AssuredPartners
COLORADO

6 Ways SMBs Can Create an Effective Cybersecurity Strategy

(Source from PropertyCasualty360, "6 Ways SMBs Can Create an Effective Cybersecurity Strategy" by Michael Fitzgibbon)

A West Coast real estate developer, a New England confectionery and an East Coast construction firm all have something in common: They each lost as much as $1 million to cybercriminals who employed an arsenal of sophisticated weapons.

As hackers recognize that good things come in small packages, and as large enterprises improve their information security, these thieves are increasingly targeting small- and medium-sized businesses (SMB).

Limited resources, budgets and staffing make these businesses easy targets for cybercriminals, who also manage to find their way around security roadblocks, requiring every business to constantly be alert.

SMBs face life-threatening reputational, financial and operational risks should a breach occur, now is a crucial time for them to concentrate on creating an effective cybersecurity strategy that maximizes their protection and minimizes their risk.

Consider these alarming statistics:

- Forty-three percent of cyberattacks target small businesses;
- Only 14% of small businesses consider their cyber defenses to be highly effective;
- The average SMB data breach costs $86,500 in recovery costs; and
- Sixty percent of small companies fail within six months of a breach.

The real impact of data thefts

Several different scenarios can open the door to data theft. Its impact usually extends well beyond the business itself to customers, partners and others. For SMBs, the top security concerns are:

- Targeted phishing attacks against employees or vendors;
- Identity theft;
- Financial access;
- Advanced persistent threats;
- Ransomware;
- Denial-of-service attacks; and
- The proliferation of employees permitted to use their own mobile devices.

In the case of the real estate developer, for example, a hacked email account between him and his bookkeeper triggered that theft. At the confectionery, a data breach led to stolen customer information. At the construction firm, malware installed on the company's system led to online cash transfers from its bank accounts to the crooks.

So, how can SMBs defend themselves against what information security experts consider the increasingly inevitable cybertheft? While no one magic bullet exists, SMBs can take these six steps to become more security-conscious and prepared.

Assess Your Vulnerability to a Cyberattack

Retain a firm that specializes in cybersecurity and knows how to spot network, infrastructure and other related exposures. While almost all SMBs have an information technology professional or several onboard, they don't necessarily understand how to conduct a true security audit and deal with the weaknesses identified. Your insurer or other SMBs can usually help identify local cybersecurity professionals. Comparison shop to help you make your decision. Check their expertise and experience, consult their references about customer experiences and check the difference among candidates. The audit should examine entry points into your system – workstations, communications and mobile devices, the internet and cameras – and assess the threat of a breach from emails, passwords, client lists, data logs and backups, among others. Be sure to judge the vulnerability you give to customers and vendors.

Identify and Protect Sensitive Personal Information

Find out where sensitive personal information is stored and how it is used and sent. Determine all the risks that could lead to a breach of confidential files and sensitive information. This should include the SMB's banking, financial and other personal data, as well as the invaluable private information about employees, customers, vendors and others within your system. Develop data protection policies that apply to all servers, networks and endpoints. Review and update them regularly and conduct regular tests and audits to ensure security controls are performing as intended.

Establish a Secure Backup System

You never know when you may have to restore a part of the network or infrastructure, so a proper backup system must be as secure as your principle defenses. An enterprise-level cloud system can prove a good, secure standby. But it must deliver protections in particular for its platform, the data it processes, access control, authentication and encryption.

Use Security Safeguards that Mitigate Risks

Reduce the transfer of sensitive data by banning or severely limiting its shift from one device to another external device. This can include restricting the download of private and personal information from those devices cybercriminals often favor; defining and limiting who has access to sensitive data; and forbidding any unencrypted device as they are susceptible to attack. Set strong password requirements that ensure hard-to-crack passwords and change them from time to time. Two-factor authentication helps mitigate risk since an attacker must get past more than a password. When disposing of data storage equipment, including computers, delete all the files and folders so that information can't be retrieved.

Provide Security Training

Require employees to take privacy and security training that includes the threat of cyberattacks. Provide such training to others, including clients and those responsible for data-related activities. It is vital that employees especially understand the importance of data privacy and security and the costly consequences of a data breach. Security training is increasingly critical because personal data privacy laws in Europe and elsewhere apply to SMBs everywhere who collect personal data about customers and clients. Security training courses and tutorials are available online or through third parties and employees should be required to take and pass them. They should include the common causes of data breaches, including phishing attacks and malware, and how to spot them. The training modules should be available on an SMB's intranet and HR should remind employees frequently about any new or updated tutorials. In addition, the CEO should communicate the importance of cybersecurity training and their commitment to providing it. It is recommended to update training annually.

Consider Obtaining Cyber Insurance

It has been available for several years but still is emerging as companies, including SMBs, recognize cyberattacks are growing commonplace. Also, large enterprises are increasingly mandating cyber insurance for small business. Nearly 30% of SMBs bought such insurance in April 2017 for contract compliance reasons, by one estimate. SMBs can contact their insurance broker to find out the options available for cyber insurance. A cyber insurance policy can include up to a dozen coverage agreements, but not all apply to each business. Your broker will work with you to get comparative proposals from insurers, explain the pros and cons of each one, and make a professional recommendation to you. With data breaches making daily headlines and security fears rising about a possible contagious global malware, or so-called Bashe attack, more SMBs recognize the necessity of a secure and protected data network and system. They especially grasp that a serious cyberattack could ruin their reputation, revenues and very reality.