Malayan Colleges Mindanao

M3|FINAL PROJECT

IS102 - Professional Issues in Information System

Submitted By :

Alfred Ashley F. Andrion

Bachelor of Science in Information System

To be submitted to:

Cherry Lisondra

College of Computer and Information Science (CCIS)

Date of Submission:

January 24, 2022

A CASE STUDY ABOUT THE JULY 2020 TWITTER ACCOUNT HACKING

Introduction:

A small group of hackers led by a teenager persuaded internal Twitter employees into disclosing administrative tool credentials in July 2020. Twitter can use these tools to manage any account on the platform. Some of the most well-known Twitter accounts were hacked, notably Barack Obama, Jeff Bezos, and Elon Musk. They tweeted a hoax involving collecting bitcoin from followers in exchange for a value double following their access gain. The tweet meant that if they would send any bitcoin amount to a certain bitcoin wallet address, then the amount sent back to them would be doubled since when you send a cryptocurrency from one wallet to another, the point of origin can be traced back. Therefore, it is easy to send money anywhere through crypto, so many people target others who have vulnerable crypto assets. Before Twitter forcibly removed the fraudulent posts, more than 320 transactions, totaling $110,000, had already occurred on one wallet. A total of eight non-verified accounts' communication histories were also obtained. It was one of the most significant hacks of a major social media platform to date. In addition to causing havoc and harming Twitter's brand, the attack raised concerns about the company's influence over its users. More than 1,500 full-time workers and contractors can make changes to user accounts. By the end of July, the authorities arrested three individuals. They charged them with wire fraud, money laundering, identity theft, and unauthorized computer access related to scams.

According to forensic examination of the scam, it began with accounts with a short distinguishing name, such as @6. It then moved on to cryptocurrency accounts, such as Coinbase, Coindesk, and Binance, some of the most well-known cryptocurrency exchanges. Later, they expanded their

hacking to include high-profile accounts with millions of followers and significant corporations like Apple, Uber, and Cash App. They stated that their money would double any bitcoin amount contributed to the wallet as part of a COVID-19 rescue effort, with tweets created and sent from IP addresses linked to many locations. They disguised the wallet address by sending fraudulent links from multiple cryptocurrency companies; the website holding the links was taken down immediately after the tweets were sent, and Twitter even erased the rephrasing of tweets as part of their response to the scam. Even while the "twice the amount" fraud has been around for a while on social media sites, this was the first time they used high-profile accounts. Experts suspect the scammers used a "smash and grab" approach, which involves making a significant amount of money in a short amount of time. The majority of the assets annexed are thought to have come from Chinese accounts, with roughly a quarter coming from US wallets. After receiving it, they move a particular amount of bitcoin to numerous wallets to hide their identities and make it more difficult to track them down. Twitter was made aware of a security breach affecting some Twitter accounts. The reused phrasing tweets aided Twitter in taking corrective action, such as removing or restricting certain functionalities for specific Twitter accounts. Twitter felt it had addressed all of the compromised accounts and restored its credentials to its rightful users three hours after the theft began. Coinbase, a cryptocurrency exchange, claims to have banned bitcoin addresses to prevent money from being sent and claims to have halted over a thousand transactions worth over $280,000.

Given the difficulties raised by the Twitter hack, regulatory guidance is required to ensure that large social media businesses have adequate safeguards in place to combat ever-changing dangers effectively. There is currently no dedicated regulation for social media firms. They are subject to the same broad scrutiny as other businesses. For example, the SEC's rules for all public firms apply

to public social media companies, and the Department of Justice and the Federal Trade Commission's antitrust and related laws and regulations apply to social media companies as they do to all corporations. The General Data Protection Regulation (GDPR) of the European Union, which governs the storage and use of personal data, also applies to social media companies doing business in Europe. However, no agencies have the authority to oversee social media sites that operate via the internet uniformly and address the cybersecurity vulnerabilities raised in this report. It's time to fill that regulatory void.

Ethics Worksheet for Case Studies

1. What is the ethical issue/problem in one sentence? State this in the form of an ethical question an IT practitioner would need to consider.

A series of cyberattacks was done through social engineering some social media company employees, which led to illegal activities such as Wire fraud, money laundering, identity theft, and unauthorized computer access related to scams, which stained the reputable values of integrity and professionalism of IT practitioners.

2. What facts have the most bearing on the ethical decision you must render in this case? Note: facts do not include ethical judgments at this point.

• A small group of hackers managed to coerce an internal company employee to provide the administrative tools for them to begin their hacking.

• Many people felt vulnerable when they became aware of the company's restrictions due to the hacking activities; therefore, they possibly knew that their account was targeted and needed to be retrieved by the company.

