BSc in Computer Engineering
CMP4103
Computer Systems and Network Security

Lecture 10

Legal, Regulations, Compliance and Investigations

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Table of Contents

This page intentionally left blank

1. Computer Crime

Computer crime encompasses a broad range of potentially illegal activities. It is generally divided into one of two types of categories:

- Crimes that target computer networks or devices directly
    - Malware (malicious code).
    - Denial-of-service attacks.
    - Computer viruses.
- Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.
    - Cyber stalking.
    - Fraud and identity theft.
    - Phishing scams.
    - Information warfare.

A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is an excellent device for record keeping, particularly given the power to encrypt the data. If this evidence can be obtained and decrypted, it can be of great value to criminal investigators.

1.1 Specific Computer crimes

- Spam
    - Spam, or the unsolicited sending of bulk email for commercial purposes.
- Fraud
    - Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss.
- Obscene or offensive content
    - The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal.
- Harassment
    - Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation.
- Drug trafficking
    - Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology.

- Cyber terrorism
    - There is a growing concern among law enforcement that Internet problems and server scans are part of an organised effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems.

1.2 Global Initiatives in the fight against Cybercrime

The Computer Misuse Act 1990 in the UK was one of the earliest legal enactments against cybercrime. This Act was enacted with an express purpose of making "provision for securing computer material against unauthorised access or modification." The major provisions of the Computer Misuse Act 1990 relate to:

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

This act was subsequently amended by:

- Criminal Justice and Public Order Act 1994,
- Criminal Justice (Terrorism and Conspiracy) Act 1998,
- Police and Justice Act 2006
- Serious Crime Act 2015

A number of US States developed their own legal solutions to the problem:

- Florida Electronic Security Act
- Illinois Electronic Commerce Security Act
- Texas Penal Code - Computer Crimes Statute
- Maine Criminal Code - Computer Crimes

The US Federal Government has enacted a number of acts to legislate for this area also:

- Computer Fraud and Abuse Act (CFAA)
- Electronic Signatures in Global and National Commerce Act
- Uniform Electronic Transactions Act - adopted by 46 states
- Digital Signature And Electronic Authentication Law
- Government Paperwork Elimination Act (GPEA)
- The Uniform Commercial Code (UCC)

The Council of Europe (CoE) ETS No. 185 Convention on Cybercrime is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.

On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalise the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

Forty-three nations have signed the treaty. The Convention entered into force in the United States in 2007.

In the European Union (EU) the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was published and had to be implemented in all member states by July 19, 2001.

This directive was repealed on 1/7/2016 and replaced by regulation for electronic identification and e-signatures (eIDAS).

The e-signatures directive only dealt with the validity of electronic signatures and did not provide a complete framework for secure transactions. In a bid to move ever more towards a Digital Single Market and harmonise the rules, the regulations expand the scope of the directive and cover, amongst others, trust services (services which provide authentication), electronic seals, electronic time stamps, electronic documents and website authorisations.

The Council of the EU Framework Decision 2005/222/JHA on attacks against information systems in 2005 was designed to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems. This includes the so-called "*hacking*" and "*DoS attacks*" as well as the spreading of malicious code, spyware and malware and viruses. This was subsequently replaced in August 2013 by Directive 2013/40/EU of the European Parliament (EP) and of the Council. The new directive aimed to tackle the increasingly sophisticated and large-scale forms of attacks against information systems, which have emerged since the adoption of Framework Decision 2005/222/JHA.

The Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data is the EU directive adopted in 1995 which regulates the processing of personal data within the Union. It is an important component of EU privacy and human rights law. However this directive and the nationals laws that were developed from it is being replaced by the General Data Protection Regulation (GDPR), adopted in April 2016, will supersede the Data Protection Directive and is planned to be enforceable starting on 25 May 2018.

2. Intellectual Property (IP)

Is a term referring to a number of distinct types of legal monopolies over creations of the mind, both artistic and commercial, and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions.

2.1 Patent

This term refers to a right granted to anyone by the state (Government patent office) who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof.

A patent provides the right to exclude others from making, using, selling, offering for sale, or importing the patented invention for the term of the patent, which is usually 20 years from the filing date subject to the payment of maintenance fees.

