Josiah Schmitz

CEG-4420

8/31/25

Module 1 Assignment

One form of harm that a company might suffer from is the leak or theft of personally identifiable information (PII). PII refers to any information that relates to an individual connected to a particular company, including but not limited to employees and customers. If PII is leaked or stolen by an attacker, it can lead to immediate consequences such as identity theft of the individuals whose information was stolen and long-term consequences like damage to the company’s public image. For example, say a healthcare company is the victim of a phishing attack where the attacker manages to get all the health records and personal information about the employees and patients involved with the company. If this story is released publicly (which would be highly likely), not only would the healthcare company lose much of the public’s trust in them, but there could also be severe legal ramifications for such a gross mishandling of PII. Additionally, they would most likely lose future customers or have their stock dip significantly due to their now damaged public image.

Another type of harm that could occur to a company is a disruption to employee morale. This could be due to a systems attack that temporarily disables the company’s method of paying their employees electronically for instance, leading to a potential delay in payment for an extended period of time. As a result of this lack of expected pay, employee morale would be significantly negatively impacted, with the downstream effect of less work being accomplished or tension between employees and their employers. The long-term consequence of this would be decreased company productivity, some of the impacted employees quitting, or a potential loss of competition with other companies in the industry.

A third form of harm would be the loss of contracts for a company due to illegally accessed classified data. Take a defense contractor in America, for example. There are certain safety measures these companies are required to take in order to protect government data marked Secret or Top-Secret. If one of these contractors were to accidentally let a malicious party (individual or group) on their premises who gained access to unauthorized files, they would not only be subject to severe legal consequences, but they would be unable to gain any new contracts from the US government and would very likely lose any existing contracts that were being worked on at the time of attack. This could potentially lead to the company going bankrupt entirely due to a lack of work and complete loss government trust.