Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

Cybersecurity Risk Assessment in a portfolio of Assets

Performing a cyber security risk assessment helps organizations strengthen their overall security. The primary goal for any asset management to have a risk profile that intertwines cyber-risks to assets is first to determine what the critical assets are and if what type of cyber threats can exploit those assets. Importantly, how much it would cost to mitigate those risks and to protect these critical assets from a breach.

The diversity of asset types and their sheer volume, even in small organisations, can make cyber asset management a challenging task. Hardware, software, virtual infrastructure, information, and online accounts must all be considered. It is important and a fundamental first step to assess and identify the assets vulnerable to cyberattacks and the type of cyber security incidents. One needs to have the right visibility of assets where it's needed gives you the chance to take remedial action, before a cyber incident takes full – effect and can develop into an unresolvable problem.

To perform a cyber security risk assessment, you need consider three factors:

- Importance of the assets at risk
- Severity of the threat
- Vulnerability of the system

The general definition of a cyber security risk assessment is: A cyber security risk assessment is the fundamental approach for companies to assess, identify, and modify their security protocols and enable strong security operations to safeguard it against attackers or attempted cyber breaches.

It is good to begin by valuating the various types of data generated and stored across the organization by various efforts. An organisation needs to determine the value of one's data, it is quite difficult to prioritize and assign resources where they are needed the most? And why?

A cyber security risk assessment also considers how a company generates revenue, how employees and assets affect the profitability of the organization, and what potential risks could lead to monetary and financial losses for the company. The identified of all these resources and assets would enhance the IT infrastructure to invest in targeted solutions that help in reducing potential risks that might lead to financial losses to the organization.

Furthermore, a cyber security risk assessment must help and inform decision makers and support proper risk and incident responses. Most C-suite executives and higher management professionals don't have the time to delve into the minute details of understanding the basics of company's cyber security operations, incident management solutions or risk aversive mechanisms. A cyber security risk analysis serves as a summary to help them make informed decisions about security for their organization. For cyber risk assessment, one must review documentation, highlight the importance of data owners and make them understand the value of the data they hold and the risk of losing the day in terms of financial losses. A company must also analyse the IT infrastructure and systems.

Take 1: Determine the value of the Information held by an organisation.

It is important to limit the scope of one's assessment to the most critical business information. The organisation must invest time and allocate adequate resources at defining a standard for determining the importance of information and prioritizing it. Companies often include asset value, business importance, and legal standing. The standard must be embedded in the organization's cyber security risk analysis solution, to categorize information as minor, major, or critical. Ask the following questions to your data and information experts.

- How valuable is this information to competitors or attackers?
- If this information is lost, could you recreate the information? How long would it take? What would be the associated costs?

- Are there any financial or legal penalties associated with losing or exposing the information?
- Would losing the information impact the company's day-to-day operations?
- What would be the financial damage of the data being leaked or stolen?
- What would be the long-term impacts of the information being lost completely or exposed? Would it cause reputational damage? How could you recover from it?

Take 2: Identify and Prioritize Assets

The second most important step to perform a cyber security risk assessment is to evaluate and determine the scope of the assessment. This means to identify and prioritize which data assets to assess, by conducting an assessment of all employees, buildings, trade secrets, electronic data, or office devices. Creating a comprehensive list of all the valuable assets is essential. Some assets could be valuable because they largely impact company revenue, while others could be valuable because they ensure data integrity to your users. Identification of crucial assets for the assessment, is followed by collecting the following information:

- Data
- Purpose
- Criticality
- Software
- Functional requirements
- Information flow
- Interface
- End-users
- Hardware
- Information security policies
- Information security architecture
- Network topology
- Technical security controls
- Physical security controls
- Environmental security
- Information storage protection
- Support personal

Take 3: Identify Cyber Threats

Once identified and prioritization of assets is completed, the next step is to identify threats that could impact the organization. A cyberthreat can be defined as an incident occurrence, individual action, or any electronic action that has the potential to harm operations, systems and/or exploit vulnerabilities to circumvent the IT security of the organization. There is a wide range of cyber threats that could impact an enterprise ranging from malware, IT security risks, insider threats, attackers, etc. For example:

- **Data leaks:** Leakage of sensitive data such as personally identifiable information (PII). These data leaks could occur due to poor configuration of cloud services, insufficient IT security policies in place, or weak authentication.
- **Insider threats:** Often, authorized users misuse their access to information and cause data breaches. These threats pose a great risk to companies as they could have devastating financial and reputational impact.

