How to Overcome the Threat of Complacency in Cybersecurity

Despite a constant stream of high-profile cyber-attacks, too many organizations drag their feet in strengthening cybersecurity measures. Some fear the price tag associated with cybersecurity. Others turn security over to an MSP and forget about it, or they trust strategies implemented years ago. But complacency in cybersecurity poses a grave threat.

When organizations turn a blind eye to cyber threats, or when they assume current measures will prove sufficient, they put their companies at risk. The digital landscape changes daily. New software programs require additional security controls. Remote workers expand the attack surface. And hackers constantly develop new weapons.

Complacent organizations run the risk of exposing sensitive data and critical systems. This can result in reputational damage, profit losses and significant legal penalties. However, companies can solve the complacency problem with basic cybersecurity, comprehensive vulnerability testing and a solid understanding of the tools and regulations in play.

Implement Basic Cybersecurity Best Practices

Many security breaches are preventable. In those cases, revisiting basic cybersecurity can mean the difference between safety and disaster. For instance, an organization may have implemented automated backups. But if they neglect to store a copy of the backups offline and offsite, the backup data can become corrupted and worthless in a ransomware attack.

Likewise, organizations need to apply security patches quickly and keep systems up to date. They should also tighten access controls, ensure encryption of sensitive data both in transit and at rest and implement multi-factor authentication where possible.

Additionally, every cybersecurity strategy needs to include targeted, repeated cybersecurity awareness training. Officials from CISA warn that educating employees about phishing campaigns ranks near the top of the list of critical cybersecurity measures.

Uncover Vulnerabilities with an Outside Security Evaluation

Organizations that want to invest their security budget wisely will hire an outside consultant to conduct a cybersecurity evaluation. This often involves penetration testing, during which the consultant simulates cyber-attacks to uncover vulnerabilities.

A consultant will also discuss current policies, procedures, and security controls. And they will look at the office environment and the company's internet presence from the perspective of a bad actor. For instance, could a hacker gather enough information from social media to launch a successful spear-phishing campaign? Do employees leave sensitive information easily visible?

Know Your Tools and Applicable Regulations

Too many companies hand their IT function over to an isolated team or a third party and then forget them. As long as the computers work and they can accomplish their work, they assume all is well.

However, effective cybersecurity requires more than a break fix approach. And if a breach occurs, customers and regulatory agencies will look to the company leadership, not the MSP, to answer.

Consequently, even companies that use an MSP for their cybersecurity need to adopt a security mindset throughout the organization. They need to be aware of the tools in use and the security measures employed. They also need to keep abreast of privacy regulations to ensure compliance.

Start Now to Overcome Complacency in Cybersecurity

Cybersecurity can seem daunting, particularly for SMBs. But even small steps away from complacency in cybersecurity make a difference. Start with a security risk assessment to identify vulnerabilities and build a security strategy tailored to your specific environment and needs. There is no one-size-fits-all approach when protecting digital assets.

The cybersecurity experts at eMazzanti can help. We will conduct a risk assessment and guide you through implementing security measures designed specifically for your environment. For instance, we can help you implement remote workforce security. And we can provide 24/7 monitoring for regulatory compliance and network anomalies.