Transcript week 3

Welcome to this video presentation (slides with voiceover), on an introduction to Security & Risk Management in a Digital Environment, and why is it needed?

It is important to understand the role of managing security and risk and its relevance to both organisations and any digital environment. We will begin by exploring the wider context and discuss the background to what has given rise to the importance of security and risk management.

The changes in technology over the last 3 decades has given many benefits to our lives, however, it has also imposed many negative aspects that have given rise to cyber threats. Amongst some of these technologies are Artificial Intelligence, the Internet of Things (IoT), Nanotechnology, Robotics and so on, and these are all having major impacts and can pose a number of increasing security threats. The intangibility of digital systems, creates a greater problem of dealing with these issues and consequently puts greater pressure on managing the security and risks, as many of these are not always known.

We will now take a look at what security and risk management actually mean. Computer Security is the protection of the assets of a computer system; the hardware, software, and most importantly the confidential data and information, and this is whether it be in an organisation, or someone's home.
Assets are anything that has value to an individual or an organisation. These assets need to be protected from all types of attacks and misuse; from illicit access, use disclosure, alteration, destruction, and/or theft – all that can result in a loss to an organisation or individual and we will be looking at these in more detail later in the module.
Here we can see the issues that could occur with a lack of adequate and effective management of these assets resulting in many different levels of loss. The National Institute of Standards and Technology (NIST) computer security definition of Security and Risk management is: *"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources".* It includes hardware, software, firmware, information/data, and telecommunications).

We continue with defining 'Security'. Security is the protection of computer systems to protect the assets of the organisation and Cyber security to protect computer systems that communicate over computer networks. Security is aimed at preventing loss or disclosure of data while maintaining authorised access. Risk is about the possibility or probability of an event that could damage, destroy or disclose data and other resources without any authorisation.
We know that management is the practice of managing, handling, or controlling something, and coupled with security and risk, it improves security by using threat analysis and risk assessment in order to protect the organisations assets. In order to understand risk management, it is essential to ensure governance and legal proof of due care and diligence. Skills that are needed in this context are practical, analytical skills in understanding the sources of risks using basic mathematical methods for calculating risks, and the ability to make good judgments and decisions about which risks should be controlled, and how they might be controlled. There are no actions without decisions as information gives us power to make informed decisions. It is essential that the right decisions are made in this field.

So why is security and risk management needed?

The Information Security Threat (ISTR) Report 2019, stated that 1 in 10 URLs are malicious web attacks and the average number of websites compromised with Formjacking each month is 4,800, and Supply Chain attacks were increased by 78%!

Formjacking is a type of cyber-attack where hackers inject malicious JavaScript code into a webpage form, and this is usually done via a payment page form. When someone enters their payment card information on a site and clicks submit, malicious code collects not only the payment card number, but also other information such as the customer's name, address, and phone number. The code then sends this information to another location of the attackers' choosing.

Formjacking is part of a larger group of attacks known as "supply chain attacks" where hackers target a vulnerable provider within the service/supply chain.

In this diagram, we are given the information that 48% of malicious email attachments are office files, and this is a rise of 5% in the 2 years from 2017 to 2019. During this time the increase in malicious PowerShell scripts are increased by 1,000%. PowerShell is a scripting language that provides unprecedented access to the inner core of a machine. It can run a script directly in memory and is increasingly used to perpetrate fileless malware attacks. This type of attach uses legitimate programs to infect a machine and is particularly challenging to detect and destroy as it does not rely on files and leaves no footprint.

The diagram at the bottom of this slide, shows arrows depicting the flow of the attack. This begins with an email disguised as a notification, for example an invoice or a receipt. This then moves on to an attached office file that contains malicious script and then flows onto the attachment being opened and executes the script that downloads the malware.

Emails are one of the prime sources of disruption for end users and organisations. They have propagation of ransomware and targeted spear-phishing where the scammer pretends to be the CEO or senior staff and might request large money transfers.

Continuing on with information from the ISTR report, we can see in the first diagram that more Cryptojacking events were blocked in 2018 vs 2017, and a drop in them between January and December 2018.

Cryptojacking is the malicious use of a person or persons' computing power to mine cryptocurrencies without consent. The victim tends to have no idea their device is being used. This has become one of the most common forms of malware and tends to not target data, but the processing power.

In the second diagram we see that enterprise ransomware was up by 12% during this time but the overall ransomware was down by 20%, however, mobile ransomware was on the increase by 33%.

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.

The diagram below informs us that the number of attack groups using destructive malware was up by 25% and the average number of organisations targeted by each attack group was an average of 55. All this information shows us how changeable these attacks are and that in itself, makes security and risk management a very difficult task.

In summary, in the preceding slides we have seen a number of issues raised demonstrating the importance of Security and Risk Management. There are many types of risks and threats (many of which cannot always be detected directly), and these need to be eliminated wherever possible.

There are two quotes taken from Marc Goodman's book on Future Crimes referenced on the next slide.

"An analysis of the threat-actor landscape in cyberspace reveals hacktivists, criminals, proxy warriors, terrorists, and rogue governments, all fully capable of exploiting the insecurity of the technological infrastructure of our world."

and the second quote:

Data is constantly being generated by everything around us. Every digital process, sensor, mobile phone, GPS device, car engine, medical lab test, credit card transaction, hotel door lock, report card, and social media exchange produces date. Smart phones are turning human being into human sensors, generating vast sums of information about us."

These are the reasons why all these technologies have to be managed effectively and give us some answers as to why Security and Risk Management is essential.

Take a break and reflect on what we have learned so far before moving on to the next task for the week.

The references used in this presentation are: 1. Symantec February 2019 - VOLUME 24 https://www.symantec.com/security-center/threat-report

2. Marc Goodman, *'Future Crimes: A Journey to the Dark Side of Technology – and How to Survive It'*. Penguin 2016