

Journal Entry: Economic and Social Science Theories in a Data Breach Notification

Journal Entry: Economic and Social Science Theories in a Data Breach Notification

Hussein Al Saffar

CYSE201S

Matthew Umphlet

Old Dominion University

July 27th, 2025

Journal Entry: Economic and Social Science Theories in a Data Breach Notification

The *Glasswasherparts.com* sample breach notification illustrates important connections between cybersecurity incidents and both economic and social science theories. From an **economic perspective**, the first relevant theory is **cost–benefit analysis**, specifically the Gordon–Loeb model. Companies must decide how much to invest in cybersecurity relative to potential losses from breaches. The notification letter shows how the company is investing in mitigation—offering credit monitoring and investigation services—balancing the cost of these measures against legal, reputational, and financial harm (Gordon & Loeb, 2002). This reflects a calculated approach to reducing long-term costs.

The second economic theory is **negative externalities**. When personal data is exposed, customers suffer harm such as identity theft, which the company might not directly bear. Breach notification laws help internalize these external costs by forcing transparency and encouraging companies to improve security (Kesan & Hayes, 2012). The letter functions as a corrective tool, informing consumers so they can protect themselves.

From a **social science standpoint**, **social contract theory** is key. Customers entrust companies with sensitive information, expecting it to be protected. The breach letter is an effort to honor that social contract after it has been broken by acknowledging the issue and providing remedies, aiming to rebuild trust (Rawls, 1971).

Lastly, **trust theory** explains how breaches damage institutional trust. The company's notification and remediation efforts seek to repair this trust and demonstrate accountability, which is crucial to maintaining customer relationships and social legitimacy (Lewicki & Bunker, 1996).

Journal Entry: Economic and Social Science Theories in a Data Breach Notification

In summary, this breach notification letter exemplifies how cybersecurity events are intertwined with economic decision-making and social obligations, emphasizing that effective responses require both understanding.

Journal Entry: Economic and Social Science Theories in a Data Breach Notification

References

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457.

Kesan, J. P., & Hayes, C. (2012). Strengthening breach notification laws: Lessons from state laws. *Journal of Law, Technology & Policy*, 2012(2), 447–477.

Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations* (pp. 114–139). Sage.

Rawls, J. (1971). *A theory of justice*. Harvard University Press.