Assignment 1.1: Cybercrime Analysis

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

06/28/2025

Case Overview – The 5Ws and Context

Roman Valeryevich Seleznev, the son of a prominent Russian lawmaker, orchestrated one of the most financially damaging cyberattacks against American businesses. Using the alias "Track2," Seleznev operated an international credit card theft ring that compromised over 1.7 million payment card numbers and targeted more than 4,000 small businesses between 2009 and 2013 (Perlroth, 2017). These attacks caused an estimated $169 million in losses to merchants and financial institutions.

Seleznev employed SQL injection attacks to exploit vulnerabilities in point-of-sale (POS) systems. These attacks enabled unauthorized access to databases containing sensitive cardholder data. The stolen data was then sold on darknet forums and carding marketplaces. Although based in Russia, Seleznev was arrested in 2014 while vacationing in the Maldives. He was extradited to the United States, tried in federal court, and sentenced in 2017.

His case illustrates several key cybersecurity themes: the vulnerability of small businesses with minimal defenses, the globalization of cybercrime, and the increasing willingness of U.S. courts to assert jurisdiction over foreign nationals who commit cybercrimes against American interests.

Applicable Laws – Criminal and Civil Aspects

Seleznev was prosecuted under several U.S. federal statutes addressing fraud and computer crime:

- **18 U.S.C. § 1029** – Fraud and related activity in connection with access devices

- **18 U.S.C. § 1030** – Computer Fraud and Abuse Act (CFAA)

- **18 U.S.C. § 1343** – Wire fraud

- **18 U.S.C. § 1956** – Money laundering

He was convicted on 38 counts and found responsible for more than $169 million in damages. The U.S. Department of Justice noted this was the longest sentence handed down for cybercrime at the time (U.S. Department of Justice, 2017).

In addition to criminal proceedings, Seleznev's attacks triggered civil litigation and regulatory scrutiny for the affected businesses. While few pursued direct legal action against Seleznev due to jurisdictional limitations, many businesses faced downstream liability. Several were fined by payment card brands for non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) and exposed to lawsuits for failure to implement "reasonable security measures" (Solove & Citron, 2023). These events exemplify how data breaches often reveal latent violations of state privacy laws and security obligations.

Leadership Lessons – Preventing Crime and Mitigating Legal Risk

In a cybersecurity leadership position at one of the targeted businesses, several critical actions could have been implemented to mitigate both the incident and the resulting liability. According to Solove and Citron (2023), the legal standard for cybersecurity negligence frequently revolves around the implementation of "reasonable security measures." This standard

is evolving and is often evaluated by courts through expert testimony based on the specific technologies and threats at issue.

To mitigate both technical and legal exposure, organizations should implement a layered approach to technical controls, including web application firewalls (WAFs), endpoint protection, network segmentation, and encryption. Vulnerability scans and regular patching cycles are critical. As noted by Kerr and Solove (2023), even highly skilled developers cannot prevent every flaw in large codebases, and unpatched systems are frequently the initial vector for breaches.

The organizations affected by Seleznev also failed in maintaining basic cyber hygiene. Many used outdated POS software with known vulnerabilities. The lack of system updates allowed SQL injection attacks to succeed. As emphasized in Principles of Cybersecurity Law, these types of omissions often become central to litigation and agency investigations once breaches are reported (Schreider, 2020).

Beyond technical safeguards, a cybersecurity leader must ensure that incident response plans, third-party risk assessments, and cyber liability insurance are in place. Legal counsel should review contracts with vendors and ensure compliance with state breach notification laws. These preparations not only protect sensitive data but also demonstrate due diligence, a crucial factor in regulatory and civil evaluations following an incident.

Finally, cybersecurity awareness must be embedded into the organizational culture. Although Seleznev's attack vector was technical, many data breaches also involve social engineering or internal negligence. Employee training, phishing simulations, and clear data

handling policies help reduce the likelihood of human error, which remains a major contributor to cyber incidents.

Conclusion

The case of Roman Seleznev highlights the intersection of cybersecurity failure, criminal prosecution, and organizational liability. Although Seleznev was the primary actor, the scope of damage was magnified by inadequate security practices among his targets. U.S. law provides robust tools for prosecuting cybercrime, but preventing these crimes requires proactive leadership. By enforcing reasonable security standards, patching known vulnerabilities, and building a culture of cybersecurity awareness, organizations can significantly reduce both the risk of attack and their exposure to regulatory or civil action. As the legal and threat landscape continues to evolve, strong cybersecurity leadership remains essential.

References

Kerr, O. S., & Solove, D. J. (2023). *Cybersecurity law: Technology and actors* (Ch. 2). West Academic Publishing.

Perlroth, N. (2017, April 21). *Russian man sentenced to 27 years for hacking scheme*. The New York Times. https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html

Schreider, T. (2020). *Building an effective cybersecurity program* (2nd ed.). CRC Press.

Solove, D. J., & Citron, D. K. (2023). *Principles of cybersecurity law* (2nd ed.). West Academic Publishing.

U.S. Department of Justice. (2017, April 21). *Russian cyber-criminal sentenced to 27 years in prison for hacking and credit card fraud scheme*. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme