Assignment 3.1: Hacking Wall Street

Joshua A Wortz

University of San Diego

Course Number: CSOL-500

Dr. Michelle Moore

01/27/2024

Cyberattacks' increasing frequency and sophistication have brought significant risks to critical financial infrastructures. These attacks often target major institutions and service providers, posing potential threats to the global economy. One of the largest banks in the world, JPMorgan Chase invests approximately $600 million annually and employs over 3,000 cybersecurity professionals to safeguard its operations (Zetter, 2021). Despite such substantial investments, experts argue that current preparedness measures, including rehearsals, are insufficient to address the complexity and scale of potential cyberattacks.

Rehearsals are simulated exercises that mimic potential cyberattack scenarios to test an organization's readiness and identify vulnerabilities. These exercises refine response protocols, train staff, and enhance department coordination. By simulating incidents like ransomware attacks or denial-of-service campaigns, rehearsals provide opportunities to evaluate and strengthen an organization's cybersecurity defenses (Brown, 2023). The primary objective of rehearsals is to ensure that critical infrastructure remains operational during a cyber incident. However, while rehearsals help identify gaps in response plans, they do not directly address data preservation or system restoration. In addition to rehearsals, organizations must integrate robust mechanisms for data loss prevention to safeguard sensitive information (Liu & Kuhn, 2010).

Although rehearsals are an essential aspect of preparedness, they have inherent limitations. One significant drawback is their inability to replicate real-world cyberattacks' full scope and duration. Large-scale attacks often involve cascading effects across interconnected systems, which rehearsals may fail to capture (Zetter, 2021). For example, data breaches caused by sophisticated threats can lead to the loss and compromise of critical data, amplifying the risk to an organization's operations and reputation (Liu & Kuhn, 2010).

Another limitation is the over-reliance on rehearsals, which can create a false sense of security. Rehearsals alone cannot mitigate the long-term consequences of a cyberattack without incorporating comprehensive strategies like data backups and disaster recovery plans (DRPs). For instance, incidents affecting cloud-based storage systems, where we do not have physical access to devices, and the deletion of large amounts of data rapidly highlight the importance of having reliable backups and robust recovery mechanisms to restore operations efficiently.

A DRP is a structured framework to restore an organization's operations following a disruptive event. Rehearsals are critical to a DRP as they validate response strategies and ensure team readiness. Effective rehearsals can be likened to the U.S. military's "train as we fight, fight like we train," emphasizing realistic practice to build muscle memory (Brown, 2023). While rehearsals are crucial in refining incident response playbooks and enhancing team coordination, organizations must integrate them with other DRP elements, such as secure backups and robust preventative measures. This holistic approach equips organizations to address immediate disruptions and long-term challenges posed by cyberattacks (Schreider, 2020).

While rehearsals focus on testing an organization's readiness through simulated exercises, backups and disaster recovery plans serve broader purposes in safeguarding and restoring critical data and operations during and after a cyberattack. Backups involve creating secure copies of critical data to prevent permanent loss or alteration. On the other hand, DRPs include rehearsals and backups, providing a comprehensive approach to incident response and recovery (Schreider, 2020). For example, rehearsals may identify vulnerabilities in response protocols, while backups ensure data integrity during an attack. Together, these elements form an integrated strategy that addresses both immediate and long-term challenges posed by cyber threats.

Despite their value, rehearsals alone are insufficient to address the evolving nature of cyber threats. Modern attacks often exploit vulnerabilities in interconnected systems and third-party providers, causing widespread disruptions that rehearsals may not anticipate. Additionally, rehearsals cannot fully account for the complexities of data loss, which can result from breaches, accidental damage, or inadequate backups (Liu & Kuhn, 2010). To mitigate these risks, organizations must adopt a multifaceted approach to cybersecurity. This includes investing in advanced detection tools, implementing robust data loss prevention measures, and developing comprehensive DRPs that address various scenarios.

Rehearsals are vital to cybersecurity preparedness, enabling organizations to test and refine their response strategies. They must integrate with data loss prevention measures and DRPs to form a comprehensive defense against cyber threats. While rehearsals improve coordination and confidence, they alone cannot address the scale and complexity of modern cyberattacks. Protecting critical financial infrastructure requires a holistic approach that combines preventive measures, advanced technologies, and cross-sector collaboration. As cyber threats evolve, organizations must remain vigilant and committed to strengthening their cybersecurity frameworks to safeguard their operations and public trust.

References

Brown, J. (2023). *Executive's Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program*. Packt Publishing, Limited.

Liu, S., & Kuhn, R. (2010, March-April). Data Loss Prevention. *IT Professional*, *12*(2), 10-13. 10.1109/MITP.2010.52

Schreider, T. (2019). *Building an Effective Cybersecurity Program, 2nd Edition*. Rothstein Publishing.

Zetter, K. (2021, 07 20). Hacking Wall Street: DealBook Newsletter. *The New York Times*. https://www.nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html