Vermont Bar Association
2018 Tech Show Seminar Materials

Legal Obligations and Best Practices When Facing Data Breaches

May 16, 2018
DoubleTree (formerly Sheraton)
S. Burlington, VT

Speakers:

Ryan Kriger, Esq.

Legal Obligations & Best Practices When Facing Data Breaches

Ryan Kriger, CIPP/US

Assistant Attorney General, Public Protection Division

May 16, 2018

Takeaways:

1. Know what laws affect you
2. Train your employees
3. Think data security *before* you get hit
4. Have response plan for *after* you get hit
5. Get Cyber Insurance
6. Vendors/Contractors/Cloud Providers

Know What Laws You Have To Comply With

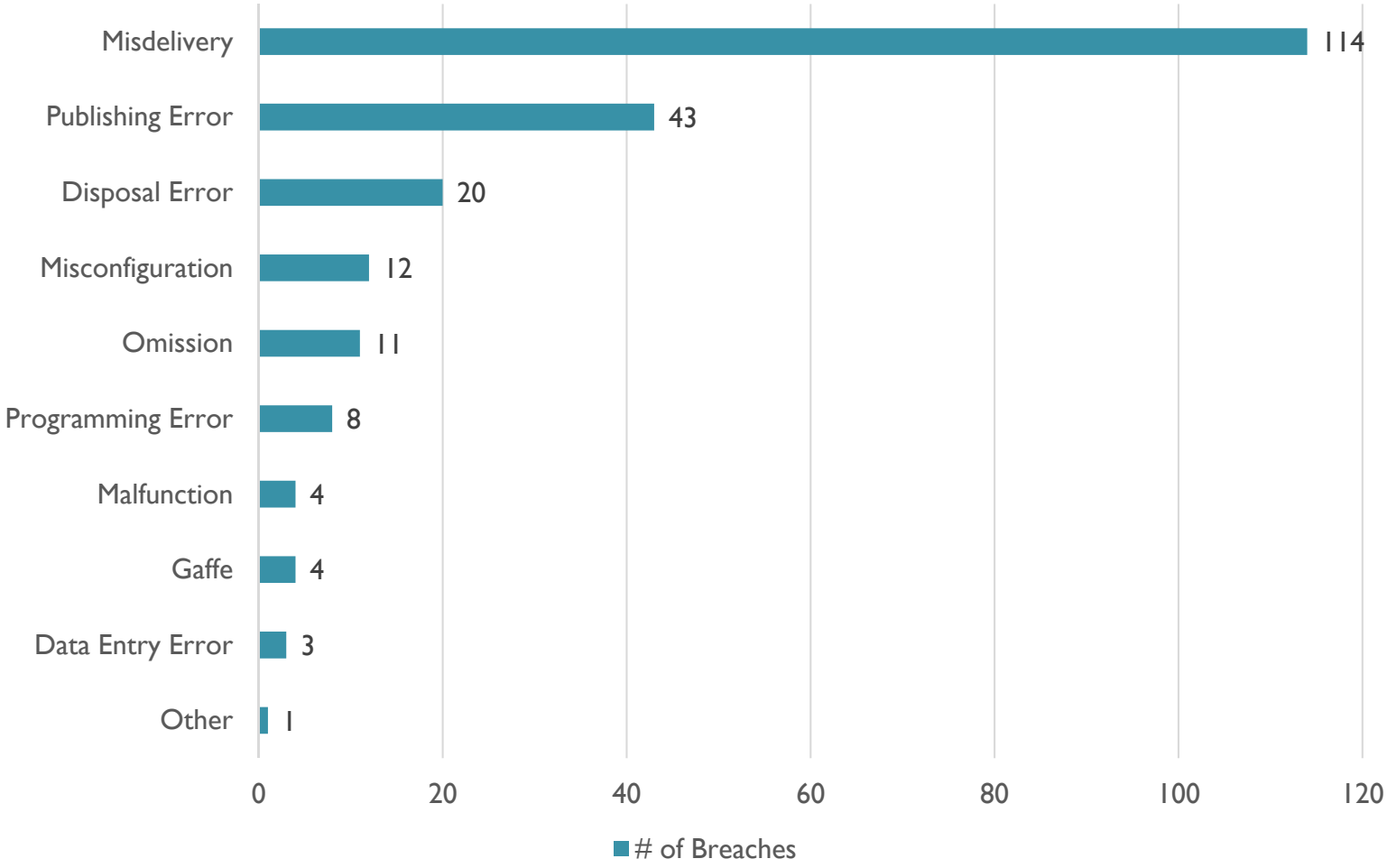
- **Consumer Protection Act**: EVERYONE
- **Security Breach Notice Act**: EVERYONE
- **SSN Protection Act**: Do you Collect SSN
- **HIPAA**: Do you do medical work?
- **FERPA**: Do you work with schools/universities?
- **COPPA**: Do you sell to kids under 13?
- **GLB**: Do you work with financial institutions?

