The Virginia Information Security Program

A Guide for Insurance Agents

Smart Choice Virginia

INTERNAL DRAFT: FOR AGENT USE ONLY

By Roger Gill & Daniel Brown

Original Posted August 11, 2020
Updated October 13, 2020

Purpose

This document has been written to educate Independent Insurance Agencies on how to meet the new State and Federal Cyber Security and Data Breach Laws to Protect their agencies, which now includes Cyber Security Awareness Training, Development of a Cyber Security Program, Privacy and Data Breach Response Policy Manuals, Employee and Associate Contractor Cyber Security Program Training and more.

The new Virginia Data Security Law based on the NAIC Data Security Model Law became effective July 1, 2020. This law and associated regulations (not completed as of yet by the BOI) places a much higher level of compliance on Virginia Insurance Agencies. **Failure to comply may result in costly fines.** Similar laws based on the NAIC Model Law have been passed in many other states and likely to be passed by most other states soon---requiring Agencies to comply that sell in multiple states.

Failure to report a Cyber Breach may result in costly fines also. "If a company fails to give notice when it is required, the Attorney General may bring an action against it for up to $150,000 per breach." (What To Do First When Data Is Hacked: A Guide To Mandatory Notification For Virginia Businesses, by JOLT, Allen, Spencer. Nov 9, 2017, Blog Posts)

The following will provide an overview of the Virginia Data Security Law and how it impacts Insurance Agencies immediately and also address the components of the Law that will become effective in 2022 and 2023.

Specifically addressed will be an overview of the Components of the New Virginia Law, Compliance Requirements, Prevention Tools and Resources, Required Training for Staff, How to Develop a Data Security Policy and Breach Response Plan, and How to Implement a Data Security Program Plan.

Also provided will be information on Comprehensive Solutions for Compliance and Data Security Breach Protection for Insurance Agencies and on how to sell Cyber Security Protection Programs to other businesses.

Overviews from Two Virginia Law Firms

Virginia 2020 Data Security Law Overview

By Bobby Turnage, Jr, an attorney with the Sands Anderson Law Firm

Bobby Turnage, Jr, an attorney with the Sands Anderson Law Firm, has provided an overview of the new Virginia 2020 Data Security Law in an article published April 2, 2020 (Insurers & Producers in Virginia: Get Ready for New Data Security and Notification Requirements!).

> Virginia has a new law, the Insurance Data Security Act (New Law), **going into effect on July 1, 2020,** which will expand the data security and incident notification requirements on insurers licensed in the Commonwealth. The New Law is similar to the National Association of Insurance Commissioners' Insurance Data Security Model Law – with some important modifications. Below is a high-level overview of the New Law, along with a focus on certain specifics, to help you gain a better understanding of what will be required.
>
> **Information Security Program**
>
> The New Law will **maintain** the current requirement for implementing a **comprehensive written information security program** (InfoSec

Program) with appropriate administrative, technical and physical (ATP) safeguards; **however, it also calls out the following specific requirements that must be addressed:**

Risk assessment. The InfoSec Program must be based on licensee's risk assessment;

Data retention and destruction. The InfoSec Program must define and provide for periodic reevaluation of a data retention schedule and mechanisms for destruction of nonpublic information (defined in the next section, below);

1. Responsibility designation. Licensees must designate an employee, affiliate or vendor to be responsible for the InfoSec Program;

2. Systems access controls. Licensees must establish access controls on information systems;

3. Physical access restrictions. Licensees must restrict access at physical locations that contain nonpublic information;

4. Environmental hazard measures. Licensees must implement measures to protect against destruction, loss or damage of nonpublic information from environmental hazards (e.g., fire, water, other catastrophes, and technological failures);

5. Secure disposal. Licensees must implement and maintain procedures for the secure disposal of nonpublic information;

6. Stay informed. Licensees must stay informed of emerging threats and vulnerabilities;

7. Security when sharing. Licensees must use reasonable security measures when sharing information (based on the type of sharing and type of information);

8. Training. Licensees must provide personnel with cybersecurity awareness training;

9. Board involvement. The board of directors (if there is one) must require the organization's information executive management (or its delegates) to (i) develop, implement and maintain the InfoSec Program, and (ii) report to the board in writing concerning program status and licensee compliance with the New Law, and material matters related to the program (such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations – and management's responses, and recommendations for changes in the InfoSec Program);

10. Monitor and adjust. Licensees must monitor, evaluate, and adjust the InfoSec Program consistent with changes in technology, sensitivity of nonpublic information, internal and external threats to information, changing business arrangements (e.g., M&A, alliances, joint ventures, and outsourcing), and changes to information systems; and

11. Incident Response Plan. Licensees must establish a written incident response plan that complies with requirements in the New Law.

Beginning on July 1, 2022, covered licensee's will be required to (i) exercise due diligence in selecting third-party service providers (TPSPs), and (ii) require TPSPs to implement reasonable ATP measures to protect systems and information.

Beginning on January 1, 2023, insurers domiciled in Virginia will need to (i) begin annual compliance certifications to the Bureau of Insurance, (ii) document improvement areas and remediation efforts, and (iii) maintain compliance documentation for five years.

Cybersecurity Events Generally

Until July 1, 2020, insurers will continue to be governed by Virginia's general data breach notification requirements; however, the New Law will put in place a new set of requirements for cyber security investigation and notification by insurers. It's important to note that a ***"cybersecurity event"*** is broadly defined in the New Law to basically be an event that results in **unauthorized access to, disruption of, or misuse of** an **information system** or **nonpublic information**. It's also important to note that ***"nonpublic information"*** is defined under the New Law generally as information that **is (i) business information**, the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact on the licensee, or **(ii) identifiable consumer information** in combination with pieces of certain sensitive information (e.g., social security number, financial account, biometric records, etc.), **or (iii) consumer healthcare** treatment, payment or condition information. These definitions become important when analyzing an organization's obligations related to security incidents.

Cybersecurity Event Investigations

Significantly, the New Law requires a prompt investigation after learning that a cybersecurity event has *or may have* occurred. It also specifies minimum information that must be determined, if possible, and steps that must be taken by a licensee. The New Law also requires the same level of effort regarding any cybersecurity event occurring in a TPSP system. Finally, a licensee must retain for five years all records regarding the cybersecurity event (and make them available to the Insurance Commissioner upon request).

Notice to Commissioner

Notice to the Commissioner of an *actual* cybersecurity event will be required (i) in the case of domestic insurers and producers, if the cybersecurity event meets **thresholds** and other requirements **prescribed by the State Corporation Commission**, and (ii) in the case of licensees generally, if they reasonably believe the cybersecurity event involves nonpublic information of **250 or more** consumers residing in Virginia, or if notice is required to any self-regulatory agency or government/supervisory body under federal law or the laws of another state. The New Law predictably outlines specific pieces of information that must be provided in the notice, such as how the incident happened, how the incident was discovered, what information was acquired, the period of compromise, and the number of consumers affected. Importantly, however, **licensees will also have to either identify lapses in controls and procedures, or confirm that all controls and procedures were followed.**

Notice to the Commissioner must be provided as promptly as possible but **in no event later than three business days,** and it must be provided in accordance with **requirements prescribed by the Commission.** Licensees will have an ongoing obligation to update the notice to the Commissioner. Based on the language noted above, we can expect to see cybersecurity thresholds and other requirements from the Commission pertaining to notification under the New Law.

