Information Technology Incident Report and Summary

Brett Logan

Southern New Hampshire University: Global Campus

IT 659: Cyberlaw and Ethics

Professor: Dr. Mark Cohen, Ph.D., J.D.

February 6, 2021

Table of Contents

I. Executive Summary

The following report provides an in-depth case analysis of the hacking incident involving Twitter Inc. in July of 2020. This information technology incidence report will address the cyberlaw, ethics, security, culture, and global impacts of the incident through the lens of legal and compliance issues and current ethical standards. The findings and recommendations contained herein are intended to augment successful management in information technology and prevent future security incidents.

II. Introduction

A. Application of Cyber Principles

Entire industries such as e-commerce and e-communication have arisen due to the advancements in internet technology and its ability to connect anyone, from anywhere, across the globe. Companies such as Google, eBay, Amazon, and Twitter have achieved immense success by harnessing that reach and bringing their goods and services to the world. With this newfound reach, these businesses have likewise become exposed to a new style of attack, the cyber-attack. Perpetrators of such attacks may take action from anywhere in the world. An integral part of e-business is to safeguard customers by maintaining ethical obligations to respect cyberlaw and security principles, "the purpose of the cyber security principles is to provide strategic guidance on how organisations [*sic*] can protect their systems and information from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond" (ACSC 2020). Those principles echo the United States of America's cyber strategy which declares: “cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents” (Whitehouse 2018). Businesses must in kind develop their own cyber security strategy, making a concerted effort to protect themselves and their customers from cybercrime. The following principles may be used as a guide:

- *Governance* involves identification and management of security risks, such as the anticipation of how cyber-attacks could potentially occur. This involves management from the very top, and major companies within the aforementioned industries should have a Chief Information Security Officer to oversee security protocols and establish company-wide cyber security culture and hygiene.
- *Protection* means implementing security protocols to mitigate risks. This includes the utilization of security software, encryption, data back-up, etc. In e-communications, this also means safeguarding user accounts and controlling access to them.
- *Detection* means just that, the ability to detect/identify security breaches when they do occur, quickly and efficiently. E-businesses must have a monitoring system in place to alert of potential breaches in security.
- *Response* consists of the actions taken by a company in reaction to a security incident. This principle determines the extent of damage sustained and successful recovery from that incident, as well as identifying necessary actions to prevent a similar occurrence from happening again.

As online businesses continue to grow, the threat of attack in the cyber realm does as well. These principles, if properly followed, amount to an effective defense, but what happens when a company fails to adhere to some or all of them?

B. Summary of Case

E-communication platform Twitter suffered such a fate on the morning of July 15, 2020. After gaining access to Twitter's administrative tools, "attackers targeted 130 Twitter accounts, ultimately Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7" (Twitter Inc. 2020). Over the course of that day, many afflicted accounts had their passwords changed and were tweeting out a Bitcoin scam to trick people into sending money. As one of the world's most powerful communication tools, the breech is a pivotal moment in history that provides insight into the importance of cyber principles, which take on even greater meaning when the subject of attack is an industry titan: "Twitter's accessibility, format, app-specific features, global reach, and interconnectivity within the app have allowed it to not only change its users' communication but altered the landscape of global communication as well" (Baker 2018). This incident was a direct result of failure in basic security protocols such as employee education and vigilance, and back-door access to user data. "The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections" (Twitter Inc. 2020).

The following incident report will take a deeper look at the attack, providing analysis, findings, and conclusions from which recommendations will be made.

III. Case Analysis

A. Ethical Issues

The July Twitter hack can in part be blamed on a lapse in organizational ethics. The incident could not have occurred without numerous Twitter employees falling for a spear-phishing scam over the phone, which resulted in them providing their credentials to the hacker. The hacker then used these credentials to take over user accounts and send out tweets from them. The potential harm that could come from such a lapse in judgement is immense, "the threat here is not simply user privacy and data security, though those threats are real and substantial. It is about the striking potential of Twitter to incite real-world chaos through impersonation and fraud" (Newton 2020). One must ponder how employees at such a potentially powerful company could fall prey. The most obvious answer involves several ethical failures including lack of training, insufficient security protocols, and a failure in organizational security culture.

