Balancing Security and Privacy: Case Study Analysis

Case Study Analysis of the 2014 Sony Pictures Hack and the CFAA

Written by Zhaire Robinson

Course: CCJ 4933 ST: Cybersecurity Policy

Instructor: Dr. C. Jordan Howell

Date: September 18th, 2025

Case Study Analysis of the 2014
Sony Pictures Hack and the CFAA

Introduction:

The Computer Fraud and Abuse Act, or CFAA, was passed in the United States in 1986. The purpose of this law was to combat cyberattacks by making it illegal to hack into computer systems. This law has been used in the prosecution of many hackers for decades, but it was not without flaws. There was a point in time when the CFAA was not designed for attacks by foreign governments or state-sponsored hackers. One major example of this oversight in the production of the law was in 2014, the Sony Pictures Hack, where a group of hackers calling themselves "Guardians of Peace" led a cyberattack that stole and leaked many emails, employee information, and unreleased films at Sony Pictures (Vox, 2015). The hackers were later identified to be North Korean state-backed hackers, and one of the main perpetrators was an individual named Park Jin Hyok (U.S Department of Justice, 2018). This attack was an example of how weak points within the CFAA limited the number of charges to be filed and demonstrated how cyberattacks can be used to bring about disruption and chaos through politically motivated attacks.

How the CFAA Was Applied to the Sony Pictures Hack:

The "Guardians of Peace" used forms of malware and phishing attacks in order to gain access to Sony Pictures' internal systems. Once they had access, they began deleting critical files, leaking private emails, unreleased movies, and financial information online. As Vox (2015) explained, the release of all of these private and vital assets was extremely damaging to Sony and showed just how destructive on a non-violent scale these types of cyberattacks can be. Under the CFAA, the Department of Justice was able to charge Park Jin Hyok, a North Korean programmer, for unauthorized access, conspiracy, and damage to protected computers (U.S Department of Justice, 2018). The DOJ officials uncovered that Park was a part of a hacking group tied to the North Korean government, making the attack politically motivated.

Although the CFAA was able to allow the U.S to present charges against Park Jin Hyok and formally respond to the perpetrator of the Sony hack, enforcement of those charges turned out to be difficult. One major issue was jurisdiction, due to Park Jin Hyok being a hacker who is in North Korea and working under the Lazarus group, The U.S had no jurisdiction or ability to enforce those charges and arrest him. Along with a jurisdiction issue, the Computer Fraud and Abuse Act was an older law that had no protections surrounding cyberattacks committed by state-sponsored hackers and foreign governments at the time (HG.org, n.d.). The CFAA was only enough to enable charges to be filed, but it in no way prevented or protected hackers from stealing sensitive data or leaking unreleased films in the first place.

Although the CFAA provides a legal framework for accountability regarding cyberattacks, those weaknesses within the law have struggled to fully protect victims and deter large-scale cyberattacks, limiting the practical effectiveness the CFAA is supposed to provide.

Improving the CFAA Against Modern Cyberattacks:

In order for the CFAA to be more effective, one improvement would be to update it regularly, and explicitly cover attacks from foreign governments or state-sponsored hackers, and to make efforts to strengthen international cooperation with other countries, so that in the event the law does all it needs to, the U.S.. is still able to go out and extradite bad actors who commit politically motivated cyberattacks against the country. It would also be a good idea to encourage more partnerships between government agencies and private companies so that certain threats can be detected earlier, and there is more room to act and prevent cyberattacks from happening (Framework Security n.d.). These changes could help prevent future attacks like the Sony Pictures hack and allow the U.S to develop better cybersecurity practices and protections for businesses and individuals.

Conclusion:

Overall, the 2014 Sony Pictures hack demonstrates how serious and politically charged modern cyberattacks can be, and the full-on damage and cyber-insecurity they can cause among organizations and individuals. Improving laws like the CFAA would not only allow the U.S to enforce charges against hackers, but an update to the laws could better prepare the country to defend against more state-backed cyberattacks and other types of unique hacks, and allow the U.S to hold all hackers accountable in the future.

References

Computer fraud and abuse act (CFAA). NACDL. (n.d.). https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

Harrison, B. (2018). *The CFAA in practice: Lessons from high-profile cyber cases*. Pace University Digital Commons. https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1058&context=pipself

Lee, T. B., & James, E. St. (2015, January 20). *The 2014 Sony hacks, explained*. Vox. https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions. Office of Public Affairs | North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions | United States Department of Justice. (2025, February 6). https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

The Sony Pictures Breach: A deep dive into a landmark cyber attack. Sep 15, 2023. (n.d.). https://frameworksecurity.com/post/the-sony-pictures-breach-a-deep-dive-into-a-landmark-cyber-attack