The New Law also provides direction for handling cybersecurity events involving TPSPs, ceding insurers and independent insurance producers. Fortunately, the New Law will not prevent or abrogate agreements between licensees and other parties to fulfill the investigative or notification requirements under the New Law.

Notice to Consumers

Consumers must be notified of a cybersecurity event if (or **if the licensee reasonably believes**) the consumers' nonpublic information was **accessed and acquired** by an unauthorized person, **and** the cybersecurity event has a **reasonable likelihood** of causing or has caused **identity theft or other fraud** to the consumers. Notice must be given without undue delay after a determination (or receiving notice) that a cybersecurity event has occurred. The New Law specifies the information that must be included in the notice (e.g., general description, types of information involved, actions being taken, etc.), and the methods that may be used for notification (postal, telephonic or electronic), including substitute notice. Information will have to be provided to the major credit reporting agencies when more than 1,000 consumers are notified. Where notice is required to the Commissioner (see above), a copy of the notice to consumers must also be provided to the Commissioner. As with most breach notification statutes, the New Law provides for a delay around law enforcement investigations. Finally, TPSPs can provide the notice to consumers where the incident occurs in their systems, but responsibility for notification ultimately rests with the licensee.

Upcoming Regulations

The New Law directs the Commissioner to **adopt rules and regulations** implementing the New Law. There's more to come on that front.

Exceptions

There are three situations where **licensees will be exempt or deemed in compliance** with certain aspects of the New Law: **(1)** Licensees subject to **HIPAA**, that submit certain certifications, and that comply with the relevant provisions of HIPAA, will be considered compliant with the InfoSec Program, investigation and consumer notification requirements of the New Law; **(2)** A **licensee who is also an employee, agent, representative or designee** (the Agent Licensee) of another licensee (the Primary Licensee) is exempt from the InfoSec Program, investigation and notification requirements under the New Law to the extent the Agent Licensee is covered by the InfoSec Program, investigation and notification obligations of the Primary Licensee; and **(3)** Licensees **affiliated with a depository institution** that maintains an InfoSec Program in compliance with Interagency Guidelines under GLBA (the Guidelines) will be considered to meet the InfoSec Program requirements, provided the licensee produces, upon request, documentation satisfactory to independently validate the depository institution's adoption of an InfoSec Program satisfying the Guidelines.

It's also helpful to the *[sic]* note that the term **"licensee"** under the New Law **does not include** (i) a purchasing group or risk retention group chartered and licensed in a different state, or (ii) an assuming insurer that is domiciled in another state or jurisdiction.

Confidentiality

The New Law provides for the confidential and privileged status of most information and materials provided to, or obtained by, the Commissioner as a part of certifications, notices, examinations and investigations, along with protections against subpoena and discovery in civil proceedings. However, the Commission is permitted to use the information and materials in furtherance of its regulatory or legal

actions, and (with appropriate safeguards) to share the information and materials with certain third parties, such as consultants, other agencies and law enforcement.

Conclusion

Insurers and producers operating in Virginia need to review their current programs, policies and procedures to ensure they are ready to comply with the New Law. An important step in implementing the robust InfoSec Program requirements under the New Law is to conduct a risk assessment to help an organization identify and understand existing threats, risks and vulnerabilities. While the New Law will create more statutory and regulatory requirements, the good news is that compliance can also serve to improve an organization's overall cybersecurity posture.

Sands Anderson's Cybersecurity and Technology Team advises clients of all sizes concerning their data security obligations and risks, and we're here to help with any questions or concerns you might have. Please reach out to any of our team members and we'll be happy to help.

Virginia 2020 Data Security Law Overview

*By **Daniel R. Bumpus** with the Maquire Woods Law Firm*

Daniel R. Bumpus, an attorney with the Maquire Woods Law Firm, has provided an overview of the new Virginia 2020 Data Security Law in an article published May 22, 2020 (The Virginia Insurance Data Security Act – What You Need to Know).

On March 11th, 2020, Virginia Governor Northam signed the Insurance Data Security Act (the "Act") — HB 1334 — imposing requirements on all entities regulated by the Virginia Bureau of Insurance ("BOI" or the "Bureau") to:

- maintain an information security program,
- investigate all cybersecurity events,
- notify the Commissioner of Insurance of cybersecurity events, and
- notify consumers affected by cybersecurity events.

The Act is effective on July 1, 2020 but there are several components with phased-in compliance deadlines. The State Corporation Commission, which houses the Bureau, is also required to adopt regulations to implement the law.

The Act makes Virginia the latest state to adopt the National Association of Insurance Commissioners ("NAIC") Insurance Data Security Model Law, even though there are some differences between the Act and the NAIC's Model Law.

Reporting Change. Along with creating the new requirements detailed below, the Act sets forth the "exclusive state standards" for data security, security of nonpublic information, investigation of cybersecurity events, and reporting requirements for cybersecurity events for BOI-regulated entities. This includes a change in reporting of cybersecurity events from the Office of the Attorney General to the Commissioner of Insurance for BOI-regulated entities.

Licensees. The Act applies to "licensees." The term is defined as "any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of the Commonwealth." "Licensee" does not include a

purchasing group or risk retention group chartered or licensed in another state or a person acting as an assuming insurer that is domiciled in another state.

Information Security Program. Each licensee is required to "develop, implement, and maintain a comprehensive written information security program." The Act spells out the requirements of the program, including:

- that the program is to be commensurate with the size and complexity of the licensee,
- a mandate for cybersecurity training,
- due diligence of third-party service providers (starting July 1, 2022), and
- submission of a written certification of compliance with the information security program requirements (starting February 15, 2023)

Additional guidance is likely to come in forthcoming Commission regulations.

Duty to Investigate. The Act requires licensees that learn a cybersecurity event has or may have occurred, to conduct a "prompt investigation" to:

- determine whether a cybersecurity event has occurred,
- assess the nature and scope of the cybersecurity event,
- identify any nonpublic information that may have been involved in the cybersecurity event, and
- implement reasonable measures to restore the security of the information systems compromised in the cybersecurity.

A "cybersecurity event" is defined as "an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information in the possession, custody, or control of a licensee or an authorized person." A "cybersecurity event" excludes acquisition of encrypted information, as long as the key is also not acquired, and any event where the licensee has determined that the nonpublic

information accessed has not been used or released and has been returned or destroyed.

Commissioner Notice. If a licensee has determined that a cybersecurity event has actually occurred, it must notify the Commissioner of Insurance "as promptly as possible but in no event later than three business days from such determination." Notice is required if:

(1) the licensee is a domestic insurance company or a producer with Virginia as its home state, or

(2) the licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in the Commonwealth, or notice is required by federal, other state regulator, or self-regulatory or supervisory body.

