

Journal Entry 11: Data Breach Notification Analysis

Nicholas Duggins

07/26/2026

Journal Entry 11: Data Breach Notification Analysis

The Glasswasherparts.com data breach letter shows how both economic and social science theories help explain what happened and why cybersecurity is important. One economic theory that relates to this breach is cost-benefit analysis. Companies have limited resources, so they must decide how much money to spend on cybersecurity compared to other business expenses. In this case, the third-party platform provider was compromised by malware, showing that not investing enough in security can end up costing much more through financial losses, damaged reputation, and loss of customer trust.

Another economic theory is information asymmetry. The company and its platform provider knew about the breach before customers did, while customers continued to believe their information was secure. This imbalance of information can reduce trust and make it difficult for customers to make informed decisions about protecting their personal data.

One social science theory that fits this situation is Routine Activities Theory. This theory states that crime occurs when there is a motivated offender, a suitable target, and a lack of capable guardianship. The hackers were motivated offenders, customer payment information was the target, and weaknesses in the platform provider's security allowed the attack to happen.

Another theory is the Theory of Planned Behavior. After receiving the notification, customers are encouraged to contact their bank, replace their payment cards, and monitor their accounts. Their decision to take these protective actions depends on their attitudes toward the risk, the recommendations in the letter, and whether they believe they can successfully protect themselves from fraud. Overall, this breach shows that cybersecurity is influenced by both economic decisions and human behavior, not just technology.

References:

Montana Department of Justice. (2017). Sample data breach notification. https://dojmt.gov/wp-content/uploads/Glasswasherparts.com_.pdf

Journal Entry 11 2: Analysis of Bug Bounty Economics

Nicholas Duggins

07/26/2024

Journal Entry 11 2: Analysis of Bug Bounty Economics

Bug bounty programs are a smart way for companies to improve their cybersecurity while keeping costs under control. Instead of relying only on their own security teams, companies pay ethical hackers to find vulnerabilities before cybercriminals can take advantage of them. The article explains that there is a worldwide shortage of cybersecurity professionals, making it difficult for many organizations, especially small businesses, to hire enough qualified employees. Bug bounty programs help solve this problem by allowing companies to use skilled researchers from around the world. The literature review also discusses Linus's Law, which states that the more people who examine software, the more likely they are to find security weaknesses. This makes bug bounty programs an effective way to identify problems that internal teams may miss (Sridhar & Ng, 2021).

I thought the findings were interesting because they showed that money is not the only thing motivating ethical hackers. The researchers found that many hackers also participate because they enjoy the challenge, want to improve their skills, and build their reputation. The study also found that smaller companies can benefit just as much as larger companies because a company's size or reputation does not have a major impact on the number of valid vulnerabilities reports it receives. Another important finding was that bug bounty programs become less effective over time because the easiest vulnerabilities are found first. However, companies can continue to receive valuable reports by expanding the scope of their bug bounty programs.

Overall, I think bug bounty programs are a great example of using economics to improve cybersecurity. They give organizations a cost-effective way to find security weaknesses before attackers do while rewarding ethical hackers for helping make systems more secure.

References:

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of bug bounties. *Journal of Cybersecurity*, 7(1), tyab007.

<https://doi.org/10.1093/cybsec/tyab007>

Journal Entry 12

Nicholas Duggins

08/02/2026

Journal Entry 12

Journal Entry: Everyday Illegal Internet Activities

Most people use the internet every day without thinking about whether some of the things they do are illegal. After reading Andriy Slynchuk's article, I realized that a lot of common online behaviors can have serious legal and ethical consequences. While many people think cybercrime only involves hacking into computers, there are many illegal activities that happen through everyday actions that violate someone's privacy or rights (Slynchuk, 2026).

The five behaviors that stood out to me as the most serious were collecting data from children under 13 without parental consent, cyberbullying, doxxing, creating fake identities to deceive people, and recording VoIP calls without permission. Collecting children's information is especially concerning because kids are more vulnerable online and deserve extra protection. Cyberbullying and doxxing can seriously affect someone's mental health and personal safety, and in some cases can even lead to physical harm or identity theft. Creating fake identities online is another major issue because it is often used to scam or manipulate people. Recording someone's private conversations without their knowledge also violates their privacy and breaks state and federal laws.

What I took away from this article is that cybersecurity is not just about protecting computers. It is also about respecting other people's privacy, following the law, and making responsible decisions online. Thinking before posting or sharing information online can help make the internet a safer place for everyone.

References:

Slynychuk, A. (2026, January 4). 11 illegal things you unknowingly do on the internet. Clario.
<https://clario.co/blog/illegal-things-you-do-online/>