Lack of Training: Employees should have been properly trained to detect attempts being made to trick them into divulging passwords and sensitive information.

Insufficient Security Protocols: Individual employees should not have been able to bypass 2FA and reset account permissions. Multiple employees resetting passwords and accessing administrative privileges simultaneously should have raised a security alarm somewhere in the company, "establishing a baseline for workflows and employee behavior and then using security analytics and user behavior analytics to detect anomalies and deviations from that baseline can also be a good approach that complements preventive controls" (Conklin 2020).

Failure in Security Culture: Macro emphasis on security issues, such as hiring executives and focusing primarily on software vulnerabilities may have led to the simple, everyday security precautions being overlooked. There was a vacant Chief Information Security Officer position for an entire seven months leading up to the incident.

B. Legal Compliance

Twitter is legally bound to protect user data integrity and comply with regulations put in place to protect consumers. Such regulations include the General Data Protection Regulation (GDPR) of the E.U., the California Consumer Privacy Act (CCPA), as well as Breach laws in effect in all fifty states. These regulations stipulate the steps an organization must take in the event of a breach or compromise, such as customer notification of the incident.
Twitter officially acknowledged a "security incident" at 2:45 PM the day of the attack, and by July 17 had posted a briefing summarizing what happened, how, who was affected, and what actions were being taken. In doing so Twitter was in compliance with notification laws and regulations.

The ability of the attacker to manipulate employees into giving out passwords and thus gain the ability to access administrative accounts and take over user accounts leads to grey areas in regard to regulation adherence. Further clarification on the exact extent of minimum security protocols must be established in order to determine an official breach in compliance of the GDPR and CCPA.

Other legal issues arise with the overall access that the attacker gained. One potential scenario is the possibility of widespread market manipulation being achieved through the hijacked Twitter accounts. For example, the attacker takes out a position in Tesla stock before tweeting erroneous news or information from the official Tesla twitter account, causing a sudden increase in stock price upon which the hacker exits their position. This ability to manipulate the markets could have been sold to others, and ultimately violated insider trading laws and regulations. This potentiality is another illustration of the true power of Twitter and the importance of defensive IT Security.

C. Societal and Cultural Impact

The ethical failure by Twitter to train employees at a very basic level could have lasting implications. This lack of security awareness and protocol implementation affects the way big tech companies are viewed based on perceived priorities.

Such a public failure in any major company's IT security undoubtably calls into question how safe user data truly is. While, thus far, no data has been shown to have been used maliciously, and the hacker was simply tweeting out a Bitcoin scam, the high-profile nature of targeted accounts displayed to the world a certain fragility in cyber defense. The incident raises questions that society must readily entertain, such as the rights of users and obligations of companies. Additionally, a particular subset of society was targeted, which may lead to lasting impressions. The hack targeted cryptocurrency holders in an effort to steal their Bitcoin, "twitter scammers collected 13 bitcoin amounting to more than $110,000 after hacking high-profile accounts and posting fake donation links under victims' names" (Conklin 2020). This kind of event likely contributes to the notion that Bitcoin is related to criminal activity and can harm the ongoing cultural adoption of cryptocurrency in general. As many countries' governments are currently developing their own central bank digital currency (CBDC) for their populations to transact with in the future, the acceptance and trust in such digital assets is paramount to successful implementation and forward economic thinking. This incident serves as a setback in that regard.

Additionally, this incident negatively affected Twitter Inc. stockholders: post-attack, "shares of Twitter dropped by more than 4% in pre-market trading, erasing roughly $1.3 billion in market value" (Holmes 2020). This is a dangerous moment for any publicly traded company, as loss of investor confidence could hinder future growth funding and contribute to further devaluation of stock prices. Finally, such drastic price movement can activate trading bots to exit their positions, leading to a cascading effect and mass-market sell-off.