• The hackers did the scam fast, just like a smash and grab scheme; therefore, it did not last long. The company somehow managed to sniff out the attack; thus, the company quickly responded by connecting to the figures and companies affected and restricting access to any fraudulent activities during that time. They informed companies that were being used and involved to block off the bitcoin addresses the hackers used by either blocking it from receiving any amount of Bitcoin(BTC) being sent to their address.

3. Are there any other external or internal factors to be considered? (Economic, political, etc.)

During the month of the incident, there was a concern regarding the 2020 United States presidential election. They were concerned that information on social media platforms would be vulnerable and can be easily manipulated through social engineering, which might cause security concerns because it can cause a big impact on social media discussions, especially since it was an election period. Thankfully after the case was brought up to a close, the social media company, Twitter, clarified that it was just a fraudulent hack. None of it concerns outside factors politically and economically.

4. Who are the claimants, and in what way are you obligated to each of them? (List all affected by your decision.)

Although Twitter did not clear all the individuals, who were affected, they just reported that there were eight compromised accounts where their account data was downloaded. It includes all created posts/tweets and direct messages. There is also a suspicion that more than 30 accounts had their

direct messages (dm's) accessed but not downloaded, including the Dutch Parliament Representative Geert Wilders. Still, other than him, they believe that no other government officials were affected. Every person/company involved has the right to voice out their concerns. Individually they have the right to be informed, the right to damages, the right to file a complaint, and the right to object to formally and legally document whatever written request or complaint the claimants have and pursue legal obligations. In any case, if there are points that can be addressed and solved, then it is better to amend things for better data security and protection. High-profile Twitter account owners and fraud victims are among those who can be identified as claimants.

5. What are the operant ideals? Note: ideals are values and behaviors based on them.

• For you.

If feasible, I will use projects, leadership, and accredited educational programs to demonstrate my capabilities, encouraging others to do the same. In this case, I will also not hesitate to seek assistance or guidance from legal departments or professionals when faced with challenges beyond my abilities or experience. I will ask for other peoples' advice and guidance which would serve as a new learning experience for me and my shortcomings, and I will do the same if my assistance is needed and share the things I learned and experienced with others.

• For the client/organization/profession.

If I were some IT personnel inside the Twitter company, I would highly recommend enforcing safety regulations regarding data privacy risks and monitoring employees who have access to the administrative tools that manage the user's accounts. If possible, I would also suggest a better way of having different forms of authentication that provide them better security and a safer option than the client may be comfortable with according to their preference and whichever is convenient for

them. To avoid such a case from happening again in the future, the organization should monitor suspicious activities proactively and have an action plan in advance. When a cyberattack occurs, speed is the number one factor preventing further damages and data privacy loss. As IT practitioners, we should always respect the confidentiality and privacy of the clients and provide them with the best service that the IT practitioner can offer. We should not condone vile acts, and whenever you can stop one, you should do your best to save the integrity and professionalism of the IT profession.

6. Do any of these ideas conflict? In what order would you honor them?

Ideas will only get conflicted if one were to negate the other or if it's not technically feasible. First, before we consider anything else, we need to lessen the damage done by the attackers to the organization and the system. After sorting things out, we then try to negotiate with the victims as to what we want to happen or can offer to do, and we should also hear out their complaints regarding the issue so we can make a compromise because in doing so, we are putting value to our clients. Lastly, to minimize and prevent further damage, we should always try to learn from the shortcomings of the people and the system because by doing so, we can learn to improve in the areas that we are lacking. At the same time, it makes the people and the company grow even though it experiences a little loss from time to time. Experiencing problems helps us grow, and it exploits the current issues that need to be addressed.

7. What are your options, and which would be favored by each affected party? (List at least three.)

• To track down and punish those involved for the crimes and damages they have done to the affected users.

• To provide compensation to those severely affected if there is any harm or loss done.

• To strengthen data privacy measures and implement a better way of securing authentication processes. It is best to provide a regulatory approach to help lessen risk-based cybersecurity systems.

8. Which options could cause harm to any claimant?

There would be no options that should cause harm to any claimant, in my honest opinion, mainly because we are offering our services to please the clients to continue using the company's product. Therefore, we value them by providing our best services.

9. Would honoring any of the ideals listed above invalidate any of your options?

No, ideas may be possible to be ruled out if they were in a different case. But in this case, the options mentioned above are the only viable ones for this study.

10. Are there any rules, principles, or codes (legal, professional, organizational, or other) that automatically invalidate any of your options?

There are no rules, principles, or codes that would automatically invalidate any of my options because I based it on the interest of the SANS IT Code of Ethics.

