Sprint 4 Summary:
Legal, Regulatory, and Compliance Implementation on Security Controls

Cyber Security & Networking , The Knowledge House, May 21, 2023
Instructor: George Robbins

For a non-profit organization, legal and regulatory compliance with regards to data security refers to the NPO's adherence to laws and regulations that govern the handling and protection of confidential data. These laws can include federal legislation such as the Gramm-Leach-Bliley Act (GLBA) or state-specific legislation like New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act. Regulatory compliance, on the other hand, typically pertains to rules and guidelines set forth by industry-specific bodies, which may include frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and standards such as the Payment Card Industry Data Security Standard (PCI DSS). Compliance is essential for non-profits as violations could result in substantial fines, reputational damage, and loss of trust among donors, partners, and beneficiaries. A robust cybersecurity program is integral to ensuring and maintaining this compliance, as it serves to prevent unauthorized access, detect potential threats, respond to incidents, and recover from breaches efficiently and effectively. Such a program typically aligns with both legal and regulatory standards, thereby helping the non-profit to avoid penalties and continue its mission.

State laws around cybersecurity exist to protect the sensitive information of individuals and organizations from unauthorized access, use, or disclosure. Cybersecurity laws aim to establish standards, guidelines, and requirements for the protection of data and to ensure that organizations take appropriate measures to safeguard information from cyber threats and data breaches.

This summary seeks to focus on the legal, regulatory, and compliance implementations on security controls in the context of creating a secure program for The Knowledge House. Through a few of the laws and regulations, with an emphasis on the Payment Card Industry Data Security Standard (PCI DSS), this summary also aims to outline the essential legal and regulatory frameworks that will guide the secure program's implementation and launch strategy.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all entities involved in payment card processing handle cardholder data securely. Established in 2004 by major payment card issuers, such as VISA and MasterCard, the PCI DSS was conceived to consolidate various industry data security standards into one unified framework for safeguarding cardholder data (PCI Security Standards Council, 2021; Vijayan, 2007). It emphasizes six crucial components: building a secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy (PCI Security Standards Council, 2021).

Medium-sized non-profit organizations such as The Knowledge House, which process card payments—most commonly for donations—must adhere to the PCI DSS. This means they are obligated to implement robust network security measures, encrypt cardholder data, regularly update anti-virus software, restrict access to cardholder data, monitor network resources, and develop an information security policy (Williams, 2016; PCI Security Standards Council, 2021).

Compliance with the PCI DSS carries substantial implications for non-profit organizations. Aside from avoiding monetary penalties and elevated transaction fees associated with non-compliance, adherence to the PCI DSS safeguards the organization against reputational damage and potential loss of credit card privileges resulting from data breaches (Fenton, 2018; Gibson, 2018). Additionally, it helps foster

trust among donors and stakeholders, thereby facilitating the organization's fundraising efforts.

The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act is a data security and breach notification law enacted in New York State. It was signed into law on July 25, 2019, and it became effective on March 21, 2020. The SHIELD Act aims to enhance data security practices and protect the personal information of New York residents. The SHIELD Act applies to any person or business that owns or licenses computerized data that includes personal information of New York residents, regardless of whether they conduct business in New York. It applies to both small and large businesses, including organizations outside of New York State that handle the personal information of New York residents. The New York SHIELD Act reinforces the importance of data security and breach notification, aiming to protect individuals' personal information and promote data privacy. It serves as a reminder for businesses to implement comprehensive data security measures and promptly respond to data breaches.

GA/SS-08-016 refers to a document or guideline related to Computer Operations Center Security in the state of Georgia. The specific details and contents of GA/SS-08-016 are not readily available in my training data, as it pertains to a specific state-level security guideline. However, the reference you provided, NIST SP 800-12 Information Security Handbook (Chapter 15), indicates that GA/SS-08-016 is likely a security standard or guideline based on the recommendations outlined in Chapter 15 of the NIST Special Publication 800-12.

The General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy law that was implemented by the European Union (EU) on May 25, 2018. It replaced the Data Protection Directive 95/46/EC and is designed to harmonize and strengthen data protection laws across EU member states. The key objectives of the GDPR are to enhance the rights of individuals regarding their personal data and to

establish clear responsibilities for organizations that collect, process, and store personal data. Some key aspects of the GDPR include:

The GDPR significantly strengthens the rights of individuals regarding their personal data and imposes strict obligations on organizations that handle such data. It aims to protect individuals' privacy, enhance data security, and establish a consistent and high standard of data protection across the EU.

New York General Business Law (GBL) §899-aa, also known as the New York State Data Breach Notification Law, is a statute that establishes requirements for businesses operating in New York State in the event of a data breach involving personal information. Failure to comply with the provisions of GBL §899-aa can result in penalties and enforcement actions by the New York State Attorney General's Office, including monetary fines. It's important to note that laws can be amended or updated, so it's advisable to consult the official sources or seek legal advice to ensure you have the most accurate and current information regarding GBL §899-aa.

The New York Nonprofit Revitalization Act (NPRA) is a law enacted in 2013 that introduced significant reforms and modernizations to the governance and operations of nonprofit organizations in the state of New York. The NPRA aims to enhance transparency, accountability, and effectiveness in the nonprofit sector. The New York Nonprofit Revitalization Act applies to most nonprofit organizations incorporated or operating in the state of New York, regardless of their size or purpose. It is designed to strengthen the governance and operations of nonprofit organizations, ensuring they fulfill their missions effectively, maintain public trust, and operate in accordance with best practices. It's important to note that while this information is based on the knowledge available up to September 2021, the NPRA may have undergone amendments or updates since then. To obtain the most accurate and current information, it is recommended to consult the official sources or seek legal advice regarding the New York Nonprofit Revitalization Act.

When it comes to non-profit educational programs, they often handle and store sensitive information, including student records, personal data of staff and volunteers, financial information, and potentially research data. This makes them valuable targets for cybercriminals seeking to exploit vulnerabilities and gain unauthorized access to this information. Therefore, it is imperative for organizations like The Knowledge House to have a cybersecurity program that is in alignment with legal and regulatory requirements such as the PCI DSS. Not only does such adherence secure the organization and its confidential data from potential cyber threats, but it also reinforces donor and stakeholder faith and trust, crucial elements for non-profits to sustain and further their mission.

References:

Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk

Gibson, J. (2018). The Consequences of PCI DSS Non-Compliance. Tripwire. Retrieved from https://www.tripwire.com/state-of-security/regulatory-compliance/pci/consequences-of-pci-dss-non-compliance/

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

New York State. (2020). Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). https://www.nysenate.gov/legislation/laws/GBS/899-AA

United States Congress. (2002). Federal Information Security Management Act of 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf