protection Act 1998 to include 'unstructured' records
- Freedom of Information refers to non-personal data
- Freedom of Information refers to information that is not sensitive
- Changes 'need to know' to 'right to know'
- Requests are in writing (e.g. fax) or by email, stating clearly the information that you want to know
- Response from bodies must say if the information exists, if it does, it must be shared
- Bodies must give cost and time limit for request (20 working days or until fee is paid, max 3 months)

However, absolute exceptions include:

- Security services
- Trade secrets (protecting new designs)
- Court records (confidential)
- 'Vexacious' requests (e.g., spamming a company for lots of information)

and qualified exceptions include:

- Subject to prejudice test (crime detection)
- Not in the public interest

5.1 Publication Schemes

Freedom of Information (FOI) Act requires every public body to publish information proactively. The publication schemes should:

- Have list of information to be published by types of organisations
- Need approval from Information Commissioner
- Information that is of interest to the general public should be available
- Use 'model publication schemes', the organisation no longer needs to respond to all requests

The Information Commissioner can adjudicate and can enforce disclosure, but the public authority's complaints process must be followed first. Lastly, the information commissioner can be overruled by an appropriate government.

5.2 Issues

- Data sharing - the sharing of data between organisations
- Government disallows a request - why would it do this
- Credit agencies - where do credit agencies get their data
- DNA databases - who owns your DNA and who should be allowed to know the information
- Cross-border data - should different countries share information

6 Computer Misuse

6.1 Computer Misuse Act (CMA) 1990

Introduced the following case of 1987 case of Regina vs Gold and Schifreen - stolen credentials via shoulder surfing.

Definition 6.1. Shoulder surfing - the practice of spying on the user of cash-dispensing machines or other electronic devices in order to obtain their personal identification number, password etc.

Convictions were being overturned so new law was required to deal with the changing tech landscape. The CMA as a result was introduced with new offenses:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate further offences
- Unauthorised modification of computer material

Definition 6.2. Computer System - any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

Definition 6.3. Computer Data - any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

6.2 Offenses

6.2.1 Unauthorised access

I.e., unauthorised access to computer material
Causing 'a computer to perform any function with intent to secure access to any program or data held in any computer' such that the access is knowingly unauthorised. The unauthorised access is the offence - not any damage done.

6.2.2 Unauthorised access with Intent

I.e., unauthorised access with intent to further facilitate commission of further offences. Intent to commit a crime carries a punishment of 5 year prison or more plus an unlimited fine. It is not necessary to prove that the intended further offence has actually been committed.

6.2.3 Unauthorised modification

I.e., unauthorised acts with intent to impair, or with recklessness as to impairing the operation of a computer.
The intention is to

- Impair the operation of the target computer
- Prevent or hinder access to any program or data
- Impair the operation of a program or the reliability of any data

6.2.4 Section 3ZA

I.e., unauthorised acts causing, or creating risk of, serious damage.
The maximum sentence of indictment is 14 years and an unlimited fine, unless the offense caused or created a significant risk of serious damage to human welfare or national security, in which case a person guilty of offence is liable to imprisonment for life.

6.2.5 Note

The location of the equipment is vague on purpose meaning that it is irrelevant where it happens.

6.3 Police and Justice Act 2006

This amends the Computer Misuses Act by:

- Allows extradition for the offence under the original act e.g., unauthorised access
- Addresses deficiencies in the CMA e.g., denial of service attack
- Increases penalties for hacking
- Criminalises the use of tools which can be used for computer offences

6.4 University of Warwick Regulations

The regulations refers to Acts of parliament and Jisc AUP, but also specific references to:

- No harassment, pornography, racial abuse, libel
- No password disclosure
- Do not bring the university into disrepute
- The duty is on users to protect programs/data from unauthorised access

6.5 Regulation of Investigatory Powers Act 2000

This governs teh use of covert surveillance by public bodies. The definition of the act includes

- Communication
- Surveillance and Covert Human Intelligence Sources
- Investigation of Electronic Data Protected by Encryption
- Scrutiny etc., of Investigatory Powers and of the Functions of the Intelligence Services
- Miscellaneous

Furthermore, RIPA handles the following:

- Interception - requires warrants. Security services, police and government can apply for a warrant. Decision on warrants is given by Secretary of State and reason for warrant include national security, crime, covert investigations etc.
- Encryption - keys must be surrendered if the data cannot be provided unencrypted, there is a trust issue or timeliness is crucial.
- Scrutiny - commissioners (judges) check that powers under the act are not being abused through an annual report. Trubunal hears public complaints.