11. Which ethical theories support or reject which options? Explain.

The ethical theory that supports the ideas mentioned above is Nonconsequential: Kant's "Categorical imperative" because it dictates that "One should constantly respect the dignity of others and only act under rules that apply to everybody. ". The categorical imperatives decree that "MORAL OBLIGATIONS ARE DERIVED FROM PURE REASON, AND YOU MUST Respect THEM REGARDLESS OF ANY DESIRES." which correlates and supports the ideas which are

mainly concerned with legal actions. This theory's goal benefits the greater good of things by abiding by the law and proper order.

12. Determine a course of action based on your analysis.

As an IT practitioner, I would continue to practice proactively reviewing malicious activity on the web, especially when trying to target one of the company's applications or software. Such effort is important to build up the trust and confidence needed to survive in the industry. At some point, we should also educate people on how important it is to be cautious of fraudulent ads/activities. We should also enable them to easily identify potential risks that may result in data privacy loss.

13. Defend your decision in writing to your most adamant detractor.

Although regulations regarding social media data are still not that strict in the Philippines, the government should already have action plans in advance to protect the usage of information because it is systematically crucial for all of us voters, consumers, organizations/companies, and especially to the government. Information should be well protected and should always be used to maintain stability. All companies, locally and globally, essentially need to regulate themselves. Even without the government's backing, they already have action plans that would be terminated if a conditional situation were about to happen. As a consumer, even if the government wouldn't be able to fully dedicate a federal regulator that could ensure cybersecurity practice to prevent fraud, disinformation, and other systematic threats to its people, there still should be a council or organization that provides the monitoring and supervision of the cybersecurity of big social media companies and its platforms.

Conclusion:

Twitter was brought to its knees by the Twitter Hack. A group of unsophisticated cyber thieves who utilized social media to cause enormous disruption for hundreds of millions of users was the David to this Goliath's Goliath. With the election just weeks away, it's was more important than ever to tighten cybersecurity to prevent social media platform misuse. More than half of Americans use social media to keep up with news and communicate with coworkers, family, and friends. This shift needs a regulatory framework that recognizes social media as an important infrastructure.

References:

•Sai Chavali (June 25,2018). 5 Examples of Malicious Insider Data and Information Misuse. Retrieved from: https://www.proofpoint.com/us/blog/insider-threat-management/5-examples-malicious-insider-data-and-information-misuse

•Wikipedia contributors (2020). 2020 Twitter account hijacking. Retrieved from: https://en.wikipedia.org/wiki/2020_Twitter_account_hijacking

•Wikipedia contributors (n.d.). Social engineering (security). Retrieved from:https://en.wikipedia.org/wiki/Social_engineering_(security)

•Sheera Frenkel, Nathaniel Popper, Kate Conger and David E. Sanger (July 15, 2020). A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam. Retrieved from: https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html

•Joanne Berman, Jonathan Blattmachr, Debra Brookes, Shirin Emami, Robert Francis, Marcia Henry, Justin Herring, Matthew Homer, Katherine Lemire, Sasha Mathew, Chris Mulvihill, and Richard Weber (N.D.). Twitter Investigation Report. Retrieved from: https://www.dfs.ny.gov/Twitter_Report#:~:text=On%20July%2015%2C%202020%2C%20a,assigned%20to%20high%2Dprofile%20users

•Nicholas Thompson, Brian Barret (September 24, 2020). How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One. Retrieved from: https://www.wired.com/story/inside-twitter-hack-election-plan/

•National Privacy Commision(N.D.). Know Your Data Privacy Rights. Retrieved from: https://www.privacy.gov.ph/know-your-rights/

•Peter H. Gregory (N.D.). SANS IT Code of Ethics. Retrieved from: https://peterhgregory.wordpress.com/professional-background/sans-it-code-of-ethics/

•Lindsey O'Donnell (November 6, 2019). Rogue Trend Micro Employee Sold Customer Data for 68K Accounts. Retrieved from: https://threatpost.com/trend-micro-rogue-employee-68k-customers/149946/

•Ashley Watters (July 1,2021). 5 Ethical Issues in Technology to Watch for in 2021. Retrieved from: https://connect.comptia.org/blog/ethical-issues-in-technology

• Kailee Kodama Muscente (July 13,2020). Categorical Imperatives. Retrieved from: https://www.tc.columbia.edu/institutional-review-board/irb-blog/categorical-imperatives-and-the-case-for-deception-part-i/#:~:text=The%20idea%20of%20categorical%20imperatives,a%20philosopher%20from%20the%201700s.&text=Kant%20defines%20categorical%20imperatives%20as,imperatives%20are%20binding%20on%20everyone