STANLEY ONYEDIKA EPUNA

STUDENT ID: 45731365

STRATEGIC CYBERSECURIY ROADMAP FOR THE BOARD (UNATRAC HOLDING LIMITED)

Introduction

Though they are benefits in using the internet, the vast rise in connection to the internet surpasses the ability to properly protect the digital world at larger (Alkhali et al., 2019). Security has always been an increasing concern in the digital business world. These cyber-attacks are becoming more intelligent, damaging and disruptive (Cichonski et al., 2012). Even after security controls have been put in place to predict how cyber breaches will take place, many companies still get hurt from numerous breaches (Lubbers et al., 2016). Data breaches normally occur when personal or confidential information are being gotten illegally through electronic or by paper for fraudulent purposes (Holtfreter, 2015).

Most times data breaches usually occur due to computer errors, human errors, or even through malicious activity. High percentage of these breaches are linked to human errors (Evans et al., 2018). Malicious attacks normally come in the form of Email messages, where the user opens or download email messages from untrusted email addresses. Phishing attacks capitalizes on these human errors which exposes confidential information. (Rosenberg, 2019).

This paper talks about the sophisticated cyber-attack carried out by a Nigerian entrepreneur named Obiwanne Okeke Invictus who performed his attack using Phishing on this particular data breach of interest. The impacts of this breach and actions taken will be thoroughly examined. Also, a strategic cybersecurity plan for this case study will be created together with how the data breach could be avoided.

The reason for choosing the case study.

My interest was on the attacker, who is identified under the Forbes list as African most promising entrepreneur (Dolan, A.2016); he is the CEO of Invictus group. He was truly looked up in Africa as a role model. Unatrac Holding Limited are one of the major distributors of construction equipment and power supply through the Mantrac group. This Mantrac group are big contributors to the economy in Africa, especially the Nigerian market, which is the biggest economy in Africa. the attack used on this company was through Business Email Compromise (BEC). This mode of attack is really becoming a global concern in both the industries and financial institutions. What interest me about this attack was how the victim fell using the phishing tricks being deployed.

The perpetrator of this attack

This data breach was being devised by the Nigerian entrepreneur syndicate by name Obiwanne Okeke Invictus. Being celebrated as a figure head. He was rated as one of the most promising young African aged under 30 in 2018 according to reports. (federal bureau of investigation, 2018). Obiwanne had a company named Invictus group which motto signifies reigning and unbeatable. This shows his zeal despite being brought up form a very poor background. The attack on the company was carried out through his associate company where the email account of the Chief Financial Officer of Unatrac Holdiing Limited was being compromised (Ferguson, 2019). Obinwanne took out this attack in April 2018 on Unatrac Holding Limited, which is a subsidiary of a U.S company that produces power generators and construction machineries. Obiwanne was apprehended on the airport where he was

waiting to catch a flight to Nigeria. He has been charged for computer fraud and wire fraud. Currently in the prison walls in Virginia.

Impact of the data breaches on the company and suitable actions taken.

Unatrac Holding lost so much money from this Business Email Compromise (BEC) attack, also a lot of data was stolen (Gatzlaff and McCullough, 2008).

The company was tricked through their financial team to pay the amount between $278,000 - $1.95 million in the form of vendor invoices to local companies like "Pak Fei Trading Limited" and also $2 million to oversea companies (Ferguson, 2019). Obiwanne accessed the CFO email and company's information for a month. The data stolen could also be sold to other people on the dark web. The effect on this data breach cannot be ascertained immediately because it takes years for it to be fully uncovered (Meja, 2019). So, the resulting effect affects the customer relationship and brand reputation, and this creates a roadblock in building relationship which could ruin the company.

Companies like Wells Fargo, Bank of America, and Barnes and Noble have all been a victim of data theft and these attack takes years to discover.

Companies that are hit by data breach usually recover in so many different ways. In this case this company contacted the bank to recover part of the transfers from the scammers. Furthermore, Unatrac holding performed an audit to show how much the fraudsters stole from the CFO, checking whether emails of staffs were also compromised, also how much was transferred to the impersonator. Thirdly, an official complaint was made by Unatrac to the FBI in June 2018 stating the email of its CFO has been compromised with money stolen during the process (Ogundipe, 2018).

Cybersecurity plan for Unatrac Holding Limited

The ever-increasing threat from these cyber attackers on financial institutions and organisations has made companies develop cybersecurity plans to manage and access the cyber risk. So, in this case Unatrac Holding needs to find a cybersecurity plan that assess, identify, and manage cyber risk. The plan to develop a plan is important irrespective of how large the organisation is and how sophisticated the threat is.

