

Cyber Security, Privacy and Data Protection

Jared A. Kasschau, Esq.
Alan M. Winchester, Esq.

Cybersecurity and Municipalities

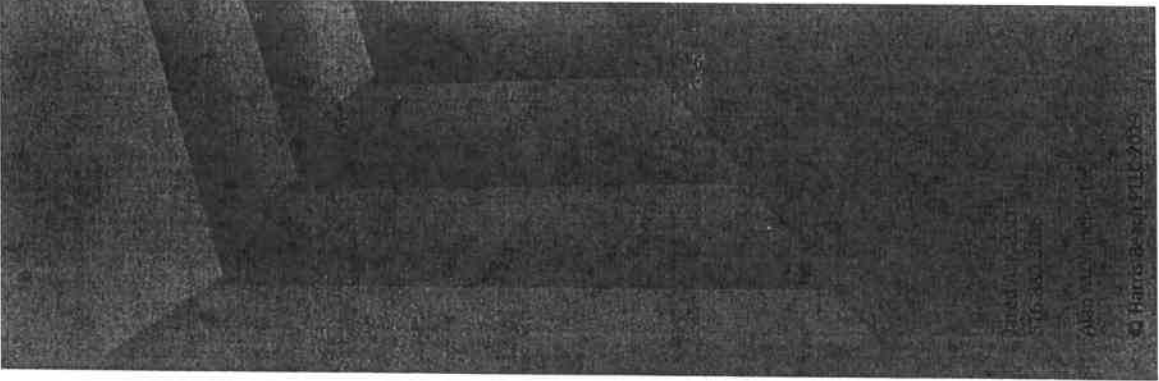
Jared A. Kasschau
516.880.8106

Alan M. Winchester

© Harris Beach PLLC 2019

About Jared

- Served as chief legal officer of Nassau County
- Co-leader of the political law team
- Helps municipalities manage their risk and better serve their communities

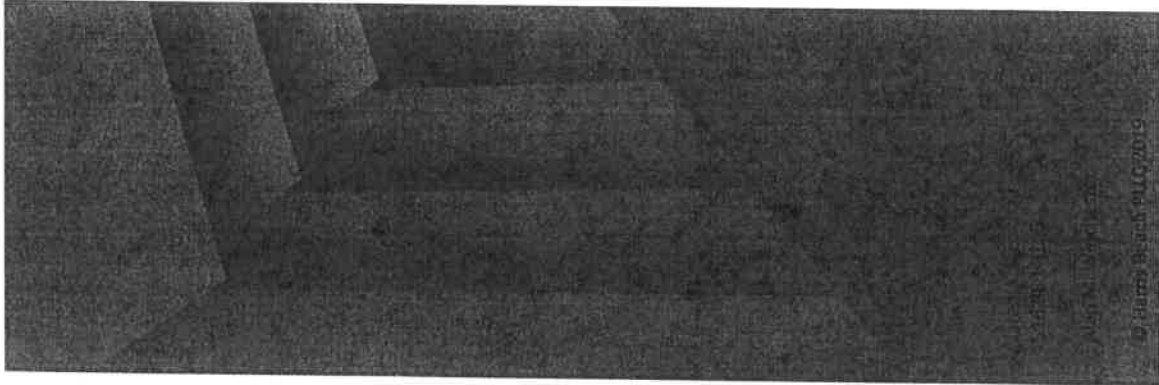


About Alan

- Cybersecurity and data privacy attorney who works with companies to develop ways to safely share and use the information they control.
- Cybersecurity Protection & Response PG Leader.
- Support firm clients with cyber-related services across range of industries – energy, health care, educational institutions, financial institutions, municipalities & more.
- Can help clients both pre- and post incident.



HARRIS BEACH
ATTORNEYS AT LAW
Discover True Engagement®



Agenda



Primary cybersecurity concerns for municipalities



What can municipalities do to reduce risk?



My systems are in “the cloud.” Is it no longer my problem?



