Get a Cyber Security Assessment Now to Know Your Risk

In today's business world, cyber vulnerabilities can drastically affect an organization's performance and reputation. Gaining a clear understanding of cyber risk thus becomes a critical component of business strategy. A cyber security assessment delivers insights companies need to avoid costly security breaches, achieve regulatory compliance and improve efficiency.

A cyber security assessment involves evaluating the security posture of the organization's information systems and digital assets. In the process, the assessment identifies vulnerabilities and threats that could compromise the availability, confidentiality, and integrity of company data. It then delivers recommendations for improving security and mitigating risks.

Benefits of a Cyber Security Assessment

Cyber security assessments deliver many benefits, including:

- **Regulatory compliance** – Privacy laws and industry regulations require organizations to protect their data and systems from cyber-attacks. Not only do assessments guide that process, but many regulations mandate regular security assessments.

- **Avoid costly breaches** – When companies understand and address security risks, they minimize the chance of cyber incidents that could damage the company's reputation, customer trust, and the bottom line.

- **Gain a competitive advantage** – Regular assessments demonstrate to company stakeholders and customers a strong commitment to security.

- **Improve productivity** – When companies act on the recommendations from a cyber security assessment, they prevent or minimize security incidents and data breaches. This reduces downtime, errors and waste caused by cyber incidents.

- **Reduce costs** – According to IBM's 2022 Data Breach Report, the average cost of a data breach in the United States has risen to $9.4 million. Identifying and addressing potential threats and vulnerabilities before a breach occurs saves money.

What Happens in a Cyber Security Assessment?

Cyber security assessments can take different forms. However, the assessment will generally begin with an inventory that includes both the data and the information systems that support data assets. It also includes the policies, processes and security controls that govern data storage, movement, and access.

Next, the assessment will evaluate existing security measures against industry standards, regulatory requirements, and business needs. This may include detailed penetration testing. The resulting reports will outline gaps between security targets and existing controls.

With the results of the cyber security assessment in hand, the organization can then build a strategy to close security gaps. This will necessarily involve prioritizing actions and resource allocation according to identified risk and the value of each asset.

Some of the items a cyber security assessment considers include:

- Security policies and procedures, as well as the means for enforcing them
- Security awareness training
- Device management
- Identity and access management, including privileged user management
- Information governance (knowing where data lives, where it travels, who owns it and who can access it)
- Data security controls, including items such as encryption and email security
- Security monitoring
- Patch management procedures
- Business continuity and disaster recovery plans and data backups
- Supply chain management

Penetration Testing

A critical component of the cyber security assessment process involves penetration testing. Penetration tests simulate real-world attacks, but under controlled conditions. This allows the organization to pinpoint actual risks from the perspective of a motivated attacker. The security team can then proactively address weak points before hackers can exploit them.

How to Choose a Provider to Conduct the Assessment

To get the most value out of a cyber security assessment, seek a qualified and experienced security provider to conduct the assessment. When evaluating providers, look for the following:

- A proven track record of delivering high-quality cyber security assessments for organizations like yours.
- A comprehensive methodology that covers all aspects of your information systems and assets, including network, web, cloud, mobile, IoT, etc.
- A team of certified and skilled professionals who can perform the assessment using the latest tools and techniques.
- A clear and concise report that summarizes the findings and recommendations of the assessment in a way that is easy to understand and act upon.

While critical, regular cyber security assessments represent just one piece of an ongoing cyber security strategy. The cyber security experts at eMazzanti will help you design and implement a comprehensive security strategy designed around organizational needs and business goals.