Patents are the strongest form of IP and is a legally enforceable right to prevent others from using the invention for the period of the patent.

2.2 Trademark

A trademark is a distinctive sign or indicator used by an individual, business organisation, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities.

A trademark is designated by the following symbols:

- ™ Unregistered trade mark
- SM Unregistered service mark
- ® Registered trademark

The owner of a registered trademark may commence legal proceedings for trademark infringement to prevent unauthorised use of that trademark. However, registration is not required. The owner of a common law trademark may also file suit, but an unregistered mark may be protectable only within the geographical area within which it has been used or in geographical areas into which it may be reasonably expected to expand.

A service mark differs from a trademark in that the mark is used on the advertising of the service rather than on the packaging or delivery of the service, since there is generally no "*package*" to place the mark on, which is the practice for trademarks.

2.3 Copyright

Copyright is a form of intellectual property that gives the author of an original work exclusive right for a certain time period in relation to that work, including its publication, distribution and adaptation, after which time the work is said to enter the public domain. Copyright applies to any expressible form of an idea or information that is substantive and discrete and fixed in a medium.

Copyright protection extends to the following works:

- original literary, dramatic, musical or artistic works
- sound recordings and films
- broadcasts and TV programmes
- the typographical arrangement of published editions
- computer programmes
- original databases.

Copyright takes effect as soon as the work is put on paper, film, or other fixed medium such as CD-ROM, DVD, Internet, etc. No protection is provided for ideas while the ideas are in a person's mind. Copyright law protects the form of expression of ideas, not the ideas themselves.

Copyright is a weaker IP right than a patent but its duration is much longer. It typically applies for 50 – 70 years depending on the form of work.

2.3.1 Copyleft

Copyleft is a play on the word copyright to describe the practice of using copyright law to remove restrictions on distributing copies and modified versions of a work for others and requiring that the same freedoms be preserved in modified versions.

Copyleft is a form of licensing and can be used to modify copyrights for works such as computer software, documents, music and art. In general, copyleft licensing scheme, give every person who receives a copy of a work permission to reproduce, adapt or distribute the work as long as any resulting copies or adaptations are also bound by the same copyleft licensing scheme.

Common practice for using copyleft is to codify the copying terms for a work with a license. Any such license typically gives each person possessing a copy of the work the same freedoms as the author, including (from the Free Software Definition):

- the freedom to use the work
- the freedom to study the work
- the freedom to copy and share the work with others
- the freedom to modify the work, and the freedom to distribute modified and therefore derivative works

The GNU General Public License, originally written by Richard Stallman, was the first copyleft license to see extensive use, and continues to dominate the licensing of copylefted software.

2.4 Trade Secret

A trade secret is information that:

- Is not generally known to the public.
- Confers some sort of economic benefit on its holder.
- Is the subject of reasonable efforts to maintain its secret?

A company can protect its confidential information through non-competitive and non-disclosure agreements (NDA) with its employees. The law of protection of confidential information effectively allows a perpetual monopoly in secret information. It does not expire as would a patent. The lack of formal protection, however, means that a third party is not prevented from independently duplicating and using the secret information once it is discovered.

2.5 International trade

International trade is exchange of capital, goods, and services across international borders or territories. It refers to exports of goods and services by a firm to a foreign-based buyer or importer.

International trade is in principle not different from domestic trade as the motivation and the behaviour of parties involved in a trade does not change fundamentally depending on whether trade is across a border or not. The main difference is that international trade is typically more costly than domestic trade. The reason is that a border typically imposes additional costs such as tariffs, time costs due to border delays and costs associated with country differences such as language, the legal system or a different culture.

The regulation of international trade is done through the World Trade Organisation (WTO) at the global level, and through several other regional arrangements such as the European Union between member states, MERcado COmún del SUR (Spanish) Southern Common Market (MERCOSUR) in South America and the North American Free Trade Agreement (NAFTA) between the United States, Canada and Mexico.

