THE CREDIT SUISSE DATA LEAK:
AN IN-DEPTH EXAMINATION OF CYBERSECURITY AND HACK-BACK POLICIES

ABSTRACT

This paper will explore the leakage of Credit Suisse's data by an anonymous whistleblower. Specifically, it will discuss possible vulnerabilities within the system that hackers were able to exploit and suggest possible solutions that the bank could utilize to protect itself against future attacks. Based on decisions made by the bank in light of the attack, it is hypothesized that the hackers found entry points to Credit Suisse's network, possibly through the bank's supply chain with third-party suppliers, and used phishing emails to gather classified information from employees. The paper will also discuss the legal framework within which the bank operates to explore whether certain decisions could be considered legal and ethical such as serving clients with criminal backgrounds and conducting cyber attacks on the hackers themselves as a means of protection.

INTRODUCTION

On February 20th, 2022, an anonymous whistleblower leaked Credit Suisse's data to the German newspaper Süddeutsche Zeitung, exposing the existence of 30,000 accounts worth more than 100 billion Swiss francs owned by clients involved in "torture, drug trafficking, money laundering, corruption, and other serious crimes." While the bank responded by stating that the accounts were old and from a time when "laws, practices, and expectations of financial institutions were very different from where they are now," two-thirds of the accounts were opened in the last two decades, and quite a few were still open when the data was leaked. They spanned across the globe, from Venezuela to Egypt to Ukraine, as did the bank's 3,500 'relationship managers' who were responsible for finding and serving wealthy clients. Many of these countries are still presently ridden with corruption that results in powerful individuals in politics and finance hiding their money offshore so that it cannot be traced (Pegg et al., 2022).

This data leak highlighted the failure of both Credit Suisse and the Swiss legal system. The bank's due diligence process has come under scrutiny. It is required to assess clients every three years and every year for those deemed high-risk. If this process had been carried out rigorously, individuals with criminal backgrounds would not have been permitted to hold accounts. Even when the bank identified such clients and froze their accounts, the actions were executed slowly. As explained by a former Credit Suisse employee, the bank fosters a culture that encourages employees to overlook clients' backgrounds. However, the bank technically operated within the legal bounds of the region where it is located. Switzerland's banking secrecy law, enacted in 1934, "criminalized the disclosure of client banking information to foreign authorities." This is a long-standing practice, with the Great Council of Geneva's decision in 1713 to prohibit bankers from disclosing information about the assets of European aristocrats. This secretive legal and financial atmosphere was notoriously advantageous for international crime, and "half the assets managed by Swiss financial institutions belong to foreign clients" (Pegg et al., 2022).

In Switzerland, "banking whistleblowers are often held in contempt" and, in this case, there is an argument to be made in support of both the nation and the bank. In 2014, Switzerland was compelled to adopt the common reporting standard (CRS) by other nations and has been exchanging information about its clients with tax authorities in foreign countries since 2018, four years prior to the data leak (Pegg et al., 2022). Regarding Credit Suisse, having international clients with an account in Switzerland is not inherently illegal (BBC News, 2022), and about 90% of the accounts whose data was leaked were closed or in the process of being closed by 2022 (Credit Suisse, 2022). Therefore, while the whistleblower correctly highlighted unethical practices that have persisted for decades, it might not accurately reflect current practices, raising questions about the ethics of the situation. This includes whether ignoring the right to privacy of individuals whose information was disclosed, some of whom might have been innocent, is wrong. If so, it then raises questions about what offensive and defensive actions Credit Suisse is permitted to take. This paper will aim to answer these questions by exploring the cybersecurity practices within the bank, whether a 'hack back' policy would be helpful in this regard, and providing suggestions on how the bank might protect itself.

THE DATA BREACH

According to the whistleblower, Credit Suisse was hacked and the data was shared with the goal of highlighting the immorality of Swiss banking secrecy laws that aided clients who made their fortune through criminal activities. Credit Suisse has been battling allegations and facing penalties for its involvement in unlawful activities, such as tax evasion and money laundering, for three decades and has had to pay more than $4.2 billion in fines and settlements. During the time the data was leaked, the bank was grappling with setbacks resulting from its chairman breaking Covid-19 regulations, its involvement in a loan scandal in Mozambique, and allegations of helping the Bulgarian mafia launder money from the cocaine trade (Pegg et al., 2022).

