PRIVACY & DATA SECURITY 2019:
BUILDING A WRITTEN INFORMATION SECURITY PLAN

KARIN MCGINNIS AND TODD TAYLOR, MOORE & VAN ALLEN, PLLC
MIKE HOLLAND AND JEFFERSON PIKE, FORTALICE SOLUTIONS

February 21, 2019

Why a WISP?

- A WISP can help reduce security incidents.
- Some laws require a security plan.
- A WISP can help show compliance with other laws.
- A WISP (if implemented) can help defend against claims (*i.e.*, negligence).
- A WISP is useful in obtaining cyber insurance.
- Framework for testing your company's information security.

Fines under the GDPR – CNPD/Portugal

- **Barreiro-Montijo Hospital Center**
  - allowed others access to patient files that should have been reserved to physicians;
  - maintained 985 active physician accounts but only 285 doctors were active.
- **CNPD found**
  - hospital lacked technical and organizational measures necessary to ensure security of personal data (*e.g.*, lacked adequate internal rules for account creation and granting different levels of access to clinical information).
  - Violation of GDPR Article 5(1)(f).
- **€400,000 fine imposed**

Laws Requiring WISP or Data Security Procedures

State Data Security Laws

Currently, at least 22 states have some form of general data security requirement:

- Alabama
- Arkansas
- California
- Colorado
- Connecticut*
- Delaware
- Florida
- Illinois
- Indiana
- Kansas
- Louisiana
- Maryland
- Massachusetts
- Minnesota*
- Nebraska
- Nevada
- New Mexico
- Oregon
- Rhode Island
- Texas
- Utah
- Vermont*

Special State Legislation

SC Insurance Data Security Act
(S.C. Code §§ 38-99-10 to 38-99-100)

- Requires persons subject to licensing pursuant to S.C. insurance laws to develop, implement and maintain comprehensive written information security program containing administrative, technical and physical safeguards to protect NPI and the insurer's information system.

Ohio: WISP as Defense to Tort Claims

A. Affirmative defense under ORC §§ 1354.01- 1354.05 to tort actions alleging failure to implement reasonable information security controls if

- the covered entity creates, maintains, and complies with a risk based written cybersecurity program containing administrative, technical, and physical safeguards for protection of PI (and restricted information, if applicable), and
- program reasonably conforms to an industry recognized framework.

B. The program must be designed to:

- protect the security and confidentiality of the information;
- protect against any anticipated threats or hazards to the security or integrity of the information; and
- protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

ORC: Reasonable Industry Standards

A. Frameworks/Standards:

- NIST *Framework for Improving Critical Infrastructure Cybersecurity*;
- NIST Special Publication 800-171;
- NIST Special Publications 800-53 and 800-53a;
- FedRAMP *Security Assessment Framework*;
- CIS *Critical Security Controls for Effective Cyber Defense;*
- (ISO) 27000 Standards.

When a final revision to a framework is published, a covered entity whose cybersecurity program reasonably conforms to that framework must reasonably conform to the revised framework not later than one year after the publication date stated in the revision.

B. If already regulated by federal or state law (GLBA, HIPAA, HiTECH or FISMA), compliance with any cyber security requirements of that program suffices.

C. Compliance with BOTH current versions of PCI-DSS and the standards in A.

State Data Security Laws

- Most states simply require that the entity implement and maintain reasonable security practices appropriate to the nature of the information to protect from unauthorized access, destruction, use, modification or disclosure.
- AL, CT, MA, NV, OR and VT have more robust requirements.
- AR, CA, CO, IL, MD, NE, NV, NM and RI require entity to impose obligations on vendor/service provider.
- CT, MA and VT require WISP.

Alabama

Reasonable security measures = security measures practicable to implement and maintain, including consideration of all of the following:

- Designation of employee to coordinate security measures to protect against breach;
- Identification of internal and external risks of a breach;
- Adoption of appropriate information safeguards to address identified risks of a breach, and assess the effectiveness of such safeguards;
- Retention of service providers that are contractually required to maintain appropriate safeguards for sensitive personally identifying information;
- Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information;
- Keeping management of the covered entity appropriately informed of the overall status of its security measures.

Ala. Code 8-38-3 (Section 3)

- Secure disposal of personally identifiable information (Section 10).

Massachusetts Standards for the Protection of Personal Information (*201 CMR §§17.01 & 17.03)*

- Imposes detailed obligations on person or entity that owns or licenses personal information (paper or electronic) of Massachusetts residents to develop, implement, and maintain a comprehensive written information security program.

- These are minimum standards.

Massachusetts Standards for the Protection of Personal Information (*201 CMR §17.03(1)*)

Must contain administrative, technical, and physical safeguards that are appropriate to:

- the size, scope, and type of business;
- the amount of resources available;
- the amount of stored data; and
- the need for security and confidentiality of both consumer and employee information.