2.5.1 Encryption Export Control

Encryption export controls became a matter of public concern with the introduction of the PC. Phil Zimmermann's PGP cryptosystem and its distribution on the Internet in 1991 was the first major *'individual level*' challenge to controls on export of cryptography. The growth of electronic commerce in the 1990s created additional pressure for reduced restrictions. Shortly afterwards, Netscape's SSL technology was widely adopted as a method for protecting credit card transactions using public key cryptography.

SSL-encrypted messages used the RC4 cipher, and used 128-bit keys. United States government export regulations would not permit crypto systems using 128-bit keys to be exported.

The longest key size allowed for export without individual license proceedings was 40 bits, so Netscape developed two versions of its web browser. The "*United States edition*" had the full 128-bit strength. The "*International Edition*" had its effective key length reduced to 40 bits by revealing 88 bits of the key in the SSL protocol. Acquiring the United States domestic version turned out to be sufficient hassle that most computer users, even in the United States, ended up with the '*International*' version, whose weak 40-bit encryption could be broken in a matter of days using a single personal computer.

Legal challenges by civil libertarians and privacy advocates, the widespread availability of encryption software outside the United States, and the perception by many companies that adverse publicity about weak encryption was limiting their sales and the growth of e-commerce, led to a series of relaxations in United States export controls, culminating in 1996 in President Bill Clinton signing the Executive order 13026 transferring the commercial encryption from the Munition List to the Commerce Control List. Furthermore, the order stated that, the software shall not be considered or treated as "*technology*" in the sense of Export Administration Regulations. This order permitted the United States Department of Commerce to implement rules that greatly simplified the export of commercial and open source software containing cryptography.

2.6 Current status

As of 2009, non-military cryptography exports from the United States are controlled by the Department of Commerce's Bureau of Industry and Security. Some restrictions still exist, even for mass market products, particularly with regard to export to "rogue states" and terrorist organisations. Militarised encryption equipment, TEMPEST-approved electronics, custom cryptographic software, and even cryptographic consulting services still require an export license.

2.7 Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a Multilateral Export Control Regime (MECR) with 40 participating states.

It is the successor to the Cold war-era Coordinating Committee for Multilateral Export Controls (COCOM), and was established on May 12, 1996, in the Dutch town of Wassenaar, near The Hague. The Wassenaar Arrangement is considerably less strict than COCOM, focusing primarily on the transparency of national export control regimes and not granting veto power to individual members over organisational decisions. A Secretariat for administrating the agreement is located in Vienna, Austria.

3. Liability and Negligence

Legal liability is the legal bound obligation to pay debts. A person is said to be legally liable when they are financially and legally responsible for something. Legal liability concerns both civil law and criminal law. Payment of damages usually resolved the liability. In commercial law, limited liability is a form of business ownership in which business owners are legally responsible for no more than the amount that they have contributed to a venture. If for example, a business goes bankrupt an owner with limited liability will not lose unrelated assets such as a personal residence (assuming they do not give personal guarantees). This is the standard model for larger businesses, in which a shareholder will only lose the amount invested (in the form of stock value decreasing).

Manufacturer's liability is a legal concept in most countries that reflects the fact that producers have a responsibility not to sell a defective product.

Negligence is a type of delectation or civil wrong. It can be considered the gap or difference between Actions where due diligence is expected and due care as defined in a policy. Or the gap between the policy and best practice or regulation.

Negligence is not the same as carelessness, because someone might be exercising as much care as they are capable of, yet still fall below the level of competence expected of them.

Through civil litigation, if an injured person proves that another person acted negligently to cause his injury, he can recover damages to compensate for his harm.

4. Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

4.1 Data privacy

This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information.

Various types of personal information often come under privacy concerns.

- Financial privacy.
- Internet privacy.
- Medical privacy.
- Sexual privacy.
- Political privacy.

4.1.1 EU Data Protection Directive

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is a European Union directive which regulates the processing of personal data within the Union member states. It is an important component of EU privacy and human rights law and was implemented in 1995 by the European Commission. The European model is not to allow access to private information with any group or country that does not have compatible legislation governing the collection, storage and use of data.

4.1.2 General Data Protection Regulation (GDPR)

The GDPR covers the protection of all personal data that a business collects and processes.