Incident Response and Business Continuity Plans



Tabletop exercises and their importance



HARRIS BEACH
ATTORNEYS AT LAW
Discover True Engagement™

Information Types

Information protected by State Technology Law § 208

- Personally identifiable AND
- SSN; Drivers License; Credit card information; Access to financial institutions; biometrics; Access to on-line accounts

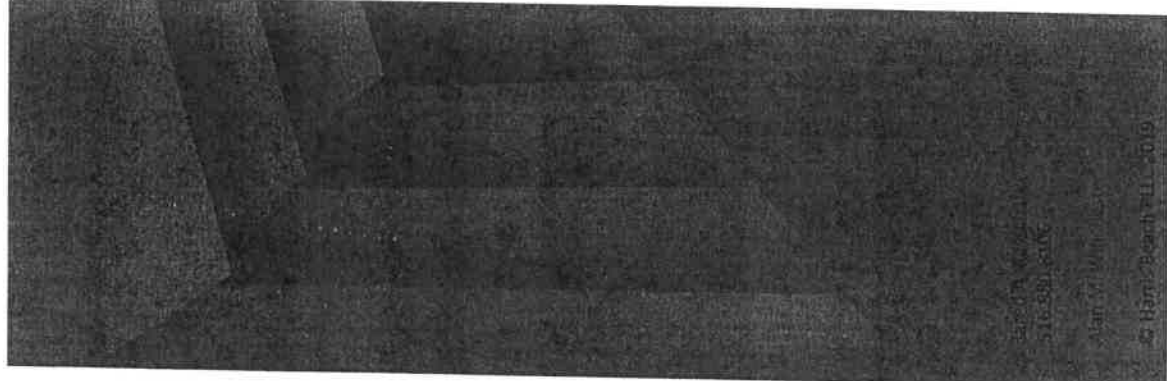
HIPAA information if covered entity or business associate

- Medical information
- Health Insurance information

Everything else

PLLC

Discover True Engagement®



State Technology Law § 208

- Essentially a verbatim copy of GBL § 899-aa
- Requires a municipality to develop notification procedures when there is unauthorized access to PII
 - Initially exempts municipalities in section 1(c)(2) but then applies to the with paragraph 10
- Does NOT establish protection requirements outlined in GBL § 899-bb (NY SHIELD), but does adopt the expanded definition of PII
- Requires a written report from Office of Information Technology on how to improve security following a breach.

See Amended Law attached



HARRIS BEACH
ATTORNEYS AT LAW
Discover True Engagement®

Risks Municipalities Should Address

Ransomware

- Recent ransomware attacks have been more successful against smaller municipalities
- The number of reported events are consistent over the last four years

Privacy Loss

- Occurs in roughly half of the ransomware attacks
- Occurs with Phishing attacks
- Human error