While neither Credit Suisse nor the whistleblower disclosed the weaknesses in the system that opened the doorway for the data to be leaked, certain scenarios can be hypothesized by studying the annual reports released by Credit Suisse. In the section about technology and cyber risks in their 2022 annual report, released a few months after the incident, the bank mentioned that technology risks lie in "the people and processes that interact with [their IT assets], including through dependency on third-party suppliers and worldwide telecommunication infrastructure." They "could also be required to expend significant additional resources to investigate and remediate vulnerabilities or other exposures" and "regularly assess the effectiveness of key controls and conduct ongoing employee training and awareness activities, including for key management personnel" (Credit Suisse Group AG, 2022).

Looking at their cybersecurity report in 2023, the main implementation that the bank made between 2022 and 2023 has been for data leakage prevention. They did this by defining "requirements for information handling, including classification and ownership" and "access control requirements based on the need-to-know principle", enabled "information rights management tools", and implemented monitoring procedures for the "surveillance of email communication" (Credit Suisse, 2023).

The analysis and solutions offer a couple of suggestions on what might have gone wrong. Firstly, the hackers might have been able to send out phishing emails that confused employees into

providing sensitive information, such as passwords or classified documents, which provided the hackers with the tools required to access the bank's network. The hackers might have also performed Man-in-the-Middle attacks by eavesdropping into the conversation between different employees and gaining access to sensitive information in that regard. Lastly, it is also possible that they found vulnerabilities in the supply chains between the bank and its third-party vendors, allowing them to enter the network and conduct password attacks.

HACK BACK POLICY

The 'hack back' policy is one that would legally allow companies to conduct cyberattacks in response to being attacked by malicious hackers. This policy has been heavily debated in various countries. In Switzerland, where Credit Suisse is headquartered, an argument in support of the policy is that a company protecting itself through defensive actions is not a sustainable solution in the long run or an effective one in the short run. A supporter of this idea, Sanija Ameti, suggests that the Swiss defense department can be responsible for overseeing all activities to make sure companies follow certain guidelines. Issues with the policy have also been brought up by others, including Fabian Reinhard, who said that giving companies the permission to collect offensive capabilities would escalate the situation, and a solution lies in strengthening international cooperation to find cybercriminals instead (Soesanto, 2021).

The policy has garnered more support in America recently. President Biden is moving towards approving companies to conduct cyberattacks on hackers, albeit under heavy regulations as outlined in the 'National Cybersecurity Strategy'. Current guidelines and defensive measures have left companies and the U.S. government vulnerable to cybercrime attacks, especially from international parties (Kaplan, 2023). A counter strike would help a company shut down an ongoing cyberattack or even prevent it from happening (Cohn, 2013).
However, there are also many moral, ethical, and geopolitical issues that could arise from passing such policies. Hacking back could escalate the situation. "Critics fear legalizing counter-hacking would allow companies to carry out their own vigilante justice against the accused with no due process of law" and "private companies may launch attacks indiscriminately with little evidence" (Winstead, 2020). This could harm innocent parties, disrupt critical

infrastructure, and could also escalate the issue to an international conflict if a company unknowingly attacks a nation-state. Ethically, it also violates laws such as the Computer Fraud and Abuse Act, which "prohibits accessing computer systems without authorization" (B., 2023).

For a company like Credit Suisse, being legally allowed to carry out a counterattack might have helped in stopping the data leakage sooner, but it could easily have faced some of the negative consequences mentioned above. For example, given that many of the issues were due to its involvement in international criminal cases, the bank could have unknowingly attacked a nation-state. As a multinational organization, it is important for the bank to stay informed about all the changing policies, as it is required to function within the legal boundaries set by its host nations.

RECOMMENDATIONS

Even though Credit Suisse had an extensive defense mechanism, the hackers were still able to access the data successfully. While the attack was ongoing, Credit Suisse could have contained the breach to a limited location by disconnecting networks, systems, and devices from the access points (Chin, 2023). It could have also utilized frameworks developed by NIST and Lockheed to identify and prevent cyber intrusion activities. These frameworks would have provided the bank with insights into how and why hackers might attack it and help develop defensive solutions accordingly.

As mentioned above, Credit Suisse has since remedied the situation and taken measures to strengthen its defense against cyber attacks. However, there are quite a few things that could still be done. Looking at the analysis done by UpGuard, the bank needs to improve its website security. It is currently using insecure cookies, which allows third parties to infer information from them. Its cipher suites are also relatively weak and can be broken. Moreover, its domain will expire soon, which means that a hacker will be able to purchase it and gather information from clients by pretending to be Credit Suisse (UpGuard, 2023). The company can also implement firewalls and antivirus software to protect assets (Combs, 2022). It should also save data in backups so that it can be easily restored (Combs, 2022). Lastly, it should secure all

endpoints, such as desktops, laptops, and IoT (Internet of Things) devices, to prevent attackers from using them as entry points to the organization's network (Goldman, 2023).