The Act requires that notice to the Commissioner be provided in electronic form and spells out the content of the notice.

Consumer Notice. A licensee that maintains "consumers' nonpublic information shall notify the consumer of any cybersecurity event without unreasonable delay after making a determination or receiving notice that a cybersecurity event has occurred." The licensee's consumer notice obligation is triggered only if "consumers' nonpublic information was accessed and acquired by an unauthorized person or such licensee reasonably believes consumers' nonpublic information was accessed and acquired by an unauthorized person and the cybersecurity event has a reasonable likelihood of causing or has caused identity theft or other fraud to such consumers."

Such notice shall include a description of the following:

- The incident in general terms;
- The type of nonpublic information that was subject to the unauthorized access and acquisition;
- The general acts of the licensee to protect the consumer's nonpublic information from further unauthorized access;
- A telephone number that the consumer may call for further information and assistance, if one exists; and
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring the consumer's credit reports.

The Act provides that consumer notice may be delayed if, after notification of a law enforcement agency, the law enforcement agency determines and advises that the notice will impede a criminal or civil investigation or jeopardize national or homeland security. The Act also states that a licensee must treat cybersecurity events of its third-party service providers as its own cybersecurity event, unless the third-party service provider provides the required customer notice.

Exceptions. The Act carves out exceptions from its various requirements for certain classes of licensees:

Those subject to and compliant with HIPAA are considered in compliance with the information security program requirements and customer notification requirements;

- Those affiliated with a depository institution maintaining an information security program in compliance with GLBA are considered in compliance with the information security program requirements; and

- Those that are employees, agents, representatives, or designees of another licensee are exempt from the Act's requirements if covered by information security program, investigation, and notification obligations of the other licensee.

Impact. While the Act may not change much beyond the regulator receiving notice of a cybersecurity incident for sophisticated licensees who are already in compliance with the New York Department of Financial Services Cybersecurity Regulation, which is not a safe harbor under the Act, the Act imposes significant requirements on licensees regardless of size. All licensees should assess their data security program for compliance with the Act before the July 1, 2020 effective date and stay tuned for more guidance expected in the upcoming regulations.

Virginia Information Security Program

Code of Virginia

Table of Contents » Title 38.2. Insurance » Chapter 6. Insurance Information and Privacy Protection » Article 2. Insurance Data Security Act » § 38.2-623. Information security program

§ 38.2-623. Information security program.

A. Commensurate with the size and complexity of the licensee; the nature and scope of the licensee's activities, including its use of third-party service providers; and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's assessment of the licensee's risk and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

B. Each licensee's information security program shall be designed to:

1. Protect the security and confidentiality of nonpublic information and the security of the information system;

2. Protect against any reasonably foreseeable threats or hazards to the security or integrity of nonpublic information and the information system;

3. Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and

4. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction.

C. Each licensee shall:

1. Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee who is responsible for the information security program;

2. Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee; the nature and scope of the licensee's activities, including its use of third-party service providers; and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control;

3. Place access controls on information systems, including controls to authenticate and permit access only to authorized persons to protect against the unauthorized acquisition of nonpublic information;

4. At physical locations containing nonpublic information, restrict access to nonpublic information to authorized persons only;

5. Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures;

6. Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format;

7. Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

8. Provide its personnel with cybersecurity awareness training.

D. (In Respect to Board of Directors)

1. If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, require the licensee's information executive management or its delegates to (i) develop, implement, and maintain the licensee's information security program and (ii) report in writing (a) the overall

status of the information security program and the licensee's compliance with this article and (b) material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program.

2. If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate and shall receive a report from the delegate complying with the requirements of subdivision 1.

E. Beginning July 1, 2022, if a licensee utilizes a third-party service provider, the licensee shall:

1. Exercise due diligence in selecting its third-party service provider; and

2. Require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

F. Each licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

G. As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession; the licensee's information systems; or the continuing functionality of any aspect of the licensee's business or operations. Such incident response plan shall address:

1. The internal process for responding to a cybersecurity event;

2. The goals of the incident response plan;

3. The definition of clear roles, responsibilities, and levels of decision-making authority;

4. External and internal communications and information sharing;

5. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

6. Documentation and reporting regarding cybersecurity events and related incident response activities; and

7. The evaluation and revision, as necessary, of the incident response plan following a cybersecurity event.

H. Beginning in 2023 and annually thereafter, each insurer domiciled in the Commonwealth shall, by February 15, submit to the Commissioner a written statement certifying that the insurer is in compliance with the requirements set forth in this section, any rules adopted pursuant to this article, and any requirements prescribed by the Commission. Each insurer shall maintain for examination by the Bureau all records, schedules, and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems, or processes. Such documentation must be available for inspection by the Commissioner.

Virginia Insurance Data Security Act

The Virginia Insurance Data Security Act was enacted by the 2020 Virginia General Assembly.This legislation is modeled on the NAIC Insurance Data Security Model Law. The Act defines the requirements applicable to a licensee and establishes standards for data security, cybersecurity investigations, and notification to the Commissioner of cybersecurity events. It also provides the standards for notification to consumers, if applicable.

Email BOIDataSec@scc.virginia.gov to receive instructions for reporting a cybersecurity event or with any related questions.

Virginia Insurance Data Security Act Requirement Effective Dates

July 1, 2020

- Virginia Insurance Data Security Act becomes effective for cybersecurity events that occur on or after July 1, 2020.
- Licensees shall report cybersecurity events to the Commissioner of Insurance no later than 3 business days after determining that a cybersecurity event has actually occurred when certain criteria are met.
- Licensees subject to the Virginia Insurance Data Security Act shall implement Section 38.2-623 by this date. This section requires that licensees establish a comprehensive, written information security program by July 1, 2020.

July 1, 2022

- Licensees subject to Act who use the services of third-party service providers shall implement the provisions of Section 38.2-623 E by this date. This section details additional requirements for licensees who contract with third-party service providers that maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

February 15, 2023

- Beginning on this date, each insurer domiciled in Virginia must annually submit to the Bureau of Insurance a written statement certifying that the insurer is in compliance with the requirements set forth in Section 38.2-623. Domestic insurers required to submit a written statement will be contacted directly by the Financial Regulation & Solvency Division with further instructions prior to the February 15th deadline.

Cyber Event Notification Requirements

Instructions for Notification to the Commissioner of a Cybersecurity Event

• Licensees must notify the Commissioner of Insurance of any cybersecurity event that occurs on or after July 1, 2020.

• Licensees must notify the Commissioner as soon as possible but not more than three days after determining the occurrence of a cybersecurity event.

• To report an event, email the Bureau at: BOIDataSec@scc.virginia.gov.

• This email notification must include the name, telephone number, and email address of the licensee's designated contact for the cybersecurity event.

• The Bureau will provide the licensee with a secure site to provide updates on its investigation of the cybersecurity event.

