est. 1914 BLOCK INSURANCE

HOW WELL DO YOU KNOW YOUR BUSINESS' CYBER EXPOSURES?

1. Does your business retain physical or electronic records of employees or other third parties with any of the following?

a. Social security numbers ____
b. Drivers' license numbers ____
c. Tax identification numbers ____
d. Birth dates ____
e. Medical/health records _____
f. Court records ____
g. Banking information (checking/savings accounts) ____
h. Email address or home addresses ____

FACT: If you checked any of the above, your organization is in control of "Personally Identifiable Information," and therefore, required to protect that data subject to State and Federal privacy and data breach notifaction laws.

2. Does your business have employees? If so, how many? ○ **Yes** How Many? ____ ○ **No**

FACT: Most data breaches involve an employee mistake. They can lose a mobile device, laptop or paper records, or make costly errors such as opening an unauthorized email containing malware. In addition, they can even intentionally steal data.

3. Does your business have an active website? ○ **Yes** ○ **No**

FACT: Material posted electronically, or in written format, may lead to copyright or trademark infringement, or defamation litigation. If the website is transactional, additional exposures include possible hacking or disruption of your business via denial or service attacks.

4. Does your business use third-party vendors (e.g., cloud, IT services?) ○ **Yes** ○ **No**

FACT: Businesses in possession of personally identifiable information may be held liable for privacy breaches caused by their vendors or other third parties. As the owner of the data, your business is ultimately responsible for protecting it.

5. Does your business use mobile technology (e.g., smartphones, tablets, laptops) ○ **Yes** ○ **No**

FACT: Loss of mobile devices and the electronic content contained therein is one of the leading causes of data breaches.

6. Does your business accept credit card payments, other electronic payments or online bill pay? ○ **Yes** ○ **No**

FACT: Over 25% of all data stolen is credit card and other payment information. This is a category of data that is highly desired by criminals for resale on the black market.

7. Does your business allow employees to use personal devices to connect to your network? ○ **Yes** ○ **No**

FACT: Personal devices may not have the same security software and other connectivity procedures as the company provided devices. As a result, when these personal devices are connected to your network, there may be a higher exposure to a virus or malware threat.

8. Does your business train employees on proper email use and other privacy issues? ○ **Yes** ○ **No**

FACT: Employee negligence and/or errors are one of the top three contributors of lost or stolen data.

9. Does your business store your customers' corporate confidential information? ○ **Yes** ○ **No**

FACT: Companies face liability for failing to protect their customers' and business partners' confidential information.

10. Does your business have access to online cyber risk management tools? ○ **Yes** ○ **No**

FACT: When you place your cyber insurance through Block, you are getting more than just words on a paper. We offer all of our Acrisure Cyber policyholders, free of charge, a wide range of best-of-breed services aimed at improving security before crisis strikes.

11. What is your business' yearly revenue? $ _____

12. What is the single largest ($ amount) banking transaction made by your business in any given year? $_____

If you answered 'yes' to one or more of these questions, your business has exposures which could lead to cyber related claims. Can you afford to self-insure these exposures?

To learn more about Cyber Insurance, contact Andy Runyan.

870.219.1339
arunyan@blockinsurance.com
@ARunyanBlockIns

est. 1914 BLOCK INSURANCE