Wire Fraud

- Business Email Compromise
- Phishing



Reducing Risk

Implement and measure controls

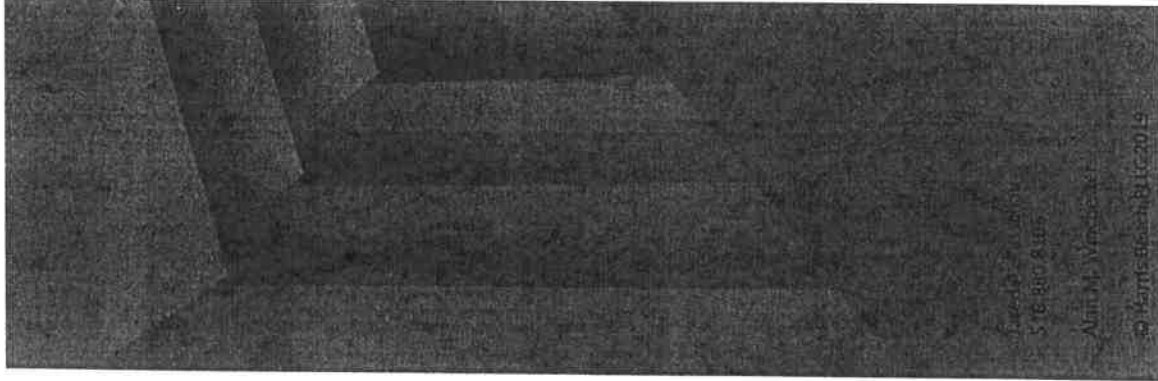
- NIST 800-53
- CIS
- ISO

Cybersecurity program officer

- Technical knowledge is not a prerequisite
- Communicate strengths and weaknesses in terms of a framework (CSF, CISA, Etc.)

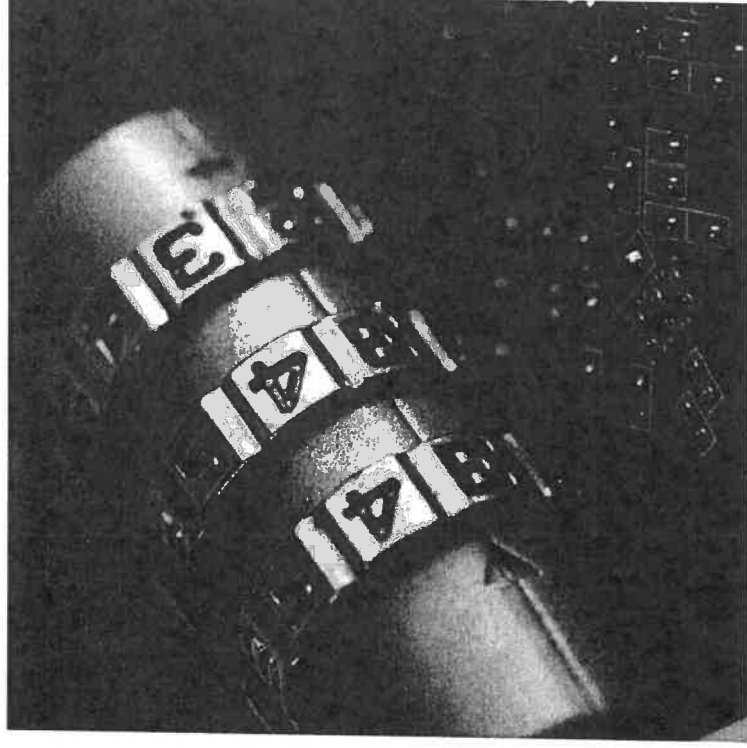


HARRIS BEACH
ATTORNEYS AT LAW
Discover True Engagement



Reducing Risk Continued

- Do these now:
 - Multifactor using a PIN code for remote access
 - No shared accounts
 - Make sure your systems are still supported
 - Patch and turn on auto update
 - User training
 - Do a risk assessment



In the cloud, but not off your desk...



**Systems in the cloud relieve you of patching;
but not much else.**



You still are responsible for:

The data stored in those sites

Notification to affected data subjects following unauthorized access

Auditing the security of the third-party provider

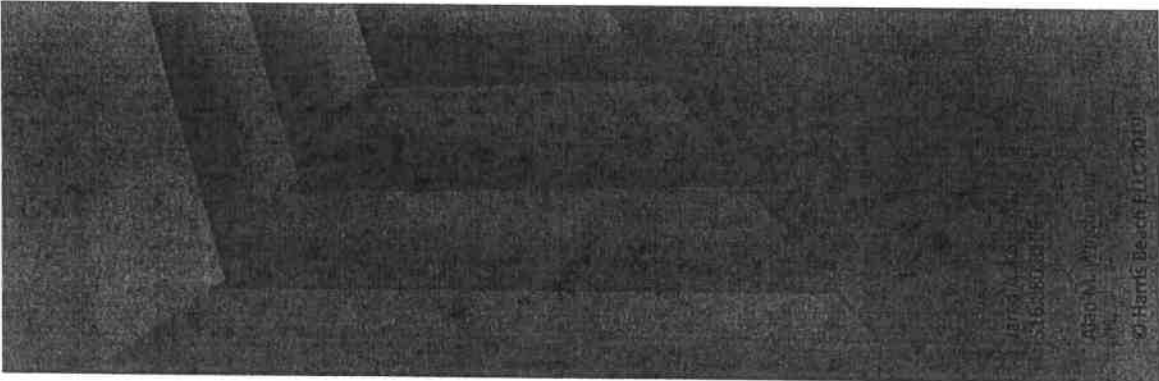
Your own administration of the system:

