The evolving nature of internet and subsequent increase in cyber crimes has made it necessary for organizations to ensure their cyber security. In order to protect your data from cyber risks, it’s important to conduct security risk assessments. It allows you to protect against cyber threats and risks by giving suggestions for further improvement.

**What is a Security Risk Assessment?**

Security risk assessment is one of the most important party of cybersecurity practices. As the name suggests, it involves the identification and mitigation of security risks that can threaten your organization.

It also helps you comply with security standards and industry frameworks by measuring your organization’s security posture. There are a number of security risk assessments that assess antivirus updates, open ports, patch management, password policies, encryption, and more. By doing this, a cyber security professional can analyze how efficient are the organization’s controls, what the risk factors are, and what should be the detailed solutions and options of alleviating the risks.

**Benefits of a Security Risk Assessment**

Let’s briefly look at some of the benefits.

1. **Identifies Vulnerabilities**

It helps identify vulnerabilities and security loopholes in your system. Hence, you can understand the drawbacks and faults in your security policies and their implementation. By getting a list of potential threats and risks, you can improve and plan ways to strengthen your security practices.

1. **Documents Security**

An assessment of security risks can help you document the progress made for protecting the company asset. A common challenge that CISO’s face is to document the value they are providing. For instance, it is hard to measure the impact of a security breach that was prevented by the security team. However, with documenting a risk assessment, the team can document the process and highlight the impact a breach could have had it not been avoided. Documentation can also verify the remediation progress made since the last assessment.

1. **Ensures Compliance**

Many industries now require an organization to comply with certain security standards. For instance, payment card organizations need to comply with requirements of Payment Card Industry – Data Security Standard (PCI-DSS) to ensure cardholder data safety. Similarly, HIPAA compliance for healthcare industry and GDPR in the European countries.

1. Educates Employees

In order to convey your work culture and security practices, the best way is to give them a practical experience of why cyber security is important. Conducting awareness sessions and trainings is good, but unless they get a hand-on knowledge of what can go wrong, they might not take it seriously.

It’s important to regularly conduct risk assessments for your organization. Even better is to take help from a cyber security consultancy that is qualified and experience to better assess and manage your organization’s data’s security.