India Henry

CYSE201 - 7:25

3 April 2024

Read this https://dojmt.gov/wp-content/uploads/Glasswasherparts.com_.pdf sample breach letter "SAMPLE DATA BREACH NOTIFICATION" and describe how two different economics theories and two different social sciences theories relate to the letter.

The letter gives an example of a letter that a compromised company would send to customers who bought from them online. One economic theory that would relate to this is classical economic theory because it is the belief that any information that is willingly provided to a company is subject to the "supply-demand" formula and can be monetized. That doesn't mean that the company gave away their customer's information on purpose, especially because it was a cyberattack, but it would mean that little government intervention could happen to the company. This would leave a company's reputation up to its customers.

In the case of classical economic theory, the social science theory that can relate to this sample is determinism. Determinism is the theory that there is a cause in the past that affects the actions of the future. The cause in this case would be the economic theory, the ideology that the government cannot interfere in business. If the government cannot interfere, then regulations to protect the safety of customers won't be made and businesses won't spend money on something they don't have to implement.

This also relates to the social science theory of ethical neutrality. It questions if the data that companies collect from their customers and if how they use it is ethical.

This can also question if these companies must take their customer’s sensitive information (credit card numbers, social security, etc.) if it is ethical to not have the proper security to protect that sensitive information.

On the other hand, Keynesian economic theory suggests for the government to invest in cybersecurity will help to stimulate the economy in a way that won’t increase taxes. This relates back to the sample because inside of the document it states that the company *has* a cybersecurity team that found the data breach and was actively working to patch it.