- Authenticated users
- Access levels
- Passwords
- Data use and sharing
- Pretty much everything



HARRIS BEACH
ATTORNEYS AT LAW

Discover True Engagement™



When bad things happen

Business Continuity Plan – How will the County continue to deliver on its mission without the systems covered by the plan.

- Identify important and essential systems
- How will things continue to work if these systems don't?
- How long could this go before the County fails in its mission?

Incident Response Plan – Play book of what the Country will do should certain events occur.

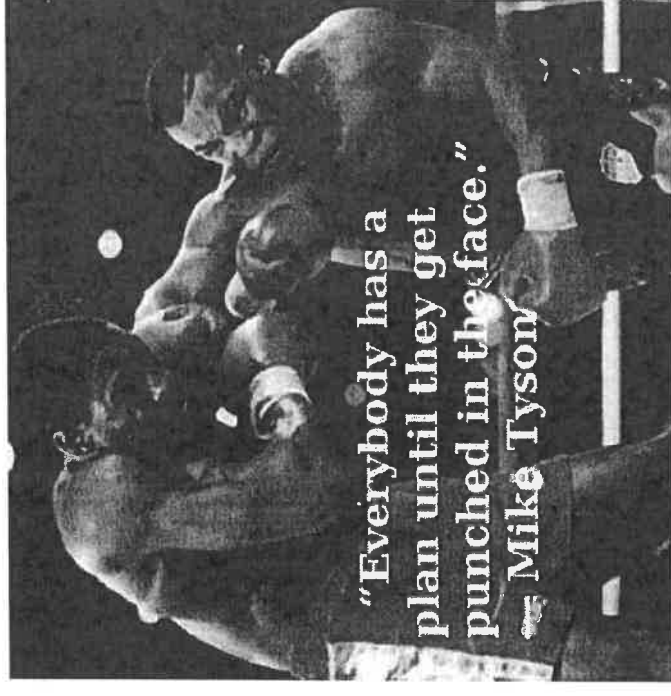
- Declaring an Incident
- Defining actions to take
- Defining who should be involved and how to engage them



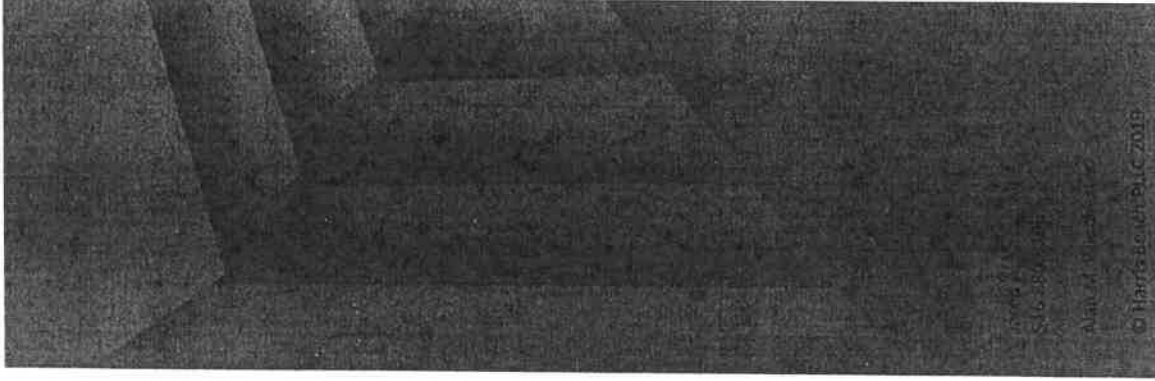
HARRIS BEACH
ATTORNEYS AT LAW
Discover. True Engagement®

