How well do you know your business' cyber exposures?

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

- ☐ Social Security Number
- ☐ Driver's License Information
- ☐ Tax identification numbers
- ☐ Birth dates
- ☐ Medical/health records
- ☐ Court records
- ☐ Police records
- ☐ Banking information (checking/savings accts.)
- ☐ Email addresses or home addresses

► 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.

Does your business have employees? Yes No
Fact: Most data breaches involve employee mistakes. They can lose a mobile device or paper records, or make costly errors such as opening an unauthorized email containing malware. Even theft of data occurs.

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 data via denial of service attacks.

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 today. [1]

Does your business accept credit card payments, other electronic payments or have online bill pay? Yes No
Fact: Almost 40% of all data stolen is credit card and other payment information. [2] This is a category of data that is highly desired by criminals for resale on the black market.

[1] Ponemon Institute 2015 Cost of Data Breach Study
[2] NetDiligence Cyber Claims Study 2014

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 result, when these personal devices are connected to your network, there may be a higher exposure to virus or malware threats.	Yes	No
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. [3]	Yes	No
Does your business store your customers' corporate confidential information? **Fact:** Companies face liability for failing to protect their customers' and business partners' confidential information.	Yes	No
Does your business have access to online cyber risk management tools? **Fact:** At V.F. McNeil Insurance, we have access to several insurance carriers who can provide information portals to help your business successfully prevent and respond to cyber events. Some items included are reference materials, news updates and other tools, as well as access to breach coaches for consultations if you have a data breach event.	Yes	No

If you answered yes to one or more of the questions above, your business has exposures which may lead to cyber-related crimes or law suits.

Can you afford to self-insure these exposures?

At V.F. McNeil, we understand the complexity of cyber threats and have solutions to help protect your business. Regardless of your business' size or industry, we can provide you with cyber insurance to fit your specific needs.

To learn more, contact V.F. McNeil Insurance today at (203) 481-2684. Don't leave your business to chance.

V.F. McNeil Insurance

This material is for informational purposes only. For an actual description of all coverages, terms and conditions, refer specifically to the insurance policy and/or contact your agent.

[3] Ponemon Institute 2015 Cost of Data Breach Study