Unatrac would implement a framework that is scalable, flexible and adaptive to other cybersecurity international standards like National Institute of Standard and Technology (NIST) framework to promote innovations in technology.

Developing a Framework core function using the NIST Plan to help stakeholders manage cybersecurity risk. This framework consists of these elements: identify, protect, detect, respond, and recover.

Identify

The aim of this framework function is to create a framework that would help in managing the data, risk, assets, and systems of Unatrac Holding Limited (National Institute of Standards and Technology, 2018). The activities include:

- Unatrac Information Technology (IT) unit should always maintain the record of the devices, software and systems in the organisation, and it should be characterized on their business values. Staffs together with other third-party vendors should always register their personal devices and fill the BYOD form. The task should be monitored by the inventory management system.
- The policies should be formulated with their email and password guidelines established on the regulatory and legal department requirements.

- The cybersecurity team would detect risks to their business in the internal and external channels through collaborating with forums and other sources which shares threat intelligences and vulnerabilities. With this information the IT team would respond quickly to threats.
- The company's management and IT department ought to agree on which contractors, suppliers they choose that renders services to the company. They shall be critically evaluated frequently so that their products and services are being complying with their obligation.

Protect

This function manages the implementation and development of the security method used in ensuring confidentiality, integrity, and availability (CIA) of services (National Institute of Standards and Technology, 2018) these tasks are:

- The access to confidential infrastructure like Network devices, software services, Email platforms should be limited to authorised users. Networking tools like DNS configurations, Security Technologies, network segments and password management provides security of systems and services. Privilege mode should be granted based on your job specification.
- Cybersecurity awareness and suitable training should be provided to the staffs and partners of the company to perform well in their roles relating to cyber risk. One of such training is the ability to detect threat in the company.
- The IT configuration manager should handle the configuration of the network systems. Backups ought to be taken regularly and kept in a safe place in case the business suffers from a disaster. This protect function helps in ensuring that the policies are being met and improved.
- The IT department should always ensure that repairs, maintenance, and changes should be documented and approved. One example is the change management committee which helps in repairs and maintenance.
- Audit log should be kept protected by the IT team using suitable security tools and also should be documented and reviewed using the company's policy. If irregularities are found, the company should commence an investigation.

Detect

This core function identifies any cybersecurity event in real time or intervals (National Institute of Standards and Technology, 2018). The task are as follows:

- Monitoring of remote connection and network operation to identify irregularities in cybersecurity events and email systems should be continuous. One example is anomaly detection tools which help the bank to identify stolen cards used for fraud. This detection tools are configured on monitoring with incident alert to the IT team when anomalies happen.
- Attention on personal activities is monitored by the IT team, connection patterns, flaws in code, software behaviours and third-party providers are also monitored. Assessment should be done on each vulnerability to determine wrong configuration ports and devices.
- Various IT personnel know their responsibilities and detection roles according to the requirement being put in place. Detection software are being tested and improved.
- Reports on suspicious activity are told to the IT department for investigation.

Respond

This emphasizes on how detected threats and support recovery are handled (National Institute of Standards and Technology, 2018). All members of the company are involved in this segment. The tasks are:

- Response to cybersecurity events needs to be updated to guarantee processes are well executed with proper software tools at the right time.
- Cybersecurity incident should be reported to the third-party and internal stakeholders. The different departments should know their task and responsibilities when situation arises so they could be able to contact law enforcement, insurance, banks, service providers and press.
- The first point of contact hen an incident occurs should be the IT department. forensic analysis and investigation should be conducted to determine the effect on the company. The internal communication of the incident within the company should be handled by the corporate communication department.
- The IT Team makes sure the threat is controlled, reduced and resolved. Unatrac Holding network system should be turned off to halt the spread of the attack. Changing of network and system password should commenced.
- Cyber incidents that occur should be documented for learning purposes.

Recover

This framework includes plans to be carried to restore services through tough authorization without suitable impact on export sales to the Unatrac customers.

- Recovery from a cybersecurity incident can be activated after or during a cybersecurity event. The departments in the company knows each of their roles and responsibilities during the recovery. An example is, how the communication department forward messages to the press in order to redeem the company's image and reputation, also during this period the IT teams should have restored backup they saved, furthermore the accounting department should figure out ways to recover from the financial loss.
- The head of committee should communicate with the CEO, stakeholders, executive team and the management of Unatrac Holding Limited of the recovery plans been made.

Analysis on the ways the data breach at Unatrac Holding Limited could have been prevented.

