Legal Concerns in Incident Response

Alexis Watson

School of Cyber Studies, The University of Tulsa

CYB4863: Special Topics in Incident Response

Justin Miller, MS, MA

March 30, 2025

Legal Concerns in Incident Response

Incident response is one of the most important aspects of a business's continuity plan; organizations are ever more being victimized by growing cyber threat actors. An incident response scenario brings with it many different concerns, all of which require immediate attention. Some situations can put the business at risk of financial loss or reputation damage, while others might have impacts that spill over to seemingly discrete areas of life. In some situations, the interplay between the business and its country of origin means that the company is held to much higher standards because it has much more to be held accountable for. Often, laws are enacted to ensure that information is being properly handled by all involved entities. Adherence to such data protection legislation is the most important part of a company's incident response protocol and overall security posture.

The history of cyberattacks is largely understood to begin with the Morris worm in 1988. Named after the Cornell student Robert Morris who created it, it was created as an academic experiment with no malicious intent. This fact alone seems to separate it from all the widely-known cyberattacks of the new millennium; it still lives in infamy due to its rapid, widespread infection of thousands of computers. Due to its impact, the Morris worm was able to act as a proof-of-concept for individuals and organized groups that would seek to damage digital systems and commit fraud. In 2000, when cyberattacks were beginning to enter the zeitgeist, then-President Clinton noted the dangers of these new technologies: "Yet, someone can sit at the same computer, hack into a computer system and potentially paralyze a company, a city, or a government" (Clinton, 2000, p. 14). A while later, in 2017, the top-three credit reporting company Equifax suffered a data breach in Argentina due to the insecure username/password combination "admin/admin" (Krebs, 2017). Then again, in 2021, the US-based oil company

Colonial Pipeline, which is responsible for a large portion of gasoline and other fossil fuel supplies to America's East Coast, was affected by a ransomware attack and their operations were ceased for several days. It is still seen as the most emblematic cyberattack in America for disrupting critical economic and physical infrastructure, shown by the several dozens of pieces of cybersecurity legislation passed in its wake (Wood, 2023). Although cyberattacks were not noted in mainstream media until the late 20th century, they have grown in frequency and severity, and will continue to do so.

Cyberattacks carry with them immense potential for loss to the affected organization and the broader society. Anderson et al. (2013) describe four types of costs incurred by cybercrime: criminal revenue, direct losses, indirect losses, and defense costs. Criminal revenue, a portion of direct losses, is the amount of money or prestige that the attackers are able to retain after the attack. Direct losses are the amount that is specifically lost as a result of the attack, such as the roughly $1.9 million that Colonial Pipeline lost from their ransom payment (Wood, 2023), digital infrastructure damage, and leaked personally identifying information (PII) like the 14,000 records exposed by Equifax in Argentina (Krebs, 2017). Indirect losses includes all those things which perhaps come less immediately to mind, such as reputation damage, lost opportunity cost, and stock devaluation. Indirect losses also include the fees and fines that are caused by legal battles with victims and governments. Defense costs are the expenses that the company takes on in order to increase their security posture. Although each type of cost is incredibly important and should be carefully considered, companies often give direct and indirect losses the highest priority as they tend to have the greatest impact on the company's bottom line and legal standing.

Because of the ever-growing threat of cyberattacks that lead to varieties of fraud or theft that individuals face, some districts, countries, and international unions have established laws to

protect these individuals' PII. The American state of California has enacted their California Consumer Privacy Act (CCPA). The CCPA "gives consumers more control over the personal information that businesses collect about them," including the ability for an individual to pursue litigation if their PII was leaked due to improper security practices (State of California Department of Justice, 2024). At the national level, the United States' Securities and Exchange Commission (SEC) requires public companies to disclose a data breach within four days of the company determining the incident to be material, as well as mandating an annual report on "cybersecurity risk management, strategy, and governance" (Gerding, 2023). With this ruling, the SEC provides federal protections to individuals who may be affected by a data breach of a public company. Across the Atlantic Ocean, the European Union's Regulation (EU) 2016/679, known widely as the General Data Protection Regulation (GDPR), is considered the hallmark of individuals' data protection regulations. The GDPR outlines quite clearly what is to be expected: "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay" (European Union, 2016, art. 34, § 1). To rephrase, if a PII leak can pose a danger, the company must alert the individual affected as soon as possible. These laws are representative of legislative bodies attempting to catch up to a rapidly evolving cyberspace, and place much of the burden of maintaining secure data on the companies.