All of these things serve to undermine consumer confidence in IT related companies, from a security, financial, and user experience (i.e. privacy and trust) perspective. Our interconnected global economy relies on consumer participation to keep things running and growing; the world simply cannot afford to lose faith in major influential businesses without cross-industry impact.

IV. Incident Impact

A. Regulations

The incident caused widespread concern, even into the upper echelons of government: "Republican Senator Josh Hawley wrote to Twitter imploring founder Jack Dorsey to cooperate with federal officials in investigating the attack…one option is decentralizing Twitter to remove its "single point of failure" " (Hamacher 2020). Decentralization would involve open protocols and a better-defined set of rules and network stability, and Twitter CEO Jack Dorsey is currently considering such a move.

Conversations are now occurring in an attempt to identify and address regulations which could prevent such attacks from being successful in the future, "[There] are no regulators that have the authority to uniformly regulate social media platforms that operate over the internet, and to address the cybersecurity concerns identified in this Report," notes the Department of Financial

Services report. "That regulatory vacuum must be filled" (Morse 2020). The same report specifically named Twitter and identified this incident, using it as an example for why anti-trust regulation is needed. With the presidential transition occurring in 2021, the new administration is likely to take up this issue and seek further regulatory clarity.

B. Standards

Deviance from industry standards played a role in the success of this attack. Very basic accepted security protocols were not followed, "they shouldn't have given the ability to a single employee to remove both email address on file and two-factor authentication" (Tidy 2020). This step alone would have thwarted the attacker. This failure was not catastrophic in itself, however, and the attack could have still been stopped at the next step: "organizations need to consider in their threat modelling what happens when an administrator is compromised and what controls they can put in place to detect that or to prevent it from having a big impact on their systems" (Constantin 2020).

Another common IT industry standard is the role of Chief Information Security Officer (CISO), and at the time of the occurrence, Twitter had been without one for seven months. It is the role of the CISO to set the top-down leadership, security stance, and security culture of a company, all clearly lacking at the time of incident.

C. Cultural Impact

The Twitter hack highlighted to the world how important IT security is. Where social media was once looked at as a mere communication tool to connect people, the true scope of its influence was illustrated by this incident. The fact that it occurred in an election year sparked multiple conversations on the power and influence of big tech companies and how they can be used. When that power falls into the hands of a hacker it causes great concern and affects the way the public views IT, as the access gained "could undermine elections, damage responses to health or climate emergencies through compromising critical communications links with the public, and in a worst-case scenario lead to a conflict between state actors" (Hamacher 2020). This incident has encouraged legislators to look at needed regulations and forced IT companies to take a close look at their security protocols and culture. At the end of the day, users of the platform drive its success, and these users need to feel confident and protected. The past six months have brought increased communication and reassurance from Twitter, and as time goes by more industry regulations are likely to follow.

On a positive note, the incident has served to bring widespread attention to both phishing-type scams, and cryptocurrency giveaway scams. The public has been made aware that even though an account they follow on Twitter is "verified", there is always a chance that what they are reading or seeing originated from someone else, and thus caution is warranted, especially when an offer seems too good to be true.   Ultimately, the regulations and security innovations that arise from this incident will be a benefit to all.

V. Recommendations

A. Organizational Changes

There are certain relevant changes Twitter could, or could have, adopt(ed) which would have potentially prevented the July hacking incident. At its core, the method of attack was considerably uncomplicated, as the hackers "used basic techniques more akin to those of a traditional scam artist: phone calls where they pretended to be from Twitter's Information Technology department. The extraordinary access the Hackers obtained with this simple technique underscores Twitter's cybersecurity vulnerability and the potential for devastating consequences" (NYS 2020). To prevent such an occurrence, the following organizational changes are recommended:

-*Security Leadership*: Twitter must maintain a Chief Information Security Officer (CISO) to set the overall tone and direction of the company's IT security culture. Prior to the incident, the CISO position was vacant for at least seven months.