Massachusetts Standards for the Protection of Personal Information (*201 CMR §17.03(2)*)

Every information security program shall include:

- *Responsible Persons*
- *Risk Assessment*
- *Employees/Employer Training*
- *Discipline*
- *Limit Access by terminated employees*
- *Vendor Oversight*
- *Restrictions on Physical Access*
- *Monitoring of the program*
- *Audits*
- *Security Incident Documentation*

Massachusetts – New

- Massachusetts data breach statute amendment effective April 11, 2019.
- Requires data breach notice (to consumers and regulators) stating whether the company has a WISP.
- Means regulators will know if the company is not complying with the WISP requirement under state law, and the company will face fines/penalties.

NC State Bar 2011 FEO 7: States that a lawyer has

- affirmative duties to educate himself regularly as to the security risks of online banking;
- to actively maintain end-user security at the law firm through safety practices such as strong password policies and procedures, the use of encryption and security software, and the hiring of an information technology consultant to advise the lawyer or firm employees; and
- to insure that all staff members who assist with the management of the trust account receive training on and abide by the security measures adopted by the firm.

EU General Data Protection Regulation

Article 32 of the **GDPR** requires the following:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement* ***appropriate technical and organisational measures*** *to ensure a level of security appropriate to the risk … account shall be taken in particular of the risks that are presented by processing … which could lead to physical, material or non-material damage."*

GDPR, Art. 32

- Measures to ensure an appropriate level of security include:
  - *Encryption:* the pseudonymisation and encryption of personal data;
  - *Systems:* the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - *Restoration:* the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - *Auditing:* a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

  GDPR, Art. 32(1)(a)

- Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may demonstrate compliance.

  GDPR, Art.32(3)

Gramm-Leach-Bliley Act (15 USC §6801)

- Requires financial institutions to implement safeguards to protect consumer information.
- Individual regulators have imposed detailed regulations and guidance regarding information security program requirements (*e.g.*, Interagency Guidelines Establishing Information Security Standards).
- Reasonable technical, physical and administrative protections include:
  - *Responsible Person:* designation of one or more employees to coordinate the program;
  - *Risk Assessment:* conducting risk assessments;
  - *Safeguards*: implementation of safeguards to address risks identified in risk assessments;
  - *Vendors:* oversight of service providers; and
  - *Auditing*: evaluation and revision of the program in light of material changes to the financial institution's business.

NY Dept of Financial Services (NY DFS) Cybersecurity Regulations (23 NYCRR Part 500)

- Effective March 1, 2017.
- Applicable to entities that are subject to licensing by NY DFS.
- Covered entities are required to maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of the company's information system.
- Requires procedures and policies to protect information systems and nonpublic information on the systems.

NY DFS Cybersecurity Regulations (23 NYCRR Part 500)

Components:

- Risk assessment
- Incident response
- Info security
- Network and systems security
- Data governance/classification
- Access controls/id management
- Continuity/disaster recovery
- Continuity/disaster recovery
- Systems/network monitoring
- Physical security
- Vendor management
- Data disposal

PCI-DSS

- Requirements Imposed by Major Card Brands with regards to protection of Cardholder Data.

- Applies to ***all*** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers.

Other Federal Laws for Reference

- HIPAA Security Rule – Requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- Federal Trade Commission Act, Section 5(n) – Defines an unfair act or practice as an: *"act or practice [that] causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."*
  - The FTC has brought claims under the *unfairness* prong of Section 5(a) based on failure to have adequate data security measures – though many of these cases ended in settlement (*e.g.*, U.S. v. Choicepoint, Civ. Action No. 1 06-CV-0198 (ND Ga. 2006)).
  - Security program is often part of consent decrees/settlements with FTC (*e.g.*, *Uber*).

- FTC Start with Security: A Guide for Business – Offers ten lessons learned from its data security enforcement actions, with practical guidance on how to reduce risks for all businesses.

DRAFTING A WISP

Process – Risk Assessment

- Types of information held, applicable laws and potential vulnerabilities.
  - Valuable to have a third party certified entity perform it.
- Consider industry data (*i.e.*, Advisen) showing higher targeted industries – healthcare, finance and insurance – because value of data.
- What higher risk practices does the business engage in?
  - *e.g.*, if frequent wire transfers, consider BECs/wire fraud.

Example: BECs and Ransomware

- BECs are happening regularly in the Carolinas
  - Fortalice has worked cases with MVA Law - BEC and cyber fraud
  - Companies need a cybersecurity process to follow
  - Awareness of phishing, proper cyber tools and a foundational cybersecurity program are critical
- Ransomware— is also happening here – just ask the IT team at Mecklenburg County
  - Practice a digital disaster before one occurs, not as it happens
  - Take steps to prevent: increase password protections, change open remote port from the default port, multifactor authentication
- Then Audit and Monitor for compliance

What Should a WISP Look Like?