Testing your plans: Tabletop drills

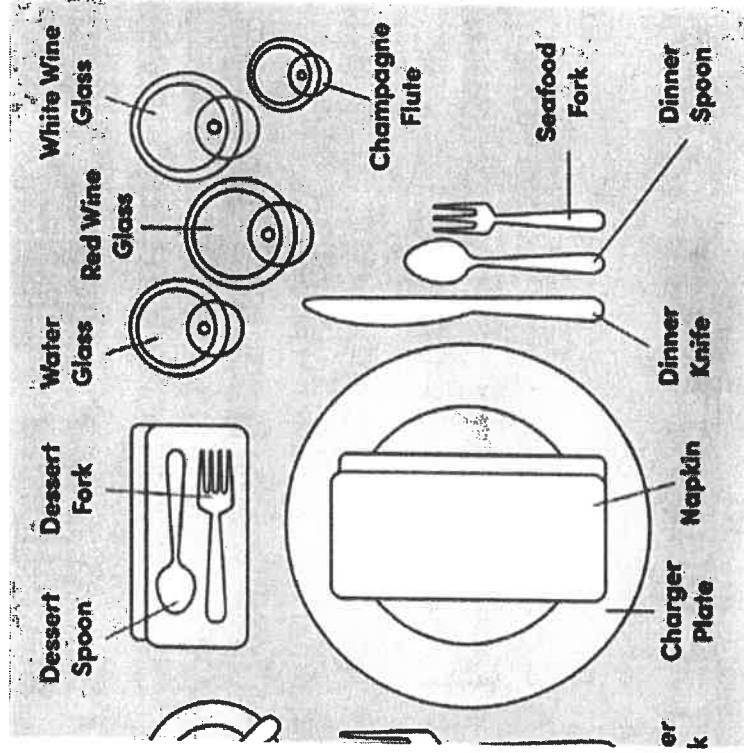
- Cost effective and surprisingly effective
 - Managed by the Incident Response Team
 - Does not test functionality of the plan components
 - Opportunity to identify what is missing or unclear



HARRIS BEACH
ATTORNEYS AT LAW
Discover True Engagement™



Preparing for tabletops



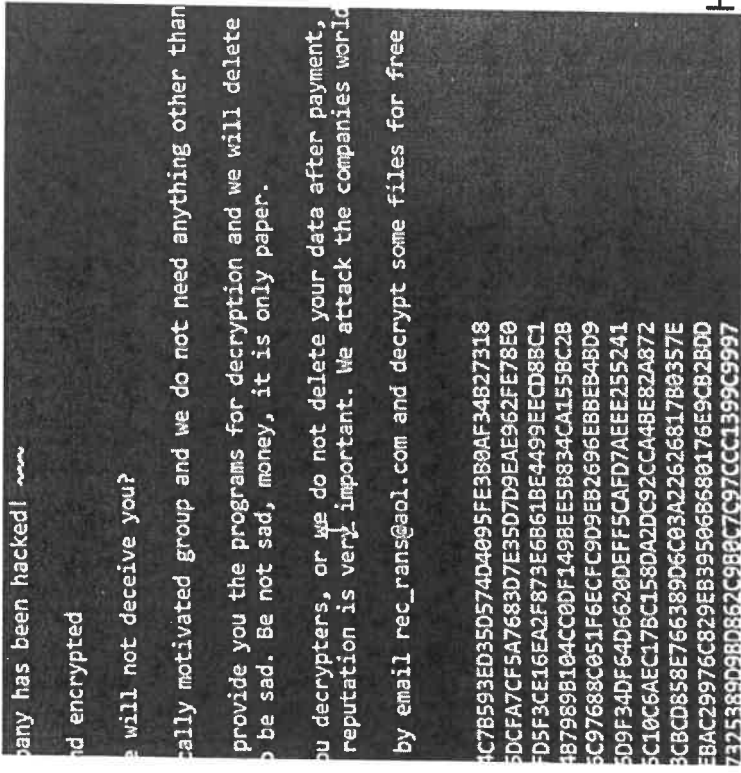
- Circulate the plan to the IR team
- Solicit from primary business groups the following
 - Define key personal and how to reach them
 - Critical vendors and how to reach them
 - Essential systems to the mission of that business unit
 - Essential data for the success of that group's mission
 - Acceptable time without those systems (Recovery Time Objective)
 - Acceptable data loss without mission failure(Recovery Point Objective)
- Define the event(s) for the team to contemplate

