CLIENT ALERTS & INSIGHTS

Ohio Proposes Act to Incentivize Consumer Data Security

NOVEMBER 21, 2017

Authors: Michael D. Stovsky

The Proposed Act

Legislation was recently introduced in Ohio encouraging businesses to take steps in protecting consumer data. Ohio Senate Bill 220, The Data Protection Act (the "Act"), provides businesses that take certain commercially reasonable and industry standard data security measures, a safe harbor against legal claims upon a breach of consumer data. The Act does not set forth a minimum standard that needs to be met by businesses, but simply provides compliant businesses an affirmative defense against consumer claims that allege the failure to implement reasonable information security controls resulted in a data breach. The Act is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action.

The safe harbor/affirmative defense applies to business that implement a cybersecurity program that complies with the National Institute of Standards and Technology ("NIST") cybersecurity framework, or other industry recognized data security frameworks. The current bill sets forth the following industry standard, including certain industry specific, data security frameworks on which a business could base its data security program to be afforded safe harbor protection.

The eight frameworks include:

(1) NIST special publication 800-171;

(2) NIST special publications 800-53 and 800-53a;

(3) The federal risk and authorization management program;

(4) Center for internet security critical security controls; and

(5) International organization for standardization (ISO)/international electrotechnical commission 27000 family - information security management systems.

If the business is regulated by the state and the federal government, the following industry specific frameworks include:

(6) The security requirements of the "Health Insurance Portability and Accountability Act of 1996," as set forth in 45 CFR Part 164 Subpart C;

(7) Title V of the "Gramm-Leach-Bliley Act of 1999," Public Law 106-102, as amended; and

(8) The "Federal Information Security Modernization Act of 2014," Public Law 113-283.

The bill is currently pending committee assignment.

Recommendations

We recommend that each company immediately take steps to assess its collection of consumer data, and implement a comprehensive data security program and incident response plan to better protect itself in case of a security incident. The data security program should be modeled after one of the above referenced frameworks.

For further information, please contact Michael D. Stovsky, Partner, Benesch, Friedlander, Coplan & Aronoff LLP, 200 Public Square, Suite 2300, Cleveland, Ohio 44115, (216) 363-4626, or mstovsky@beneschlaw.com.