Risk Assessments

Risk is, at its core, the probability that a threat will be realised. Risk is a continual balancing act of vulnerability versus threat. In future lessons, we're going to discuss how we balance these against each other in order to manage risk well. Now, as cybersecurity professionals, our job is to minimise vulnerabilities.

Vulnerabilities are any weakness in the design or implementation of a system. We're given control over vulnerabilities because they come from internal factors such as software bugs, misconfigured software, improperly protected network devices, lacking physical security, or other such issues. Vulnerabilities are within our control, or at least within our organisation's control. Whether we choose to address those vulnerabilities, though, is a decision in risk management.

This is because a **threat** is any condition that can cause harm, loss, damage, or compromise to our information technology systems. These threats come from external sources, such as natural disasters, cyber attackers, data integrity breaches, disclosure of our confidential information, and numerous other issues that arise during our daily operations. Remember, threats are external to you and you can't control them, you can only mitigate them. If somebody wants to attack you, they are the threat. You can't control whether or not they're going to attack you, right? You can only try to minimise your vulnerabilities so that their attack won't be successful. **Vulnerabilities are completely within your control, threats are not.**

Risk Avoidance

The first one is risk avoidance, this is a strategy that requires stopping the activity the has the risk or choosing a less risky alternative.

Risk Transfer

Now, the second thing we could do is we could transfer the risk. Risk transfer is a strategy that passes the risk to a third party, most commonly to an insurance company. A good example of this would be if your organisation is worried about the risk of your offices being destroyed by floods. If this is a concern for you, you could purchase an insurance policy to transfer the risk of losing all of your computers and all of your assets to another third party, the insurance company.

Risk Mitigation

Risk mitigation is a strategy that seeks to minimise the risk to an acceptable level, where the organization can then accept the remaining risk. For example, if you're running a server that's been identified to have five critical vulnerabilities, two high vulnerabilities, four medium, and 17 low vulnerabilities, you can then decide which ones you're going to deal with first.

Risk Acceptance

With risk acceptance, we're seeking to accept the current level of risk and the costs that are associated with it, if that risk was realized. Generally, this would be a proper strategy if the asset is a very low cost item, or the impact to the organization overall would be rather low.

Residual Risk

Now, even if we avoid the risk, transfer the risk, or mitigate the risk, there may still be some amount of risk left over. This is known as residual risk. Residual risk is simply the risk that's left over after you've tried avoiding, transferring, and mitigating the risk. It's uncommon that there is no residual risk leftover because risk simply exists in every single thing that we do.

Qualitative Risk

Qualitative risk analysis uses intuition, experience, and other best practices to assign relative values to a given risk. These values could be low, medium, high, and critical. Or you can use any other designated categorization system that you want. You can even use numbers. But numbers aren't really an exact measure in this case. For example, if I asked you to score this lesson, you can give it a one through a five star rating. This isn't a mathematical analysis, it's just a number that's representing your opinion, with five being great and one being horrible. Therefore, it's qualitative in nature, not quantitative in nature. The best practices here include techniques to measure risk such as brainstorming sessions, focus groups, surveys, interviews, and estimating the likelihood of events.

Quantitative Risk

Now, we're going to look at the other side of the equation, quantitative risk analysis, which heavily relies on numbers and monetary values for all parts of the risk analysis. This includes numerically assigning values to the value of the assets, the threat frequency, the severity of the vulnerabilities, and the impact of the realization of a given threat. Now, with quantitative risk analysis, this is going to remove much of the estimation and guesswork from a risk assessment because it's going to turn this into a large math problem instead. Equations are used to determine the total and residual risk, as well as provide you with a cost directly associated with those risks. This is going to allow us to have a numerical method to represent the magnitude of the impact of a risk. The magnitude of impact is an estimation of the amount of damage that a negative risk might achieve. This is also known as a risk impact, and it can be measured financially using quantitative methods or qualitative methods.