- ***Transparency and Accountability***: General requirement for organisations to be accountable about data processing and a greater emphasis on transparency.
- ***Employee rights***: The other rights of employees as data subjects include (1) the right to be informed; (2) the right to be forgotten; (3) the right to data portability; and (4) the right to rectification and restriction.
- ***Data Breach Notification***: Under the GDPR, businesses are required to notify data breaches within 72 hours.
- ***Subject Access Requests*** (SAR): Must be handled within one month.

- ***Appointment of a Data Protection Officer (DPO)***
- ***Record keeping***: Through the increased focus on transparency and accountability, there will be much tighter standards upon the nature of data employers can retain and for how long, meaning that the retention periods for records will need to be identified and monitored and you will also need to keep better records of your decision making process.
- ***Privacy by design and Privacy Impact Assessments (PIA)***: The GDPR advocates privacy by design – which means that employers will be obliged to adopt an approach that promotes privacy and data protection compliance from the outset of any project or process. PIAs will need to be carried out at the beginning of any new process.

4.1.2.1 Sanctions

A fine of up to €20,000,000 can be imposed or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

The regulation applies from the 25 May 2018 in all member states of the EU.

4.1.3 Uganda Data Protection and Privacy Bill, 2016

The Uganda Data Protection and Privacy Bill, 2016 has been proposed to protect the privacy of the individual and of personal data by collecting and regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters.

- Principles of Data Protection
- Data Collection and Processing
  - Consent, protection of privacy
- Security of Data - breach notification to NITA-U
- Rights of subjects
  - Access, prevent processing, etc..
- Sanctions
  - Individuals: 4,800,000 Ugx and/or 10 years prison.
  - Corporations: All individuals involved.

4.1.4 US Health Insurance Portability & Accountability Act (HIPPA)

HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs it requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

4.1.5 Canadian Personal Information Protection & Electronic Documents Act (PIPEDA)

PIPEDA requires private-sector organisations to collect, use or disclose your personal information by fair and lawful means, with your consent, and only for purposes that are stated and reasonable.

They're also obliged to protect your personal information through appropriate security measures, and to destroy it when it's no longer needed for the original purposes.

4.1.6 Recommendations

- Robust **Data Breach Incident Management Policy**
- **Pseudonymisation of personal data**
  - Separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately
- **Encryption of data**
- **Assess** applications and critical infrastructure for security vulnerabilities and the effectiveness of security controls
  - Vulnerability Testing
  - Penetration Testing
  - Control Testing.

4.2 Privacy at work

Today companies are under increasing pressure to monitor employees electronically, and workers should assume they are being watched. A large percentage of companies are now conducting some form of *active monitoring* of their employees, particularly E-mail monitoring.

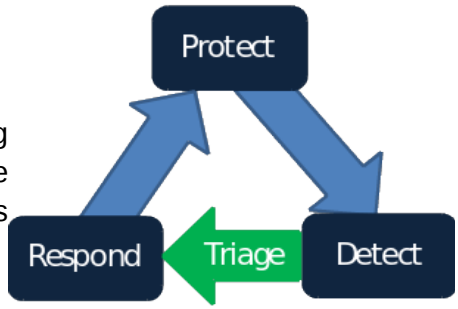
Employees generally have a right to privacy based on a '*reasonable expectation of privacy'* but a written policy notifying employees of monitoring lifts somewhat the expectation of privacy.

This means that if an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated. But, if the company informs its employees that, for example, e-mail sent over the company's network is monitored, then the employee can no longer claim an expectation of privacy.

The key for successfully managing the balancing act between privacy and security is for firms to make clear to their employees that their privacy at work is limited.

It's not really about Big Brother watching either, e-mail is quite often used as a tool of harassment and employers have a duty to be sure harassment isn't being propagated. For the company to exercise its responsibility it needs to monitor or at least record the e-mail traffic.

5. Incident Management



This is about proactively preparing for and reacting to an incident. Proactive preparation involves the preparation of policies to deal with possible events and the implementation of a continuous cycle of auditing and improvement of these policies.

Reaction is the measures carried out on the detection of an incident. How the incident was detected, what triage classification and prioritisation was carried out and how the response was conducted.

Good source of information are the:

- NIST SP 800-61 Computer Security Incident Handling Guide.
- Software Engineering Institute (SEI)
  - Handbook for Computer Security Incident Response Teams (CSIRTs).