• The licensee shall provide all the information required by § 38.2-625 of the Code of Virginia as its investigation proceeds.

• The licensee shall provide the Commissioner with the template of the notice it has provided to consumers if a notice is required by § 38.2-626 of the Code of Virginia

Virginia Code Data Security Related Sections

§ 18.2-186.6. Breach of personal information notification.

A. As used in this section:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

"Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

"Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

"Financial institution" has the meaning given that term in 15 U.S.C. § 6809(3).

"Individual" means a natural person.

"Notice" means:

1. Written notice to the last known postal address in the records of the individual or entity;

2. Telephone notice;

3. Electronic notice; or

4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of all of the following:

a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

c. Notice to major statewide media.

Notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a.

Notice required by this section shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the individual or entity to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Social security number;

2. Driver's license number or state identification card number issued in lieu of a driver's license number;

3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;

4. Passport number; or

5. Military identification number.

The term does 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.

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

1. Five digits of a social security number; or

2. The last four digits of a driver's license number, state identification card number, or account number.

B. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any

breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay.

Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

C. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

D. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.

E. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting

agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a (p), of the timing, distribution, and content of the notice.

F. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system.

G. An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.

H. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section.

I. Except as provided by subsections J and K, pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of this section. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.

J. A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.

K. Nothing in this section shall apply to an individual or entity regulated by the State Corporation Commission's Bureau of Insurance.

L. The provisions of this section shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.

M. Notwithstanding any other provision of this section, any employer or payroll service provider that owns or licenses computerized data relating to income tax withheld pursuant to Article 16 (§ 58.1-460 et seq.) of Chapter 3 of Title 58.1 shall notify the Office of the Attorney General without unreasonable delay after the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. With respect to employers, this subsection applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other non-employees.

Such employer or payroll service provider shall provide the Office of the Attorney General with the name and federal employer identification number of the employer as defined in § 58.1-460 that may be affected by the compromise in confidentiality. Upon receipt of such notice, the Office of the Attorney General shall notify the Department of Taxation of the compromise in confidentiality. The notification required under this subsection that does not otherwise require notification under this section shall not be subject to any other notification, requirement, exemption, or penalty contained in this section.

2008, cc. 566, 801; 2017, cc. 419, 427; 2019, c. 484; 2020, c. 264.

The chapters of the acts of assembly referenced in the historical citation at the end of this section may not constitute a comprehensive list of such chapters and may exclude chapters whose provisions have expired.

- **Article 2. Insurance Data Security Act**
  - § 38.2-621 Definitions
  - § 38.2-622 Private cause of action; neither created nor curtailed
  - § 38.2-623 Information security program
  - § 38.2-624 Investigation of a cybersecurity event
  - § 38.2-625 Notice to Commissioner
  - § 38.2-626 Notice to consumers
  - § 38.2-627 Powers and duties of the Commission; exclusive state standards
  - § 38.2-628 Confidentiality
  - § 38.2-629 Exceptions

Resources Provided by Virginia SCC

National Institute of Standards and Technology – NIST

- Cybersecurity Framework (PDF and Excel)
- Small Business Information Security (PDF)
- Risk Assessment SP 800-30 (PDF)
- Risk Assessment SP 800-39 (PDF)
- Information Security SP 800-53 (PDF)
- Information Security SP 800-171 (PDF)
- Incident Response SP 800-61 (PDF)
- NIST Educational Resources
  - Baldrige Cybersecurity Excellence Builder

    - Baldrige Cybersecurity Initiative
    - National Initiative for Cybersecurity Education (NICE)
    - NICE Resource Center

ISACA – COBIT Framework

- COBIT Toolkit
- ISACA Cybersecurity Training & Resources

SANS Institute – CIS Controls

- SANS CIS
- CIS Controls
- CIS Controls for Small & Medium Sized Enterprises
- Other SANS CIS Resources

International Organization for Standardization – ISO

- ISO 27000
- ISO 27001
- ISO 27002

Virginia Cyber Security Approach

This document provides an overview of Cyber Security in Virginia

---

Cyber & Data Security Training

Education and Training is a major component of a Cyber Security Program and is now required for compliance. Below are Resources that will help Agencies and other businesses develop Education and Training Programs.

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

Free and low cost online Cyber Security Training.

During this unusual time in our lives, many of us find we want to improve our knowledge, skills or even prepare for new career opportunities. If you are interested in cybersecurity careers, there are numerous online education providers to choose from. Many online courses are available from your local community college, four-year universities, even the prestigious Centers of Academic Excellence programs – please review all options.

The following links are for free and low-cost online educational content on topics such as information technology and cybersecurity. Some, not all, may contribute towards professional learning objectives or lead to industry certifications and online degrees. Please note that this site will continue to be updated as new information is gathered and edited for clarity and accuracy.

Career and Professional Development

Employee Awareness Training

Educator Training and Curriculum

K12 Education and Games

This page is continually updated. Please contact us for more information on how to add additional materials or to correct an error.

CAREER AND PROFESSIONAL DEVELOPMENT

Name and Hyperlink to Materials*	**Description****

Center for Development of Security Excellence Cybersecurity eLearning	Free cybersecurity eLearning courses for the *Department of Defense (DoD) and other U.S. Government personnel and contractors* within the National Industrial Security Program (NISP).
Chief Information Security Officer (CISO) Workshop Training	Training provided by Microsoft that includes a collection of security learnings, principles, and recommendations for modernizing security in your organization.
CompTIA	Free online training for CompTIA IT Fundamentals and other resources.
Critical Knowledge Explorer	CyberVista offering that includes more than 22 hours of free on-demand training and discounted labs covering Network Fundamentals, Threats and Attacks, and Network Security.

Cyberbit Range Remote Training	Free remote training for SOC teams, providing live, simulated cyberattacks on Cyberbit's cloud-based Cyber Range.
CyberTraining 365 Online Academy	Free courses and *low cost* subscriptions to help you master cybersecurity techniques such as Analyzing Malware, Penetration Testing, Advanced Persistent Threats, and much more. A low cost lifetime subscription is also available.
Cyber Skyline Professional	*Heavily discounted* scenario-driven cybersecurity labs/challenges *for students* (use .edu email to sign up). Over 100+ scenarios ranging from forensic analysis to offensive cybersecurity skills that are delivered on an on-demand platform with no time limits and a vibrant Slack community.

Cybrary	Free information technology and cybersecurity training portal.
EC-Council	Free resources for the information security community in the form of webinars, blogs, online video training, and much more.
Elastic	Free on-demand Elastic Stack, observability, and security courses.
Federal Virtual Training Environment (FedVTE)	Free online cybersecurity training for federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans.
Fortinet	Free access to the FortiGate Essentials Training Course and Network Security Expert courses.
Hacker101	Free class for web security.

