**Design a Cybersecurity Legal Program**

Jose Flores

CSOL-540-01-FA22: Cybersecurity Law & Privacy

Dr. Michelle Moore

October 24, 2022

TN-Tech is a tactical network retail company that started by producing only switches and routers locally. The company has rapidly grown and produces radios, motherboards, and other products used to develop a network system nationally and internationally. With the company’s national and international sales being made online, it is paramount to consider local, state, federal, and international laws. Designing and implementing a cybersecurity law program will reduce the chances of losses due to criminal activity and civil litigation and include cybersecurity liability insurance in case the legal efforts are not won in court.

**Duties**

The TN-Tech leadership team has multiple duties to abide by to ensure the best practices are being done to protect the client’s information. These duties include Duty of Care, Failure to Act, and Reasonable Person Doctrine. The Duty of Care Doctrine is a cybersecurity tort law that includes: the duty to provide reasonable security, reveal security breaches, accurately disclose safeguards, and protect information (Schreider, 2020). The duty to provide reasonable security is identifying foreseeable threats and taking action to implement security controls and policies to protect customers. The duty to reveal security breaches is notifying the customers that their data has been compromised due to a security breach. The leadership team must elaborate on what security controls were put in place when the breach occurred. The duty to accurately disclose safeguards is, to be honest with the security controls used to protect data. The management’s statements and disclosure will represent the value of the company’s integrity. The duty to protect information is to take steps to safeguard customers’ or confidential information. The Duty of Care Doctrine is a standard that the leadership team should understand to avoid civil lawsuits.

The Failure to Act Doctrine is another cybersecurity tort law that includes: failure to act duty, failure to warn duty, and Good Samaritan law. The failure to act duty is not taken the required steps to ensure the sensitive information is safeguarded. The failure to warn duty is initially not warning the known danger to others. The Good Samaritan law is not sharing information about cyber threats with other organizations. Sharing information with other entities will increase situational awareness and possibly create a solution to prevent future cyber attacks. The Reasonable Person Doctrine ensures that the leadership team has the average amount of skills, care, and judgment to perform their duties (Schreider, 2020). Ensuring the person has proper standards will be the critical difference between negligence and accident.

**Laws**

Payment Card Industry- Data Security Standard (PCI-DSS) is a uniform security standard used to combat credit theft and fraud (Schreider, 2020). It was created in 2004 by four credit card companies: Visa, Mastercard, Discover, and American Express (TechTarget, 2020). The standard has six objectives and twelve requirements to ensure that the best practices are being utilized to protect customer data. These security standards provided by PCI-DSS are baseline security controls that may be applied anywhere where payment card processing is involved. A few requirements to be PCI DSS complaints include maintaining a firewall, encrypting data at rest/transit, and maintaining systems. Customer trust can be established by ensuring they are protected from unauthorized charges (Morse & Raval, 2008).

General Data Protection Regulation (GDPR) is Europe's data privacy and security law that applies to anyone who collects data related to those residing in the European Union (EU) (GDPR, 2022). This regulation is paramount because TN-Tech online sales are open to any country, including the EU. GDPR requires no more than 72-hour notification to the supervisory authority if a personal data breach occurs (GDPR, 2018). This notification requires an in-depth explanation of how it happened, who is involved, and what actions were taken to address and mitigate the breach.

The Data Security and Breach Notification Act of 2015 is a federal data breach act designed to protect consumers (Schreider, 2020). This law requires rational security policies and procedures to protect Personally Identifiable Information (PII). It also requires disclosing to the public if their PII has been involved in a breach, just like the GDPR in Europe. The Personal Data Notification and Protection Act requires businesses to report breaches by size (Schreider, 2020). Each state has different data privacy laws and court procedures depending on where the organization resides.

**Frameworks**

The National Institute of Standards and Technology (NIST) cybersecurity framework has five critical components to build a successful framework. These components are: Identity, Protect, Detect, Respond, and Recover (NIST, 2018). Each component has multiple special publications to refer to and utilize while building the cybersecurity framework. The special publications can be guided to specific companies’ goals or concerns. The NIST cybersecurity framework is essential because it will implement data-safeguarding standards that may also be used as GDPR complaints. The International Organization for Standardization (ISO) Security Standards is a framework that provides best practices for managing risk, response plans, and security programs (Schreider, 2020). Implementing the best practices in a response plan is paramount to reducing the exposure in case of a data breach.