Data Breaches:
Some stats from 2016*

- **75%** of breaches were perpetrated by outsiders
- **25%** involved internal actors
- **51%** involved organized criminal groups
- **81%** of hacking-related breaches leveraged either stolen and/or weak passwords
- **14%** involved errors
- **14%** involved privilege misuse
- **15%** of the victims were Retail & Accommodation
- **66%** of malware was installed via email attachment

*Source: Verizon 2017 Data Breach Investigations Report

Data Breaches: Errors*



*Source: Verizon 2017 Data Breach Investigations Report

Data Breaches: Accommodation & Food Services*

Frequency	96% External, 4% Internal
Top 3 patterns	Point of Sale Intrusions, Everything Else and Privilege Misuse represent 96% of all data breaches within Accommodation
Threat actors	96% External, 4% Internal
Actor motives	99% Financial, <1% Grudge
Data compromised	96% Payment, 2% Personal, 1% Credentials
Summary	This vertical was dominated by POS breaches. Most of them are opportunistic and financially motivated and involve primarily malware and hacking threat actions. Time-to-compromise is quick but time-to-discovery and containment remains in the months category. Fraud detection is increasing compared to previous years.

*Source: Verizon 2017 Data Breach Investigations Report

Data Breaches: Retail*

Frequency	326 incidents, 93 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Payment Card Skimming represent 81% of all security incidents within Retail
Threat actors	92% External, 7% Internal, <1% Partner
Actor motives	96% Financial, 2% Espionage, 2% Curiosity
Data compromised	57% Payment, 27% Personal, 17% Credentials
Summary	Online retailers are consistent targets of DoS attacks, and POS environments continue to be compromised for financial motivations.

*Source: Verizon 2017 Data Breach Investigations Report

Three Numbers

14	Days: Time to Confidentially Provide Preliminary Notice of Breach to AG
45	Days: Maximum Time to Send Notice to Consumers (It Can Often Be Sooner)
10,000	Dollars: Maximum Civil Penalty Per Violation

What Sort of Data Should You Be Protecting?

- Credit Card info
- Social Security Numbers
- Financial Information
- Passwords
- Anything sensitive that someone might not want to fall into the wrong hands

Whose Data Should You Be Protecting?

- Consumers
- Employees
- Clients (holding their data for their use – storage, payroll, legal, etc.)

Have Data Collection Policies:

- Encrypt your data
- Don't collect data you don't need
- Only keep data as long as you need it
- Consider using a 3rd party vendor to handle sensitive data

What Happens If You Lose Sensitive Data?

I've Had a Data Breach, What Next?

1. Secure Your Data
2. Contact Law Enforcement
3. Contact Cyber Insurance
4. Contact Entities From Which You Obtained the Data
5. Notify the Attorney General's Office Of The Breach
6. Notify Consumers Of The Breach
7. Notify the Credit Reporting Agencies (if more than 1,000 consumers)

Vermont's Security Breach Notice Act

- 9 V.S.A. § 2430 and § 2435
- Applies to Businesses and State Agencies
  - Enforced by either AG or DFR (was BISHCA)
  - Does Not Apply to Certain Financial Institutions
- Applies to Loss of "Personally Identifiable Information"
- Amended Effective May 8, 2012

What is Personally Identifiable Information (PII)?

First Name or First Initial & Last Name (if it has not been encrypted or rendered unreadable), AND

- Social Security number; OR
- Motor vehicle operator's license number or non-driver identification card number; OR
- Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; OR
- Account passwords or personal identification numbers or other access codes for a financial account.

Definition of "Security Breach"

"unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's **personally identifiable information** maintained by the data collector."

Definition of "Security Breach"

"does not include **good faith** but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a **legitimate purpose of the data collector**, provided that the personally identifiable information is **not used for a purpose unrelated to the data collector's business** or subject to further unauthorized disclosure."

Definition of "Security Breach"

Factors to consider when determining if a breach has occurred:

(i) Information is in someone else's physical custody (*i.e.* stolen laptop);

(ii) Information has been downloaded or copied (*i.e.* hacking, malware, unauthorized use);

(iii) Information has been used by an unauthorized person (*i.e.* reports of fraudulent accounts opened or ID Theft); or

(iv) that the information has been made public.

I've Had a Data Breach, What Next?

1. Secure Your Data
2. Contact Law Enforcement
3. Contact Entities From Which You Obtained the Data
4. Notify the Attorney General's Office Of The Breach
5. Notify Consumers Of The Breach
6. Notify the Credit Reporting Agencies (if more than 1,000 consumers)

Contact Law Enforcement

1. Call the FBI, Secret Service
2. Inform Them Of Your Duty To Notify Customers
3. Determine Whether Law Enforcement Wants You To Delay Notification

Timing of Notice Requirements

1. All Notices Should Go Out In The Most Expedient Time Possible
2. 14 Day Preliminary Notice to AG (non-public)
3. Final Notice to AG and to Customers (public) within 45 days
4. May only be delayed on request from law enforcement

Contents of Notice Requirements

- Incident in general terms.
- Type of PII accessed
- General acts taken to protect the PII from further breaches
- Telephone number, toll-free if available, for further information.
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
- The approximate date of the security breach.

Manner of Notice Requirements

- Direct Notice
  - Mail
  - Email (if requirements are met)
  - Telephone (not prerecorded)
- Substitute Notice (Website and Major Media)
  - If cost would exceed $5,000
  - If number of customers exceeds 5,000
  - If insufficient contact information

No Harm Letter

- Notice Not Required if Misuse of Personal Information is Not Reasonably Possible
- Notice of this determination with detailed explanation sent to Vermont Attorney General

Penalty for Noncompliance

- Violation of the Consumer Protection Act
- $10,000 Civil Penalty per Violation
- Violation = Customer Not Noticed Per Day

Online Resources

- VT Attorney General Site (ago.vermont.gov/focus/consumer-info/privacy-and-data-security1.php)
- OnGuardOnline.gov
- business.ftc.gov
- IAPP: www.privacyassociation.org

Questions About Data Breaches?

Contact Us:

802-828-3171

ago.datasecurity@Vermont.gov

Report Breaches:

ago. securitybreach@Vermont.gov

Remember Your Ethical Obligations

Vermont Rules of Professional Conduct:

1.1: Competence

1.6: Confidentiality of Information

Comments 16-17

Remember Your Ethical Obligations

Acting Competently to Preserve Confidentiality

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

Questions About Data Breaches?

Contact Us:

802-828-3171

ago.datasecurity@Vermont.gov

Report Breaches:

ago. securitybreach@Vermont.gov

How Do You Protect Sensitive Data?

Technology Suggestions
Credit Cards:

- Search your systems to make sure you're not storing data
- Search for key loggers
- Frequent system scans
- Watch your employees
- Consider scanners that encrypt at swipe
- NO web browsing on POS Systems

Watch Out For Portable Data:

- Cell Phones
- Tablets
- Laptops
- External Hard Drives
- Thumb Drives
- Data In Transit (including E-Mail)
- And Don't Forget Back-up Tapes

Protect Portable Data:

- Password Protection
- Remote Wipe Capability
- Encryption
- Ask yourself: Should this be in a portable medium?

Good Reads

- American Bar Security Site
- Protecting Consumer Privacy in an Era of Rapid Change (the FTC "Privacy by Design Report")
- Protecting Personal Information: A Guide for Business
- Start with Security: Lessons Learned from FTC Cases

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:

17.01 **Purpose and Scope**

(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope
The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:
(a) Designating one or more employees to maintain the comprehensive information security program;
(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. means for detecting and preventing security system failures.
(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
(e) Preventing terminated employees from accessing records containing personal information.
(f) Oversee service providers, by:
1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.
(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.
(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a

security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:
(1) Secure user authentication protocols including:
(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
(2) Secure access control measures that:
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: **Compliance Deadline**

(1)Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY

201 CMR 17.00: M.G.L. c. 93H