- Can be all-in-one plan or general plan with references to various policies.
- General plan with separate policies easier to administer and update.
- Mark Confidential & Proprietary

Components of a WISP

- Purpose
- Scope
- Definitions
    - Personal Information
    - Sensitive Information
- Identify Qualified Responsible Person
- Provisions for Risk Assessment
- Outline Info Sec Policies
    - access controls
    - Password policies
    - Security patches
    - network segmentation
    - multi-factor authentication
    - multi-factor authentication
    - encryption
    - Firewalls
    - Log maintenance
    - Backups/disaster recovery

Components of a WISP (cont.)

- Safeguards
  - Administrative (policies)
  - Technical (*i.e.*, anti-virus software, encryption)
  - Physical (secure premises, clean desk rules, locks)
- Vendor/TP service provider management (contracts, requirements)
- Incident Response Plan
- Training
- Data disposal
- Audit/Review of Plan, policies
- Monitoring
- Enforcement (discipline if violation)
- Effective Date of Plan and updates

Ancillary Policies

- Data Incident Response Plan
- Technology/Internet/Computer Use Policies
- Record Retention/Disposal Policies
- Vendor Management Policies
- Security Awareness Training Policies
- Password Policies
- Facility Access Policies

Jefferson Pike, Fortalice Solutions, LLC

Director, Cyber Risk & Compliance at Fortalice Solutions, LLC

Jefferson Pike is a forerunner in the field of cyber risk analysis and management. A veteran of the U.S. Navy, he has twenty years of professional experience leading risk management teams, assessing the information security posture of organizations and their vendors, and developing business performance standards, policies and procedures.

Throughout Jefferson's career, he has held multiple leadership positions, including IT Senior Lead Auditor for Wells Fargo, Manager of IT Risk Management for Spectrum, Cybersecurity Risk Analyst, NOC Manager for BellSouth Telecommunications, and Enlisted Surface Warfare Specialist in the U. S. Navy.

Fortalice

Jefferson Pike, Fortalice Solutions, LLC

In his role as Director of Cyber Risk and Compliance for Fortalice Solutions, Jefferson leads the Commercial Risk Team, and applies his skill set and knowledge to delivering solutions and services to clients. His Fortalice duties include performing cyber risk assessments to determine the security posture of organizations; assisting client's technical and non-technical staff in implementing or optimizing new cybersecurity capabilities such as vulnerability management, incident response, and governance programs or initiatives; developing custom risk frameworks, policies and procedures; performing cost/benefit analysis and providing clear recommendations based on the specific client environment; and leading a team of junior analysts in the completion and delivery of client solutions.

Jefferson earned his Bachelor of Science Degree in Management from Montreat College, and graduated from the University of Maryland University College with his Master of Science in Cybersecurity, as well as an MBA.

Fortalice

Mike Holland, Fortalice Solutions, LLC

Executive Vice President of Client Relations

Mike Holland is a strategic business development executive with an earned record of professional success in international business development, clientele management, and employee training and education. As Executive Vice President of Client Relations for Fortalice Solutions, Holland is responsible for all private sector client partnerships. He ensures client satisfaction for all cyber-related work; and serves as liaison between the technical team and client business risk owners, including boards and C-suite executives.

Fortalice

Mike Holland, Fortalice Solutions, LLC

An ambitious and savvy entrepreneur, Holland founded the Blue Line Group, a company which specializes in business development and sales consulting. At Blue Line, he served as president and assembled an impressive clientele which included a European software company, an energy conservation firm, and an Asian original design manufacturer.

Holland has driven multiple sales channels to exceed quota, led supply chain teams, and taken ownership of vendor relationships, showing himself to be a vastly capable and versatile leader. His incredible work ethic caught the attention of The Charlotte Business Journal and earned him the 40 Under 40 Award (2006), which recognizes top business leaders in the Charlotte area.

Fortalice

Mike Holland, Fortalice Solutions, LLC

Holland has served in the position of Vice President for multiple companies, including Ubee Airwalk (VP of Business Development for Europe and the Americas) and Mobinnova (VP of Business Development) where he oversaw the development of beneficial business relationships, engineered successful planning and execution of sales strategy to increase company growth and provided leadership and direction. In his position as Area Vice President of Sales and Operations for AT&T Wireless, Holland owned P&L in excess of $275M and earned three Circle of Excellence Awards, a peer-to-peer award given to the top 2% of the company's 35,000+ employees.

Mike Holland is a graduate of Auburn University, where he earned his Masters of Business Administration and Bachelors of Science in Finance. He also completed the Southwestern Bell Communications Leadership Development Program in 1992, and holds a certificate from the Center for Creative Leadership in "Developing the Strategic Leader".

Fortalice

Attorney Contacts

Karin McGinnis
Member
704.331.1078
karinmcginnis@mvalaw.com

Todd Taylor
Member
704.331.1112
toddtaylor@mvalaw.com

Moore&VanAllen

Questions