Business Journal News Network
CNY's only source for business news, research, and events

Breaking Down the New York SHIELD Act

MICHAEL MONTAGLIANO
Viewpoint

New York's new Stop Hacks and Improve Electronic Data Security (SHIELD) Act is broadening the state's security breach notification requirements (899-AA) and requiring businesses to implement reasonable administrative, technical, and physical safeguards for New York residents' private information (899-BB). Signed by Gov. Andrew Cuomo on July 26, 2019, SHIELD's breach-notification requirements took effect in October of this year, with safeguard requirements due by March 2020.

Why the SHIELD Act is needed

The updated breach-notification law was designed to "keep pace with current technology." And if we look at technology's current state, that's easily understood.

Organizations have seen a digital transformation over the past few years as workloads move from on-premise to multiple cloud services, including software (SaaS), platform (PaaS), and infrastructure (IaaS). Data is being transferred and dispersed — and the attack surface broadened — making information containment and control much more challenging.

The threat landscape has changed dramatically. Hackers are taking advantage of advanced technologies — such as artificial intelligence, machine learning, and data analytics — to build new capabilities, including shapeshifter malware with the ability to analyze network defenses and modify malicious code on the fly to circumvent those defenses.

Cybercrime economics statistics are staggering, with $6 trillion in annual global losses expected by 2021. For New York State, the cost of a lost record is $148, up 4.8 percent from 2018, and the average recovery cost from a breach stands at $3.86 million.

So, the need for the new SHIELD Act is evident in the numbers.

When the SHIELD Act applies

The SHIELD Act applies to any person or business that owns or licenses computerized data that includes a New York resident's private information. And not just those that conduct business within New York state.

The law applies to both regulated and unregulated companies, but "without imposing duplicate obligations on those already subject to other federal or New York State data security regulations." That means if a person or company (the Department of Financial Services, for example) is already regulated by existing New York or federal data regulations (including the Gramm-Leach-Bliley Act or HIPAA), they should already have the appropriate level of controls in place to be considered compliant with the SHIELD Act. However, companies should keep in mind that those controls must be applied to any additional data types included in the SHIELD Act.

Protected private information for New York residents includes:

- User names or email addresses in combination with a password or security question and answer that would permit access to an online account
- A name or other information that can be used to identify a specific person, in combination with any of the following:
  – Social Security number
  – Driver's license number or non-driver identification card number
  – Account, credit, or debit-card number in combination with any required security code, access code, password or other information that would permit access to an individual's financial account
  – Account, credit, or debit-card number, if the number could be used to access an individual's financial account without additional identifying information, security code, access code or password
  – Biometric information, specifically data generated by electronic measurements of an individual's unique physical characteristics, including fingerprint, voiceprint, or retina or iris image, or other unique physical representation or digital representations used to authenticate an individual's identity.

Defining a breach

Prior versions of the law defined a breach as the unauthorized acquisition of private information. A breach only needed to be reported if you were confident information was exfiltrated from the network.

Starting Oct. 23, the SHIELD Act expanded the definition of a breach to include any unauthorized access to private or personal information. Now, any unauthorized viewing of private or personal information is considered a breach and requires notification to the attorney general, even if there is no evidence the data was removed.

Security requirements

The SHIELD Act requires organizations to develop, implement, and maintain "reasonable" administrative, technical, and physical safeguards to protect and securely dispose of New York residents' private information. However, the requirements read more like mission statements than specific control requirements, so here's an attempt at translating the requirements into high-level action plans for organizations.

Administrative safeguards

- Designate one or more employees to coordinate the security program: assign security responsibility, appoint or outsource CISO
- Identify reasonably foreseeable internal and external risk: develop a risk-management plan
- Assess the sufficiency of safeguards in place to control the identified risks: perform a gap analysis to identify deficiencies and develop a plan of action for remediation
- Train and manage employees in security program practices and procedures: implement a training program aligned with organization policies and procedures, security reminders and user testing
- Select service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract: develop a third-party security audit and contractual process for onboarding service providers and for ongoing safeguard evaluation
- Adjust the security program in light of business changes or new circumstances: implement change management

Technical safeguards

- Assess risks in network and software design: vulnerability management, including authenticated scans of external and internal network assets
- Assess risks in information processing, transmission and storage: monitor data flows and boundary defenses
- Detect, prevent, and respond to attacks or system failures: develop a documented incident-response plan
- Regularly test and monitor the effectiveness of key controls, systems, and procedures: develop an internal-audit process

Physical safeguards

- Assess risks of information storage and disposal: develop storage-media policies and procedures
- Detect, prevent and respond to intrusions: again, develop a documented incident-response plan
- Protect against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information: implement access-control policies and procedures
- Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so the information cannot be read or reconstructed: develop documented data retention and media disposal policy

Fines and penalties

The penalties for violating the SHIELD Act are somewhat murky. The state attorney general may prosecute the offending organization if it fails to implement reasonable administrative, technical and physical safeguards to secure New York residents' private or personal information.

If an organization fails to comply with the SHIELD Act's breach notification requirements, the attorney general may impose a civil penalty of the greater of $5,000 or $20 per instance of failed notification, with a new ceiling of $250,000 — twice the previous penalty.

The March 23 deadline is quickly approaching, and for organizations that are starting at square one, getting to compliance with the SHIELD Act is going to require a substantial effort. The clock is ticking. Go. ■

Michael Montagliano is the chief technology officer at iV4 (www.iv4.com), an IT consulting, support, and professional services firm with offices in Fairport, Syracuse, and Amherst. Contact him at mmontagliano@iv4.com