The three most common calculations used in determining the magnitude of an impact in a quantitative risk analysis is the Single Loss Expectancy, or SLE, the Annualized Rate of Occurrence, or ARO, and the Annualized Loss Expectancy or ALE.

Single Loss Expectancy

Single Loss Expectancy is the cost associated with the realization of each individualized threat that occurs. It's calculated by multiplying the asset's value times an exposure factor. Now, the exposure factor is simply the amount of the asset that's going to be lost if the threat is realized.

Annualized Rate of Occurrence

ARO is calculated simply by determining how many times per year is a threat going to be realized.

Annualized Loss Expectancy

Now, the Annual Loss Expectancy, on the other hand, is the expected cost of a realized threat over a given year. This is calculated by multiplying the Single Loss Expectancy times the Annual Rate of Occurrence.

Methodologies

Well, there’s many different types of security assessments that are used by an organization to protect their enterprise networks.
And these security assessments verify that the organization's security posture is designed and configured properly to help thwart all those different types of attacks and threats that are out there.
These security assessments include vulnerability assessments, penetration testing, internal and external audits, self-assessments, password analysis, and many other types.

Now, there are two main types of methodologies that are used in these assessments. There's active and passive.

Active

Active assessments utilize a more intrusive technique, more things like scanning and hands-on testing, and probing your network to determine what vulnerabilities might exist. This can actually result in your networks or servers being forced offline if you're too aggressive in your active scans.

Passive

Now, a passive assessment, on the other hand, utilizes open source information, the passive collection and analysis of network data, and other unobtrusive methods without ever making direct contact with the targeted networker systems.

Security Controls

Now, security controls are first broken down into three types, physical, technical, and administrative.

Physical

Physical controls are security measures that are designed to deter or prevent unauthorized access to sensitive information or the systems that contain it, by preventing physical access. So, when we discussed physical security earlier in this course, we were focused on a lot of physical controls like fences and door locks and alarm systems and security guards, all of these things are focused on protecting the

physical computers, servers, and networks from being accessed by people outside our organization.

Technical

Our second type of security control is called the technical control. Technical controls are safeguards and countermeasures. They're used to avoid, detect, counteract, and minimize our security risks to our systems and information. So, when we talk about using passwords and access controllers, and encryption for our hard drives, and multi-factor authentication, we're really talking about technical controls here.

Administrative

The third type of security control is called an administrative control. Administrative controls are focused on changing the behaviour of people instead of removing the actual risk involved. So, if I create a policy or procedure, that states that every employee has to lock their computer whenever they're going to be away from their desk. This is an administrative control.

Now, the National Institute of Standards and Technology or NIST, actually has three other categories that we organize Security Controls in, as well. These are management controls, operational controls, and technical controls.

Management Controls

Management controls are security controls that are focused on decision-making and the management of risk. This usually includes things like policies, procedures, legal compliance, software development methodologies that you choose, setting up a good vulnerability management program, and other things like that. Management controls are all about how your system's security is going to be managed and overseen.

Operational Controls

Now, operational controls are focused on things that are done by people. With operational controls, I'm trying to increase the security of the system by controlling the actions of the individuals and the groups who use it. This includes user training, configuration management, testing our disaster recovery plans, and conducting incident handling. These controls are performed by technical people in order to carry out the overall direction that was provided by management controls

Technical Controls

The third category NIST uses is called technical controls. These are logical controls that are put into a system to help secure it. This is things like AAA, the authentication, authorization, and accounting, access control, encryption technology, passwords, and configuring your security devices. Anything that is technical and performed by the computer can really be put into this category.

We have yet another group of three that can be used to describe security controls. They are preventive, detective, and corrective.

Preventive

Preventative/deterrent controls are security controls that are installed before an event happens and they're designed to prevent something from occurring. For example, you might install a technical control like a RAID in your file server to ensure that your data always has redundancy available and prevent data loss from occurring.

