Does Your Business Need Cyber Risk Check Up?

Did you know that 55% of small businesses have experienced a data breach, and 53% have suffered multiple data breaches? New York state suffered the second most data breaches in the country. Between 2006 and 2013, the amount of data breaches in New York or affecting New York tripled. With the number of businesses and corporations suffering from hacks and data breaches on the rise, it may be time for your business to get a cyber risk check up.

Is It Time For a Cyber Risk Check-up?

Here are a few questions to consider about the cyber health of your business/company:

1. How often do you train your employees on Phishing, Security Awareness, etc.?
2. Does your business/company have an incident response plan?
3. Do you have email filters for your employees?
4. Does your software ensure that passwords are high quality?
5. Do you have a 24/7 security operations center?
6. Does your business/company perform vulnerability assessments frequently?
7. Are your cyber risks reviewed by the top leadership of your company?
8. Does your company/business have someone assigned to the oversight of cybersecurity?
9. How often does your business/company conduct phishing tests?
10. Does your business/company have cyber insurance?

If you answered “no” or “never” to any of these questions, it may be time for your business to look at your cyber risk, and implement some new policies.

More Common Than You Think

Don't think you're vulnerable? Here are just a few of the many recent cyber breaches/attacks:

- On May 29th, a nonprofit organization based in New York State, People Inc., stated that they learned of a data security incident that involved protected health information belonging to some current and former clients. This data breach compromised many employee email accounts.
- *The Canadian Press* revealed that in March 2019, Natural Health Services, a medical cannabis clinic, suffered a data breach involving the personal health information of about 34,000 medical marijuana patients.
- In 2014, Ameriforge Group Inc. was the victim of CEO phishing attack that cost them close to half-a-million dollars. The company's accountant received an email from someone pretending to be their CEO. They instructed the accountant to work with a lawyer from another company on a highly sensitive matter. This matter "required" the accountant to wire $480,000 to a bank account in China. By the time the accountant realized something was not right, the money and the scammers were gone without a trace.
- Volunteer Voyages, a single-owner of a small business lost over $14,000 due to a stolen debit card. The company leads humanitarian volunteer trips abroad, and after returning from a trip to Peru, the owner was surprised to find his account overdrawn. Someone had stolen the company's card number and emptied the account. Despite notifying his bank of the trip abroad, the bank refused to reimburse him.

How To Keep Your Company Safe

Did you know that in 2017, cyber attacks cost small and medium sized businesses an average of $2.3 million?

One way to protect your business is by implementing employee cyber security awareness training. Cyber security awareness training can be offered face to face or online, and periodic testing should be performed to determine the success of the training or to identify areas to focus on in future training.

Protect information sent by email by using email signing certificates. Email signing certificates enable executives and other employees to digitally "sign" their emails so their recipients can easily verify that they are who they say they are. These certificates are issued by industry-trusted certificate authorities (CA). By making email signing certificates mandatory, it is easier to verify the identity of the email sender.

Look into cyber insurance. Without cyber insurance, recovering from a cyber attack or breach can be incredibly difficult. There is no singular definition of “cyber insurance” since cyber policies can include everything from identity theft to cyber extortion, data breach, cloud data breach and credit card fraud (all which can happen due to phishing attacks). In general, cyber insurance covers your business for risks relating to information technology infrastructure and activities, and from data breaches involving sensitive customer and employee information such as Social Security numbers, credit card numbers, account numbers, driver’s license numbers and health records.

Cyber Insurance

Which businesses need cyber insurance? Pretty much all of them - if you have an online form fill, conduct credit card transactions, handle medical information, or store customer data digitally, you’re at risk. Many small businesses assume they’re too small to be noticed by cyber predators and don’t need insurance, but the truth is, you’re an inviting target. Cybercriminals are drawn to small businesses since they are less likely to have a strong defense against hackers, and are more likely to store customer information, and conduct business online.

Lastly, a data breach can damage more than just your systems, it can damage your brand and your reputation while putting your customers and/or employees at risk. Bottom line: cyber insurance is a smart precaution for any size business.

When was the last time your business had a cyber risk check up?