# Medium and Small Businesses are a Big Target for Cyber Attacks

October is “National Cyber Security Awareness Month.” How can anyone not be aware of cyber security? Reports of large-scale data breaches, hacking and cyberattacks appear in the media almost daily. The recent Equifax breach alone has exposed sensitive personal information of over 143 million Americans. Phishing and ransomware attacks are also on the rise. Phishing attacks are used to steal user data, such as bank account or social security numbers, or log-in credentials. In a ransomware attack, the attacker encrypts a company’s data and makes it unavailable to the company until a “ransom” of some amount is paid.

One common misconception is that these cyber-attacks only happen to large companies. In reality, attackers also frequently target medium and small businesses, but you are less likely to hear about them on the news. A recent study by the security firm Symantec reports that 31 percent of all breaches occur at organizations with 100 or fewer employees, and that 61 percent of all breaches occur at organizations with 250 or fewer employees. Microsoft Corporation has also stated that 20 percent of small to medium businesses already have been targets of cyber-attacks. In 2015, 43 percent of all phishing attacks targeted small businesses. These statistics demonstrate that smaller businesses particularly are at risk.

Other common misconceptions are that “our type of business is not at risk,” and “we don’t possess sensitive information.” However, the facts show that every business in every industry is at risk. In addition, every business possesses some sensitive information that criminals can use, even if it is the personal and health information of its employees, or customer and vendor payment and contact information.

A fourth misconception is that the business can absorb the cost of a data breach. This could be a very costly mistake. A June 2017 report from the Ponemon Institute finds that the average cost for each lost or stolen record containing sensitive information is $225, that the average total cost of a data breach is $7.35 million, and that the average number of records involved in a data breach is 28,512. Few businesses can absorb such costs without crippling adverse effects.
What should businesses be doing to minimize the risk of losses from cyberattacks? The exact details will vary from business to business, but here are some steps that all businesses should take:

- Undertake a security risk assessment. Businesses need to determine what sensitive and personal information of others they possess, as well as what information is most valuable to the business. In addition, the business needs to understand its assets and operations, and potential vulnerabilities.
- Develop and implement a security program to address the risks. Based on the risk assessment, the business should adopt a program appropriate for its industry, the types of information and assets involved, and the specific risks it faces. Typically this involves a written plan, which would address physical security measures (such as fences, locks, alarms and guards), administrative security measures (such as policies regarding operating procedures, administrative controls, and employee training), and technological security measures (such as firewalls, controlling access to sensitive information, passwords, encryption, and the like).
- Evaluate the risk from third parties. Increasingly, the vendor chain is becoming a security risk, as trusted vendors often have access or connections to a business’s information systems. Businesses need to assess and monitor the security practices of their vendors, as an attack on an insecure vendor could also disrupt the business.
- Develop and practice a written incident response plan. The plan should include who is to be notified in the event of a security incident (including legal counsel), the actions and escalation steps to be taken to identify and resolve the issue, and how the business will comply with applicable federal and state laws if it turns out that there has been a security breach.
- Investigate cyber liability insurance. Given the high costs of a security breach or ransomware attack, a

business should also investigate the types and costs of available insurance coverage.  Ideally, a policy should include first party coverage (for losses to the business due to loss of data or business interruption), and well as third party coverage (for costs and expenses and liability due to a data breach).  Crime coverage is also important to address phishing scams and attacks that take over a corporate account.

Unfortunately, defending against cyberattacks has become a cost of doing business for all businesses, not just large companies.  All companies need to take steps to mitigate their risks or face potentially crippling exposure if a cyberattack does occur.

Click here to read the version of this article that appeared in Providence Business News.

**Date Created**
October 13, 2017