Defining the scope

- Examine the ability to respond to a ransomware attack.
- Evaluate the ability to coordinate information sharing during a ransomware attack.
- Inform development and update Incident Response materials, including policy, plan, and playbook.
- Explore processes for engaging additional Incident response resources as needed, including external resources such as a breach coach, forensic investigator, ransom negotiator, etc.
- Explore processes for communicating Incidents (to internal stakeholders, clients, media, and others).
- Explore policy and procedure related to the payment of ransom.

Create a Scenario

People are arriving at work to find ransom messages displayed on their computer screens and are unable to access some files. They begin to contact the Help Desk and others in IT to report the issue. IT begins to investigate and realizes that we have been infected with ransomware. Further investigation shows that files stored on internal servers and local computers have been encrypted by the ransomware and the encryption is still spreading. What now?



Company has been hacked! ~~~~
Files encrypted
We will not deceive you?
I am a highly motivated group and we do not need anything other than
to provide you the programs for decryption and we will delete
them. Be sad. Be not sad, money, it is only paper.
If you decrypters, or we do not delete your data after payment,
your reputation is very important. We attack the companies world
by email rec_rans@aol.com and decrypt some files for free

4C7B593ED350574D4095FE3B80AF34B27318
5DCFA7CF5A7683D7E35D7D9EAE962FE78E0
FD5F3CE16EA2F873E6B61BE4499EECD88C1
4B7989B104CC0DF149BEE5B834CA1558C2B
5C97688C051F6ECFC9D9EB2696EBEB48D9
5D9F34DF64D6628DEFF5CAFD7AE5EE25241
5C10C6AEC17BC158DA2DC92CCA48E82A872
8C8CDB58E766389D6C03A22626817B0357E
EBAC29976C829EB39506B680176E9CB2BDD
7315389D9RD862C988C7C97CC1399C9997

H
FILE

ATTORNEYS AT LAW
Discover True Engagement

Test the plan



Does it address how to stop the spread?



Does it address how to preserve evidence?



Does it address how to recover?



Does it address how to continue operations?



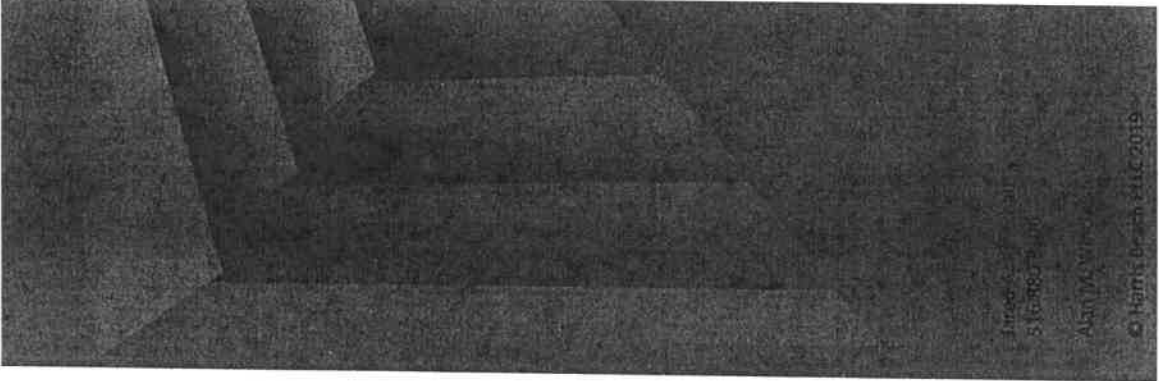
If files can't be recovered, does it address whether and how to pay the ransom?