In 2016, it was updated to include:

- Equipment interference by security services including "large operations"
- Mandatory storage (12 months) of internet history data by ISPs
- Collection of "Bulk personal datasets" by security services
- New criminal offence of unlawfully accessing Internet data.

Lastly, it is legal to monitor and record for:

- Standard purposes
- Compliance with regulation
- Effective system use
- Prevention or detection of crime
- Detecting unauthorised use

However, it is only legal to monitor:

- Checking if related to the business
- Confidential phone lines

7 Ethics and the Internet

7.1 Ethics and Morals

Definition 7.1. Ethics - defined as "principles of conduct", "rules of conduct" and "moral principles". In other words, it relates to the processes for making decisions about right and wrong where the morality is not necessarily clear, typically internalised within a sector of society.

Definition 7.2. Morals - defined as "Good or bad", "right or wrong", "good or evil". Are what is generally (and clearly) accepted as being right or wrong, and often externally imposed (through laws).

Morals are generally agreed and are typically imposed by law and ethics are about the process for making decisions and fine turning the grey areas - about understanding why things are right or wrong and how that judgement was made.

7.2 Theories of Ethics

Definition 7.3. Consequentialism - an act is good if the outcome of that act is good. For example, if you help someone to cross the road and they are happy to get safely to the other side, you did the right thing. E.g., John Stuart Mill - Utilitarianism

Definition 7.4. Deontology - An act is good if the motivation for carrying out that act is good. For example, if you help someone to cross the road safely but they did not want to get to other side, you still did the right thing. E.g., Immanuel Kant - Categorical Imperatives

8 Computer Security

8.1 Standard and legislation

8.1.1 Health and Insurance Portability Act (HIPAA)

was created to 'improve the portability and accountability of health insurance coverage' for employees between jobs in 1996 USA.

8.1.2 Gramm-Leach-Bliley Act (GLBA)

created in 1999 USA, requires financial institutions to explain how they share and protect their customers' private information

8.1.3 Homeland Security Act

included the Federal Information Security Act (FISMA).

8.1.4 European Union Agency for Cybersecurity (ENISA)

Was set up for the purpose of raising Network and Information Security (NIS) in the EU

8.1.5 Congress Report

A june 2013 congressional report found that there were over 50 statutes relevant to cyber security compliance in the US.

8.1.6 General Data Protection Regulation (GDPR)

The GDPR brings a single standard for data protection among all EU member states. It came into force in May 2018 and was set into place in April 2016.

8.1.7 Security of National Information Systems (NIS)

In 2016 the European Parliament set into policy the direction of NIS to achieve a high common standard of network and information security across all EU member states.

8.2 Framework

One aim of studying a subject is to grain a mental map, a framework that helps makes sense of the whole. It may not always fit perfectly, but it provides a common ground in terms of terminology and concepts. A common framework for computer security is the CIA triangle:

Figure 1: CIA Triangle of Data

In particular,

Definition 8.1. Confidentiality - no unauthorised disclosure

Definition 8.2. Availability - users are not denied access to resources. No unwarranted delay.

Definition 8.3. Integrity - no unauthorised change

8.3 Encryption

Encryption is a process of securing information by covering it with an encryption and decryption key. The encryption key allows data to be stored securely, while decryption key decrypts the secured data into real data. It provides very good level security so much so that governments are worried that it might be used by criminals.

Definition 8.4. Key escrow - Key escrow is a method of storing important cryptographic keys. Each key stored in an escrow system is tied to the original user and subsequently encrypted for security purposes.

Definition 8.5. Key disclosure - Key disclosure laws, also known as mandatory key disclosure, is legislation that requires individuals to surrender cryptographic keys to law enforcement. The purpose is to allow access to material for confiscation or digital forensics purposes and use it either as evidence in a court of law or to enforce national security interests.

8.4 the Morris Worm

In 1988 Robert Morris exploited program bugs to write a worm. It rapidly infected 10% of all machines on the Arpanet. It replicated by mistake on each machine - harm was unintentional. The worm exploited programming bugs - e.g., buffer overflow and a common 'debug' mode. Morris was issued a penalty under US 1986 Computer Fraud and Abuse Act - 3 years probation, community service and a fine of over $10,000$ USD.

