Teesside University

SOCIAL ENGINEERING: ALL THINGS FIBRE CASE ANALYSIS

By (Name)

Course Title and Code

Professor

City – State

Due Date

Table of Contents

List of Figures

Social Engineering: All Things Fibre Case Analysis

1. Introduction

Social engineering is the art of manipulating the psychology of individuals to make them behave in a manner they do not wish, causing them to divulge confidential information (Mouton et al., 2014). Organizations have taken bold steps to implement advanced security systems, but the human element has remained a significant weak point for cyber attackers to perform attacks. Typically, social engineering differs from social engineering attacks in that the former is an 'art' while the latter is the 'process' of manipulating human actions to divulge confidential information (Mouton et al., 2014). Recent cybersecurity reports show that social engineering is quickly growing and has become a serious threat to contemporary society. The attackers use methods such as phishing, vishing, baiting, quid pro quo, pretexting, and tailgating.

The system administrators experience difficulty preventing the social engineering attacks because most of the current system securities rely on humans rather than technical security frameworks. According to Verizon's 2015 cybersecurity report on social engineering, humans contribute to 90 percent of the security incidents (Fan, Kevin and Rong, 2017). The majority of the social engineering attacks are carried out through phishing, pretexting and vishing. A recent cybersecurity report on social engineering showed that five out of six large companies with at least 2,500 employees are targeted by attackers that use a phishing approach. The report also showed that companies with an average of 10,000 employees spend about $3.7 million in an effort to address the increased cases of phishing (Fan, Kevin and Rong, 2017).

This paper seeks to analyze the case of "All Things Fibre" company using the I-E based model of human weakness for social engineering investigation framework. The paper also seeks to recommend suitable solutions to the attack and discuss the ethical issues surrounding the case.

1.1 Case Scenario

All things fibre is a spinning, weaving, knitting and crochet trading firm founded by Pat and Maggie five years ago. The company uses both the in-store and online business approaches to market and sell its spinning and weaving equipment and supplies. “All things fibre” also offers weaving and knitting courses in its workshop. Pat and Maggie are assisted by Jill and Katie, who work as workshop tutors part-time. Pat’s husband, Dave, is also an important staff at the firm, helping with the IT tasks. Sam is a website designer and developer who designed the logo and created the e-commerce platform for the firm at a friendly cost.

The first incident involved a nicely dressed middle-aged woman who visited the shop on a Monday morning, and Jill offered to assist her. The woman pretended to be interested in spinning and knitting, which manipulated the friendly Jill’s actions to divulge the sensitive information about the organization’s operations, increased profits and order posting trends. Pat cut the conversation short by sending Jill to get something from the store. The woman returned the following and pretended that she wanted to enrol on the workshop course. As Jill booked her to the workshop, she kept looking over her shoulder.

A week later, a stranger claiming to be a customer called via phone(vishing), demanding a refund for a faulty range spinning wheel worth £1000. More surprisingly, the stranger seemed to understand the firm perfectly as they mentioned everything, including names right. The client threatened to take legal action and provide a negative rating and review if she was not refunded.

Pat, who received the call, got suspicious and declined to comply. After this incident, the woman who pretended to be deeply interested in the workshop course never showed up again.

In a different incident, Jill came with her gaming laptop to the workshop and asked Maggie to connect it to the firm's Wi-Fi. Since Maggie wanted to show that she was supportive to her employees, she allowed Jill to connect it without even pausing to imagine the associated security threats. A malware attack message popped after switching the laptop on, showing, "Gotcha now, mate! Give us the password to your Minecraft account, and you can have your laptop back." In the third incident, Jill and Katie received a scam text message about an order to be delivered by DHL and prompted them to follow a certain link (pretext). Pat and Maggie confirmed that no order was expected that day, and the message was a scam.

PART 1

2. Analysis of Data Breach

2.1 Social Engineering Framework

I-E based model of human weakness for social engineering investigation framework best suits analysis of the social engineering attacks in "All things fibre" because it shows how the attacker exploits the human weaknesses to accomplish desired goals, as shown in *figure 1*.

