What is Cyber Security? 6 Steps to Supporting Profitability and Preventing Chaos

Organizations of all kinds demonstrate an increasing reliance on technology such as the cloud and mobile devices. Technology advances, combined with the explosion of data and the hybrid work environment, make cyber security more important than ever. What is cyber security? The protection of systems, networks, devices, and data from cyber-attack.

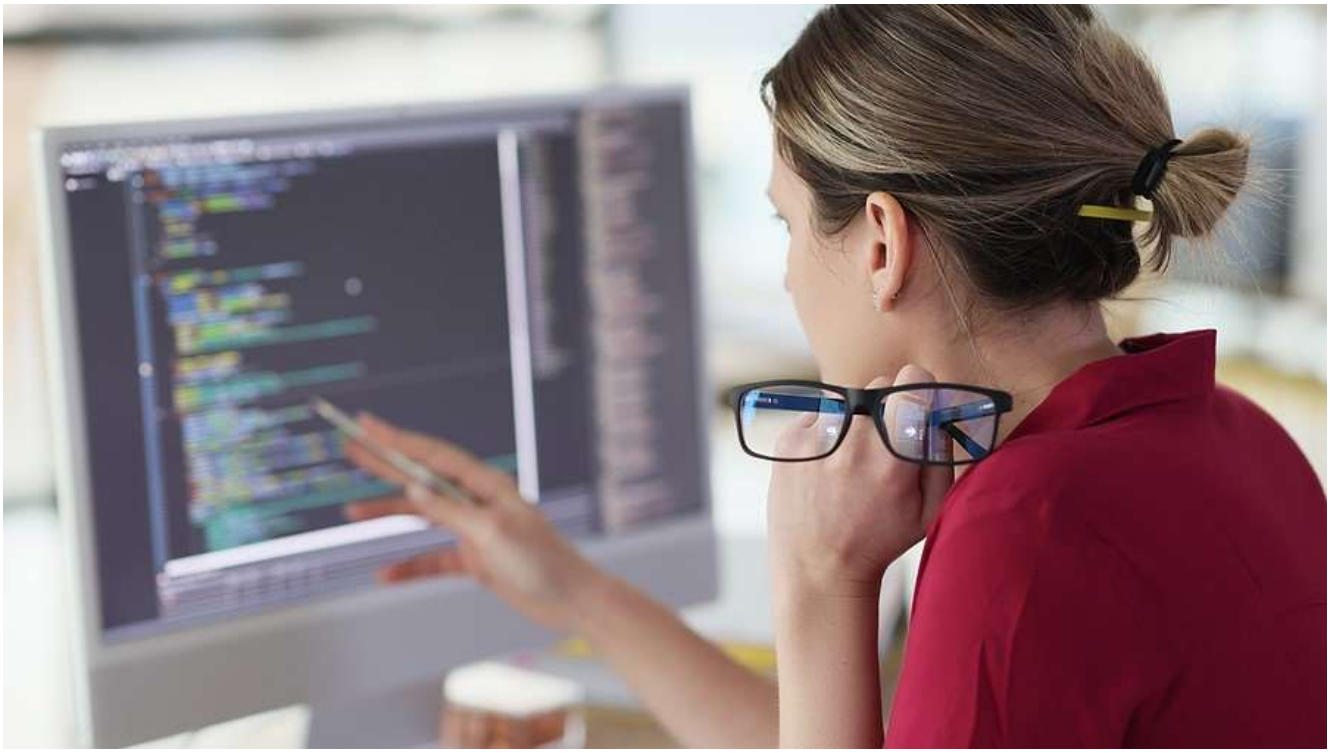
Of course, putting this simple definition into practice requires a complex combination of tools and strategies. Data plays a critical role in driving business strategy and retaining customers. And the consequences of a data breach can include substantial economic costs, as well as reputational damage and productivity loss.

A comprehensive cyber security plan involves many layers and moving parts. The following six steps will get you started.

1. Educate Staff

In 2019, 90 percent of data breaches resulted from human error. That suggests that employees represent the weakest link in the security chain. However, it also suggests that a staff educated in security awareness can prove an essential line of defense. Consequently, any cyber security strategy must include targeted security awareness training.

Effective security awareness training will teach employees how to recognize and address threats such as phishing and business email compromise (BEC). It will target specific audiences. And it will include multiple facets, from formal training to visual reminders and periodic phishing simulations.



2. Secure All Endpoints

With the prevalence of remote and hybrid workforces, as well as BYOD policies, organizations must make endpoint security a priority. Every computer, server and mobile device connected to the network represents a possible entry point for attackers.

Endpoint security involves ensuring that all devices have the proper security controls and that they follow security protocols. It also includes continual monitoring of all devices to detect potential vulnerabilities and identify suspicious behavior. Security administrators should be able to view and manage user permissions for all endpoints from a central location.

3. Ensure Email Protection

Email, while essential to business productivity, can present significant risk to the organization if not managed effectively. Not only does 92 percent of malware enter the organization through email, but email also represents a major vehicle for data leaks.

Email protection begins with email filters to block spam and phishing attempts. Additionally, carefully constructed electronic communications policies can automate the enforcement of email rules that prevent the improper sharing of sensitive information. ePolicies also address email encryption and automate essential retention policies.

4. Strengthen Cloud Security

While the cloud brings many critical advantages, such as accessibility and scalability, it also introduces significant security concerns. Organizations must adjust security practices to address the unique risks inherent to computing in the cloud.

In the first place, operating in the cloud means that the perimeter of the traditional on-premises network has disappeared. Every connected device means a potential doorway for attackers. Protecting data in a hybrid cloud environment that involves multiple clouds and on-premises networks further complicates the security environment.

Additionally, operating in the cloud means understanding the shared responsibility model of cloud security. While cloud providers make security a priority, cloud customers have responsibility for certain elements. This includes securing all devices, protecting data and identities, and ensuring proper authentication and access management.

5. Monitor, Monitor, Monitor

Enhanced by AI and machine learning, automated 24/7 monitoring can identify suspicious activity in the system and alert appropriate personnel before a breach occurs. A SIEM (Security Incident Event Monitoring) solution, for example, collects and analyzes log and event data in real time from across the system.

6. Implement Business Continuity Strategies

Even the best cyber security strategies cannot guarantee against data breach. Thus, companies need to implement business continuity and disaster recovery programs. These include comprehensive

backup and recovery solutions. Additionally, a detailed incident response plan will help the company respond quickly and effectively when a security incident does occur.

What is Cyber Security? Strategic Partnerships Pull It All Together

Guarding against cyber threats requires a multi-faceted approach implemented by knowledgeable security professionals. For many organizations, including small to medium businesses, hiring that expertise in-house can prove difficult. Fortunately, a managed services provider can help fill the gaps.

The security professionals at eMazzanti will help your organization implement the security controls necessary to protect endpoints and secure a complex cloud environment. They will conduct risk assessments and 24/7 security monitoring, assess ePolicies and help you ensure business continuity.