Economic theory vs social theories

Audrey Gyane

Old Dominion University

Cybersecurity and Social Science 201s

Professor Matthew Umphlet

Apr 3, 2024

describe how two different economics theories and two different social sciences theories relate to the letter.

The first economic theory I saw while reading is rational theory. It is rational theory because it shows that the company's and the affected buyer's choice are all centered on cutting costs and increasing advantages. The company has reacted rationally to reduce damage to its brand and maintain trust among their clients, as evidenced by its prompt customer communications, working alongside cybersecurity experts, and swift execution of preventive safeguards. Additionally, clients act sensibly by keeping an eye on their bank records and contacting their banks in order to lessen the risk of identity theft and the ensuing monetary damages. Complying with legal obligations and assisting the police, which can find an agreement between protecting clients interest and lawful needs, are other examples of rational theory. With all factors looked at, the event highlights how intentional decisions improve response to breaches of information, stressing the need of being cautious in reducing cybersecurity threats and safeguarding private information. The second economic theory that showed itself was marxian economic theory. This theory demonstrates how individuals in roles that hold power, in this letter, the service providers and possibly the intruders, are exploiting others in disempowered positions for financial gain which shows us how marxian economic theory is displayed. The company's dependency on a third party provider results in the use of clients credit card information highlights power imbalances in the economy. These organizations are able to take advantage of weaknesses in order to obtain value, often at the price of individuals economic security and privacy. Users were not informed of the attack until a long time afterwards than was required, and the emphasis on adopting own behaviors to limit risks shows

how financial structures have the potential to increase unfairness and move the burden of safeguarding to the vulnerable sides.

For social sciences the first one is determinism. It fits determinism because it holds that the circumstances and things that came before them affects everything that happens such as what people do and decide. Under this instance, the first attack may be considered as the beginning of a series of effects that include the breach and the system's provider's and users' next step. Malware that was installed in the system provider's servers and allowed unwanted access to client data became the root cause of the incident. The reaction of customers to safeguard their banking data along with provider's assistance with the police and cybersecurity specialists are examples of next steps that are impacted by the factors that led to the breach. This viewpoint emphasizes how linked actions and outcomes inside situations, highlighting how outside forces and conditions may in advance affect events and decisions. The discussion around this event and the way it is open, legitimacy, fairness, and the supply of goods and services for protection exemplify the values of objectivity. A dedication to truth and honesty in revealing findings is demonstrated by the company's alerts of the breach, which includes details about the timeframe, the stolen information, and the participation of the police. By granting the police the authority to investigate and postponing notifying customers as a result, the corporation shows objectivity and a readiness to let outside investigators carry out a full examination.