Daniel Weinert
CIS-4450
7/09/2022

Domain 1.5:

Understand legal and regulatory issues that pertain to information security in a holistic context

Understanding the legal and regulatory requirements for an organization or enterprise can be a huge challenge. Depending on the size and scope of the business, there can be countless laws from the local and state level up to the federal and international level that could impact the organization. In order to stay compliant with such regulations the business needs a clearly defined scope and know exactly in what locations its operating and to what extent. A lot of the regulations pertain to data, more specifically personal identifiable information or PII. Almost every person that comes in contact with an organization either through employment or business will probably have some kind of PII collected and stored. An organization needs to make sure that they have a compliance team made up of legal and technical people to ensure that collecting and storing such information is lawful. The legal side of things make sures that everything is going lawful specifically to the legal text and that the organizations is allowed to record the PII in the first place for example. The technology side of it will make sure that requirements from legal texts are actually carried out as interpreted by the legal people. Some regulations might require technical controls such as encryption or specific policies like retention schedules. The nature of the data collected is also a major determining factor of which regulations apply, data such as health information or payment/credit card information have their own stringent requirements to them and laws to follow such as the Health Insurance Portability and Accountability Act (HIPPA) and the Payment Card Industry-Data Security Standards (PCI-DSS). The type of entity or physical location of the person that the data is collected from also plays a huge role, someone from California might be governed under the California Consumer Privacy Act (CCPA) even if the organization doesn’t have any physical location in California, or

if you are dealing with the government an organization might have to adhere to the Federal Information Security Modernization Act (FISMA) and other regulations.

Cybercrime is another topic that plays a huge role in policy making and general cybersecurity. Every organization is dealing with threats from cybercriminals such as potential breaches that steal data or denial of service attacks that shut down business. Some of such crimes are covered by criminal laws and regulations in some countries but not all. Companies also need to be aware of certain breach notification laws that pertain to specific data in case they experience an incident. Cooperation between countries and places can also be hard to an organization that is multinational since the laws and attitudes towards cybercrime can change a lot. One of the only international actions against cybercrime is the Council of Europe's Convention on Cybercrime with aims to make investigations easier on an international level by coordination laws and communication channels between law enforcement.

Last big topic in 1.5 is the European privacy regulation the General Data Protection Regulation (GDPR) and the general topic of transborder data flow. Different countries and even states in the US have laws that specify where you are allowed to transfer other entities data based on the location's privacy and security strength. For example, under GDPR you are only allowed to transfer an EU's citizens data with their permission and if the transfer location meets the standard of the GDPR requirements. Up until a while ago it was legal for data to be moved between the EU and US under an agreement called privacy shield that covered the requirements. In 2020 the agreement became invalid because the EU court of justice struck it down, this rendered the free flow of data between the two areas illegal. Organizations needed to switch to a method of striking transfer agreements with specific contractual clauses between entities that allowed such a transfer to happen and would put the requirements on the organizations itself.

Daniel Weinert
CIS-4450
7/09/2022

Sources:

Fennessy, C. (2020, July 16). The “Schrems II” decision: EU-US data transfers in question [IAPP]. *Privacy Tracker*. https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/

Harris, S., & Maymi, F. (2019). *All in One: CISSP* (8th ed.). Mc-Graw Hill.

Prof. Fustos. (n.d.). *Chapter #1* [PowerPoint]. Retrieved July 10, 2022, from https://msudenver-my.sharepoint.com/:p:/r/personal/lintonc_msudenver_edu/_layouts/15/Doc.aspx?sourcedoc=%7BBC2C1430-1902-43F2-9538-81BE9B9E3253%7D&file=chapter01.pptx&action=edit&mobileredirect=true

Multiple Choice Question:

Q: When an organization fails to properly protect the privacy of its customers data, it increases the likelihood of a/an _____?

A:

a. Audit

b. Data Breach

c. Criminal Investigation

d. Systems Failure

Correct Answer: b. Data Breach