Small Business Insights

Cybersecurity Best Practices

Provided by: Wheeler & Taylor Insurance

Cybersecurity Best Practices

Cyberattacks are becoming more frequent and complex, and businesses of all sizes and industries are potential targets. In fact, cybercriminals increasingly go after small businesses since they contain much of the same types of sensitive information as larger enterprises but often have weaker cybersecurity defenses. Verizon's Data Breach Investigations Report found that 43% of all cyberattacks target small businesses, and 60% of those victims go out of business within six months of the attack.

Even if a small business survives a cyberattack, there can still be devastating consequences, such as high costs, reputational damage and unanticipated downtime. To best combat these risks, it is important for small business owners to be aware of common cyberthreats they may face, including:

- **Phishing**—Phishing is a type of cyberattack that utilizes deceptive emails or other electronic communication to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. While emails are the most common delivery method for phishing attempts, cybercriminals may also use text messages, social media messages, fake or misleading websites, voicemails or even live

A Small Business Administration survey found that 88% of small business owners feel their business is vulnerable to a cyberattack.

WT | Celebrating 150 Years SINCE 1871

phone calls.

- **Business email compromise (BEC)** — A BEC scam entails a cybercriminal impersonating a seemingly legitimate source—such as a senior-level employee, supplier, vendor, business partner or other organization—via email. The cybercriminal uses these emails to gain the trust of their target, thus tricking the victim into believing they are communicating with a genuine sender. From there, the cybercriminal convinces their target to wire money, share sensitive information (e.g., customer and employee data, proprietary knowledge or trade secrets) or engage in other compromising activities.

- **Malware**—Malware is a general term that describes viruses, worms, Trojan horses, spyware, adware, rootkits and other unwanted software or programs. Once a malware program has gained access to a device, it can disrupt normal computing operations, collect information and control system resources.

- **Insider threats**—Workers with access to sensitive information, including contractors who have access to the company's network, may be aware of existing security weaknesses and can exploit them more easily than an outsider.

- **Password attacks**—Using weak or easily guessed passwords or using the same password for multiple accounts can result in compromised data. In fact, over 70% of employees working at small businesses have had their passwords stolen or compromised, according to data from the Ponemon Institute.

To limit the risk of cyberattacks, small business owners should implement the following cybersecurity best practices:

- **Employee education**—Employees are the most significant cybersecurity vulnerability to any organization, including small businesses. Workforce cybersecurity education is essential to teach employees to identify phishing attacks, social engineering and other cyberthreats.

- **Security software**—A network firewall can prevent unauthorized users from accessing company websites, email servers and other sources of information accessed through the internet. In addition, high-quality antivirus software can perform automatic device scans to detect and remove malicious software and provide protection from various online threats and security breaches. The latest patches and updates should be installed as soon as possible to limit cybercriminals' opportunity to exploit any network vulnerabilities.

- **Multifactor authentication (MFA)**—Important accounts, including email, social media and banking apps, should require MFA to limit the opportunity for cybercriminals to steal data.

- **Data backups**—Essential files should be backed up in a separate location, such as on an external hard drive or in the cloud.

As cyberthreats become more frequent and severe, small businesses should take protective measures to secure all company, personal and financial information. For more small business insights and risk management guidance, contact us today.