Cyber Security Risk Assessment

What is Cyber Risk Assessment

- **Cyber risk assessments** are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

- The information security risk assessment process is concerned with answering the following questions:
  - What are the organization's most important information technology assets?
  - What data breach would have a major impact on business whether from malware, cyber attack or human error?
  - What are the relevant threats and the threat sources to the organization?
  - What are the internal and external vulnerabilities?
  - What is the impact if those vulnerabilities are exploited?
  - What is the likelihood of exploitation?
  - What cyber attacks, cyber threats, or security incidents could impact affect the ability of the business to function?
  - What is the level of risk the organization is comfortable taking?

Why perform a cyber risk assessment?

- There are a number of reasons you want to perform a cyber risk assessment.
  - Reduce of long-term costs
  - Provides a cyber security risk assessment template for future assessments
  - Better organizational knowledge
  - Avoid data breaches
  - Avoid regulatory issues
  - Avoid application downtime
  - Data loss

How to perform a cyber risk assessment

Step 1: Determine information value

There are many questions you can ask to determine value:

- Are there financial or legal penalties associated with exposing or losing this information?
- How valuable is this information to a competitor?
- Could we recreate this information from scratch? How long would it take and what would be the associated costs?
- Would losing this information have an impact on revenue or profitability?
- Would losing this data impact day-to-day business operations? Could our staff work without it?
- What would be the reputational damage of this data being leaked?

How to perform a cyber risk assessment

Step 2: Identify and prioritize assets

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

How to perform a cyber risk assessment

Step 3: Identify cyber threats

Some common threats that affect every organization include:

- **Unauthorized access:** both from attackers, malware, employee error
- **Misuse of information by authorized users**: typically an insider threat where data is altered, deleted or used without approval
- **Data leaks:** Personally identifiable information (PII) and other sensitive data, by attackers or via poor configuration of cloud services
- **Loss of data:** organization loses or accidentally deleted data as part of poor backup or replication
- **Service disruption:** loss of revenue or reputational damage due to downtime

How to perform a cyber risk assessment

Step 4: Identify vulnerabilities

- A vulnerability is a weakness that a threat can exploit to breach security, harm your organization, or steal sensitive data.
- Vulnerabilities are found through vulnerability analysis, audit reports, the National Institute for Standards and Technology (NIST) vulnerability database, vendor data, incident response teams, and software security analysis.

How to perform a cyber risk assessment

Step 5: Analyze controls and implement new controls

- Controls can be implemented through technical means or through nontechnical means.
- Controls should be classified as preventative or detective controls.
  - Preventative controls attempt to stop attacks like encryption, antivirus or continuous security monitoring,
  - Detective controls try to discover when an attack has occurred like continuous data exposure detection.

How to perform a cyber risk assessment

Step 6: Calculate the likelihood and impact of various scenarios on a per-year basis

For example

- Information value=$100 million
- Data loss=half of the information value
- Likelihood= 1/5
- Estimated loss=$1 million per year

How to perform a cyber risk assessment

Step 7: Prioritize risks based on the cost of prevention vs information value

Use risk level as a basis and determine actions for senior management or other responsible individuals to mitigate the risk.

- High - corrective measures to be developed as soon as possible
- Medium - correct measures developed within a reasonable period of time
- Low - decide whether to accept the risk or mitigate

How to perform a cyber risk assessment

Step 8: Document results in risk assessment report

The report should at least include the following:

- Scope of the risk assessment
- The techniques used for the assessment: for example questionnaire, interview, site visiting, tools
- Vulnerability statement
- Threat statement
- Select a Risk model: for example high risk, medium risk and low risk
- Provide recommend controls

Let’s recap the key points

1. Identify company assets – these could be proprietary information, hardware, software, client information, network topology, etc.
2. What are the threats? – be aware of these main sources of threats: natural disasters, human error, malicious intent, system failure
3. What are the vulnerabilities? – vulnerabilities are weaknesses in security that can expose assets to threats. Conduct internal audits, penetration testing, etc, to find vulnerabilities in your organization.
4. Likelihood of incidents – assess the assets’ vulnerability to threats and the likelihood of an incident happening.
5. What are the possible repercussions? – One or a combination of the following can happen if company assets get impacted by threats: legal action, data loss, production downtime, fines and penalties, negative impact on company reputation, etc.
6. Determine controls – Determine what controls are already existing to mitigate threats. New controls may need to be implemented or old ones updated to adapt to new and changing threats.
7. Continuous improvement – Document and review the results of risk assessments and always watch out for new threats.

Vulnerability 1	
Threat & vulnerability	
Vulnerability	User’s new laptop was not password protected
Threat	Unauthorized access can delete, alter or steal data
Techniques used to identify the risk	Site visiting, Observation
Existing controls	All laptops have designated users who are responsible for the security of the data and device. All laptops are kept in designated lockers after the day. Door has magnetic lock that can be opened by proximity card of employees.
Risk rating	
Consequence	Medium
likelihood	Unlikely
Risk rating	Low
Recommended Control	
Recommended controls or alternative options for reducing risk	User need to create a strong password to protect his laptop from unintended use.

Top Risk Assessment Software

Enablon: Enablon provides the most complete Environmental Management software solutions on the market designed for Fortune 500 companies.

HITRUST Assessment Xchange: is a risk management software designed to help businesses handle risk assessment and compliance information from external parties. It enables organizations to streamline supply chain operations and collaborate with vendors.

Integrum: Integrum is a singular cloud-based risk and compliance solution designed specifically for Quality, Health, Safety and Environment (QHSE) management.

Optial: is a modular software platform comprising solutions across incident, risk, compliance and audit management, plus business continuity and EHS capabilities.