Detective

The second type of control is called a detective control. Detective controls are used during an event to find out whether or not something bad may have happened. If you have a closed-circuit TV system being monitored by a security guard, this is a type of detective control. Intrusion detection systems, audit logs, and alarms are all different types of detective controls, as well, when they have logging enabled.

Corrective

The third type of control is called a corrective control. Corrective controls are used after an event occurs. So, let's say somebody hacks into your server and they erase your hard drive. Well, if this happens, you're going to hope you have a good backup copy somewhere. If you've been doing good tape backups, this is called a corrective control because it's going to allow you to recover from this data loss and by fixing something after it happens, it becomes a corrective control.

Compensating Control

Now, a compensating control is used whenever you can’t meet the requirements for a normal control. For example, let's say your organization has a physical security policy that states that every door to a networking closet or server room has to have a

retina scan-enabled door lock to protect the devices in those rooms. Well, maybe one of your branch offices is located in some far off country overseas and they have no retina scan-enabled door locks being sold in that region. Well, instead of using a retina scan door lock, you decide to install a cipher door lock. The cipher lock will be considered a compensating control until you can get a retina scan-enabled door lock ordered, shipped, and installed at this location.

Types of Risk

This includes external risk, internal risk, legacy systems, multiparty, intellectual property theft, and software compliance and licensing.

External risk

This is a type of risk that is produced by a non-human source and is beyond human control. Now, what are some good examples of external risk? Well, we have things like wildfires. If there are wildfires burning in your area, you really can't control that.

Internal risk

Now, when we start talking about internal risk, internal risk is those risks that are formed within the organization itself. They arise during normal operations and often they're forecastable, meaning, you can see them coming and therefore, you can plan around them. A great example of this would be server crashes.

Legacy systems

Now, when I talk about a legacy system, this is any old method, technology, computer system, or application program which includes an outdated computer system that's still in use. A great example of this is if you just look down into your ICS and SCADA networks. Most of these have outdated things that are still being run. For example, many of them are still running on Windows XP.

Multiparty

Well, a multiparty risk is any risk that's referring to the connection of multiple systems or organizations, with each of them bringing their own inherent risks. So, let's say you owned a company and I own a company and we decided we wanted to go into business together. Well, if we did that and we start connecting our systems together, that is a multiparty risk because I am now assuming the risk that you're bringing to the party and you're assuming the risk that I bring into the party.

Intellectual property theft

A lot of times when hackers are breaking into networks, it's not because they want to cause you harm or take down your systems necessarily, it's because they want to steal what you have. Now, again, that is going to cause you harm but not harm in the way of taking down your servers harm. And so, when we think about IP theft, we're really talking about the risks associated with business assets and property being stolen from your organization. And this can cause economic damage, the loss of a competitive edge, or a slowdown in business growth. All of these things are risks associated with IP theft. Now, when you're dealing with IP theft, you really are worried about protecting your stuff. And so, one of the greatest ways to protect against IP theft is making sure you have data loss prevention systems.

Software compliance and licensing

Now, when we talk about software compliance and licensing, we have some risks associated with this, too. And I know you might be thinking, "What kind of risk do I have with software compliance and licensing? If I buy a licence, there is no risk." Well, there are risks associated with a company not being aware of what software components are actually being installed on their network. And that's what software compliance is all about. So, for example, if I'm running an organization with 10,000 people, and somebody decides to go to the store and buy a program and put it on the network, even though they have the licence for it and they install that thing on the network, I still am now assuming the risks of that software because when they installed it, that is now something else that brings vulnerabilities to the network.

Now, on the other side of this, we also have the licensing angle. Now, when you have people who are installing software, a lot of times they're just downloading it off the Internet or bringing it in from home and they don't have the proper licensing in place. So, let's say you wanted to create some new servers and you decided to just download the Windows Server 2016 and install on some systems. Well, if you don't have the proper licensing for that and Microsoft finds out, they might cripple that server or they might sue you for damages because you're using their programs without licensing.