Minimize the Cost of Small Business Data Breaches with Proactive Security

Last year, Marriott, Facebook, Capitol One and the Russian government all made headline news with devastating data breaches. However, between 43 and 60 percent of all cyber-attacks in 2019 actually targeted small to medium businesses (SMBs). And the cost of small business data breaches goes far beyond the immediate damages.

Small businesses make an attractive target for cyber criminals for two reasons. First, SMBs often lack sufficient security, leaving them vulnerable to attack. Second, criminals see small businesses as a back door to the more lucrative large enterprises. Think of the Target attack several years ago, in which hackers gained access to the retailer through a refrigeration vendor.

State of SMB Cyber Security

Over half of SMBs endured data breaches in 2019. For many of these businesses, lack of security personnel and insufficient budget topped the list of security obstacles. Small businesses struggle to attract and retain security professionals with the necessary training and experience. And security solutions require significant investment of resources already stretched thin.

But despite limited resources, small businesses face the same threats as larger organizations. Phishing and web-based attacks continue to rise. An increasingly mobile workforce means that mobile devices and laptops open hundreds of avenues for attack. And regulatory compliance further increases the security burden.

Cost of Data Breaches for Small Businesses Extends Beyond the Budget

A recent study by data security research firm Ponemon estimates that the average data breach costs small businesses $3,533 per employee. Contrast this with an estimated $204 per employee cost for large enterprises. Security incidents place a disproportionate burden on smaller businesses.

However, the true cost of data breaches for small businesses includes far more than ransomware paid or remediation costs. The true costs lie in disruption of normal operations and loss of consumer trust. In fact, a 2019 study by Ping Identity showed that 81 percent of respondents would stop buying a brand online in the wake of a data breach.

While large enterprises can recover from temporary loss of business, for many small businesses, the setbacks prove too much. It can take months to recover from a data breach, and in that time many SMBs find themselves faced with business closure.

These costs affect individuals, in addition to organizations. When businesses close their doors, employees lose jobs. And customers not only suffer the compromise of their personal information but also the loss of services they depend on.

SMB Security Tips

By taking a proactive approach to security, organizations can mitigate the potential cost of data breaches for small businesses. Start with these cyber security steps.

- **Create and enforce password policies** – Nearly half of SMBs have suffered password-related cyber-attacks. Educate your employees on password guidelines and automate policy enforcement wherever possible. Additionally, increase security with multi-factor authentication.

- **Know your vendors** – Third party vendors significantly increase the risk of data breach. Maintain a comprehensive inventory of all third parties with access to confidential or sensitive information. Ensure that vendor contracts address evolving cyber security threats.

- **Control and monitor data access** – Today's document management systems include flexible security features. For instance, take advantage of features that allow you to restrict access to folders and documents according to job function.
- **Prioritize cyber security training and communication** – According to a recent IBM report, nearly one quarter of data breaches result from simple human error. Provide regular, up-to-date security training for all employees, as well as top-down communication about emerging threats.

Partner with Security Experts

At eMazzanti, we keep up to date on security technology and best practices so that you can focus on your core business. We will help you design and implement a cyber security strategy specifically targeted to your business needs and budget.