8.5 Social Engineering

In the 1980s and 1990s Kevin Mitnick was a notorious hacker for his master of social engineering. He conned people to divulge personal information such as passwords, usually over phone. He pretended to be company's IT security group and phones human resources to get a list of new employees on the pretext of organising a security seminar. He then rings a new employee and pretends it's routine practice for security advice to be offered to

new workers. During a useful discussion the hacker raised the topic and lure the employee into disclosing their password.

8.6 Cyxymu

In August 2009 there was a massive DoS attack against social network sites used by Georgian Blogger 'Cyxymu'. It was one of a spate of incidents in which countries and people who were political irritations to Russia were attacked. The attack came from within Russia - there is no proof, but many pointed the finger at Russian government collusion rather than just hackers.

8.7 Biometric Passports

Biometric passports have been cloned to fool passport readers before:

- Biometric passports are now used by many countries and the biometric information is encrypted.
- In 2008, 3000 blank passports were stolen
- Passports have been cloned and fooled passport readers
- Although there is a database of passport keys, most places won't check

8.8 Advanced Persistent Threat

Stuxnet was a highly sophisticated worm (multiple zero-day windows sttacks, precision engineering towards particular system, rootkit, public keys stolen from several companies) and it specifically attacked Siemens' SCADA control software. It tracks were covered with a man-in-the-middle attack so that normal operation was reported.

8.9 Hactivism

In Jan 2012 executives of Megauploads.com were arrested and the site was taken down. Retaliation DoS attacks started within hours and Anonymous took down US government organisation websites: White House, Department of Justice, FBI. Music sites attacked too: Universal music and warner music. The attack was coordinated, decentralised and very effective.

8.10 Physical Security

In 2010 a computer programmer was taken hostage in Russia. He was handcuffed to a radiator and beaten to force him to hack into bank web sites. He was eventually saved by the police and the kidnappers were sentenced to 15 years in prison.

8.11 Cyber-attacks on the increase

The cases begin to show the diversity of computer security and the number of attacks continue to rise steadily. The proportion of UK firms reporting a cyber-attack has jumped... 55% had faced an attack in 2019, compared to 40% last year.

8.12 Terminology

Definition 8.6. Asset - anything we value and want to protect

Definition 8.7. Vulnerability - a flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's security policy.

Definition 8.8. Threat - a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm

Definition 8.9. Attack - an assault on system security that derives from an intelligent threat i.e., an intelligent act that is a deliberate attempt to evade security services and violate the security police of a system.

Definition 8.10. Risk - an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Definition 8.11. Countermeasure - an action, device, procedure or technique that reduces a threat, vulnerability or attack by eliminating or preventing it, by minimising the harm it can cause, or by discovering and reporting it as that corrective action can be taken.

Definition 8.12. Risk assessment

$$\text{Exposure} = \text{Assets} \times \text{Threats} \times \text{Vulnerabilities}$$

9 Organisations

9.1 Legal Entity

Definition 9.1. Legal entity - is an individual, company or organisation that has legal rights and obligations. It can be entered into contracts, be taken to court etc.

Definition 9.2. Unlimited liability - you can lose everything i.e., there is no limit on how much you can be sued for

Some examples of legal entities include:

- Sole trader
- Partnership
- Corporation
- Cooperatives

9.2 Creating a corporation

A company can be created through

9.2.1 Royal Charter

Organisations used to be created in a simple - whoever was governing issued a document creating that organisation. The University of Warwick was created by a Royal Charter.

9.2.2 Act of Parliament

Organisations can be created through an Act of Parliament e.g., governing institutions, councils, some statutory companies

9.2.3 Companies Act

Most organisations are limited companies that are created through the Companies Act

9.3 Limited Companies

9.3.1 Public Limited Company (PLC)

PLCs can sell shares to general public - shares and bonds. This means that its stocks are traded on stock exchange. Must adhere to regulations and reporting standards and can be vulnerable to takeovers.

9.3.2 Private Limited Company (LTD)

Shares aren't traded but can be sold to private investors or venture capitalists. Stocks traded between investors and there are fewer regulations e.g., < 500 shareholders and < 10 million USD.

