Transcript 9

Welcome to our third lecture this week and a video presentation on Cyberethics and Policy Management.

It is essential to understand the importance of identifying the ethical considerations for security and risk management and the relevance of policy management.

Firstly, if we can go back to what we learned last week about the importance of security and risk management, and this slide reminds us why risk management is essential before we proceed on with looking at the ethical considerations.

Risk management is needed to sustain a secure environment that means having responsible management. It is a process of identifying factors damaging or disclosing data, mitigating and or reducing risk. It is also to develop and implement information security strategies to reduce risk and support the organisational mission and objectives. These all require a professional, responsible approach by management.

This slide just reinforces some of what we have seen in the previous slide. It highlights considerations that are needed for example; Professionalism that can be defined as 'acting to meet the standards set by a profession in terms of individual conduct, competence and integrity'. Other essential considerations are Social Responsibility and Accountability; where a computer professional is a moral individual therefore standards and evidence of transparency and accountability should be maintained. Finally 'Due Diligence', where management and execution of due care should be constant. So how far are these considerations carried out within organisations?

What is ethics or cyber ethics? We know that ethics involves the principle of morality, it is the discipline dealing with what is good and bad and right and wrong. It is based on our understanding and reasonable thinking with moral duty and obligation and above all concerns individual human opinions and beliefs, values and norms that apply to our daily lives. With the digital revolution, social and ethical issues can no longer be considered in isolation for the national and international context.

In the lectures so far this week, we have seen examples of where none of the considerations of ethics, responsibility etc have been remotely thought of. What responsibility and respect for others do people adhere to in cyberspace, and does cyberspace require a new set of laws? What role does ethics play in regulatory frameworks? and do the fundamental principles of ethics remain the same in cyberspace?

Now, please pause/stop the video before continuing to listen to the rest of the lecture, and let us now take a short break and reflect on the questions from the previous slide.

What responsibility and respect for others do people adhere to in cyberspace and does cyberspace require a new set of laws? What role does ethics play in regulatory frameworks?

Do the fundamental principles of ethics remain the same in cyberspace?

Welcome back after taking that break, I hope that you have had some thought on the questions. We can now continue with re-visiting the C-I-A Triad.

What is the C-I-A Triad?

It forms the basis of information security in that it identifies the need for Confidentiality, Integrity and Availability and it sometimes also includes two other characteristics, Authentication and Nonrepudiation. This is a security model that is used in the development of security policies for identifying problem areas and providing solutions for information security. It highlights core data security objectives and consequently serves as a guideline for organisations to protect their sensitive data from attack and unauthorised access.

Confidentiality of the C-I-A Triad ensures authorised access to information, Integrity provides assurance of accuracy of information processing methods and Availability provides timely and reliable access to information to those who have authorised access.

What about Responsibility and Accountability? Organisational security policies should be transparent and accountable and it is everyone's responsibility. There should be compliance with security requirements designated by the organisation but we have seen that not all members in the organisation take on the role of responsibility and accountability. It is everyone's responsibility to be aware of suspicious activity, security violation and any concerns in this respect.

Security frameworks should be employed to ensure good practice in an organisation for example Control Objectives for Information and Related Technologies (COBIT) that is a framework for good practice. COBOT enables clear policy development, good practice for IT control and emphasises regulatory compliance.

Last week, we saw how cyber-attacks have no global boundaries, and it is essential to have consideration for globalisation and culture. Laws and regulations relevant to information security differ throughout the world and an awareness of these issues is essential. Many computer crimes and information security laws were made some time ago and their relevance today may be questionable.

There are many challenges to be faced, such as Privacy, Data breaches, Identification of threats and vulnerabilities. Risk assessments have to be made but many attacks go undetected and stay in systems for considerable amounts of time. There are issues with compliance; who has read any policies and procedures in their organisation, do they understand them and are they enforced? There are also the People issues!

Now, please pause/stop the video before continuing to listen to the rest of the lecture, and let us now take a short break and reflect on what we have learned so far before moving on to the next part of the lecture where we will look at Security Policy Management!

Welcome back after taking that break, we can now continue with looking at Policy Management.

What is a Policy? It can be seen as a business requirement on actions or processes performed by an organisation. Security policies require placement of controls in processes specific to the system. For example, COBIT 5, (2012), is specifically related to information security.

Security Policy Management should consider standards, policies, risk frameworks, legislation and guidelines. There are also Codes of Practice and Conduct and Professional Ethics that provide guidelines for good practice. For example the ACM Code of Profession Ethics that has been recently updated, provides guidelines and examples of good practice and there is a link to this at the end of the lecture One of the major issues and consideration, is how far is the enforcement of these policies, codes and procedures carried out?

Is there a perfect world? Policies and procedures should produce the perfect product, and employees should follow policies and procedures at all times but as we have intimated previously, do they have access to them, and are they easily understood? Business processes need timely information and good decision making especially with security and risk management, as it is essential in making decisions with regard to mitigating risks.

This slide show us the difficulties presented in creating a perfect world where increasingly complex technologies instigate more vulnerability. There is a reliance on technologies that instigates increased vulnerability and the ever-changing technology is difficult to keep pace with, both with cost and up to date policies.

Business processes are vulnerable to both loss and theft and it is also difficult to keep up with weaknesses and failures. There are also technical and human challenges with implementing policies and procedures that make the management of these issues increasingly difficult.

Security Policy management faces many challenges as we have seen that creating a perfect world is difficult. There are problems with enforcement issues, understanding risks, and the struggle between government control and individual rights as well as the global challenges.

We also need to turn to considering current and future challenges posed by technology. Issues with Cloud Technology, Artificial Intelligence (AI) and the unknown impact, as well as the constantly changing landscape of cyberspace. There are major challenges with Social Media and we have seen these last week with the issues of Cybercrime. There is cyberbullying, terrorist threats and the new Cryptowar, cybercrime and intellectual property and we will see additional challenges in the next slide.

Continuing on with current and future challenges, it is easy to publish truthful and valuable information but also to publish false, libellous information. There is potential to cause harm and undermine basic human rights and values. There are threats to personal privacy and cyber governance as well as free speech censorship. There should be respect for justice and fairness but all of these remain a challenge for the future.

In Summary, in the preceding slides we have covered a number of issues with regard to Cyberethics and Policy Management, and the challenges faced with both of these.

The important question raised here is; What can be done?

Take some time before the next lecture to consolidate and reflect on what you have learned in before going on to the next lecture.

The next short lecture will be related to this question and also the question you are asked for the discussion this week, and that is: “Is there a need for a ‘law of cyberspace”?

References used in this Lecture:

1. ACM Code of Ethics and Professional Conduct. 2018 “Revision”. Available at: https://www.acm.org/code-ofethics