Holistic Information Security Practitioner Institute (HISPI)	*Heavily discounted (use code HISPI-COVID-19)* online, on-demand Cyber Security Management Course.
Hopper's Roppers Security Training	Community built around a series of free courses that provide training to beginners in the security field.
IBM (hosted by Coursera)	Free (*7-day trial*) suite of courses on IT Fundamentals for Cybersecurity Specialization.
IBM Security Learning Academy	Free technical training for IBM Security products.
Infosec Skills	Free access *(7-day trial; low cost after trial)* to 500+ courses, 70+ learning paths, and 100+ browser-based labs for IT, security, and engineering professionals.

(ISC)2 Webinars and Courses	Free technical webinars and free courses for *(ISC)2 members ($125/year and pre-qualifications required)* to earn Continuing Professional Education (CPEs).
(ISC)2 Utilizing Big Data	Free course *for (ISC)2 members* (low cost for non-members) that provides an overview of Big Data components, architectures and applications.
ITProTV	Free membership (65+ hours of IT training content) and *low cost* memberships (4000+ hours of content, practice exams, and virtual labs). Free access to select CompTIA online courses for *educational institutions* during the Spring and Summer 2020 semesters – learn more.

Microsoft Cyber Security Architecture	Collection of best practices that is presented in a series of video trainings that provide clear actionable guidance for security-related decisions
Microsoft Technologies Training	Free security-related courses on Microsoft Technologies.
Mossé Cyber Security Institute	Sixty-five free exercises including Penetration Testing, Red Teaming, Security Tools, Cyber Defence, Governance, Risk, Compliance (GRC), and theory, concepts, and fundamentals of cyber security.
NICCS Education and Training Catalog	Database of free and *for pay*, online and in person courses.
NIST Cybersecurity Professional (NCSP) Awareness Training	*Low cost* course that introduces students to the basic concepts associated with Digital Transformation, Cybersecurity Risk Management, and the NIST Cybersecurity Framework.

Open P-TECH	Free digital learning on the tech skills of tomorrow.
Pluralsight	Free access to 7,000+ expert-led video courses and more during the month of April.
Project Ares by Circadence	Project Ares is a *low cost*, online, gamified learning platform that provides cybersecurity skill learning through hands on activities including concept-driven games and scenarios that emulate real-world networks and network traffic.
SANS	Free cybersecurity community resources and programs including white papers, webcasts, newsletters, tools/workstations, scholarship/community programs, templates, blogs, cyber ranges, and security posters.
SANS Cyber Aces Online	Free online course that teaches the fundamentals of cybersecurity including operating systems, networking, and systems administration.
Udemy	*Heavily discounted* online courses for various certifications.

Web Security Academy	Free online web security training.

EDUCATOR TRAINING AND CURRICULUM

Name and Hyperlink to Materials*	**Description****
CertNexus	Free online training for teachers and instructors for Cyber Secure Coder, Cybersec First Responders, and CyberSAFE. Additional resources for certifications and curriculum.
CLARK Center Plan C	Free cybersecurity curriculum that is primarily video-based or provide online assignments that can be easily integrated into a virtual learning environments.

Computer Security Education Resource Collection	Community-sourced collection of free resources related to computer security, cybersecurity, and information security education. The collection is primarily targeted at instructors looking for course materials.
CyberCIEGE Educational Video Game	Free network security simulation packaged as a video game with many scenarios, suitable for high school through graduate courses.
Labtainers Cyber Lab Exercises	Free Linux-based cybersecurity labs including automated assessment of student work, with over 50 labs prepackaged to run on student laptops.
M.E. Kabay	Free industry courses and course materials for students, teachers, and others are welcome to use for free courses and lectures.

National CyberWatch Center Cloud-Based Labs	*Heavily discounted* online labs tied to industry certifications and higher education courses; academic institutions and faculty only.
NCyTE Center Curriculum	Free cybersecurity curriculum and teaching resources for high school and college instructors. Materials can be incorporated into existing coursework or used to develop new classes.
TestOut's 2020 K12 Grant	Free TestOut courses *for K12 teachers. Application process required.*

EMPLOYEE AWARENESS TRAINING

Name and Hyperlink to Materials*	**Description****

Center for Development of Security Excellence Cybersecurity Catalog	Free security awareness resources for learners including games, posters, shorts, videos, and webinars.
Cyber Security for Remote Workers Staff Awareness E-learning Course	*Low cost* non-technical course help employees remain safe, and understand what to do if and when they experience a cyber attack or phishing scam.
CybSafe Remote Working Toolkit	Free (*3 months*) access to cyber security modules (including social engineering, public Wi-Fi, and device security) plus Assist (security FAQs, advice, and guidance) and Protect (interactive security behaviours and habits checklist) tools.
Email Security and Privacy Awareness Course	Free one-hour course to help raise awareness of email data security and privacy.

Information Security and Cyber Security Staff Awareness E-Learning Course	*Low cost* course aimed employees who are involved in processing information, use information technology in their daily job, or use the Internet as a means of conducting business.
Wizer Security Awareness Training	Free Security Awareness Training includes everything you need to train your employees how to protect themselves against cybersecurity attacks, it is 100% free forever with over 20 free videos, quizzes, employee progress reports, and certificates.
Phishing Staff Awareness E-Learning Course	*Low cost* phishing awareness training.

K12 EDUCATION AND GAMES

Name and Hyperlink to Materials*	**Description****

Career Explorations: Cybersecurity	Free cybersecurity curriculum for 5th - 10th graders.
Culture of Cybersecurity	Free downloadable kids activities to help your family learn basic cybersecurity concepts and defense strategies.
Fundamentals of Cybersecurity Information	Free *(sign up and use class code 2A4E1)* courses for middle and high school students.
NICERC at Home	Free activities and Capture the Flag challenges that teach foundational cybersecurity skills and introduction to cybersecurity careers.
Palo Alto Networks	Free activities, lessons and virtual environments that increase a students knowledge of cybersecurity through narrated content, interactions, demonstrations, and knowledge checks.

picoCTF	Free computer security game targeted at middle and high school students.

**Materials are related to coding, cybersecurity product training, certification preparation or general IT and cybersecurity skills development, and teacher training and curriculum.*

***Some of these materials may only be free or low cost (less than $100) for a limited time.*

For more information on how to add additional information or to correct an error, please email nice.nist@nist.gov.

NetDiligence® Mini Data Breach Cost Calculator

The Data Breach Cost Calculator is one of the most popular tools in the eRiskHub. Here we allow you to view a sample version that contains simplified results. The calculator allows you to run a scenario to see how much a data breach could potentially cost your company. Data breach costs can vary depending on the type of information lost, such as PII, PCI or PHI. The calculator breaks down the cost by incident investigation, customer notification costs and crisis management, regulator fines and penalties, PCI, and class action lawsuits. To learn more about

the full detailed version, please contact your insurance carrier or use the contact us link in the top right of the page.

Answer the questions in the first section. Click the 'Calculate' button to view your estimated costs based on your answers to these 7 questions.