9.4 Memorandum of Association

Up until 30 September 2009 two documents were created one of which was the memorandum of association. Included stuff are:

- Name, registered office and country - all included in detail
- Company activities - explained very broadly e.g., trading
- Liability clause - how the liability is carried out, e.g., limited by shares or guarantee
- Share capital - money initially invested
- Declaration of association - statement from initial investors

In the articles of association prior to 2009, the included stuff are:

- Dividends
- Board Meetings
- Membership of board of directors
- Directors' terms of office
- Sales of shares
- Directors' powers

After 1st October, the framework changed slightly. The Companies (Model Articles) Regulations 2008 replaced "Table A".

Definition 9.3. Table A - the first document that was presented originally. It contained detail about how the business is conducted, shares are traded, directors are elected etc.

The memorandum was subsumed into the Articles and is no longer part of the company's constitution. Now companies require the articles of association.

9.5 Organisational Models

9.5.1 Bureaucratic model

1. All tasks are split into specialised jobs in which jobholders become exxpert
2. The performance of each task is governed by precise rules
3. In order to ensure that personalities and personal relationships do not interfere with performance, employees are required to relate both to other employees and to clients in an impersonal and formal manner
4. Recruitment is based on qualifications and employees are protected against arbitrary dismissal.

9.5.2 The Organic Model

An organisation will be effective to the extent that its structure is such as to ensure a maximum probability that in all interactions and in relationships within the organisation, each member, in the light of his background, values, desires, and expectations, will view the experience as supportive and one which builds a sense of personal worth and importance.

9.5.3 Matrix Management

In the past 30 years or so the idea of matrix management has become more fashionable as a way of addressing cases where employees may have more than a single manager. It is a method trying to resolve the conflict between them. In software company, for example, database specialists may belong to a database group and report to its manager, while at the same time reporting to the project manager of the project they are working on.

9.6 2008 Financial Crisis

The 2008 financial crisis highlights the risk of companies and organisations. It was caused by an increase in the risky practice of lending for sub prime mortgages.

Definition 9.4. Subprime - refers to borrowers or loans, usually offered at rates well above the prime interest rate, that have poor credit ratings. Subprime lending is higher risk, given the lower credit rating of borrowers, and has in the past contributed to financial crises.

In September 2008, Lehman Brothers, a US investment bank went bust. Bailouts were necessary to prevent further collapse.

9.7 Structuring Principles

The structuring principles is a way to dissect how big companies are put together.

- By Function - medium sized organisations are often structured by function. In a typical company, departmental functions include production, finance, quality, marketing, research and development and human resources. A legal team may also exist if it is big enough
- By Location - For large companies where local knowledge and local regulations play a big part, such as multinationals and banks, structuring by location may be used
- By Product - structuring by product works where there is clear product differentiation.
- By market sector - Structuring by market sector works for example for service products, where there is clear sector differentiation (e.g. window cleaning for private individuals and window cleaning for large organisations).
- By technology - An example of a company structured by technology is IBM, which is used to produced PCs, mainframes and operating systems that could be separated. However it's not so easy to structure by technology now, although it make sense occasionally.

There are also structural considerations which include:

- Operational structure - by project e.g., if objectives need to be achieved by a specific deadline or by production e.g., specific activities managed by a single team
- Depth of Structure - Companies choose a chain of command which is effective. The bigger the company, the more likely it is to have more layers of management.
- Centralisation - (making the top control more in the hierarchy) is appropriate for company wide policies, for example corporate branding for a consistent look and feel.

9.8 Job design

Definition 9.5. Job enrichment - redesigning jobs so that the amount of responsibility, discretion and control required of the employee is increased

Definition 9.6. Job rotation - rotating staff through a series of jobs to prevent employees from becoming bored with a very narrow and specialised task

Definition 9.7. Job enlargement - redesign of a job so that it includes more tasks which require essentially the same level of skill and responsibility

10 Companies

10.1 Starting a company

A starting company requires:

- Capital - i.e., money
- Cash flow - i.e., money coming in and out

- Sources of finance - i.e., equity capital, loans etc.
- Gearing - ratio of loan capital to equity

Definition 10.1. Grants - sum of money given to a company by the government

Definition 10.2. Loans - sum of money lent to a company

Definition 10.3. Equity Capital - money paid to the company in exchange for a share in the ownership of the company. Usually venture capitalists or business angels use this method for companies with good prospects

Definition 10.4. Gearing / leverage - the relationship between loan capital and equity capital. High levels of gearing is generally undesirable.