-*Access Management and Authentication*: Twitter should utilize physical hardware multifactor authentication (MFA). During the incident, hackers were able to bypass Twitter's MFA by tricking employees into authenticating their application-based MFA during login. Furthermore, the number of employees given access to full administrative privileges should be limited, as this would have given the hackers fewer employees to target: "Twitter did limit access to the internal tools, but over 1,000 Twitter employees still had access to them for job functions and duties such as Twitter user account maintenance and support, content review, and responses to reports of Twitter Rules violations" (NYS 2020).

-*Employee Education and Training:* All Twitter employees should undergo routine security training including detailed explanation and education of phishing-type attacks. The CISO should implement regular phishing exercises to test and prepare employees for possible attack.

-*Security Monitoring:* Security Information and Even Management (SIEM) should be utilized to examine ongoing network access and utilization. Log management can be used to establish baseline norms, effectively helping to quicky identify and react to emergent security threats.

-*Remote Access Guidelines:* Do in part to the ongoing Covid-19 crisis, many Twitter employees were working from home and utilizing VPN connections to access the company network. The attackers took advantage of this break in routine by impersonating IT employees when engaging in the phishing attack. Establishing clear and concise remote access guidelines with declared troubleshooting directions could have mitigated the attack.

B. Ethical Guidelines

Ethics within an organization give employees a concrete sense of what is considered right and wrong, thus avoiding breaking the rules inadvertently and helping to achieve the corporate mission. One piece of corporate ethics is establishing "core values" for a company, and Twitter could benefit greatly from adding "*security*" to its core values. Combined with a top-down integration of security values, this could alter the very foundation of employee reactions to potential security events such as the phishing attack: "if they're going to really take hold in your organization, your core values need to be integrated into every employee-related process—hiring methods, performance management systems, criteria for promotions and rewards, and even dismissal policies. From the first interview to the last day of work, employees should be constantly reminded that core values form the basis for every decision the company makes" (Lencioni 2002). If Twitter were to implement this change to its core values now, there is a greater likelihood that a repeat of the type of phishing attempt seen in July would prove to be unsuccessful due to employee training and anticipation of such occurrences.

C. External Standards

Due to the evolving reach and influence of large social media platforms like Twitter, there should be a new type of designation for them. "The risks posed by social media to our consumers, economy, and democracy are no less grave than the risks posed by large financial institutions. The scale and reach of these companies, combined with the ability of adversarial actors who can manipulate these systems, require a similarly bold and assertive regulatory approach" (NYS 2020). The first step is to establish a social media regulator to declare and define applicable oversight for this growing industry. A shared set of cybersecurity norms throughout the industry could have influenced the culture at Twitter to the point of preventing employees falling for the phishing attack initiated during the July incident. Additionally, should an oversight council be put into place for social media companies, it would clear the way for them to "be subject to enhanced regulation, such as through the provision of "stress tests" to evaluate the social media companies' susceptibility to key threats, including cyberattacks and election interference" (NYS 2020). Having these types of industry wide cyber security standards would set the stage for establishing minimum accepted levels of safeguards, invite ongoing observation by outside parties, and ultimately contribute to the safety and privacy of platform users.

VI. Global Considerations

A. International Compliance

Several international compliance standards would have been relevant to this incident, including the EU General Data Protection Regulation (GDPR). "While the GDPR is an EU law, it applies to any company that makes its website or services available to EU citizens, including US companies" (GDPR 2021). Considering that the July attack relied on the ability to bypass two-factor authentication, it is concerning that in October 2019 "Twitter announced it had found that phone numbers and email addresses used for two-factor authentication may inadvertently have been used for advertising purposes" (Culliford 2019).

