Week 3: Risk Analysis and Assessment

Welcome to this lecture (slides with voiceover), on risk analysis and assessment.
It is important to understand the process of risk analysis and assessment and where these begin, and in this lecture, we will explore and discuss the importance and process that these takes. The two key elements of risk management are the risk assessment and risk treatment, and we will be looking at these in this lecture. Risk assessments are an essential part of a risk management program. The difference between a risk assessment and a risk management program, is that the risk assessment is created at a particular moment in time whereas a risk management program is an iterative continuous process. An organisations' primary considerations are the financial implications where profitability and survivability must be considered. Risk assessments assist the organisation in maintaining a balance between the two goals.

So let us firstly look at how we might define risk analysis. One definition is: *'the process of achieving risk management goals',* there are other definitions that you might look up for yourselves. This process incurs examining an environment for any possible risks that might occur and evaluating the possibility of each threat occurring and the cost of any damage that the event might incur. It also involves the process of assessing the cost of any countermeasures for each risk and developing relevant cost/benefit documentation for providing safety measures to safeguard the risks occurring. Safeguards are also known as controls as they are used to control or reduce risks. They may reduce a vulnerability or the impact from a threat.

Safeguards that might be implemented are:

- Installing software patches
- Making configuration changes
- Hiring security guards
- Altering the infrastructure
- Modifying processes
- Improving the security policy
- Training personnel
- Amongst many others

A risk analysis involves the identification of risks to be analysed in order to identify the qualitative and quantitative impact of a risk on a given project, and we will look at these approaches later on. The following steps might be used in a risk analysis by an organisation.

- Identify risks
- Define levels of uncertainty
- Estimate the impact of uncertainty
- Analyse the results
- Implement a possible solution

Risk management and risk analysis are primarily controlled by upper management. It is the responsibility of upper management to initiate and support both risk analysis and assessment by defining their actual scope and purpose. This process might then be delegated to security professionals or an evaluation team. Nevertheless, all risk assessments, results, decision making, and outcomes must be approved by upper management and this is an element of providing due care. We know that it is impossible to mitigate 100% of the risks, it is therefore essential that upper management make the final decisions as to which risks are acceptable/not acceptable. This process can only be carried out by complex risk and asset assessments. Risk assessment identifies, assesses, and implements key security controls, and focuses on preventing application security defects and vulnerabilities. Importantly, it supports management in making security control decisions which is an essential requirement to addressing key security issues. Decisions have to be

made to determine which risks should be reduced, avoided, shared or transferred, mitigated, or accepted. High priority risks should be mitigated and lower priority risks may have to be accepted.
A risk assessment enables management in assessing the cost of countermeasure for risks as well as creating a cost benefit analysis document for providing the identified safety measures.

We see that risk assessment supports management in making informed decisions for example resource allocation and security control implementation. A risk assessment begins with risk identification and detecting and defining specific element of risk assets, threats, and vulnerabilities. A model that might be employed where each of the following applies to the three elements:

- Identification of risks, threats and vulnerabilities – losses can occur when a threat exploits a vulnerability but losses can be reduced if likely threats and vulnerabilities are identified.
- Assessment of the likelihood of a risk occurring. This can be based on historical data as well as expert opinion.
- Identify asset values – these can be hardware assets, software assets, or data and identification of the asset value can help to determine the impact of a risk.
- Mitigation – safeguards or controls reduce the risk or reduce the risk's impact. Risk assessment helps determine which safeguards to implement.
- Prevention – can also be based on historical data with relevant safeguards put in place.

There are three critical steps in a risk assessment to identify:

- Scope – this is the boundary of the assessment and if this is understood it helps keep the risk assessment on track as it will be unlikely to change. If the scope is not clearly identified, it can result in scope creep which can cause overruns and missed deadlines.
- Critical areas where vulnerabilities are present
- Team members who must be 'fit for purpose'.

Risk management and risk analysis are primarily controlled by upper management and consequently delegated to security professionals or an evaluation team who will conduct the necessary investigations. The final decision-making however, will be made by senior management who decide whether or not to go ahead with the proposals put forward and give their approval of any decisions made. A senior manager is ultimately responsible for the security maintained by an organisation and they should be most concerned with the protection of its assets. They are responsible to sign off all policy issues. The whole process can only be carried out by complex risk and asset assessments. We must remember though, that technical security can only prevent technical attacks, not physical ones!

Looking at some key terminology to help us identify the relevant threats to be considered in the risk analysis and assessment.

Risk: the possibility or likelihood that a threat will exploit a vulnerability relating to an asset and involves an assessment of the probability, possibility or chance of its occurrence. Every instance of exposure is a possible risk and therefore might be quantified with a formula of 'Risk' equals 'Threat' times 'Vulnerability'. Risk = Threat * Vulnerability.

Breach: a breach is an occurrence of a security mechanism being bypassed or thwarted by a threat agent or bad actor and when a breach is combined with an attack, it can result in penetration or intrusion.

Penetration or Intrusion: this is a condition whereby a threat agent has had the possibility to gain access to an organisation's infrastructure or resources and is the result of a deliberate circumvention of security controls.

We will continue with looking at some more key terminology that is used in risk analysis and assessment in the next slide.

Other key terminology includes:

Asset Valuation: that is a monetary value assigned to an asset indicating its value that includes costs related to tangible costs such as development, maintenance, repair, replacement, staffing etc. There are

also intangible costs such as public confidence, industry support, organisational impact, productivity and so on.

Realised Threat: a realised threat is a threat event that is taking place or has already taken place.

Exposure: is being susceptible to asset loss due to a threat. Exposure is the potential future loss that might be assigned to a possible threat or vulnerability. Finally:

Mitigations: mitigations are also referred to as countermeasures and these include security controls and safeguards which are measures to reduce vulnerability and therefore risk, to protect against one or more threats and can include software patching, changing configuration, employing physical security, altering infrastructure, modifying processes, creating or amending policies and procedures, training personnel, and many more.

We will now take a look at the relationship between different elements such as assets, threats, vulnerabilities, exposures, risks and safeguards. The diagram on the right hand side of this slide shows these relationships where threats exploit vulnerabilities which results in exposure which is a risk, and a risk is mitigated by safeguards and these safeguards protect any assets that are endangered by threats.

In summary, in the preceding slides we have looked at risk analysis and assessment. Risk assessments are used to identify and quantify risks. This is carried out by identifying threats and vulnerabilities and then using a relevant methodology to prioritise the risks. The primary risk assessment methods are quantitative and qualitative and we be looking at these in more detail in the next lecture.

Now please take a break and reflect on what we have learned so far before moving on to the next task for the week which is to read Chapter 5 of the core module text on *'Defining Risk Assessment Approaches'.* This chapter will give you more in-depth information on what we have looked at in this lecture and increase your understanding of the subject area.