10.2 Balance Sheet

A balance sheet has:

- Assets - i.e., what a company owns, current vs. fixed, depreciation and debtors
- Liabilities - i.e., what a company owns and creditors
- Net Worth - i.e., assets minus liabilities

10.3 Profit and Loss Account

A profit and loss account has:

- Approximation: during a single year i.e., Change in net worth $=$ income $-$ expenditure
- Need to consider cash flow i.e., how the cash moves about
- Also need to consider depreciation and monies owing.

10.4 Cash Flow statement

Movement of cash (excludes non-cash transactions, such as depreciation) including but not limited to:

- Interest payments
- Tax
- Dividends to shareholders
- Capital expenditure
- Disposals

10.5 Relationship between them

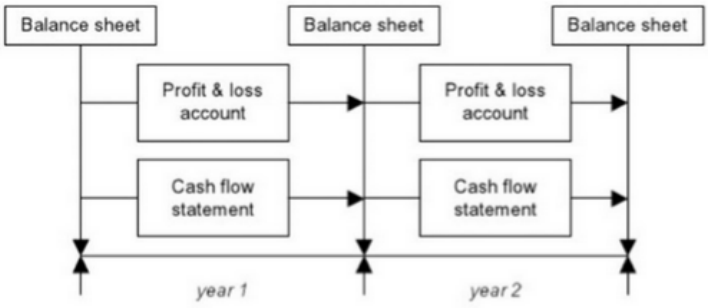


Figure 2: Relationship between Cash Flow, Profit and Loss and Balance Sheet

The relationship is that Balance sheet happens at the end of each year. Profit and loss account along with Cash Flow statement happens throughout year, for which is then used to generate the balance sheet next year.

10.6 Double Entry Bookkeeping

Conceptually, pages in a book. Every single entry appears "twice". The idea is that through ledgers you are able to make sure that when you add specific things e.g., orders, the add up correctly since you take record twice.

Cashbook

Date		Income £	Expenditure £	Ledger
01/02/12	Order #123 John Smith	350.00		Orders
07/02/13	Order #124 Bil Bloggs	400.00		Orders
12/03/13	Canley Steel		400.00	Supplies
13/03/13	The Glue Factory		70.00	Supplies
22/03/13	Midlands Electricity		73.00	Bills
22/03/13	S-T Water		62.00	Bills
01/04/13	Canley Steel (refund)	100.00		Bills
05/04/13	To Bank		245.00	Bank
	TOTAL	***850.00***	***850.00***	

Ledger "Orders"

Date		Debit £	Credit £	
01/02/12	Order #123 John Smith		350.00	Cashbook
07/02/13	Order #124 Bil Bloggs		400.00	Cashbook
05/04/13	To I&E	750.00		I&E
	TOTAL	***750.00***	***750.00***	

Ledger "Bills"

Date		Debit £	Credit £	
12/03/13	Canley Steel	400.00		Cashbook
13/03/13	The Glue Factory	70.00		Cashbook
22/03/13	Midlands Electricity	73.00		Cashbook
22/03/13	S-T Water	62.00		Cashbook
01/04/13	Canley Steel (refund)		100.00	Cashbook
05/04/13	To I&E		505.00	I&E
	TOTAL	***605.00***	***605.00***	

Bank

Date		Debit £	Credit £	
06/05/12	B/F	5000.00		
05/04/13		245.00		Cashbook
05/04/13			245.00	Balance Sheet
	TOTAL	5245.00	5245.00	

I&E Account

Date		Debit £	Credit £	
05/04/13	Orders		750.00	
05/04/13	Bills	505.00		
05/04/13	Surplus (deficit)	245.00		Acc. Fund
	TOTAL	***750.00***	***750.00***	

Balance Sheet 2013

Date		Assets £	Liabilities £	
06/04/12	HQ building	100000.00		
05/04/13	Bank	5245.00		
	TOTAL	***105245.00***		

Accumulated Fund

06/04/12	Assets on 6/4/12	105000.00		B/F
05/04/13	Surplus (deficit)	245.00		I&E
05/04/13	Assets on 5/4/13		105245.00	C/F
	TOTAL	***105245.00***	***105245.00***	

