Cybersecurity Incidents & Law Enforcement

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity, Professor Dr. Joseph Kovacic

September 21, 2025

Instructions:

The decision to escalate incidents to law enforcement is an area fraught with *(cyber)* conflict. In your opinion, what are the pros and cons of law enforcement involvement? What resources and references can you cite to back up your assertions?

Cybersecurity Incidents & Law Enforcement

I think the advantages usually outweigh the disadvantages for large-scale incidents and events that are cross-country or organized crime related. Law enforcement agencies (e.g., FBI and CISA) have access to unique resources and legal authority to help deter and dismantle threat actors that individual organizations cannot sometimes handle alone (Swinhoe, 2019; U.S. Department of Justice, 2021). Law enforcement involvement can also lead to the arrest and sentencing of cybercriminals by holding those responsible for their crimes and bringing closure to cases (U.S. Federal Trade Commission, 2021).

However, for smaller-scale/local events or when organizations prioritize quick internal remediation, notifying and involving law enforcement may be less appealing because of potential disruptions and privacy risks. First, investigations can be lengthy, chaotic, and costly. They may require organizations to preserve compromised systems and evidence, which can result in additional time and resources being spent, potentially interfering with normal business operations and recovery efforts (Swinhoe, 2019).

Second, there is also a risk of losing control over the public narrative (Swinhoe, 2019). While law enforcement agencies may disclose details of the incident to the public during an active investigation, the public may develop their own opinions (sometimes "jumping to conclusions") about the incident before all the correct and necessary information is collected for the courts to reach their final verdicts. Early public opinions regarding cybersecurity incidents and related entities can tarnish an organization's reputation, resulting in a loss of customers, revenue, and market share (Swinhoe, 2019; Kim & Solomon, 2021). Third, small-scale incidents may not meet the high thresholds required for federal law enforcement to become involved, leaving an organization to fend for itself if local law enforcement lacks jurisdiction or power to address those

cybersecurity events (Swinhoe, 2019). Thus, if events can be handled quickly, quietly, cost-effectively, and without additional noise or outside chaos, then organizations may want to handle cybersecurity incidents internally without involving law enforcement.

Lastly, in 2024, an IBM report found that involving law enforcement in a ransomware attack can reduce the total cost of a data breach by an average of $1 million (IBM, 2025). However, the 2025 IBM report shows that fewer organizations reported ransomware breaches to law enforcement when compared to 2024. In light of researchers acknowledging that involving law enforcement dramatically reduces the global average cost of a breach, organizations did not see or realize the benefit in 2025, even though the cost of extortion or ransomware attacks continues to grow year by year (IBM, 2025). Therefore, the choice for organizations to bring in law enforcement for cybersecurity incidents (e.g., data breaches, ransomware attacks, or cyber espionage) is sometimes considered a “double-edged sword" or “necessary evil,” depending on the size of the cybersecurity incident and the goals and abilities of an organization to address those events.

References

IBM Corporation & Ponemon Institute. (2025). *Cost of a Data Breach Report 2025: The AI Oversight Gap*. IBM Corporation.

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Swinhoe, D. (2019, May 30). *Why businesses don't report cybercrimes to law enforcement*. CSO Online. https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

U.S. Department of Justice, Criminal Division, Fraud Section. (2021, June 16). *Best practices for partnering with law enforcement*. https://www.justice.gov/criminal/file/1404806/dl?inline

U.S. Federal Trade Commission. (2021). *Data breach response: A guide for business*. https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business