Important Information: The numbers presented in the NetDiligence® Data Breach Cost Calculator are estimates and provided for education and illustration purposes only. Actual expenses and liability exposures due to identity theft or data breach incident may vary based on variables not considered in this calculator. Numerical results presented in the Data Breach Cost Calculator are based on a proprietary formula developed by NetDiligence and its insurance industry partners. This formula takes into account information available in the public domain and information obtained through various websites that track breach statistics. Please note: This calculator is not intended to predict insurable perils or related costs and has no bearing on any insurance policy.

NOTE: *Although this blog post was written in November 2017 and therefore, does not address the new Virginia Cyber Security Law, it does provide a good overview of the Cyber Security requirements and issues prior to July 1, 2020.*

What To Do First When Data Is Hacked:

A Guide To Mandatory Notification For Virginia Businesses

by JOLT | Nov 9, 2017 | Blog Posts

The following Blog Post was written by Spencer Allen and published November 9, 2017, on The Richmond Journal of Law and Technology (JOLT) an online law review Journal of The University of Richmond Law School.

By: Spencer Allen,

More than four-billion data records were stolen worldwide in 2016.[1] In 2014 alone, nearly half (47%) of U.S. adults had their personal information stolen.[2] Though it is the big hacks

that make the news- Yahoo (3 billion), Equifax (143 million), Verizon (6 million)—small and local businesses are no less vulnerable to data breach, and need to be ready to respond quickly when a breach happens.[3]

Virginia law requires businesses to notify affected parties in certain situations where personal data is compromised.[4] **Failure to give proper notice can be expensive—up to $150,000 *per breach***.[5] This article is intended to help Virginia businesses comply with mandatory notification procedures following a data breach.

I. What sorts of breaches require giving notice?

Virginia Code § 18.2-186.6 requires that companies give notice when each of five criteria are met: 1) unencrypted or unredacted; 2) personal information; 3) is accessed or acquired by an unauthorized person (or reasonably believed to have been accessed or acquired by an unauthorized person); 4) which causes identity theft or another fraud (or is reasonably believed to have caused or cause in the future identity theft or another fraud); 5) to any resident of Virginia.[6] Each of the five criteria must be analyzed to determine whether notice is required.[7]

1. **"Unencrypted or unredacted"**

"Encrypted" data is data that has been "scrambled" by an algorithmic process.[8] Though the precise way in which data is encrypted depends on the kind of data and the way in which the data is stored and sent, the basic idea is that an algorithm makes the data unreadable without a specific key (or series of keys).[9]

For example, imagine that we apply an algorithm that subtracts one from each number. If we apply the algorithm to an unencrypted number—4765—we arrive at an encrypted number of 3654. In this example we have no way of knowing that the unencrypted number is 4765 unless we have the key—that is, unless we know the algorithm. Without knowing the algorithm, the unencrypted number could be anything, and there is a low probability that we could figure it out by chance.

"Redacted" data is data for which identifying information or confidential information has been removed, and is thus not tied to a particular person or entity.[10] For example, imagine you come across a detailed medical record with no name attached. That data is considered "redacted" because without the identifying information the data is useless for anyone who would seek to exploit it. The data merely shows that someone, somewhere in the world has that medical history.

Basically, this first criteria for data that triggers mandatory notification is that it must be useable. The person who steals or otherwise acquires the data must be able to actually read what it says, and pair the data to particular persons or entities. If compromised data remains encrypted or is redacted, notification is not required by VA § 18.2-186.6.

2. **"Personal information"**

Though “personal information” may cover a lot of things, it is specifically defined in the statute.[11] To qualify as “personal information,” data must include:[12]

1. The first name or first initial
2. The last name
3. In combination with or linked to any of the following:
    - More than five digits of a social security number
    - More than the last 4 digits of a driver’s license number or state identification card number
    - More than the last four digits of a financial account number or credit card or debit card number in combination with any required security code, access code, or password that would permit access to the person’s financial accounts.

If the data that is stolen or compromised does not contain all three of the above, notice is not mandatory.[13]

3. **Accessed or acquired by an unauthorized person (or reasonably believed to have been accessed or acquired by an unauthorized person)**

Importantly, the statute does not require the data to have actually been stolen.[14] A company must comply with mandatory notice even if the company only has a reasonable belief that the data has been accessed or acquired by an unauthorized person.[15] “Reasonable belief” is subject to the court’s discretion.[16] The issue of reasonable belief as it relates to this statute has never been brought to trial, and thus it is better to err on the side of caution whenever a data breach is suspected.[17]

4. **“Which causes identity theft or another fraud (or the individual or entity reasonable believes has caused or will cause identity theft or another fraud)**

This part of the statute holds that mandatory notice is only triggered when an unauthorized person who receives personal data intends to misuse the data or actually misuses the data.[18] Just like the access requirement, actual identity theft or fraud does not have to occur to trigger mandatory notice, all that is required is a reasonable belief that identity theft or fraud has or will occur.[19] This allows effected parties to be notified as soon as possible—and hopefully before damage has been done. Again, as with access, if personal data is stolen it is best to err on the side of caution and assume that the data will be used for identity theft or fraud. Virginia crimes involving fraud are codified in Chapter 6 of Title 18.2 of the Code of Virginia.[20]

This part of the statute is important because it creates a carve-out so that accidental "good faith" breaches do not trigger mandatory notification.[21] For example, imagine that a business owner's mother-in-law, while snooping on her computer, opens a file called "business records." The file contains all of the transaction information from the business, including credit card numbers and personal information of customers. Without criteria four, this would trigger mandatory notification because 1) unencrypted; 2) personal information; was 3) accessed by an unauthorized person.[22]

However, because the business owner (hopefully) can trust that her mother-in-law will not use the information to commit fraud, this sort of breach does not trigger mandatory notification. The breach neither caused identity theft or fraud, nor would a person reasonably suspect that identity theft had or would happen.

5. **"To any resident of Virginia"**

Importantly, mandatory notice does not apply to persons or entities who are not residents of Virginia.[23] However, forty-eight states have mandatory disclosure statutes similar to the one in Virginia (all but Alabama and South Dakota).[24] If personal data concerning a resident of a state other than Virginia has been compromised, it is important to check the laws of that state to determine whether notice is required. For a complete list of similar state statutes, refer to appendix.

II. What happens if no notice is given?

If a company fails to give notice when it is required, the Attorney General may bring an action against it for up to $150,000 per breach. [25]

It is also possible that an individual could sue a company for damages arising out of a failure to give notice of theft of personal information.[26] This remains an unresolved legal question.[27]

III. To Whom Must Notice be Given, When, and What Must it Include?

If a data breach has occurred and it satisfies the above criteria, notice must be given "without unreasonable delay" following the discovery of the breach.[28] If the data is owned or licensed by the company where the breach occurred, notice must be given to 1) the Attorney General of Virginia; and 2) any resident of Virginia affected by the breach.[29]

Notice may be delayed if, after notifying a law enforcement agency, that agency determines that notification would impede a criminal or civil investigation, or homeland or national security.[30]

If the company where the breach occurred does not own or license the data that was compromised, that company must notify the owner or licensee of the data "without unreasonable delay" following discovery of the breach.[31]

1. **Notice to the Attorney General**

Notice to the Attorney General of Virginia must include:[32]

1. A cover letter on official letterhead notifying the VA Attorney General of the breach
2. Approximate date of the incident and how the incident was discovered
3. The cause of the breach
4. The number of Virginia residents affected by the breach
5. The steps taken to remedy the breach; and
6. A sample of the notification made to the affected parties, to include any possible offers of free credit monitoring.