5.1 Collection of Digital Evidence

Evidence is subject to strict rules regarding its admissibility in courts. To be presented, recorded in the court record and considered in the verdict, evidence must be:

- **Relevant**
  - It must pertain to the actual case.
- **Material**
  - It must prove or disprove facts that impact the question before the court.
- **Competent**
  - It must be proven to actually be what it purports to be.

So with digital evidence, “do no harm”. Do not start open the log files, shutting down the system, etc. Do as little as possible beyond disconnecting the system from the network and protecting it until it can be handed over to the police or other law enforcement.

- Don’t turn off the system as data in volatile memory (RAM) will be lost.
- Disconnect the system from the network as this prevents a hacker from covering their tracks by deleting evidence like log files.
- Don’t use the system for any reason, like running programs as you may unwittingly overwrite data in memory.

Don’t open files to examine them as you will modify the access and modify time record on the file.

Document everything you do.

5.1.1 Preserving digital evidence

The best way to preserve digital evidence in its original state is to copy it from one machine to another via a private network connection. The source computers memory should be transferred to the target computer first. The contents of the source computer's hard disk should be copied to the target computer as a bit level image not file by file to create an exact copy of the source disk data including empty space (which may include deleted residual data). A number of specialist software programs exist for this purpose.

A forensic duplicate consists of every bit of the raw bitstream stored in an identical format (e.g. using an identical disk).

On the other hand, a qualified forensic duplicate is a copy where every bit of information is still stored, but perhaps in a different form, such as an ISO image.

Both are submissible as evidence, but the "best evidence" should be used, e.g. the original disk.

5.2 Evidence Chain of Custody

Chain of Custody is the chronological documentation, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.

Who – What – When – Where – How

5.3 Process of Investigation

Identify:

- Suspects.
- Systems.
- Witnesses.
- Investigative team.
- Search warrants.

For filesystems, analyse the ownership and the modification records. What were the Means, Opportunity and Motives (MOM) of personnel can assist in narrowing down suspects to a crime.

Are there any Modus Operandi (MO), methods, choice of software or applications that may point to a particular set of habits, traits, or practices that can be used to identify a suspect.

5.4 Interviewing Suspects

Once you have identified a suspect and are in a position to talk to him or her you must plan how it is going to happen. Will you apply interview or interrogation techniques. The basic difference between interview and interrogation is that an interview is conducted in a cordial atmosphere where a suspect or witness is more comfortable physically and psychologically. When a person is questioned in an uncomfortable atmosphere under psychological pressure, it is then an interrogation.

5.5 Hearsay

Hearsay is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called hearsay evidence. Such use of "hearsay evidence" in court is generally not allowed.

In the United States there is a business records exception or business entry rule which is an exception to the hearsay rule. Such business records include any writings or records of acts, events, conditions, opinions, or diagnosis, made at or near the time by, or from information transmitted by, a person with knowledge are admissible if kept in the regular course of business and if it was the regular course of business to make that record, unless the source of information or circumstances of preparation indicate a lack of trustworthiness.

The idea behind this exception is that employees are under a duty to be accurate in observing, reporting, and recording business facts. The exception functions to allow the record to substitute for the in-court testimony of the employees, but it can only substitute for what the employee could testify about.

6. Compliance and ethics

6.1 Regulatory Compliance

Historically in all countries there have been periods of business and government excesses and subsequent legal, public and political reaction. All countries have imposed regulation of compliance to prevent and punish companies who participate in corporate malpractice.

6.1.1 US Foreign Corrupt Practices Act (FCPA)

This is an anti-bribery provision makes it unlawful for a United States citizen, and certain foreign issuers of securities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person. The law also requires publicly traded companies to maintain records that accurately and fairly represent the company's transactions. It also requires these companies to have an adequate systems of internal accounting controls.

6.1.2 US Sarbanes–Oxley Act (SOX)

The act is the US Public Company Accounting Reform and Investor Protection Act. It was enacted as a reaction to a number of major corporate and accounting scandals like that at Enron and a number of other US companies which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets.