Does it address how to identify the root source of the breach?

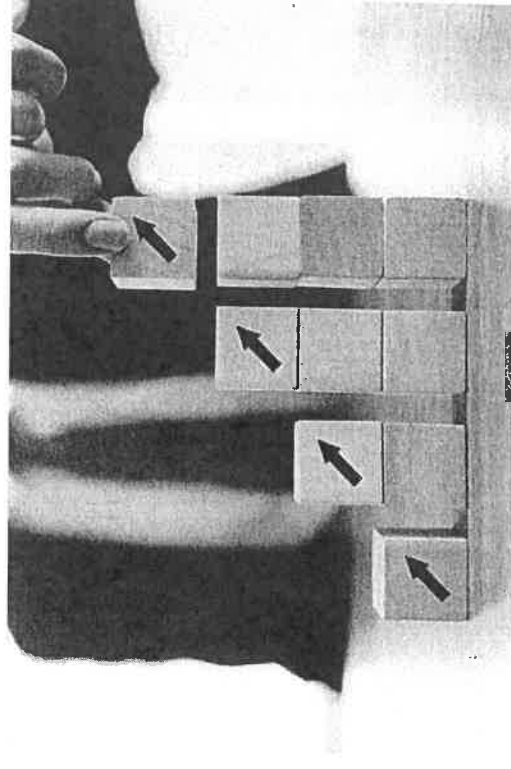


Does it address communication and notice?



Revise the plan with what you learned

- Solicit feedback while running the drill
- Survey participants
- Share the plan with your vendors
- Recirculate the plan





User Name: Alan Winchester

Date and Time: Monday, April 17, 2023 3:28:00PM EDT

Job Number: 195116614

Document (1)

1. NY CLS STATE TECHNOLOGY LAW § 208

Client/Matter: -None-

Search Terms: "state technology law" w/2 208

Search Type: Terms and Connectors

Narrowed by:

Content Type
Statutes and Legislation

Narrowed by
-None-

NY CLS STATE TECHNOLOGY LAW § 208

Current through 2023 released Chapter 1-49, 61-123

New York Consolidated Laws Service > State Technology Law (Arts. 1 — 4) > Article II Internet Security and Privacy Act (§§ 201 — 209)

§ 208. Notification; person without valid authorization has acquired private information

1. As used in this section, the following terms shall have the following meanings:

(a) "Private information" shall mean either:

(i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;

(3) account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

NY CLS STATE TECHNOLOGY LAW § 208

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(c) "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:

(1) the judiciary; and

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

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such

NY CLS STATE TECHNOLOGY LAW § 208

- rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.
3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.
 4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
 5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:
 - (a) written notice;
 - (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;
 - (c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or
 - (d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - (1) e-mail notice when such state entity has an e-mail address for the subject persons;
 - (2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and
 - (3) notification to major statewide media.
 6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.
 7.
 - (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.
 - (b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

NY CLS STATE TECHNOLOGY LAW § 208

8. The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.
9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.
10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

History

Add, L 2005. ch 442. § 3, eff Dec 7, 2005 (see 2005 note below); amd, L 2005. ch 491. §§ 2-4, eff Dec 7, 2005; L 2011. ch 62. § 27 (Part A), eff April 1, 2011 (see 2011 note below); L 2013. ch 55. § 5 (Part N), eff March 28, 2013; L 2019. ch 117. § 5, effective October 23, 2019.

New York Consolidated Laws Service
Copyright © 2023 Matthew Bender, Inc.,
a member of the LexisNexis (TM) Group All rights reserved.

End of Document