What is a Cyber Risk Assessment?

In our modern world, we now face risks that may never have been an issue before. This is largely thanks to the fact that we work, socialise and quite often live, in a somewhat virtual world.

This has meant that we need to think about the risks that are associated with the cyber world. A cyber security risk assessment is when a risk assessment, just like you would have for health and safety in a workplace, is used to look at the potential cyber risks that are associated with a business.

These assessments will not only identify key risks that the business may face over time but also estimate the likelihood of them happening and the potential impact of these risks. Having this information will then mean that the risks can be prioritised so that they can be tackled and mitigated in the right order.

What is security testing?

Along with a cyber security risk assessment, you as an organisation can also look at cybersecurity testing. The idea of cyber security testing is that it allows you to find the potential vulnerabilities that you may have within the systems or programmes that you use as a business.
These may be vulnerabilities that you already know of, but just want to see what the impact may be, or, they may be entirely unknown and unidentified risks that could end up causing a huge issue for your business.

What are the Steps of a Cyber Risk Assessment?

When it comes to carrying out a cyber risk assessment, you must move through all of the key steps. This will ensure that you cover all of the things that you need to cover and that nothing is overlooked.

To help you to work out how best to approach this form of risk assessment, we have put together the steps that you should be following when you complete one for yourself.

Assess your current capabilities Work well under pressure

It is important to be able to recognise and assess the measures that you already have in place within your security system. This is because it will allow you to think about whether or not it matches the potential risks that are out there in the cyber world, and make sure that you know what may need to be changed.

You must take the time to think about what your system can do, and also be as honest as you can about these capabilities, even if it means recognising that you have some gaps that need to be filled.

Identify threat sources

It is also important toe ensure that you know where the key cyber threats to your business are going to come from. Of course, you cannot always predict what will happen in the future (and those who wish to carry out cyber attacks are always finding new ways to threaten and cause an issue).

However, if you can identify the main threat sources, then you are well on your way to making things easier to fight when the time comes.

Identify and prioritize risk responses

Next, you need to be able to identify the responses that you as a business need to have to those risks. There will usually be more than one response that you can have to risk, and the one that you choose will depend on the nature of the threat and also the possible speed at which it can cause an impact.

You should be able to think about which responses are most relevant and the order that you will then put these responses in place.

Identify threat events

There are certain times or incidences when a threat is more likely to occur. Whilst you may not always be able to plan for this, if you can identify the main threat events, then you are going to be able to find a way to mitigate the impact it has and try to reduce the harm it could cause to your business.

Identify vulnerabilities

It is important to recognise that whilst some cyber threats are going to be out of your control (and can happen no matter what) some can be caused by your vulnerabilities in security.

A key part of the risk assessment process for cyber threats is to make sure that you identify the vulnerabilities that you may have in your current setup. That way, you can think of ways to improve it and stop these possible threats from happening.

Analyze the risk

The best way to know how to minimise (and hopefully then beat) a risk is to find out as much as you can about it and what it may mean for you. This means that a key part of the cyber risk assessment process is analyzing the risks.

Find out as much as you can about where they come from, what they may mean and of course, what impact they are likely to have on your business. All of these things give you as much information as possible about what to expect.

Determine the likelihood of exploitation

The main focus for those who carry out cyber attacks is to exploit the target. They want to either gain information or in most cases, money. This means that you need to know how likely you are to be a victim of exploitation.

Consider the different aspects of your business and think about the risk that they pose when it comes to exploitation. That way, you can ensure that you lower the risk as much as possible where you can.

Determine probable impact

Whilst you never know the impact of a cyber attack, at least not 100% you can have a carefully considered guess at what it may mean for your business. Think about what the probable impact may be from a cyber attack and what this will mean in both the short-term and the longer-term too.

Calculate the risk and impact

The next step when it comes to risk and impact, is to calculate what the correlation is between the level of risk and the impact that it may have. Identifying this can help you to prioritise what is the most important risk to avoid or to protect against.

Build a business case

If you want some additional support when it comes to protecting your business against cyber risks, then you may need to put together a business case. This will reflect everything that you have already done to identify and plan for the risks and what things you want to put in place.

Set security controls

Once all your hard work has been finished and you know what the best security measures for your business are going to be, then the time has come to set security controls and measures. Decide which is the best way to go about putting these in place and then go from there.

Monitor and review effectiveness

Whilst it is great to put the measures that you have planned out in place, if you don't check how they are doing and monitor their effectiveness, then they still may not be able to do what you need them to do.

This is why the last part of the cyber risk assessment process should be taking the time to look at the measures that you have put in place and identify whether or not they are going to be suitable for you in the long term and whether they are doing what you want them to.

Types of security testing

To ensure that the measures that you have decided on from a cyber risk assessment are working the way that they should, you can carry out a range of security testing measures.

They come in a variety of forms and they not only work well as a standalone approach to security testing but can also be combined to achieve the maximum impact possible.

Ethical hacking

The idea of ethical hacking is that you appoint hackers to gain access to your system, just as a criminal hacker would. However, these hackers are only doing so to provide you with the information that you need to be able to ensure that your business is protected. Hence the name ethical hacking.

Penetration testing

Penetration testing is much like ethical hacking; whereby a simulated attack is carried out on your systems. All to be able to provide an evaluation of how your security measures are performing and whether or not your business is protected.

Posture assessment

Posture assessments take a more end-to-end look at the security measures and capabilities of your business. This particular test is going to help you to build a strategy, rather than focus on single aspects of cyber security and give you tools and knowledge to help to reduce the chance of cyber attacks from happening within your business.

Risk assessment

We have already looked at how a risk assessment can help security. They are there to ensure that you understand and identify the main risks to your business and its cyber security and to help you to develop methods to combat this.

Security auditing

A security audit will be a more comprehensive and in-depth review of the IT and cyber infrastructure of your business as a whole. It looks at things such as policies and procedures that you have set out and whether they are offering the right level of protection that you are going to need for your business.

Security scanning

Once you have an overview of your security measures, then comes the time when you want to dive deeper into those issues. This is where security scanning can help you, security scanning will provide more information on specific vulnerabilities.

Vulnerability scanning

Another way to identify key vulnerabilities is with vulnerability scanning. This will only focus on the aspects of your network and systems which are open to attack and give you the information that you need to be able to try and stop these from happening.

Cyber Security Training

One way to protect your business and your employees is through Cyber security training.

Cybersecurity training provides numerous benefits for organizations in the UK. It increases security awareness among employees, reducing the likelihood of security incidents and data breaches. By educating employees on best practices, such as identifying phishing attempts and following secure protocols, sensitive data is better protected. Additionally, cybersecurity training ensures compliance with regulations and strengthens incident response capabilities. It fosters a culture of security, where employees actively contribute to safeguarding the organization's assets and reputation. Ultimately, investing in cybersecurity training helps create a resilient and secure environment, mitigating risks and building trust with customers.

You can find information on Learn Q's Cyber Security Awareness training by clicking here.