Tips to Weed Out Cyber Risks

Every week, a new, major cyberattack makes headlines. Government offices, healthcare companies, manufacturers, financial services and public utility providers are just a few examples of the common industries targeted by digital criminals. Unfortunately, due to technological advances, these assaults are easier and more efficient for malicious actors to execute; it's not a matter of *if* your small business will be targeted, but *when*.

According to Verizon's 2025 Data Breach Investigations Report, small- to medium-sized businesses are being targeted nearly four times more than large organizations. This is partly because smaller companies are less likely to have sophisticated data protection or dedicated IT teams to detect breaches early, making them easier targets. Learn how to mitigate your risks by familiarizing yourself with common attack patterns, steps you can take as a small business owner and how Cyber Liability Insurance can help you protect your business, finances and essential customer data.

Understanding Cyberthreats

Most cybercriminals target businesses to gain access to sensitive information, such as client data, banking credentials, financial records and more; however, the methods they use to conduct these crimes can vary. Therefore, maintaining awareness of these efforts and their hallmarks can help you avoid falling victim to their schemes.

Cyberthreats can include:

- **Data breaches –** A data breach, also known as data leakage, is the unauthorized and unlawful exposure, disclosure or loss of personal information that compromises the security, confidentiality or integrity of personal information. This information can include common client billing details, such as Social Security numbers, driver's license information and financial credentials, including account numbers, credit or debit card information, PINs and access codes. These breaches can result from malicious attacks, accidental disclosures or flaws in a digital security system. Depending on the size of the breach, you can be subject to financial penalties following regulatory action, an eroded professional reputation and lost clients.

- **Malware –** This type of malicious software is among the most common forms of cyberattacks. Examples include ransomware, a disruptive attack where data is forcibly encrypted and only unlocked after payment; spyware, illicit software that infects a computer to collect information and activity data without your consent and scareware, which pushes falsified pop-ups and a sense of urgency to encourage victims to download virus-laden and fake antivirus software. All of these attacks can result in stolen customer data, financial losses and operational disruptions.
- **Social engineering attacks –** Have you ever questioned whether the person on the other end of an email chain or phone call is truly who they claim to be? If this sounds familiar, you might have encountered an impersonation-driven cyberattack. Business email compromise (BEC) is one effort where thieves pretend to be a person you or your clients trust, such as a business partner or vendor, to trick the target into making payments or sharing sensitive data. Pretexting is a similar scam in which a false scenario is presented to gain the victim's trust and obtain illegal access to their financial information.
- **Spoofing –** Another effort that exploits human trust, spoofing is a technique where cybercriminals impersonate legitimate websites or email addresses to deceive the recipient into trusting them. These efforts can range from simplistic to complex, so be on the lookout for signs, including pixelated or fuzzy images, misspellings and formatting errors. Never click a link or download an attachment unless you are certain of its veracity. Doing so can make your systems vulnerable to malicious programs.

Protecting Your Businesses

Much like weeding invasive plants out of your clients' yards, safeguarding your business against bad actors and cyberthreats requires commitment and attention. Improperly accounting for your risks and assuming you'll be safe simply because of the size of your business or the industry you're in will result in significant financial and reputational harm. Here's how you can help reduce your likelihood of a successful cyberattack and secure valuable confidence should the worst come to pass:

Get Smart About Your Cyber Safety

The easiest target is the one that doesn't take its cybersecurity seriously. As illustrated by the Verizon report, your small size doesn't mean you won't become the target of a cyberattack — most criminals are merely seeking opportunity and visible vulnerabilities. Help protect your business by:

- Training all employees in basic cybersecurity principles and policies, such as requiring strong passwords and prohibiting the use of risky websites.
- Using up-to-date security software and operating systems, including maintaining encrypted, private Wi-Fi.
- Keeping tight control over who can access computers, business software and databases.
- Maintaining separate devices for point-of-sale and billing systems versus general web browsing.
- Reviewing and implementing best practices from experts, such as the Federal Communications Commission (FCC) and the U.S. Small Business Administration (SBA).

Update Your Insurance Portfolio

Small business owners typically carry a range of insurance policies to help protect their business and finances. Commercial auto, equipment coverage and property insurance are just a few examples of the coverages you rely on to protect your business against the cost of damages to company-owned vehicles, supplies and heavy equipment.

Adding a Cyber Liability Insurance policy to your portfolio helps ensure your business is poised to respond to the many challenges that come its way. This coverage provides valuable peace of mind by addressing the significant expenses incurred after cybercrimes, such as hiring forensic IT experts to identify the cause of the attack, contracting professionals to repair your systems, notifying affected clients and recouping any loss of business or income you may experience.

Additionally, a comprehensive cyber policy can assist if you are taken to court over the breach, covering defense costs or settlement amounts. It can also help if you're exposed to any regulatory fines or penalties stemming from your business's actions — or lack thereof if you're found to have a subpar cybersecurity plan — leading to the event.

You don't have to take on your cybersecurity journey alone. If you need assistance understanding your risk or finding coverage that fits your unique needs, contact Ashley Thomas of Gallagher Affinity at 918.764.1619 or ashley_thomas@ajg.com for a free risk analysis and coverage review. Learn more about available coverage at gallagheraffinity.com/MNLA.