In some cases which concern classified or protected information, an organization's failure to adhere to data protection legislation will have drastic consequences for both the organization and its country's international relations. Every year, the Office of the United States Trade Representative (USTR) issues the *Special 301 Report* that analyzes the state of intellectual property (IP) protections in other countries. If a country falls short of IP protections from where

the United States is, they may be vulnerable to additional tariffs and other economic sanctions. Furthermore, if an individual company fails to securely handle copyright, patent, or trade secret information and it is leaked, this will have an impact on the country's entire standing in international relations. For example, in the section of last year's *Report* that discusses India, it states that "the United States encourages India to continue working toward providing adequate and effective protection of trade secrets in India" (USTR, 2024, 54–55). One can imagine, in light of the numerous tariffs that the United States is placing, that the Indian government and Indian companies not having proper protections in place could lead to economic sanctions and a tensioning of trade relations between the two countries. Similarly, if an organization is responsible for confidential information as a matter of national security, and they do not respond properly to a cybersecurity incident or practice proper data handling, the nation is made vulnerable to attacks and is seen as a less reliable ally. One example of this might be the American Government's use of a third-party messaging platform which "is not an authorized system for preserving federal records and does not comply with recordkeeping requirements under the [Federal Records Act] or [National Archives and Records Administration] guidance" (American Oversight, 2025, 9, par. 41), and that was also previously noted by the Google Threat Intelligence Group as "being actively targeted by Russian-aligned threat groups" (Black, 2025). The failure to comply with local, national, and international data protection laws will have a profound negative impact on the organization and the geopolitical regions which it represents.

Beyond the risks to the country, violating data breach laws can have a profound impact on the well-being of the company, even to the point of the business ceasing to exist. To understand just how serious this can be, one can imagine a hypothetical situation in which there is a large, multi-national company who does not securely store and protect its clients' PII. In an

incident response scenario, the company's first priority should be to prevent the loss of PII, while managing appropriate documentation to ensure steady cooperation with law enforcement. If this PII is not protected, and especially if the documentation is not maintained, the business can first expect a number of lawsuits from the individuals protected by the area's data breach laws. These will cause the business to incur massive legal fees and a loss of public trust. Then, if the lawsuits are lost, or if the data breach is serious enough, the company can be at further risk of fines from the governments that they operate under. If the company is found to be liable under, for example, the CCPA or GDPR, then they may also be required to submit a report detailing the security and incident response shortcomings and providing a plan to avoid similar issues in the future. Beyond even just fines, it is possible that such a report may be found to be insufficient and the company may be at risk of being shut down. No cost to a business's bottom line can ever be greater than a total ceasing of operations; a company is more at risk when they are not following data security laws than in any other circumstance.

In an incident response situation, although several concerns demand an immediate fix, compliance with data protection legislation should be the issue of focus and the lens through which all other problems are handled. Without such compliance, the company can suffer financial or reputational damage, lose special distinctions, pose a threat to national and international security, and fade into nonexistence while harming millions of innocent victims at the same time. Although they are a concern for companies, data protection legislation was enacted in order to protect citizens' sensitive data, which is increasingly more often the target of cybercrime. In the current landscape, innocent civilians must place their trust in corporations; it becomes then the duty of the corporation to protect them.

References

American Oversight. (2025, March). *American Oversight v. Hegseth, Gabbard, Ratcliffe, Bessent, Rubio, and NARA Regarding Military Actions Planned on Signal Messaging App*. American Oversight. https://americanoversight.org/litigation/american-oversight-v-hegseth-gabbard-ratcliffe-bessent-rubio-and-nara-regarding-military-actions-planned-on-signal-messaging-app/

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. *The Economics of Information Security and Privacy*, 265–300. Springer Nature Link. https://doi.org/10.1007/978-3-642-39498-0_12

Black, D. (2025, February 19). Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger. Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger

Clinton, W. J. (2000). Remarks on the National Plan for Information Systems Protection and an Exchange With Reporters. *Public Papers of the Presidents of the United States*, *William J. Clinton, 2000–2001*(Book I), 13–15. United States Government Publishing Office. https://www.govinfo.gov/content/pkg/PPP-2000-book1/html/PPP-2000-book1-doc-pg13-2.htm

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*(Legislation 119), 1–88.

EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

Gerding, E. (2023). Cybersecurity Disclosure. United States Securities and Exchange Commission. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214#:~:text=To%20help%20investors%20evaluate%20this,cybersecurity%20risk%20management%2C%20strategy%2C%20and

Krebs, B. (2017, September 12). Ayuda! (Help!) Equifax Has My Data! *Krebs on Security*. https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/

Office of the United States Trade Representative. (2024). *2024 Special 301 Report*. Office of the United States Trade Representative. https://ustr.gov/sites/default/files/2024%20Special%20301%20Report.pdf

State of California Department of Justice. (2024, March 13). *California Consumer Privacy Act (CCPA)*. State of California Office of the Attorney General. https://oag.ca.gov/privacy/ccpa#sectionc

Wood, K. (2023). Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack. *The Georgetown Environmental Law Review*. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/