3 Steps to Help Manufacturers Comply with New York SHIELD Law

In July 2019, Governor Andrew Cuomo signed the Stop Hacks and Improve Electronic Data Security act (SHIELD) into law. This law affects any organization that holds private information for New York state residents. A greater understanding of key components of the New York SHIELD law will ease regulatory compliance for manufacturers and other businesses.

In summary, SHIELD expands data breach notification requirements and mandates that organizations create or update a data security program. To meet these requirements, manufacturers must address risk, review vendor compliance, and ensure proper notification in the event data becomes compromised.

1. Comply with Expanded Data Breach Notification Requirements

The strict breach notification requirements of New York's SHIELD law have already taken effect. To comply, organizations must understand how the law broadens the definitions of both "private information" and "data breach."

- **Private information** – Under old law, private information included the individual's name, in conjunction with a Social Security number or driver's license number. Additionally, it could include the name in combination with a credit/debit card number and access information such as a security code.

  The new law expands that definition to also include credit/debit card numbers and account numbers without additional information, if the number alone could be used to access an account. Further, the law covers biometric information and any combination of credentials a hacker could use to access an online account.

- **Data breach** – Previously, data breach involved unlawful *acquisition* of private information by unauthorized parties. However, SHIELD expands that definition to include unlawful *access*. For example, if an outside party simply views data without authorization, that constitutes a breach.

In the event of a breach, organizations must immediately notify the New York residents whose personal information was compromised. They must also notify the New York state attorney general and the state police.

2. Implement a Data Security Program

Organizations have until March 2020 to comply with SHIELD's data security program requirements. The law requires that organizations deploy reasonable security measures in terms of administrative, technical and physical safeguards. Some examples of these safeguards include the following:

- **Security program coordinator** – The organization must designate a data security officer to coordinate security efforts.
- **Risk assessments** – The organization must conduct assessments to determine any foreseeable risks to data. For example, this could include risks in data transmission or storage, as well as improper disposal of information.
- **Deployment of controls to address risk** – This could include proper network design, as well as threat detection and response measures. Additionally, it includes tools for ongoing security monitoring to ensure the efficacy of these controls.
- **Security training for employees** – Organizations must ensure that employees receive adequate training to follow security guidelines.
- **Data retention policies** – Review or create a data retention policy for the organization as part of an overarching information governance program. Be sure to reflect any applicable industrial regulations that apply to disposal of information.

These requirements can seem overwhelming for small manufacturers. However, the regulations do include some concessions for small businesses. New York's SHIELD law defines small businesses as those with less than 50 employees, less than $3 million in gross annual revenue or less than $5 million in total assets.

3. Review Vendor Contracts

In addition to implementing their own security programs, organizations must also assess any risk involved with third parties. For instance, many organizations outsource some storage and processing of private information to vendors. In that case, they must review and update vendor contracts to ensure that vendors also provide appropriate safeguards.

Delays in Complying with New York SHIELD Law Can Cost You

Although addressing SHIELD regulations requires an investment of time and budget, the penalties for non-compliance can prove even more costly. Violations can result in fines of up to twenty dollars per failed notification, capped at $250,000. And violations of the data security program regulations can cost up to $5,000 per single violation, with no cap.

The consultants at eMazzanti can help you build a comprehensive cyber-security program to ensure regulatory compliance. With deep experience in manufacturing data security and information governance, we will guide you through the maze of the New York SHIELD law. From risk assessment to security controls and data retention policies, we have you covered.