**Potential Impacts**

Every day, technology is growing by becoming faster and physically smaller. The Internet of Things (IoT) is a device that may connect to the internet (AWS, 2021). IoT has the potential to send data through the internet and connect itself with different hosts. The potential impact of multiple IoT is the possibility of a Denial of Service (DoS) attack on an organization. IoT devices may not have security accommodations because they were not designed that way (Schreider, 2020). IoT collects data to develop trends for daily tasks such as regulating temperatures, power on/off, and other similar functions. If bad actors obtain this data, they may use it to plan their attacks effectively on the organization.

Cybersecurity legislation is being updated and written to keep up with emerging technology daily. Due to new laws implemented, an encryption standard or protocol used today may not be allowed the next day. Being involved in a cybersecurity intelligence community will help spread awareness about new regulations being implemented for similar organizations. The Cyber Incident Reporting For Critical Infrastructure Act of 2022 (CIRCIA) brings similar cybersecurity organizations together to help resolve conflicts (CISA, 2022). The business being done between different countries is as important as the business in the United States. Some laws and regulations need to be followed when doing transactions or providing a service. Each country has different agreements to ensure they understand and respect each other's concerns. Disagreeing or not following these agreements may cause international conflict and cut business ties.

**Cybersecurity Insurance**

With multiple technical controls implemented in an organization, it is still hard to predict equipment failure and a well-organized attack. A cyber liability insurance policy will cover various topics, such as network security and privacy. With the increasing use of IoT daily, it is essential to consider network security insurance. A local coffee shop wifi hotspot can be hacked, and use all the IoT connected to the network to create a DoS. Equipment failure is unpredictable because it may be a user error or a supply chain defect. The network security liability insurance covers equipment failure and denial of service attacks (Schreider, 2020). The privacy insurance covers physical records being exposed by theft, loss, or accident (Schreider, 2020). A careless employee may improperly dispose of physical records without adequately destroying them. An organization may face a hostile event in which the robber steals documents instead of currency.

**Recommendations**

Following the NIST cybersecurity framework will ensure we follow the best cybersecurity practice. Identifying key roles in who would be managing systems, assets, and data. The individuals selected should understand their duties and responsibilities to ensure the company stays within compliance. Conducting audits and risk assessments monthly will help improve the security of the systems. Developing and implementing security controls to protect the infrastructure. Security controls such as encryption, awareness and training, least privilege, separation of duties, access control, and multi-factor authentication (MFA) are all critical to protecting assets and meeting standards. The implementation of procedures and security controls to detect cybersecurity events from occurring include intrusion detection systems, security guards, and vulnerability scanning. After detecting the cybersecurity event, responding effectively to contain that event is paramount. Creating a response plan and identifying the roles of each person may reduce the damage.

Communicating with those affected is essential to disclose and is a duty of professionals. Once the actions have been taken to contain the event, recovery and lessons learned are crucial to discuss with the organization. Understanding where it went wrong can prevent future incidents. Preserving digital evidence using volatility’s order can help further pinpoint how the incident occurred. Implementing a chain of custody procedure with help the organization win cases if done correctly. The chain of custody must be strict in protecting and tracking the whereabouts of the evidence.

Policies and procedures are being revised and updated constantly due to recommendations to meet new standards. Creating a checklist to revise each policy, procedure, and law will help maintain compliance within the organization. By hiring a third-party assessor, they can check standards and security controls to give a nonbias option to the organization. Including multiple framework, security standards will create a foundation for the organization and increase the security standards. Assigning roles and responsibilities to individuals will divide the duties and develop a point of contact in case an issue arises. With multiple technical and administrative controls in place, cybersecurity insurance is still essential because there are various factors we cannot control.

References

AWS. (2021). *What is IoT*. AWS. Retrieved October 24, 2022, from https://aws.amazon.com/what-is/iot/

CISA. (2022). *CISA welcomes input on New Cyber Incident Reporting Requirements*.

Cybersecurity and Infrastructure Security Agency CISA. Retrieved October 23, 2022, from https://www.cisa.gov/news/2022/09/09/cisa-welcomes-input-new-cyber-incident-reporting-requirements

GDPR. (2018). *Notification of a personal data breach to the supervisory authority*. General Data Protection Regulation (GDPR). Retrieved October 23, 2022, from https://gdpr-info.eu/art-33-gdpr/

GDPR. (2022). *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. Retrieved October 23, 2022, from https://gdpr.eu/what-is-gdpr/

Morse, E. A., & Raval, V. (2008). *PCI DSS: Payment card industry data security standards in context*. Science Direct. Retrieved October 23, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S0267364908000976?via%3Dihub

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. NIST. Retrieved October 25, 2022, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Schreider, T. (2020). Cybersecurity Law, standards and regulations. Rothstein

Publishing.

TechTarget. (2020). *What is PCI DSS (payment card industry data security standard)*. TechTarget. Retrieved October 24, 2022, from https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard