Hackers are Getting Savvier and Sneakier – Are You Ready?

It’s not IF, it’s WHEN.

Cyber breaches and ID theft scenarios have gone beyond stealing a credit card number and shopping away on Amazon. As retail operations tighten security, studies show a drop in point of sale cyber breaches. That doesn’t mean there is a reduction in cyber theft, it just means the hackers are smarter and have moved on to easier and more lucrative venues.

Criminals quickly learned that if they embed themselves deep within a company’s “digital system” they have access to a wealth of monetizable data within those networks. Hackers want in, and they are getting there – typically through your employees.

There is a huge misconception that only large publically owned companies are targets, when in fact smaller businesses are hot on the radar of most hackers. Why? On average, smaller businesses do not have the security measures in place nor are they as diligent with training staff on security protocols when they are in place.

So where are the weaknesses in smaller businesses?

According to the Ponemon Institute, the most prevalent attacks against smaller businesses are **web-based and phishing/social engineering**. Some of these are innocent, but negligent employees or contractors and third parties caused the most data breaches.

- **Social Engineering Fraud** is perhaps one of the scariest and savviest forms of cyber attacks as it involves your employees. The definition according to Interpol is “Social engineering fraud is a broad term that refers to the scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and funds.” Criminals exploit a person’s trust in order to find out their banking details, passwords or other personal data. Scams are carried out online – for example, by email or through social networking sites – by telephone, or even in person.

- **Password breaches**. This may seem like a shock to most, but the majority of business owners do not enforce OR monitor their employees' password security protocols. Add in mobile devices that do not have biometric security (access via thumbprint/fingerprint recognition) and the rate of hacking jumps dramatically. Business owners need to not only train staff on what makes a secure password, but have processes in place to ensure the staff is adhering to the rules. Surprisingly many people still use birthdates and yes, they still use 123456.
- **Click happy employees.** Hackers have reached new heights of phishing savviness as they clone emails to replicated big and often used brands such as DropBox, Amazon, Bank of America, Capital One and more. It's up to business owners to not only train employees on how to detect a phishing email, but reviewing the email from which it was sent, to black listing and blocking repeat offenders from getting to employee inboxes. Without fail, all business will have some type of breach or malware attack from an employee clicking on something they shouldn't.

We've seen too many of our clients experience cyber breaches, web based attacks, stolen records and as a result dollars out the door. It is no longer an option to assume hackers won't focus on the local business. It's becoming easier and easier for them to infiltrate networks via employee or third party assistance.

Are you vulnerable? The answer is yes. Even with the best security measures in place, a breach will happen on some level. We often find most companies are grossly underinsured or uninsured when it comes to cyber coverage. Remember it's not IF it's WHEN.

The solution?

The first step is strong security protocols, processes, procedures AND training your staff. The next step is having a solid risk management program including business interruption guidelines and cyber insurance including a social engineering fraud endorsement.