How well do you know your business' privacy breach/cyber exposures?

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

1. Social security numbers
2. Drivers' license information
3. Tax identification numbers
4. Birth dates
5. Medical/health records
6. Court records
7. Police records
8. Banking information (checking/savings accounts)
9. Email addresses or home addresses

- FACT: If you retain 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.
- 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.
- 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.
- 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.
- FACT: Loss of mobile devices and the electronic content contained therein is one of the leading causes of data breaches today.
- FACT: Almost 40% 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.
- 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.
- FACT: Employee negligence and/or errors are one of the top three contributors of lost/stolen data.
- FACT: Large-scale global ransomware cyber-attacks small and medium-size businesses. Ransomware attacks in which malicious software blocks access to a computer system until a sum of money is paid are a looming threat. **RANSOMWARE is the latest tactic in an ongoing war between business and cyber criminals.**

Buckman-Mitchell, Inc. is pleased to provide our clients a comprehensive Privacy/Cyber Liability Insurance Program. Coverage highlights include:

- Both 1st and 3rd Party Coverage, Data Breach Expense, Network Security, Privacy Liability, Media Liability, Regulatory Fines & Penalties, Network Extortion, PCI Fines, Assessments or Charges, Business Interruption and Data Recovery
- Services offered before a breach takes place: a complete learning center and prevention toolkit. Training may include password security, how hackers get it, working remotely, human firewall, phishing social engineering, appropriate use, backups, insider threats, data protection destruction, staying secure online and WIFI security.

Contact your Buckman-Mitchell Insurance Agent for more information or a quote.