Figure 3: Double Entry Bookkeeping

10.7 Accounts and Budgetes

Definition 10.5. Accounts - these tell you what happened

Definition 10.6. Budgets - tell you what you expect to happen

Definition 10.7. Direct costs - things that include directly in the production of a product e.g., raw materials, shipment

Definition 10.8. Indirect costs - things that are not directly in the production of a product e.g., utility bills, wages, rent

10.8 Labour

Labour includes:

- Salaries i.e., monthly, weekly or hourly, Income Tax (PAYE), Pension contributions and national insurance contributions.
- Days off sick i.e., statutory sick pay

10.9 Overheads

Definition 10.9. Overheads - expenses you can't avoid

These include

- Rental
- Vehicles
- Bills
- Telecomms
- Postage
- Insurance

10.10 Investment

The Discounted cash flow analysis includes the return on investment and the interest rate $r\%$ over t years, given with a discount factor

$$\frac{1}{(1+r)^t}$$

It also includes the rate of return. However, since this is forecasting there are some inherent problems:

- Market Conditions
- Competitors
- Credit availability
- Interest rates

which can all change.

10.11 Statutory requirements

Annual returns and accounts MUST be filed to the Companies House and sent to HMRC. Accounts must audited if the company is large enough and must also contain balance sheet, profit and loss account, notes on the accounts and directors' report if it is large enough.

Definition 10.10. Insolvency - trading with a company that did not break even over a period of time or is not in a position insolvently and it is bankrupt.

11 Contracts and Human Resources

11.1 Contracts

Definition 11.1. Contract - a legal agreement between two or more parties which must:

- Be competent
- Intend to make the contract
- Receive/provide a consideration

and contracts can be broken down into two:

1. The main agreement - this includes the signatures
2. The schedules - this details the tasks and actions associated with the contract

11.2 The Schedule

The schedule must include:

1. What is to be supplied
2. Price, deadlines, payment terms
3. Legal rights - who owns the intellectual property
4. Confidentiality
5. Delays, changes, penalty causes - e.g., if the project overruns
6. Client obligations - Logistics and hardware i.e., where will it be written
7. Milestones - Key targets to ensure that the software development life cycle is on track
8. Acceptance procedures - how is it defined if the development is complete

9. Warranty, maintenance - responsibility for fixing errors if they arise
10. Indemnity - what happens if use of the software results in damage
11. Termination - grounds at which the contract can be ended
12. Arbitration - the mechanism for resolving disputes between the parties
13. Applicable law - If in court, which law applies e.g., UK, US etc.

11.3 Consultancy contracts

The following terms are to especially watch out for:

Definition 11.2. Liability - who is responsible

Definition 11.3. Confidentiality - who can view, gain information

Definition 11.4. Terms of reference - purpose and structures of the contract and the deal

Definition 11.5. Control over deliverables - e.g., who initiates, plans, closes etc.

11.4 Human resources

Human resources consists of:

- Recruitment and selection - processes for recruiting new employees into the organisation, job descriptions to define their duties and employment contracts to attribute rights and responsibilities to the organisation and employee.
- Redundancies, dismissal and grievances - Similarly, they should have define for the above definition
- Staff support & development - To keep employee retention rates high, organisations need to help staff enhance their skills, which in turn benefits both employee and employer.

Definition 11.6. Appraisals - to help ensure staff are progressing in their job and that their skills are up-to-date, organisations should undertake regular monitoring meetings with employees

Definition 11.7. Remuneration policy - how salary is calculated and how employees can be incentivised

Definition 11.8. Employment acts - Human rights act 1998, Equality act 2006, Equality act 2010

11.5 Discrimination

Organisations are not allowed to discriminate. They are not allowed to discriminate against anyone because of the protected characteristics:

- Age
- Gender reassignment
- Being married or in a civil partnership
- Being pregnant or on maternity leave
- Disability
- Race including colour, nationality, ethnic or national origin
- Religion or belief
- Sex
- Sexual orientation

The same applies with software and web access, by Web Content Accessibility Guidelines (WCAG)

11.6 Athena Swan Charter

The Athena SWAN charter is a framework used across the global to support and transform gender equality within higher education and research. It was established in 2005 to encourage and recognise commitment to advancing careers of women in STEMM employment.

11.7 Me too movement

A me too movement against sexual harassment and assault based on breaking silence was made. It's purpose was to empower women by visibly demonstrating the extent of sexual harassment in the workplace.