CONCLUSION

The whistleblower exposing Credit Suisse had far reaching implications beyond the wrongdoings of the bank and its clients. It shined a light on the principles that governed the international legal and financial systems. Undoubtedly, the bank's past activities that turned a blind eye to the actions of its clients and the Swiss policies that permitted such activities were immoral and led to surging criminal offenses across the globe. However, in recent years, both parties have taken active steps to implement stronger measures as a response to mounting pressure from the international community.

This scenario questions the ethics surrounding cyber security as well. While the whistleblower had positive intent, hacking an organization continues to be illegal and unethical. Moreover, it provided an opportunity to question the 'hack back' policy that is currently gaining momentum, especially in America. While being legally allowed to conduct cyberattacks as a form of self-defense could be beneficial, it was concluded that it could have resulted in more dire conditions for the bank, such as the escalation of the issue into an international conflict.

Finally, while the bank has made significant progress in improving its security, it also needs to secure all its system entry points, install systems that track malicious activities, and ensure its websites are updated with the most recent defense mechanisms to protect itself from future attacks.

BIBLIOGRAPHY

B., P. Raquel. 2023. "Why Hacking the Hackers Is a Bad Idea: Ethical and Legal Implications." LinkedIn. August 15. https://www.linkedin.com/pulse/why-hacking-hackers-bad-idea-ethical-legal-penelope-raquel-bise-/.

BBC News. 2022. "Credit Suisse Denies Wrongdoing After Big Banking Data Leak." February 20. Accessed March 5, 2023. https://www.bbc.com/news/business-60456196.

Chin, Kyle. 2023. "Cybersecurity: What Should Companies Do After a Data Breach?" UpGuard. Updated March 02. https://www.upguard.com/blog/what-should-companies-do-after-a-data-breach.

Cohn, Scott. 2013. "Companies Battle Cyberattacks Using 'Hack Back.'" CNBC, June 4. https://www.cnbc.com/id/100788881.

Combs, Veronica. 2022. "Credit agency warns weak cybersecurity defenses could hurt a company's credit rating, even before an attack." Tech Republic, April 6. https://www.techrepublic.com/article/credit-agency-warns-weak-cybersecurity-defenses-could-hurt-a-companys-credit-rating-even-before-an-attack/.

Credit Suisse Group AG. 2022. "Annual Report 2022." Credit Suisse.

Credit Suisse. 2022. "Credit Suisse Group Statement." Zurich, February 20. https://www.credit-suisse.com/about-us-news/en/articles/media-releases/csg-statement-media-202202.html.

Credit Suisse. 2023. "Global Statement of Information Security 2023." Chief Security Office (CSO) and Chief Information Security Officer (CISO), Credit Suisse.

Goldman, Dov. 2023. "The Dangers of Data Leakage: How to Keep Your Data Secure." Panorays. October 15. https://panorays.com/blog/what-is-data-leakage/.

Kaplan, Fred. 2023. "When It Comes to Cybersecurity, the Biden Administration Is Getting Much More Aggressive." Slate, January 17. https://slate.com/news-and-politics/2023/01/biden-cybersecurity-inglis-neuberger.html.

Pegg, David, Kalyeena Makortoff, Martin Chulov, Paul Lewis, and Luke Harding. 2022. "Revealed: Credit Suisse Leak Unmasks Criminals, Fraudsters and Corrupt Politicians." The Guardian, February 20. https://www.theguardian.com/news/2022/feb/20/credit-suisse-secrets-leak-unmasks-criminals-fraudsters-corrupt-politicians.

Soesanto, Stefan. 2021. "Hacking Back Unpacked: an Eye For an Eye? Not So Fast." CSS ETH Zurich. https://isnblog.ethz.ch/cyber/hacking-back-unpacked-an-eye-for-an-eye-not-so-fast.

UpGuard. 2023. "Credit Suisse." Last updated December 01. https://www.upguard.com/security-report/credit-suisse.

Winstead, Nicholas. 2020. "Hack-Back: Toward A Legal Framework For Cyber Self-Defense." American University Washington, DC https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm.