Serious about cybersecurity

How Ohio companies can protect themselves by protecting their data

INTERVIEWED BY ADAM BURROUGHS

CRAIG S. HORBUS
Partner, Corporate & Securities, Technology
Brouse McDowell LPA

(330) 434-7563
chorbus@brouse.com

WEBSITE: Learn more about Brouse McDowell and Craig Horbus by visiting www.brouse.com.

Ohio's Senate Bill 220, referred to as the Ohio Data Protection Act, is in effect. It was passed to incentivize companies to voluntarily adopt what's been determined to be an appropriate cybersecurity program. Its approach offers a legal defense mechanism against lawsuits in exchange for implementation of a written cybersecurity framework.

"If you follow the rules and you take reasonable precautions to prevent a data breach, you're afforded potentially monumental relief from a civil liability standpoint in the form of a first-of-its-kind affirmative defense," says Craig S. Horbus, partner, Corporate & Securities, Technology, at Brouse McDowell LPA.

Smart Business spoke with Horbus about the law and how it affects Ohio businesses.

What are reasonable precautions?

Companies are given latitude through the law to determine what are their appropriate cybersecurity framework and protections. This takes into consideration the size and complexity of the business, the sensitivity of the information it possesses and/or controls, the cost involved and its available resources to determine the best fit.

Reasonable precaution is the new standard, which as of yet has no judicial challenge to define it more particularly. However, there are existing standards such as guidelines set by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) as well as ISO/IEC-27001 information security management, HIPPA and other niche legal guidelines that can be applied based upon the type of company and level of legally necessary data security compliance. Many companies that create, maintain and comply with NIST-based security protocols should qualify as having met reasonable precautions.

Companies that are active in e-commerce or hold any type of personally identifiable information should understand this law and take proactive steps to comply with it.

What constitutes an Ohio business and how many of them are within the law's safe harbor of protection?

According to the statute, a covered entity is any business that accesses, maintains, communicates or processes personal information or restricted information in or through one or more systems, networks or services located in or outside of Ohio.

While the expectation is that major corporations are already in compliance, most small to midsize companies treat data security as an afterthought and are not up to minimum standards.

What could happen to businesses that become victims of a data breach and have not taken reasonable precautions?

Failure to take the minimum requirements called for in the bill leaves a company at serious risk. A breach can mean more than losing money through civil torts. The fallout from a breach means damages that could impact thousands of victims and irreparable damage to a company's reputation.

A data breach isn't easy to clean up. It's a problem that lasts for years. Stolen credit card information isn't the worst of it. Typically, those can be cancelled and charges reversed quickly. But hackers that take Social Security numbers and personally identifiable information will sit on that for years before attempting to use it, making it a problem that haunts a company for many years.

What is GDPR and how does it pertain to the new Ohio law?

General Data Protection Regulation (GDPR), which comes out of the European Union, went into effect in May 2018. It is focused not on the location of the company holding sensitive information, but on the location of the data. That has implications for organizations outside the EU that monitor, process or hold information that would be considered EU-based data. Many U.S.-based companies might be unaware that they're impacted by the law.

Although not listed specifically under the Ohio law, arguably GDPR would qualify as one of the frameworks Ohio's law seeks to encourage companies to comply with. Companies that are GDPR compliant, which is more far-reaching and provides a higher level of security compliance than many other laws and could become the benchmark, should be able to recognize it as their framework in order to achieve reasonable precautions under Ohio's law. ●