How well do you know your business' cyber exposures?

1. Does your business retain physical or electronic records of employees or other 3rd parties with any of the following?

Social Security Numbers	**Court records**
Drivers' License Info	**Police records**
Tax ID Numbers	**Banking information**
Birth Dates	**Email address**
Medical Records	**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 notification laws.

2. Does your business have employees?

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 intentionally steal data.

3. Does your business have an active website?

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 of service attacks.

4. Does your business use 3rd party vendors (e.g., cloud, IT services)?

FACT: Businesses in possession of personally identifiable information may be held liable for privacy breaches caused by their vendors or other 3rd parties. As the owner of the data, your business is ultimately responsible for protecting it.

5. Does your business accept credit card payments, other electronic payments or have online bill pay?

FACT: Almost 40% of all data stolen is credit card and other payment information according the "NetDiligence Cyber Claims Study 2014". This is a category of data that is highly desired by criminals for resale on the black market.

6. Does your business use mobile technology (e.g., smartphones, tablets, laptops)?

FACT: Loss of mobile devices and the electronic content contained therein is one of the leading causes of data breaches today according to "Ponemon 2015 Cost of Data Breach Study".

7. Does your business allow employees to use personal devices to connect to your network?
FACT: Personal devices may not have the same security software and other connectivity procedures as company-provided devices. As a results, when those personal devices are connected to your network, there may be a higher exposure to virus or malware threats.

8. Does your business train employees on proper email use and other privacy issues?
FACT: Employee negligence and/or errors are one of the top three contributors of lost/stolen data according to the "Ponemon 2015 Cost of Date Breach Study".

9. Does your business store your customers' corporate confidential information?
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?

If you answered "yes" to one or more of questions 1-9, your business has exposures which may lead to cyber-related claims and suits. Can you afford to self-insure these exposures? Here at **Joyce, Jackman & Bell**, we understand the complexity of cyber threats and have solutions to help protect your assets. Regardless of your business size or industry, we have a cyber insurance solution to for your needs. to learn more about our cyber capabilities, contact us.

Questions and FACTS provided by Travelers Insurance.

Joyce, Jackman & Bell
INSURORS
JJB...with you every step of the way.

9 N. Main St., Pittston, PA 18640 | P: 570.654.5505 | F: 570.654.8275 | www.jjbins.com