Breach Incident Analysis

Midterm

Sri Dhanush Reddy Kondapalli

CWID: 10476150

FIN 545-WS

Describe the threat that manifested itself in the attack. Was the attacker an outsider? An insider? Is there any knowledge of the attacker's motivation?

In July 2020, the United States Securities and Exchange Commission (SEC) announced that it had filed charges against an individual for orchestrating a sophisticated hacking scheme that resulted in the theft of over $1.7 million from multiple brokerage firms. The SEC's complaint alleges that the individual, who is a former registered representative of a broker-dealer, used stolen customer credentials to gain unauthorized access to online brokerage accounts and then executed trades to generate profits for himself. The SEC also alleges that the individual engaged in a scheme to solicit customers of a broker-dealer to provide him with their login credentials, which he then used to gain unauthorized access to their accounts (Henning, 2019). The SEC's complaint charges the individual with violations of the federal securities laws, including the antifraud provisions. The SEC is seeking a permanent injunction, disgorgement of ill-gotten gains, and a financial penalty. This incident is an example of a cyberattack that was carried out by an insider. The attacker had access to customer credentials, which he used to gain unauthorized access to online brokerage accounts. The SEC's complaint alleges that the attacker engaged in a scheme to solicit customers of a broker-dealer to provide him with their login credentials. The SEC's complaint charges the individual with violations of the federal securities laws, including the antifraud provisions. The SEC is seeking a permanent injunction, disgorgement of ill-gotten gains, and a financial penalty.

Describe the institution's vulnerability that was exploited by the attacker. Was it a technical vulnerability, or a flaw in a business process, or perhaps a human error exploited by a social engineering attack?

The SEC's complaint alleges that the individual hacked into the online accounts of multiple victims and used those accounts to place trades in penny stocks. The trades resulted in the individual making over $1.7 million in profits. The individual then allegedly transferred the money to overseas bank accounts in an effort to hide the proceeds of the scheme. The SEC's complaint alleges that the individual hacked into the online accounts of multiple victims and used those accounts to place trades in penny stocks. The trades resulted in the individual making over $1.7 million in profits. The individual then allegedly transferred the money to overseas bank accounts in an effort to hide the proceeds of the scheme. The individual used a variety of methods to gain access to the victims' accounts, including phishing attacks and malware. In some cases, the individual was able to gain access to the accounts by correctly answering security questions. In other cases, the individual was able to reset the victims' password by correctly answering security questions. Once the individual had access to the victim's account, he used the account to place trades in penny stocks. The SEC's complaint alleges that the individual engaged in a sophisticated hacking scheme that resulted in the theft of over $1.7 million from multiple brokerage firms. The individual used a variety of methods to gain access to the victims' accounts, including phishing attacks and malware. In some cases, the individual was able to gain access to the accounts by correctly answering security questions. In other cases, the individual was able to reset the victims' password by correctly answering security questions. Once the individual had access to the victim's account, he used the account to place trades in penny stocks. The trades

resulted in the individual making over $1.7 million in profits. The individual then allegedly transferred the money to overseas bank accounts in an effort to hide the proceeds of the scheme.

Provide a summary of available information about the institution's response to the incident. Describe steps taken to react to the incident and restore normal operations.

According to the SEC's complaint, the individual used stolen customer credentials to gain unauthorized access to online brokerage accounts and then executed trades to generate profits for himself. The individual also allegedly used the stolen customer information to open new accounts in the name of the customers and funneled the proceeds from those accounts into his own bank account. The individual was finally caught when one of the brokerage firms noticed unusual activity in a customer's account and contacted the customer. The customer then confirmed that they had not authorized the trades. The brokerage firm then contacted the SEC, which launched an investigation (Stroschein *et al.,* 2020). Through the investigation, the SEC was able to identify the individual and obtain a court order freezing his assets. The SEC is now seeking to recover the stolen funds and is also seeking to bar the individual from ever working in the securities industry again. This is a prime example of why it is important for financial institutions to have strong cyber security measures in place. Had the brokerage firms had stronger security measures in place, the individual may never have been able to gain access to the accounts in the first place. There are a few key lessons that can be learned from this incident. First, it is important to have strong security measures in place to protect customer information. Second, it is important to monitor account activity for unusual activity. And finally, it is

important to contact the proper authorities if you suspect that someone has gained unauthorized access to customer accounts.

