Keyshawn Braxton

CSYE201S

Prof D. Yalpi

Case Study

## BLUF (Bottom Line Up Front)

Technical security measures are practically useless if the people managing the systems are in a financial position to be manipulated. In 2025, Coinbase lost hundreds of millions of dollars not to a technical exploit, but because overseas contractors were bribed to take pictures of customer data on their personal phones.

## Overview

In early 2025, Coinbase suffered a major data breach impacting roughly 70,000 users. Attackers didn't hack into the servers using malware or complex code. Instead, they targeted the underpaid workers. The hackers bypassed technical defenses by bribing “TaskUs” customer support contractors based in India. For just $200 per picture, these workers used their personal smartphones to capture sensitive user information right off their monitors. They exposed names, partial Social Security numbers, and government IDs. While they didn't steal passwords, the leaked data was enough for attackers to drain between $180 million and $400 million in customer assets.

## Social Science Integration

Looking at this through a social science and economic lens shows exactly why this happened. When a massive U.S. financial tech company outsources data access to third-party contractors to pay the workers less and maximize profit, it creates a massive economic vulnerability. The wealth gap between the US-based company and the overseas workers made the $200 bribes highly attractive.  This demonstrates the Rational Choice Theory. The contractors weighed the low risk of getting caught against the financial reward. On top of that, these contractors don't have the same company loyalty as directly employed Coinbase employees. The attackers knew this and exploited the economic motivation of the workers, proving that a system is only as secure as its lowest paid employee.

## Proposed Solutions and Barriers

Fixing this requires both technical and social strategies. Technically, companies need to implement strict architecture and data masking. Support agents should only see the exact data needed to close a ticket and nothing more. This would result in a less open system and make data less vulnerable to be shared or leaked. Physically, smartphones shouldn't be allowed on the floor. However, the social solution is just as important as the technical and physical, companies need to pay competitive, living wages to outsourced workers to remove the financial incentive to accept bribes or hire more employees to do these jobs in-house. The main barrier in this situation is operational cost. Paying contractors a higher wage cuts into the profit margins and defeats the purpose of outsourcing, but it is one of the safest routes you could go in this situation. Also, strict data masking can slow down how fast customer service tickets get resolved. Another major barrier is geopolitical. Law enforcement in the United States has very little power to prosecute contractors in India, which lowers the legal risks for the workers committing the crimes.

## Reflection

This case study proves that combining cybersecurity with the social sciences is mandatory. You can build the strongest firewall in the world, but it won't stop an underpaid employee with a camera phone. Real security means understanding the economic motivations and the risk

susceptibility of the people who handle the data. Cybersecurity is no longer an It issue, moving forward security teams must collaborate with HR and payroll to secure the human supply chain.

## References


Goodin, D. (2025). Inside the Coinbase breach: How $200 bribes bypassed million-dollar security. Ars Technica. https://arstechnica.com/information-technology/2025/05/coinbase-insider-breach

Krebs, B. (2025). *The human firewall fails: TaskUs contractors tied to major crypto theft*. Krebs on Security. https://krebsonsecurity.com/2025/05/coinbase-taskus-breach