Long Island BusinessNEWS
AUGUST 9-15, 2019 | OUR 66TH YEAR | NO. 32 | $2.00 | LIBN.COM

Opinion: Beware – SHIELD law to overhaul cyber security reporting

By: Commentary, Steven J. Kuperschmid, Esq., Nicole E. Della Ragione, Esq.

Businesses and individuals must be prepared to change the way they treat cybersecurity. The New York SHIELD Act has been signed into law and will overhaul the breach reporting statute and require businesses and individuals to have proactive cybersecurity measures in place if they own or license data —meaning, this law will affect virtually every business in the state by March 21, 2020.

New York General Business Law §899-aa will be overhauled by the SHIELD Act. Under the previous version of law, a cybersecurity incident would only be reported to affected individuals if it affected a limited set of data. The SHIELD Act expands the types of "private information" that can trigger data breach notifications, and requires businesses and individuals to take certain prophylactic measures to protect the data they own or license. This article will highlight some of the major changes and compliance issues that businesses will face.

As an initial matter, the definition of "private information" has been expanded to include:

- Biometric information, including a fingerprint or retina image;
- Credit or debit card numbers without a security code, if the number could be used to access an individual's financial account; and
- User names or email addresses together with passwords or security questions and answers that could permit access to an online account.

Further, the data breach notification requirements have been expanded. Now, mere unauthorized access of information can require a business to notify New York residents in the most expedient time possible and without unreasonable day. The only exception to this new requirement being if a business can verify that the exposure was inadvertent and can reasonably determine that the unauthorized access "will not likely result in misuse of such information" or financial or emotional harm to the affected persons. By expanding the definition of private information and breaches required to be reported there will be an increase in data breach notifications required, which will result in increased legal and reputational exposure for businesses.

In addition to expanding the definition of "private information" and data breach reporting requirements, the SHIELD Act now requires every business to have reasonable administrative, technical and physical safeguards in place to protect the security, confidentially and integrity of private information. A few of the many requirements outlined in the statute are: (1) designating one or more employees to coordinate the security program; (2) training and managing employees in the security program practices and procedures; (3) selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract; (4) assessing the risks of information storage and disposal; (5) detecting, preventing, and responding to intrusions; (6) protecting against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information; (7) conducting regular testing; (8) assessing risks in network and software design; and (9) disposing of private information in a reasonable time.

If a business decides not to take the steps necessary to comply with this new law, the attorney general has been given expanded powers to bring civil actions against entities and increased penalties after a data breach. Notably, the law does not create a private right of action.

Businesses must move swiftly to comply with this new law. While March 21, 2020 may seem far away, there is a lot of work that needs to be done for many businesses to come into compliance. Businesses should begin by reviewing their administrative, technical and physical safeguards, and beginning to create a plan for compliance. By being prepared and having an organized approach, businesses can avoid unnecessary enforcement actions.