- **Service disruption:** A cyber-attack might cause unexpected service disruptions which could lead to loss of reputation and revenue. This is one major disruption, especially with regards to today's digitalised and integrated world.

Take 4: Identify Vulnerabilities

A vulnerability is a weakness that could be exploited to cause data breaches or other cyber-attacks. Identifying the vulnerabilities can be in form off:

- Audit reports
- Vulnerability analysis
- Vendor data
- Software security analyses (SSA)
- Incident response teams (IRT)
- Country specific vulnerability database information portal.

The absence of a patch in an operating system could be a simple vulnerability. One must pay special attention to these software-based security vulnerabilities; as they are easy to fix, by proper patch management in place via automated forced updates. Making technical recommendations to address physical vulnerabilities is another way to avoid vulnerabilities.

Take 5: Scenario calculation of cyber-threats and Impact Analysis on a yearly basis

One should be constantly evaluating the likeliness of common and critical cyber risks and undertake scenario calculation with regards to impact. Minimising cyber-threats through virtual sand-model and war-games analysis can help mitigate and tighten losses against cyber incidents. Compliance mechanisms with information security standards are also good measures at making the impact analysis and a minimum vulnerability risk assessment automatically rolls-in with standardisation and industry specific compliance mechanisms. But, compliance with security standards can only protect one's data so far; and proper mitigation and cyber security defense strategies have to implemented n place to secure data from cyber attackers. The level and depth of information security protocols determine the level of combat practices that take shape during data breaches.

Take 6: Prioritize Cyber Risks: A balance between 'Cost of Prevention vs Information Value'

The following risk level can become the simple basis to determine what actions should be taken to mitigate risks.

- **High:** An urgent and significant threat to the organization and risk mitigation requires immediate attention.
- **Medium:** A viable threat to the organization exists, and risk mitigation should be done within a specific period of time.
- **Low:** Threats have a low impact on the assets but may pose some issues later. Consider enhancing information security policies and deploying specific security software.

It is always a cost vs information value balance. If it costs more to protect an asset that has little to negligible financial or organisational impact, it may not make much sense to invest heavily into protecting it. However, there are assets that damage reputation and trust that an organisation commands and so it's important to consider all assets.

Take 7: Risk Assessment Report

Develop a risk analysis report which describes the value, risk, and vulnerabilities for each threat. Make sure to add the likelihood and impact of occurrence and mitigation recommendations. This will help make informed decisions about policies, procedures, and budgets. It is essential to the credibility that the risk assessment report captures all the necessary information collected throughout the assessment. Having a cohesive risk analysis report enables the assessor to communicate clearly with responsible individuals and stakeholders, helping them understand how these risks were discovered, and what they must do to contribute to their mitigation. A clear and cohesive risk analysis report helps establish guidelines and rules that provide answers to what vulnerabilities and threats could cause reputational damage and financial loss and their mitigation.

Take 8: Implement and Monitor IT Security Controls

Ones the cyber security risk assessment report has been prepared, implement, and monitor all essential IT security controls to minimize or totally eliminate (if possible) the vulnerability or threat. Implementing controls through technical means, such as software or hardware, intrusion detection mechanisms, automatic updates, two-factor authentication, or encryption or through non-technical means such as physical mechanisms like keycard access are all common IT Security protocols. Continuous monitoring of these IT security controls is essential, to understand their operational effectiveness. Implementing security controls is not a one-step process but requirement continuous monitoring to ensure optimal performance.

Conclusion:

An organization can have the best IT security policies in place, but in the current constantly changing cyber security threats scenario, it is important to stay abreast of the latest cyber incidents and keep acquiring new knowledge and smart incident detection practices and that could be threat to one's organization. It is important for individuals to have a minimum Cyber awareness training and every employee of an organisation to understand that a cyber risk can erupt from the most unknown places and that all resources and assets are vulnerable to some extent and cyber risk assessment can help prevent breaches, avoid penalties and regulatory fines, and safeguard their valuable information.