

STATE OF NEW YORK

5007--A

2023-2024 Regular Sessions

IN SENATE

February 21, 2023

Introduced by Sens. GONZALEZ, SALAZAR -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- reported favorably from said committee and committed to the Committee on Finance -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

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:

1 Section 1. This act shall be known and may be cited as the "secure our
2 data act".
3 § 2. Legislative intent. The legislature finds that ransomware and
4 other malware attacks have affected the electronically stored personal
5 information relating to thousands of people statewide and millions of
6 people nationwide. The legislature also finds that state entities
7 receive such personal information from various sources, including the
8 data subjects themselves, other state entities, and the federal govern-
9 ment. In addition, the legislature finds that state entities use such
10 personal information to make determinations regarding the data subjects.
11 The legislature further finds that New Yorkers deserve to have their
12 personal information that is in the possession of a state entity stored
13 in a manner that will withstand any attempt by ransomware and other
14 malware to alter, change, or encrypt such information.
15 Therefore, the legislature enacts the secure our data act which will
16 guarantee that state entities will employ the proper technology to
17 protect the personal information stored as backup information from any
18 unauthorized alteration or change.
19 § 3. The state technology law is amended by adding a new section 210
20 to read as follows:

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

LBD09002-02-3

§ 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 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, except:

(i) the judiciary; and

(ii) all cities, counties, municipalities, villages, towns, and other local agencies.

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;

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

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

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

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

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

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

32 (b) Beginning December first, two thousand twenty-four, each state
33 entity's entire information system shall undergo vulnerability testing.
34 A report detailing the vulnerability assessment methodology and findings
35 shall be made available to the office for review no later than forty-
36 five days after such testing has been completed.

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

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

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

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

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

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

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

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

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

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

32 § 5. This act shall take effect immediately.