****

**NAME: YUSSUF SEIFUDIN**

**ID: 660411**

**FIC4040 ASSIGNMENT 1**

Q1) The Internet is a major enabler for Organized Criminal Group (OCG) activities. Most of the people within organized crime groups will have unique and valuable skill sets like those of cybercrime investigators. Identify and explain those roles that will support and enables cyber-attacks in the business model [30marks.]

With the growth of technology, there is also an exponential growth rate in cyberspace leading to new attacking vectors, that would impact any business negatively but the Organized Criminal Group targets various businesses regardless of their size that is because every business has key assets that they need to look out for such as financial records, user names, and passwords, etc.

The main reasons for there to be a cyber-attack are as follows:

1. Business financial details.
2. Customer financial details.
3. Clients lists.
4. Customer or staff login details.
5. Intellectual property.

Organized Criminal Groups conduct cyber-attacks against a business mainly because they are deliberate and motivated by financial gains, but there are also various other motives behind the cyber-attacks which are:

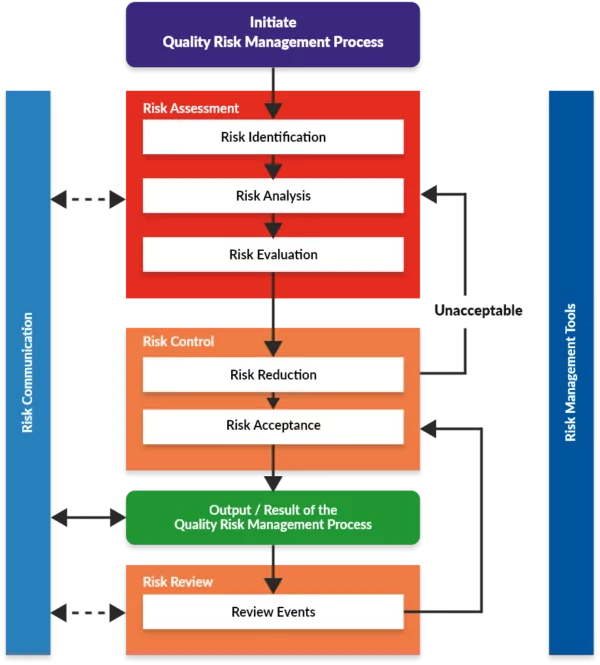
1. They might try and make a social and political point e.g. through hacktivism an example of hacktivism can be that of Pakistan (hackers) hacking into the Indian Government Database and retrieving police officer details such as their names, where they live, and work and they would upload the details they found on the internet.
2. Espionage – a classic example of cyber espionage dates back to 2009. Google reported that a company noticed a steady stream of attacks on selected Gmail account holders, which were later discovered that belonged to a Chinese Human Rights Activist.
3. Intellectual Property – The Organized Criminal Groups aim for a company’s IP, steal them, and later ask for ransoms. The IPs can range from trade secrets to product designs, and many others.

There are 2 main but broadly categorized cyber attackers that pose a threat to any business are:

1. Insider – These are individuals with physical or remote access to an organization’s assets that can pose businesses with cyber risks such as
   1. trusted employees accidentally misplacing information.
   2. Malicious insiders with legitimate access to crucial company assets.
2. Outsiders – This type of individual can come in a variety of sources which may include:
   1. Organized Criminal Groups
   2. Professional hackers, crackers that have access to crucial company assets through unauthorized means.

To limit or reduce the chances of a company being targeted by these Organized Criminal Groups can be;

1. Coming up with a Risk assessment which consists of the following steps
   1. Risk Identification – where you identify risks that could potentially halt the business entirely from achieving its goals or objectives. This process can be included by documenting and communicating the concerns.
   2. Risk Analysis – This involves examining how future project outcomes and objectives can change when risk was to occur within the company.
   3. Risk Evaluation – This process is used to compare the estimated risk a company faced against the given risk criteria to determine the significance of the risk. Within the risk evaluation it can be further divided into 5 processes:
      1. Identifying and Prioritizing Assets. – looking into all the different types of data and analyzing which of them is of high importance that could be targeted and damage the company’s image.
      2. Locating the Assets – This involves listing all the sources of the assets, this helps in tracing each asset back to its original source.
      3. Classifying the assets – As the name suggests you will need to classify each asset from one another as either public information, sensitive internal information, non-sensitive internal information, etc.
      4. Threat modeling exercise – This will involve identifying and rating all the threats faced by your top-rated assets one method that can help in this phase will Microsoft Stride method.
      5. Data Finalization and planning - Once you are done with the evaluation, it is recommended to tackle those risks, beginning with the most critical to least critical.



1. Having an elaborate Disaster Recovery plan.
2. Coming up with an elaborate Incident Response.