Article 32, Section 2 of the GDPR stipulates: "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised [*sic*] disclosure of, or access to personal data transmitted, stored or otherwise processed" (GDPR 2021). Had Twitter been in compliance at the time, personal data such as e-mail addresses and two-factor authentication data would not have been used for such purposes as advertising. This also means that being in compliance would have further safeguarded the data from exploitation leading to further network access as occurred in the July incident.

Article 32 additionally requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational [*sic*] measures for ensuring the security of the processing" (GPPR 2021). Examples of such measures that Twitter failed to test, assess, and evaluate can be seen in the lack of employee security awareness surrounding simple phishing attempts and solicited password resets. Again, compliance would have ensured employees were informed and prepared for such phishing attempts which the hacker ultimately used to gain access to the company.

B. Cultural Impacts

It can be said that the backbone of global communication and commerce is trust. When interacting online, we trust that the other party is who they claim to be. When purchasing from Amazon, a customer must have faith that the transaction is actually occurring with Amazon. Likewise, when a tweet is posted on Twitter, a user trusts that the words are coming from the actual owner of the account. Many, if not most, people around the world are not information technology savvy, and so they must trust that these things are true. The Twitter hack was a direct assault on this trust as it "created a uniquely unstable information event. First, Twitter's systems were compromised, resulting in a tsunami of disinformation. Then, in order to regain control of its systems, Twitter shut down the ability of all verified accounts to tweet anything at all, preventing both the victims of the attack, public officials, and the news media from publishing reliable information and creating a vacuum for misinformation" (Wong 2020). As a result, it became clear to an international audience that not everything posted on Twitter is guaranteed to be legitimately coming from the account owner. If accounts can be hacked, and the flow of information interrupted so that the compromised owner cannot communicate the situation, we are left with a global degradation of trust in e-communication.

Another profound international impact of the incident is the blatant revelation at the fragility of our current global communication and social media apparatus: "this incident highlights the extreme fragility of the modern information space. In a similar disinformation campaign, nation-state actors may simply announce a military or nuclear incident and provoke national havoc or spread fake news about a rival business to ruin its stock price and then purchase it for pennies" (Scroxton 2020). One aftereffect of the incident is that it can now be presumed global citizens are less likely to readily believe the things that they see and read online.

C. Global Technology Environment

As a result of the Twitter hack, there is a proposed shift in the classification of major social media companies, including labeling them as "systemically important" institutions, similar to the big banks. This paves the way for more strict oversight and penalties (such as fines) for security failures or oversights. The incident illustrated how a tech company as large as Twitter could be effectively weaponized via the potential takeover of user accounts and manipulation of public opinion. There have since been calls for the big tech companies like Twitter or Facebook to be broken up in an attempt to constrain some of this power and provide increased security: "if there were competition, different platforms would offer different security options, as well as different posting rules, different authentication guidelines—different everything" (Schneier

2020). This would make it less likely for a single security incident to have such wide-reaching ramifications.

VII. Summary

The application of cyberlaw principles, ethical needs, and legal compliance standards as applied to this incident serve to provide a lasting understanding of how it happened and the repercussions that ensued. The cyberlaw principles of governance, protection, detection, and response outline appropriate measures needed to equip organizations with the ability to face the ever-growing threat of cyber-attack. As applied to the Twitter incident, there was a failure in both protection and response, resulting in easy access for the hacker and potentially damaging repercussions when all accounts were disabled, preventing pertinent emergency information from being disseminated.

Ethical needs serve to harden an organization's defenses against attacks via their overall effect on organizational culture. This case highlights the potential damage of a lapse in ethical obligations, such as insufficient employee training and poor security culture. As a platform business model, Twitter was heavily focused on technology and the collection/utilization of user data, while concurrently neglecting the pertinent security education needs of its employees.