The attacker aimed at the Chief Financial Officer (CFO) email account. A well-documented phishing email was sent to the CFO with malicious links linking him to a fake logon Microsoft 365 account page. This was targeted so that the CFO would be redirected to a spoofing website with same appearance of the original Microsoft 365 page to collect his login details. This attack could have been altered if there was a good cybersecurity roadmap put in place by the company with two factor identification, detection and using the NIST core framework functions.

This identifies function helps the company to understand the systems which need protection in the nosiness environment (National Institute of Standards and Technology, 2018). For

Unatrac Holding, the email system can be identified. Secondly, the detection core function recognizes the implementation and creation of actions to ascertain the development of cybersecurity events that needs to be timed. Suitable examples are security continuous monitoring, detection activity, anomalies and events (National Institute of Standards and Technology, 2018). Sender policy framework (SPF) can be executed to monitor and detect malicious emails in accordance with the domain-based message authentication, and conformance and reporting (DMARC) through the guidance from this detection function for protection (Chandramouli et al., 2016).

This sender policy framework (SPF) works in detecting fake emails. The owner of most domain publishes their SPF record in their server, that is their domain name server which specify the mail server that is being permitted to send email messages for the domain. If the SPF gets an email message, it checks the validity of the sending mail server and if it's not listed in the SPF record as a permitted sender, the verification gets rejected (Australian Cyber Security Centre, 2019); and with the execution of DMARC, the domain owners recommend the recipient mail servers to implement some policies to help take results on incoming mails. The owners of the domain server have some privileges, they can request that the recipient allows, reject or quarantine mails that fail the sender policy framework (SPF) verification. Also, inform owners of domain on their emails that fail to pass verification checks; get valuable statistics and advise the domain owners on false email claiming to come form the right domain; extracted data are sent to the domain owners from a false email with false information in it like web addresses from the header and body of the mail (Australian Cyber Security Centre, 2019). With the rules in the company, the email system irregularities will be quickly detected, and strict protection would have been put in place such as quarantining the email from the hacker or rejecting it with accordance with the NIST core framework. The protection core helps to limit or contain the cybersecurity event using identity checks and control access (National Institute of Standards and Technology, 2018).

Also, adding to email system prevention with SPF and DMARC approach in accordance with the cybersecurity plan, the CFO of Untatrac Holding should be protected and identified. This protection entails establishing training programs and alertness of CFO together with other users to limit the impact of malicious attacks (National Institute of Standards and Technology, 2018). Users should be trained on how to spot unknown emails containing attachments and links (Sittig and Singh, 2018). An example is users should hover their mouse on the links to check where the link will bring them to. Moreover, proper thinking should be done by the user before clicking on links or attachments form unrecognised or external sources, when in doubt, the user should make contact with the IT team. Pending till the users are really sure, clicking the link should not be the best interest. Furthermore, conducting simulated phishing email attacks by sending fake emails that looks real can prepare users for the trouble in the cyber world. Lastly, it is recommended by Aldawood and Skinner (2019) that evaluation test on phishing attack by trained personnel would assist in checking the awareness level of the user. More trainings on this phishing subject matter would bring about more awareness of users like the CFO and clicking on the malicious link would have totally been avoided.

Conclusion

Attacks like phishing are becoming rampant in the cyber world and also making it a global threat to companies, financial institutions etc. since the use of computer and network system has been a necessity tool for businesses, so developing a strong consciousness with the failures and threat these machines expose to the cyber-attackers and cyber criminals is mandatory. Suitable plans and countermeasures should be put in place to avert the threats it brings. Its crucial for the board and management to put in place a cybersecurity plan and also a response plan against these data breaches that could occur at any time. (Dhilon, 2017). IT systems should be accessed regularly by the operational managers for possible attacks. Even after such plans has been put in place, the managers should also be aware that attacks could come from an insider in the organisation unknowingly or knowingly whereby contributing to the attack. Also, human errors contribute so much to data breaches (Evans et al., 2018). Training and awareness relating to cyber attacks should be made compulsory for employees and staffs in the organisation.

References

Australian Cyber Security Centre (2019) *How to Combat Fake Emails*. Available at:https://www.cyber.gov.au/publications/how-to-combat-fake-emails (Accessed: 11 April 2020)

Aldawood, H. and Skinner, G. (2019) 'Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues' *Future Internet*, 11(73), pp. 1 - 16, *MDPI* [Online]. Available at: https://www.mdpi.com/1999-5903/11/3/73/pdf (Accessed: 11 April 2020)

Alkhalil, Z., Hewage, C., Nawaf, L., and Khan, I., A., (2019) *The Causes and Effects of Phishing Attacks*. Available at: https://www.researchgate.net/publication/332069962_The_Causes_and_Effects_of_Phishing_Attacks (Accessed: 07 March 2020)

Bonner, L. (2012). Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. *Washington University Journal of Law & Policy, 40,* 257-278.

