Law and Ethics in Information Security

What is the role of an Information Security professional in an Organization?

- Understand Organizations' legal and ethical responsibilities
- Align these responsibilities with laws governing one's jurisdiction; stay currently informed in legal environment (e.g Data protection Act, Computer misuse and cyber crime law bill etc)
- Managing liability for privacy and security risks

An understanding of the above will

- reduce liability and risks from electronic and physical threats
- reduce losses due to legal actions

The IS officer should ensure that the management and the employees are educated on the legal and ethical obligations as they use the ICT's in the organization.

Law and Ethics in Information Security

- Organizational liability and need for counsel
- Policy versus law
- International Laws and legal bodies
- Ethics and Information Security

Law and Ethics in Information Security

As a recap of the first class, let us remind ourselves the definitions of ethics and law;

- **Laws** are rules that mandate or prohibit certain behavior; they are drawn from ethics, which define socially acceptable behaviors.
- **Ethics** in turn are based on cultural mores/behaviors: the fixed moral attitudes or customs of a particular group

The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not

Organizational Liability and need for counsel

Organization not encouraging strong behavior from it employees? Organization not behaving ethically?

Liability: legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action

Product Liability Example: https://mman.co.ke/content/product-liability-kenya-insights-consumer-protection (Accessed 20th May, 2021)

Due Care: An organization increases its liability if it refuses to take measures known as due care. **This is met** when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions.

> *In order to perform **due care**, the organization must first perform due diligence. **Due diligence** comes before **due care** and is a management process used to gather facts before making a decision*.

Due Diligence: takes longer than just fixing something immediately, it is more the investigation as to **why** that something had to be corrected in the first place. It is about detecting the reason behind either an incident, event, or breach etc.

> *This is where an organization is required to make a valid effort to protect others and continually maintains this level of effort.*

Given the Internet's global reach, those who could be injured or wronged by an organization's employees could be anywhere in the world.

In some countries, the court can assert its authority over an individual or organization if it can establish jurisdiction—that is, the court's right to hear a case if a wrong is committed in its territory or involves its citizenry. This is sometimes referred to as **long arm jurisdiction**—the long arm of the law extending across the country or around the world to draw an accused individual into its court systems.

A jurisdiction Group Discussion: Let us look at the case between SCI-HUB and Elsevier Lawsuit

Policy versus Law

- The policies/guidelines (functioning as Organizational law) describe the acceptable and unacceptable behavior by the employees of an Organization. The IS officer should ensure that all these policies/guidelines are read and understood by all.
- These guidelines are complete with penalties, judicial practices, and sanctions to require compliance
- Within an organization, information security professionals help maintain security via the establishment and enforcement of policies.
- Policy are different from the national law and therefore ignorance of a policy is an acceptable defense. This therefore demands enforcement of the policy through meeting the following criteria:

- **Dissemination (distribution)—**The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
- **Review (reading)—**The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.
- **Comprehension (understanding)—**The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
- **Compliance (agreement)—**The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
- **Uniform enforcement**—The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Only when all of these conditions are met can an organization penalize employees who violate the policy without fear of legal retribution.

Group Discussion

You are in charge of a start-up company having a potential to hit it big in a couple of years. This potential leads you and your business partner to drafting some guidelines to be followed by your potential employees. Currently you having 5 employees and in your strategic plan, you are foreseeing an increase to 20 employees by the end of 2021. You want to plan ahead; so plan your Organizational policies and how to ensure that it meets all the five criteria

Note: Use your formed groups and have your work on the shared drive.

Local and International Laws ICT

Kenya	US	England and Wales
Computer Misuse and Cybercrimes Act 2018	Privacy Act of 1974	Data protection Act 2018
Data Protection Act 2019	Foreign Intelligence Surveillance Act of 1978	Communication Act 2003
	(1986) Electronic Communication Privacy Act	Privacy and Electronic communications Regulations 2003
	Intelligence Reform and Terrorism Prevention Act 2004	The network and Information System Regulation 2018
	Homeland Security Act 2002	The computer Misuse Act 1990

Ethics and Information Security

- Many Professional groups have explicit rules governing ethical behavior in the workplace. For example, doctors and lawyers who commit egregious (outstandingly bad or shocking)violations of their professions' canons of conduct can be removed from practice.

- Unlike the medical and legal fields, however, the information technology field in general, and the information security field in particular, do not have a binding code of ethics.

- While these professional organizations can prescribe ethical conduct, they do not always have the authority to banish violators from practicing their trade.

Examples of these Professional Organizations in the field of ICT; Familiarize yourselves with these bodies and more so join them.

- Information Communication Technology Association of Kenya (ICTAK)
- The Computer Society of Kenya
- ACM (Association for Computing Machinery)
- Association for the Advancement of Artificial Intelligence (AAAI)
- Association for Women in Computing (AWC)
- Computing Research Association
- IEEE (Institution of Electrical and Electronics Engineers)
- IET (Institution of Engineering and Technology)

Offline
The Ten Commandments of Computer Ethics[13]

From The Computer Ethics Institute

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

Ethical Differences Across Cultures

- Culture can make it difficult to determine what is and is not ethical. (Pause and discuss in groups what are some of the cultural differences in our different ethnic groups vary)
- The cultural differences also vary when it comes to computer usage.
  - Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group.

Individual Assignment; Due 13th June 2022

Write short notes on how software license infringement, illicit use and misuse of corporate resources are handled in Kenya, India, England, US and any Scandinavian countries)