Assignment #1

Who to blame?

Background / Scenario

Security breaches occur when individuals or applications attempt to gain unauthorized access to data, applications, services, or devices. During these breaches, attackers, whether insiders or not, try to obtain information that they can use for financial gain or other purposes. However, not all breaches are caused by hackers or applications; some are the result of human error or negligence. This case study will demonstrate some examples of negligence and how it affects both a company and individuals.

Security Breach Research

Incident Date	Affected Organization	How many victims? What was Taken?	What exploits were used? How do you protect yourself?	Reference Source (Hyperlink)
February 28, 2022	- A Turkish carrier that specializes in low-cost domestic and international flights, **Pegasus Airlines.**	- The exposure of the unprotected data had impacted every Pegasus passenger and crew member around the world. - An AWS S3 bucket containing the airlines “Electronic Flight Bag” or EFB information was left without password protection, leaking a range of sensitive flight data.	- Over 3.2 million files contained sensitive flight data. The two most common datasets containing this information were spreadsheets (about 2.9 million files) and acceptance forms (more than 290,000 files). It also includes insurance documents, permits, safety guidelines, and SIL (safety integrity level), logs with regulations, and source code. - In my own opinion, since it is caused by human error and employee negligence, the company should always have a task manager displayed in the office of the admin to regularly monitor the data stored in the database. And the company should also foresee tragic events that will happen and regularly check their security if it can handle these problems.	Pegasus Airline
April 6, 2022	- A mobile payment service, **CashApp.**	- A total of 8.2 million customers were affected by that breach. - The following details regarding Cash App's clients were taken by the terminated employee: full names, stock trading activity, brokerage portfolio holdings, and brokerage portfolio valuations.	- The employer left the employee's access permissions in place long after the employee was fired. The employee therefore intended to steal crucial information behind the company's back, knowing that he or she could still access the resources. -Establishing a proper process for terminating employees and carrying out frequent evaluations of user access frequently aid in shielding	Cash App

			companies against data theft by departing workers. Cash App Investing would have been able to identify any suspicious behavior on their ex-employee's account and take immediate action if they had implemented a continuous user activity monitoring system.	
May 25, 2023	- An American multinational automotive and clean energy company, **Tesla.**	- 75,000 people were affected by the said breach. - Personal information of employees and production secrets are leaked by the ex-employees.	- Tesla was informed by a German news organization that they had acquired sensitive data belonging to the firm. The investigation revealed that two former Tesla employees misappropriated the information in violation of Tesla's IT security and data protection policies and shared it with the media outlet, according to Tesla's data privacy officer Steven Elentukh. The newspaper obtained more than 23,000 internal documents from Tesla, totaling 100 gigabytes of sensitive data. PII belonging to employees, financial data of consumers, production secrets of Tesla, and grievances from customers over the features of Tesla's electric cars were all contained in the documents. - Finding out someone's dependability and goals throughout the onboarding process can also be helped by performing background checks. In this instance, keeping an eye on the user activity of the employees may have made it easier to identify their malevolent behavior.	Tesla