The legislation set new or enhanced standards for all United States public company boards, management and public accounting firms. It does not apply to privately held companies. The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

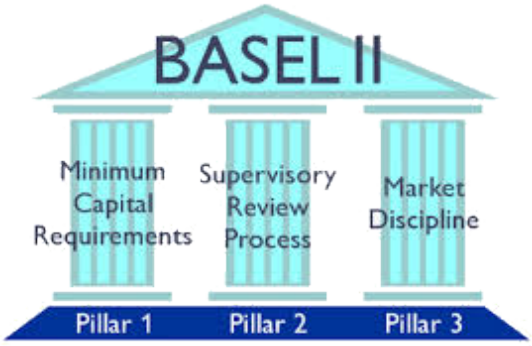
6.1.3 US Gramm-Leach-Bliley Act (GLBA)

The GLBA Act is the US Financial Services Modernisation Act to allow commercial banks, investment banks, securities firms and insurance companies to consolidate. One area of the act is the protection of the privacy of consumer information held by these organisations.

6.1.4 EU DIRECTIVE 2006/43/EC

This is a directive of the European Parliament and council from 2006 on statutory audits of annual accounts and consolidated accounts. This is considered the European Union's equivalent of the US Sarbanes–Oxley Act.

6.1.5 Basel II



This is a series of recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. This international committee encourages contacts and cooperation among its members and other banking supervisory authorities. Basel II creates an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. Advocates of Basel II believe that such an international standard can help protect the international financial system from the types of problems that might arise should a major bank or a series of banks collapse. In practice, Basel II attempts to accomplish this by setting up rigorous risk and capital management requirements designed to ensure that a bank holds capital reserves appropriate to the risk the bank exposes itself to through its lending and investment practices. Generally speaking, these rules mean that the greater risk to which the bank is exposed, the greater the amount of capital the bank needs to hold to safeguard its solvency and overall economic stability.

6.1.6 Compliance Auditing

A compliance audit is an evaluation of an organisation, its systems and process to ascertain the validity and reliability of information and to provide an assessment of an organisations internal controls against compliance to the rules of business in the various acts applied to such business. The audit is carried out by an approved third party auditor who will compare the stated policies with the actual controls in place.

Continuous auditing is an automated method of auditing by use of software program's to perform the audit on a continuous basis replacing the periodic manual audit associated with the use of an auditor.

6.2 Business Ethics

Business or corporate ethics is a form of applied ethics that examines ethical principles and moral or ethical problems that arise in a business environment. It applies to all aspects of business conduct and is relevant to the conduct of individuals and business organisations as a whole. The range and quantity of business ethical issues reflects the degree to which business is perceived to be at odds with non-economic social values.

Many companies have formulated internal policies pertaining to the ethical conduct of employees. These policies can be broad language or they can be more detailed policies, containing specific behavioural ethics codes. They are generally meant to identify the company's expectations of workers and to offer guidance on handling some of the more common ethical problems that might arise in the course of doing business. It is hoped that having such a policy will lead to greater ethical awareness, consistency in application, and the avoidance of ethical disasters.

An increasing number of companies also requires employees to attend seminars regarding business conduct, which often include discussion of the company's policies, specific case studies, and legal requirements. Some companies even require their employees to sign agreements stating that they will abide by the company's rules of conduct.

7. Bibliography

UK Computer Misuse Act 1990

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Uganda Data Protection and Privacy bill 2016, First Reading, 20 Apr, 2016

Jansen W, Grance T (2011). Guidelines on Security and Privacy in Public Cloud Computing. SP 800-144. NIST.

(ISC)² (2012) Official (ISC)² Guide to the CISSP Common Body of Knowledge. Third Edition.

Paul Cichonski, P., Millar, T., Grance, T., Scarfone, K. (2012). NIST SP 800-61 Computer Security Incident Handling Guide. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [accessed: 1 Oct 2015]. National Institute of Standards and Technology (NIST), US Department of Commerce. Aug 2012.

West-Brown, M.J., Stikvoort, D., Kossakowski, K.P., Killcrece, G., Ruefle, R., Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Available: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf [accessed: 21 Oct 2015]. Software Engineering Institute Apr 2003.

This page is intentionally blank