Chandramouli, R., Garfinkel, S., Nightingale, S., and Rose., S. (2016) *Trustworthy Email*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf (Accessed: 11 April 2020)

Cichonski, P., Millar, T., Grance, T., and Scarfone, K., (2012) *Computer security incident handling guide*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Accessed: 08 march 2020)

Dhillon, G., (2017) *What to do before and after a cybersecurity breach?.* Available at: https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf (Accessed: 12 April 2020)

Evans, M., He, Y., Yevseyeva, I., and Janicke, H., (2018) *Analysis of published public sector information security incidents and breaches to establish the proportions of human error.* Available at: https://www.dora.dmu.ac.uk/xmlui/bitstream/handle/2086/17168/HAISA%20-%20Analysis%20of%20published%20public%20sector%20information%20security%20incidents%20and%20breaches%20to%20establish%20the%20proportions%20of%20human%20error.pdf?sequence=1&isAllowed=y

Federal Bureau of Investigation (2018), *International Business E-Mail Compromise Takedown,* Available: https://www.fbi.gov/news/stories/international-bec-takedown-061118/ (Accessed 9 April 2020)

Ferguson, S., (2019) *FBI Arrests Nigerian Suspect in $11 Million BEC Scheme.*

Available at:

https://www.databreachtoday.com/fbi-arrests-nigerian-suspect-in-11-million-bec-scheme-a-12932 (Accessed: 8 April 2019)

Dolan, A., K. (2016) ‘Africa's Most Promising Entrepreneurs’, Forbes Africa 30 Under 30 For 2016

[Online] Available: https://www.forbes.com/sites/kerryadolan/2016/06/06/africas-most-promising-entrepreneurs-forbes-africas-30-under-30-for-2016/#d71e0d1f4341 (Accessed: 8 April 2020)

Gatzlaff, K. and McCullough, K., (2008) *The Effect of Data Breaches on Shareholder Wealth,* Florida: Tallahassee.

Holtfreter, R., E. (2015) ‘Data breach trends in the United States’ *Journal of Financial Crime,* 22(2), pp. 242-260

Kathleen M. Bakarich and Devon Baranek (2019) Something Phish-y is Going On Here: *A Teaching Case on Business Email Compromise.* [Online]. Available at: https://doi.org/10.2308/ciia-19-018/ (Accessed: 8 April 2020)

Lubbers, A., C., McNamara, A., Lu, Y., and Sifferath, T., (2016) ‘A Study of Organizational responses to major data breaches in the retail and healthcare industries’ *Quarterly Review of Business Disciplines,* 3(2), pp. 101 - 116.

Mejia, G. (2019) *Examining the Impact of Major Security Breaches on Organizational Performance: Should Investing in Cybersecurity Be a Requirement for Companies?*, Utica College.

National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity.* Available at:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed: 08 April)

Ogundipe, S., (2018) ‘More documents emerge in Obinwanne Okeke $11 million fraud trial’, Premium Times, 19 August [Online]. Available at: https://www.premiumtimesng.com/news/headlines/347348-download-more-documents-emerge-in-obinwanne-okekes-11-million-fraud-trial.html (Accessed: 9 April 2020)

Rosenberg, A. (2019) *Data Breaches: Risk, Recovery, and Regulation.* Available at: https://docs.legis.wisconsin.gov/misc/lrb/wisconsin_policy_project/wisconsin_policy_project_2_4.pdf (Accessed: 08 April 2020)

Scott, F (2019) *Business Email Compromise (BEC) , Fraud Management & Cybercrime* Available at: https://www.databreachtoday.com/fbi-arrests-nigerian-suspect-in-11-million-bec-scheme-a-12932 (Accessed: 8 April 2020)

Sittig, D., F. and Singh, H. (2016) *A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks.* Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4941865/ (Accessed: 11 April 2020)

Obiwanne Okeke vs the United State of America [2019] Case4:19-mj-0011 page 1

Unatrac Holding Limited (2020) *company official website*. Available at: https://www.unatrac.com/pages/about-unatrac (Accessed 8 April 2020)

Zweighaft, D. (2017), "Business email compromise and executive impersonation: are financial institutions exposed?", *Journal of Investment Compliance,* Vol. 18 No. 1, pp. 1-7. Available at: https://doi.org/10.1108/JOIC-02-2017-0001 (Accessed: 8 April 2020)