Cyber Security for Business is Critical, Regardless of Business Size

Equifax, Colonial Pipeline and Target have become cautionary tales of cyber-crime. However, thousands of attacks on smaller businesses still cause devastating damage. Consequently, cyber security for business remains a critical strategy, no matter the size of the organization. Businesses must understand and address continually evolving cyber challenges.

Importance of Prioritizing Cyber Security

While cyber security does not come cheap, it represents an essential business investment. In an environment increasingly dominated by data, digital assets often hold more value than material assets. From trade secrets to sensitive financial and personal data, organizations store a treasure trove. And hackers know it.

At the same time, the business environment becomes increasingly complex with each passing year. Companies rely on the cloud to facilitate remote work and store vast quantities of data. Employees use a variety of devices, from PCs to tablets and smartphones, to access that data. And organizations rely on a network of third parties with varying cyber security postures.

Cyber Criminals Target Small Businesses

While data breaches at large enterprises make the headlines, 60 percent of attacks focus on small businesses. In the first place, small businesses store valuable data. And because they often lack the security resources of larger organizations, criminals can gain access more easily.

Secondly, small businesses provide an access point into even more attractive targets. For instance, hackers may find it relatively easy to breach the insufficient security measures at a small billing services company. Then, with stolen credentials and network access, they can breach a more lucrative target that contracts with the smaller company.

Cyber Security for Business Best Practices

Statistics show that social engineering and malware make up the most common threats against small businesses. Email remains a common attack vector, although outward facing websites and an increasing collection of endpoints present significant risks, as well. Behavioral vulnerabilities such as poor password practices and unsafe web browsing habits add further complications.

Businesses need to employ a combination of security strategies to counter these threats. Some key strategies include the following:

- **Multi-factor authentication (MFA)**: In a recent document from the U.S. Cybersecurity and Infrastructure Agency (CISA), government experts repeatedly emphasized the importance of implementing strong MFA to protect systems. Passwords alone will not suffice.

- **Security awareness training**: Humans remain both the biggest risk factor and a critical part of cyber defense. Consequently, any viable security strategy must include engaging, regular security awareness training for users at all levels.
- **Endpoint protection**: Every device that connects to the business network broadens the attack surface. This includes PCs, laptops, mobile devices and IoT devices like security cameras. Implementing a zero-trust security stance, along with constant monitoring and encryption, help to mitigate the risks.
- **Monitoring**: Regardless of the protection measures employed, a network with any outside access remains vulnerable to attack. 24x7 network monitoring proves essential in catching and halting attacks early on. And when augmented with AI, monitoring systems can learn to spot suspicious behavior almost immediately.
- **Third-party risk management**: Every organization partners with outside vendors that provide services and often have some level of system access. If a hacker successfully compromises the vendor, they can gain access to your system. Make sure vendors use sufficient security practices, and carefully monitor their access to your systems.

Everyone Plays a Role in Security

For a cyber security strategy to prove effective, it must include every person in the company, from the CEO to the interns. CISA recommends that businesses identify a security program manager, a key person to maintain the incident response plan, host quarterly security exercises and ensure training and MFA compliance.

However, the security program manager plays just one role in the security strategy. CEOs and other executives must create and support a culture of security and provide necessary budget and support.

Additionally, IT staff enable MFA and encryption, ensure patch management, perform and test backups and otherwise ensure the technical controls are in place to secure data and networks. Finally, end users play a key role in securing the front lines by practicing safe computing and alerting security staff to any issues.

Essential Partnerships Improve Small Business Security

Security threats and the measures to protect against them evolve daily. For small businesses with minimal to no IT staff, addressing the security challenge can prove an almost insurmountable challenge. Partnering with security professionals like those at eMazzanti enables even small businesses to benefit from enterprise-class cyber security.