Lastly, legal compliance and the adherence to established cultural norms should be the groundwork for prevention of future incidents. If Twitter successfully complies with regulations such as the GDPR and CCPA, the likelihood of recurrent attacks and/or the extent of damages could be severely reduced. Regulations provide framework from which to create a successful security posture if heeded. The lessons learned in July serve to emphasize the overall importance of taking these things into consideration when addressing organizational security culture through the lens of cyberlaw and ethics.

VIII. References

Australian Cyber Security Centre. The Cyber Security Principles. https://www.cyber.gov.au/acsc/view-all-content/guidance/cyber-security-principles

Baker, Cody (2018). How Twitter Has Changed the Way Advertisers Communicate. Undergraduate Review, 14, 12-22. https://vc.bridgew.edu/undergrad_rev/vol14/iss1/7

Conklin, Audrey. 2020. Fox Business News. How Much Money Was Stolen In The Twitter Hacks? https://www.foxbusiness.com/money/amount-money-stolen-twitter-hacks

Constantin, Lucian. 2020. CSO. Twitter VIP Account Hack Highlights the Danger of Insider Threats. https://www.csoonline.com/article/3567508/twitter-vip-account-hack-highlights-the-danger-of-insider-threats.html

Culliford, Elizabeth. 2019. Reuters. Technology News. Twitter Makes Global Changes to Comply With Privacy Laws. https://www.reuters.com/article/us-twitter-privacy/twitter-makes-global-changes-to-comply-with-privacy-laws-idUSKBN1Y622J

General Data Protection Regulation (GDPR). 2021. Complete Guide to GDPR Compliance. https://gdpr.eu/article-32-security-of-processing/

Hamacher, Adriana. 2020. Decrypt News. 5 Key Things We Learned From the Twitter Hack. https://decrypt.co/35784/5-key-things-we-learned-from-the-twitter-hack

Holmes, Aaron. 2020. Business Insider. Twitter Saw $1.3 Billion in Market Value Wiped Out After a Massive Hack Targeted Barack Obama, Kim Kardashian, Elon Musk, and Other Prominent Accounts. https://markets.businessinsider.com/news/stocks/twitter-market-value-losses-after-massive-hack-2020-7-1029402144

Lencioni, Patrick. 2002. Harvard Business Review. Organizational Structure. Make Your Values Mean Something. https://hbr.org/2002/07/make-your-values-mean-something

Morse, Jack. 2020. Mashable Tech. Twitter Hack Shows Need For Cybersecurity Regulation, Govt. Report Says. https://mashable.com/article/twitter-hack-report-cybersecurity-regulations/

Newton, Casey. 2020. The Verge. The Massive Twitter Hack Could Be a Global Security Crisis. https://www.theverge.com/interface/2020/7/15/21325708/twitter-hack-global-security-crisis-nuclear-war-bitcoin-scam

New York State (NYS). 2020. Department of Financial Services. Twitter Investigation Report. https://www.dfs.ny.gov/Twitter_Report

Schneier, Bruce. 2020. The Atlantic. The Twitter Hacks Have to Stop. https://www.theatlantic.com/ideas/archive/2020/07/twitter-hacks-have-stop/614359/

Scroxton, Alex. 2020. Computer Weekly. Twitter Hack Fallout: Investigators on Trail of Cyber Criminals. https://www.computerweekly.com/news/252486303/Twitter-hack-fallout-Investigators-on-trail-of-cyber-criminals

The White House. 2018. National Cyber Security Strategy of The United States of America. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Tidy, Joe. 2020. BBC News. Twitter Hack: Staff Tricked By Phone Spear-Phishing Scam. https://www.bbc.com/news/technology-53607374

Twitter, Inc. 2020. Twitter Company Blog. An Update On Our Security Incident. https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

Wong, Julia Carrie. 2020. The Guardian. Should We Still Trust Twitter? Hack Fiasco Raises Major Security Concerns. https://www.theguardian.com/technology/2020/jul/16/twitter-hack-security-concerns-privacy