Notice to the Attorney General may be addressed to:[33]
Computer Crime Section
Virginia Attorney General's Office
202 North 9th Street
Richmond, Virginia 23219

2. **Notice to affected persons**

Notice to affected persons must include:[34]

1. A description of the incident in general terms
2. The type of personal information that was accessed by the unauthorized person
3. A description of what the company has done to prevent further unauthorized access
4. A telephone number that the person may call for further information and assistance, if one exists; and
5. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notice to affected persons may be: 1) written to the last known postal address of the person in the records of the company where the breach occurred; 2) telephone notice; or 3) Electronic notice.[35]

If the cost of providing notice exceeds $50,000, or the number of Virginia residents to be notified is more than 100,000, or the company where the breach occurred does not have adequate contact information or consent to use the contact information, substitute notice can be used.[36] Substitute notice includes:[37]

1. E-mail notice

2. Conspicuous posting of the notice on the company website of the individual or the company
3. Notice to major statewide media

APPENDIX: A List of State Notice Statutes
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-545
Arkansas	Ark. Code §§ 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat. §§ 28-51-104 to -107

Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 *et seq*., 24-4.9 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. §§ 51:3071 *et seq*.
Maine	Me. Rev. Stat. tit. 10 § 1346 *et seq.*
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.,* Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500

Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801 *et seq.*
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19 *et seq.*
New Jersey	N.J. Stat. § 56:8-161 *et seq.*
New Mexico	2017 H.B. 15, Chap. 36 (effective 6/16/2017)
New York	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65
North Dakota	N.D. Cent. Code §§ 51-30-01 *et seq.*
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628
Pennsylvania	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 *et seq.*

South Carolina	S.C. Code § 39-1-90
Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053
Utah	Utah Code §§ 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9 §§ 2430, 2435
Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. §§ 40-12-501 *et seq.*
District of Columbia	D.C. Code §§ 28- 3851 *et seq.*
Guam	9 GCA §§ 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico §§ 4051 *et seq.*
Virgin Islands	V.I. Code tit. 14, §§ 2208, 2209

[1] Herb Weisbaum, *More Than 4 Billion Data Records Were Stolen Globally in 2016*, NBC (Oct. 31, 2017, 10:43 AM), https://www.nbcnews.com/storyline/hacking-in-america/more-4-billion-data-records-were-stolen-globally-2016-n714066.
[2] Jose Pagliery, *Half of American Adults Hacked This Year*, CNN tech, (Oct. 31, 2017, 10:47 AM), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/index.html.
[3] Matt Burgess, *That Yahoo Data Breach Actually Hit Three Billion Accounts*, Wired (Oct. 31, 2017, 10:51 AM), http://www.wired.co.uk/article/hacks-data-breaches-2017; Chris Morris, *14 Million US Businesses Are at Risk of a Hacker Threat*, CNBC (Oct. 31, 2017, 10:53 AM), https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html.
[4] Va Code Ann. § 18.2-186.6 (2017).
[5] § 18.2-186.6 (I)
[6] § 18.2-186.6 (B).
[7] *Id*.
[8] Lee Bell, *Encryption Explained: How Apps and Sites Keep Your Private Data Safe (and Why That's Important)*, Wired, (Oct. 31, 2017, 11:18 AM), http://www.wired.co.uk/article/encryption-software-app-private-data-safe
[9] *Id*.
[10] Rick Borstein, *Redaction in a Digital World*, Law Practice Today (Oct. 31, 2017, 11:39 AM), https://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/july11/redaction_in_a_digital_world.html.
[11] § 18.2-186.6 (A).
[12] *Id*.
[13] *Id*.
[14] § 18.2-186.6 (B)
[15] *Id*.
[16] *Id*.
[17] The only record of § 18.2-186.6 being brought before a court is in regards to a private suit. The case was dismissed for lack of standing. *Corona v. Sony Pictures Entm't, Inc.*, 2015 U.S. Dist. LEXIS 85865 (C.D. Cal. 2015).
[18] § 18.2-186.6 (B).
[19] § 18.2-186.6 (B).
[20] Va Code Ann. § 18.2-168-246.15 (2017).
[21] § 18.2-186.6 (B).
[22] *Id*.
[23] § 18.2-186.6 (B).
[24] Refer to Appendix.
[25] § 18.2-186.6 (I).
[26] *Id*.
[27] *Supra* note 17.
[28] § 18.2-186.6 (B).
[29] *Id*.

[30] *Id*.
[31] *Id*.
[32] Office of the Attorney General of Virginia, Database Breach Notification Requirements Updated July 1, 2017 (2017), https://www.oag.state.va.us/CCSWEB2/files/Data_Breach_Notification_Req.pdf.
[33] *Id*.
[34] § 18.2-186.6 (A).
[35] *Id*.
[36] *Id*.
[37] *Id*.

Related Blog Posts

The Skeleton of a Data Breach: The Ethical and Legal Concerns

BDM Publication Version PDF Cite as: Hilary G. Buttrick et al.,The Skeleton of A Data Breach: The Ethical and Legal Concerns, 23 Rich. J.L. & Tech. 2 (2016), http://jolt.richmond.edu/wp-content/uploads/volume23_article2_Buttrick.pdf. Hilary G. Buttrick,* Jason Davidson,** Richard J. McGowan*** Introduction [1] After over thirty data breaches spanning the third and fourth quarter of 2012, Forbes… December 2, 2016 In "Article"

Protecting Your Agency and Educating Your Clients

By Bill Fahy | **May 20, 2019, Insurance Journal West Magazine**

...And now agents must be aware of a new emerging risk: the compliance requirements being imposed upon them via their carrier and brokerage contracts due to their status as an affiliate of the carrier or brokerage.

Every Business Is a Target

When it comes to cybersecurity, there's much for agents to take in. A recent McKinsey article warns: "While awareness is building, so is confusion. Executives are

overwhelmed by the challenge [to defend themselves from cyberattacks]. Only 16% say their companies are well prepared to deal with cyber risk."

The report found that businesses are "at risk of collateral damage from untargeted malware and attacks on widely used software and critical infrastructure. And despite all the new defenses, companies still need about 99 days, on average, to detect a covert attack. Imagine the damage an undetected attacker could do in that time."

Cyberattacks touch businesses of all sizes and are now prevalent in small and medium sized businesses (SMBs), which often are not as proactive or well protected as larger businesses. Criminals know they are easy targets. According to a Hiscox 2018 Cyber Report, 47% of small businesses suffered at least one cyberattack in the past 12 months, and 44% of those suffered two to four attacks.