How could the institution have prevented the incident? What should they do to prevent similar incidents from happening again?

The SEC's complaint alleges that the defendant, who was a registered representative of a brokerage firm at the time of the hacks, used stolen customer credentials to gain unauthorized access to the online accounts of other customers at different firms in order to transfer funds into his own account. The defendant then allegedly used the stolen funds to purchase bitcoin and other cryptocurrencies. The SEC's complaint further alleges that the defendant created fake online accounts in the names of some of his victims in order to conceal his identity and make it appear as if the transfers were made by the victims themselves. The defendant also allegedly impersonated a customer service representative of one of the firms in order to reset the password of a victim's account and gain access to it. The SEC's complaint charges the defendant with violating the antifraud provisions of the federal securities laws (Saundal, 2021). The SEC is seeking a permanent injunction, disgorgement of ill-gotten gains plus interest, and imposition of a civil monetary penalty. According to the SEC, the defendant's scheme highlights the importance of firms taking steps to protect their customers' accounts from cyber theft, and of customers being vigilant about protecting their own account information.

There are a number of steps that firms can take to protect their customers' accounts from cyber theft, including: Implementing strong authentication measures, such as two-factor authentication, for customer account access; Monitoring for and promptly responding to unusual

account activity; Educating customers about the importance of protecting their account information and not sharing it with anyone; and Requiring customers to use strong passwords and to change them regularly.

Customers can also take steps to protect their accounts, including: Not sharing their account passwords with anyone; Creating strong passwords and changing them regularly; Notifying their firm immediately if they suspect that their account has been hacked or if they receive suspicious emails or calls purporting to be from their firm; and Reviewing their account statements and transaction history regularly to look for unauthorized activity.

Based on the publicly available information, do you believe the incident resulted in substantial costs to the institution? Why or why not.

Based on the information that is publicly available, it does not appear that the incident resulted in substantial costs to the institution. The SEC's complaint alleges that the individual was able to gain unauthorized access to the brokerage firms' systems and then used that access to transfer funds from the firms to his own bank account. The complaint does not allege that any customer information was accessed or that any customer accounts were compromised. As a result, it does not appear that the incident resulted in any direct costs to the institution in terms of customer remediation or data breach response.

What additional information would you like to know about the incident that was not found in publicly available sources? Keep in mind that publicly available information about cyber breaches will always be incomplete. Being aware of likely gaps in information about incidents is part of the challenge.

According to the SEC's complaint, the individual, who was not named, used a variety of methods to gain unauthorized access to the brokerage firms' online accounts and then executed trades that generated millions of dollars in profits. The individual then withdrew the funds from the accounts and laundered the money through a series of cryptocurrency transactions. The SEC's complaint alleges that the individual began the scheme in February 2019 and continued it until at least July 2020. During that time, the individual accessed at least 15 different brokerage firms' accounts and made over $1.7 million in profits. The SEC's complaint charges the individual with securities fraud and seeks disgorgement of ill-gotten gains plus interest, penalties, and injunctive relief.

References.

1. Henning, P. J. (2019). A taxonomy of cryptocurrency enforcement actions. Brook. J. Corp. Fin. & Com. L., 14, 227.

2. Saundal, S. (2021). Cryptocurrencies: Analysis of the Technology and Need for Its Regulation. Available at SSRN 3903787.

3. Stroschein, J., Garnet, J., Kulm, A., Nelson, T. J., O'Brien, A., Pauli, W. E., ... & Kettani, H. (2020). CLEAR CONFERENCE COMPUTER SCIENCE ACADEMIC PAPERS. South Dakota Law Review, 65(3).