STATE OF NEW YORK

9005

IN SENATE

May 3, 2022

Introduced by Sen. SAVINO -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the state technology law, in relation to establishing the "secure our data act"

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "secure our data act".

§ 2. Legislative intent. The legislature finds that ransomware and other malware attacks have affected the electronically stored personal information relating to thousands of people statewide and millions of people nationwide. The legislature also finds that state entities receive such personal information from various sources, including the data subjects themselves, other state entities, and the federal government. In addition, the legislature finds that state entities use such personal information to make determinations regarding the data subjects. The legislature further finds that New Yorkers deserve to have their personal information that is in the possession of a state entity stored in a manner that will withstand any attempt by ransomware and other malware to alter, change, or encrypt such information.

Therefore, the legislature enacts the secure our data act which will guarantee that state entities will employ the proper technology to protect the personal information stored as backup information from any unauthorized alteration or change.

§ 3. The state technology law is amended by adding a new section 210 to read as follows:

§ 210. Ransomware and other malware protection. 1. Definitions. For purposes of this section, the following terms shall have the following meanings:

(a) "Data subject" shall mean the person who is the subject of the personal information.

(b) "Immutable" means data that is stored unchanged over time or unable to be changed. For the purposes of backups, "immutable" shall mean that, once ingested, no external or internal operation can modify

EXPLANATION--Matter in italics (underscored) is new; matter in brackets [-] is old law to be omitted.

the data and must never be available in a read/write state to the client. "Immutable" shall specifically apply to the characteristics and attributes of a backup system's file system and may not be applied to temporary systems state, time-bound or expiring configurations, or temporary conditions created by a physical air gap as is implemented in most legacy systems. An immutable file system must demonstrate characteristics that do not permit the editing or changing of any data backed up to provide agencies with complete recovery capabilities.

(c) "Information system" shall mean any good, service or a combination thereof, used by any computer, cloud service, or interconnected system that is maintained for or used by a state entity in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or voice including, but not limited to, hardware, software, information appliances, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically and electronically collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, coverage, interface, switch, or disseminate data of any kind or form.

(d) "Maintained" shall mean personal information stored by a state entity that was provided to the state entity by the data subject, a state entity, or a federal governmental entity. Such term shall also include personal information provided by an adverse party in the course of litigation or other adversarial proceeding.

(e) "Malware" shall mean malicious code included in any application, digital content, document, executable, firmware, payload, or software for the purpose of performing or executing one or more unauthorized processes designed to have an adverse impact on the availability, confidentiality, or integrity of data stored in an information system.

(f) "Ransomware" shall mean any type of malware that uses encryption technology to prevent users from accessing an information system or data stored by such information system until a ransom is paid.

(g) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York or any of its political subdivisions.

2. Data protection standards. (a) No later than one year after the effective date of this section, the director, in consultation with stakeholders and other interested parties, which shall include at least one public hearing, shall promulgate regulations that design and develop standards for:

(i) malware and ransomware protection for mission critical information systems and for personal information used by such information systems;

(ii) data backup that includes the creation of immutable backups of personal information maintained by the state entity and storage of such backups in a segmented environment, including a segmented device;

(iii) information system recovery that includes creating an identical copy of an immutable personal information backup maintained by or for the state entity that was stored in a segmented environment or on a segmented device for use when an information system has been adversely affected by rent somewhere or other malware and requires restoration from one or more backups; and

(iv) annual workforce training regarding protection from ransomware and other malware, as well as processes and procedures that should be followed in the event of a data incident involving ransomware or other malware.

(b) Such regulations may be adopted on an emergency basis. If such regulations are adopted on an emergency basis, the office shall engage in the formal rulemaking procedure no later than the day immediately following the date that the office promulgated such regulations on an emergency basis. Provided that the office has commenced the formal rule-making process, the regulations adopted on an emergency basis may be renewed no more than two times.

3. Vulnerability assessments. Notwithstanding any provision of law to the contrary, each state entity shall engage in vulnerability testing of its information systems as follows:

(a) Beginning January first, two thousand twenty-three and on a monthly basis thereafter, each state entity shall perform, or cause to be performed, a vulnerability assessment of at least one mission critical information system ensuring that each mission critical system has undergone a vulnerability assessment during the past year. A report detailing the vulnerability assessment methodology and findings shall be made available to the office for review no later than forty-five days after the testing has been completed.

(b) Beginning December first, two thousand twenty-three, each state entity's entire information system shall undergo vulnerability testing conducted by an independent third party. A report detailing the vulnerability assessment methodology and findings shall be made available to the office for review no later than forty-five days after such testing has been completed.

(c) The office shall assist state entities in complying with the provisions of this section.

4. Data and information system inventory. (a) No later than one year after the effective date of this section, each state entity shall create an inventory of the data maintained by the state entity and the purpose or purposes for which such data is maintained and used. The inventory shall include a listing of all personal information maintained by the state entity, along with the source and age of such information.

(b) No later than one year after the effective date of this section, each state entity shall create an inventory of the information systems maintained by or on behalf of the state entity and the purpose or purposes for which each such information system is maintained and used. The inventory shall denote those information systems that are mission critical and those that use personal information, and whether the information system is protected by immutable backups.

(c) Notwithstanding paragraphs (a) and (b) of this subdivision, if a state entity has already completed a data inventory or information systems inventory, such state entity shall update the previously completed data inventory or information system inventory no later than one year after the effective date of this section.

(d) Upon written request from the office, a state entity shall provide the office with either or both of the inventories required to be created or updated pursuant to this subdivision.

5. Incident management and recovery. (a) No later than eighteen months after the effective date of this section, each state entity shall have created an incident response plan for incidents involving ransomware or other malware that renders an information system or its data unavailable, and incidents involving ransomware or other malware that result in the alteration or deletion of or unauthorized access to, personal information.

(b) Such incident response plan shall include a procedure for situations where production and non-segmented information systems have been adversely affected by a data incident, as well as a procedure for the storage of personal information and mission critical backups on a segmented device or segmented portion of the state entity's information system to ensure that such personal information and mission critical systems are protected by immutable backups.

(c) Beginning January first, twenty thousand twenty-five and on an annual basis thereafter, each state entity shall complete at least one exercise of its incident response plan that includes copying the immutable personal information and mission critical applications from the segmented portion of the state entity's information system and using such copies in the state entity's restoration and recovery process. Upon completion of such exercise, the state entity shall document the incident response plan's successes and shortcomings.

6. No private right of action. Nothing set forth in this section shall be construed as creating or establishing a private cause of action.

§ 4. Severability. The provisions of this act shall be severable and if any portion thereof or the applicability thereof to any person or circumstances shall be held to be invalid, the remainder of this act and the application thereof shall not be affected thereby.

§ 5. This act shall take effect immediately.