Spam, ransomware and phishing are currently the most common forms of cybercrime that small businesses face, and according to Inc. Magazine, "60% of small businesses fold within six months of a cyberattack."

These statistics not only show that independent agents need to protect their own business, but also that there is a growing market in commercial lines for agents, especially those who are educated on the risks associated with technology and systems, cybersecurity strategies and coverages available.

Agency Protection

Independent agents who don't have a cybersecurity strategy for their agency should invest in it now — before selling cyber protection policies to others. It is vital to protect clients as well as your own business. This includes building a strategy around protecting agency data other than a basic firewall. It's necessary to define agency data and prioritize the most classified information to be protected first, in addition to identifying where the agency is vulnerable before criminals do.

Along with building a strategy, training employees at all levels is essential. Employees, not systems, remain one of the greatest risks for businesses today. For example, phony emails that trick employees into compromising passwords and/or private information is a common entry point for hackers, who may gain access to agency funds as well as customer data.

The IIABA's ACT Agency Cyber Guide includes several tips for agencies to protect themselves and meet growing compliance regulations:

- Perform an in-depth risk assessment — what needs to be protected and why?
- Test and assess the vulnerability of your system.
- Develop internal and external written security policies, for staff and third-party service providers — educate every one *[SIC]* on these policies and procedures in the event of a cyberattack.
- Have an incident response plan — make sure everyone is on the same page and assign someone to be in charge of cyber attack responses.
- Conduct staff training and teach staff how to be vigilant.
- Implement Multi-Factor Authentication where needed so only permitted staff has access to critical files.

The Right Cyber Policy

Look for a policy that provides coverage against cyber extortion and offers proper limits to cover the myriad of post-breach response expenses, including legal fees, notification costs and reputational repair.

Solid, comprehensive cyber-related policies cover (and should be in place for agents and their clients):

- Data breach response and liability, including expenses and legal liability arising from a data breach.
- Computer attacks, such as a virus or other malware or denial-of-service attack that cause damage to data and systems.
- Network security liability, with defense and liability coverage for third-party lawsuits alleging damage due to inadequately securing a computer system.
- Media liability, including legal defense costs and damages for claims asserting copyright infringement and negligent publication of media while publishing content online.
- Funds transfer fraud, including losses from the transfer of funds as a result of fraudulent instructions from a person purporting to be a vendor, client or authorized employee.
- Cyber extortion, including "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm.
- Regulatory fines and penalties.

According to RPS Executive Lines Producer Adam Connor, "the average policy cost is roughly $2,900 annually. The cost of a standard Personally Identifiable Information (PII) attack without any coverage can reach over $232,000 and will grow significantly higher if the company is caught up in a lawsuit as a result of the breach. Just tallying the cost of a forensics investigation, security remediation, and a breach coach to give legal advice can total close to $170,000."

Risk Placement Services Inc. (RPS), for example, has comprehensive coverage plans offering up to $1 million of protection against a multitude of data breach risks, with higher limits available to qualified agencies. (Note: RPS is a strategic partner of SIAA and writes many cyber policies for and with SIAA member agencies.)

Selling Cyber Coverage

Cyber risk and data breach coverage is a fast-growing niche in commercial lines and should be considered by independent agents looking to expand their books of business. Selling the right coverage — to small and medium-size businesses like themselves — means agents need to be educated.

Well-educated independent agents will develop proactive cybersecurity strategies and invest in cyber coverage for their own agencies. They stay informed of the regulatory requirements in their state, and also continue to review their carrier and brokerage contracts for the compliance standards they are required to uphold. Then, they will be

able to provide the best information to their clients to prevent devastating losses and write a cyber policy tailored to their needs.

Ongoing cybersecurity means staying in the loop about risk management and training to keep both staff and clients informed, and being aware of an ever-changing threat that can negatively impact agencies and small businesses for years to come.

Cyber Security Plan Solutions

How Can Insurance Agents meet the new Data Security Compliance requirements and protect their agencies from the high costs of a data breach?

The Cyber Security compliance responsibilities along with enhanced data protection technologies and processes are most likely beyond the abilities of an Insurance Agency.

However, the Cyber Security Solution is not as bad as it may appear, thanks to companies and organizations that specialize in this field. Below is a summary outline of immediate steps that agencies can take to meet the new compliance responsibilities and to protect their clients and agencies.

A. **Get Educated on the New Law.** Use the resources within this document. Additional resources include the large Insurance Brokers and Wholesalers Burns & Wilcox and RPS as well as The Agency Technology Counsel (ACT) of Independent Insurance Agency Association of America (BIG I).

B. **An Important note:** Agencies must appoint a Cyber Security Officer that will manage the Plan; however, the Agency Principal will be ultimately responsible.

C. **Another Note of Caution:** Agencies need to be careful in the development of all written documents associated with the Security Plan including the required Data Security Manual, Training Manual, and Breach Response Manual. Agencies most likely will be held accountable for any processes and procedures; thus do not just copy a template and put the Agency Name on it. The Agency must be able to follow and to execute all processes and procedures included. Burns & Wilcox has developed Templates for all required documents that can be easily customized. They come with their Information Security Program.

D. **Get the NODE Total Information Security Solution Program from Burns & Wilcox.** **Burns & Wilcox** developed a proprietary Information Security Total Solution for our Virginia Agents at a heavily discounted price and will meet the Virginia Law compliance requirements and protect the agency should a breach occur.

   a. **Review the Burns & Wilcox NODE Information Security Program Options.**

   b. **GET APPLICATION:** **Download the Burns & Wilcox NODE Information Security Program Application** (No Underwriting & Heavily Discounted).

   c. **Learn More about the Burns & Wilcox NODE Information Security Program**

   d. **NODE International Cyber Security Policy & Services** from the NODE Website.

More Information and the NODE Information Security Program Application is available on the SmartChoiceVirginia.com website in the All Program BREAKING NEWS section.

Cyber Security Resources

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

Cyber Security Prevention & Breach Management Information by Ready.Gov

- Department of Homeland Security (DHS) (Link)
- Cyberattack Information Sheet (PDF)
- DHS United States Computer Emergency Readiness Team (US-CERT) (Link)
- DHS Stop.Think.Connect.™ Campaign (Link)
- United States Secret Service Electronic Crimes Task Force (Link)
- Federal Bureau of Investigation (Link)
- Department of Justice (Link)
- Federal Communications Commission (Link)
- Internet Crime Complaint Center (Link)
- Federal Trade Commission (Link)
- National Cyber Security Alliance (Link)
- National Center for Missing & Exploited Children's CyberTipline (Link)
- Internet Crimes Against Children Taskforce (Link)

- NetSmartz (Link)
- iKeepSafe (Link)
- iSafe (Link)

FCC Cyber Security Planner

FTC - A Security Guide for Business

FTC Cyber Security Policy Analysis

Identity Theft Resource Center

Research Statistics Data and Systems CMS Information Security

NAIC Legislative Brief: State Adoption MAP

Security Breach Notification Laws by State from NCSL

IBM Main Data Breach Cost Study--Annually