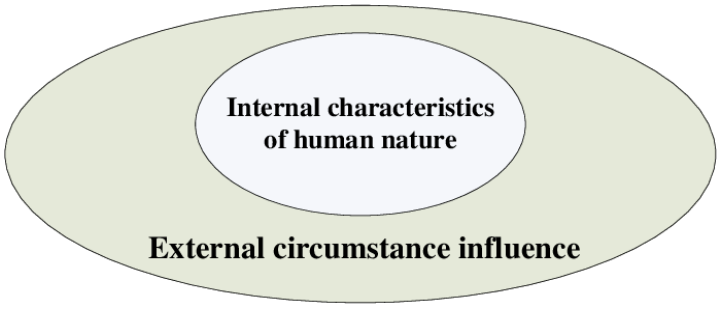

Figure 1: I-E based model of human weakness (Fan et al., 2017)

The framework is essential for this case because it presents key models that help establish the internal human elements and external factors that led to the social engineering attack. According to this framework, humans have internal characteristics that can be influenced using external social engineering strategies, manipulating their actions to divulge confidential information (Fan, Kevin and Rong, 2017). The case entails the human and personality weaknesses (Jill was too good) that were exploited to manipulate behaviours and divulge the firm's sensitive information. The framework also provides the systematic pathways involved in the social engineering attack, as shown in *figure 2* below.

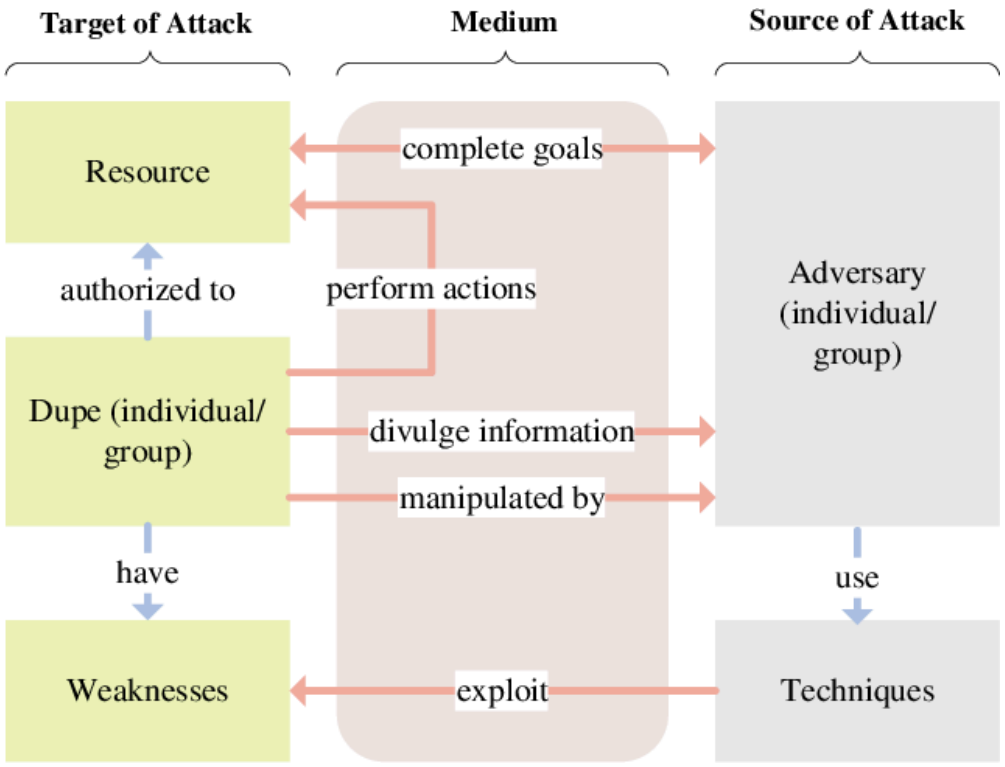

Figure 2: Workflow elements of social engineering attacks (Fan, Kevin and Rong, 2017)

2.2 Analysis

2.2.1 First Incident

In the first incident, the nicely dressed middle-aged woman who pretended to be a customer was the perpetrator of the attack while the "All things fibre" was the target. Jill was a medium that the woman intended to use to accomplish her objectives. When Jill approached the middle-aged woman to offer her assistance locating what she was looking for, the woman quickly noticed Jill's kindness as a weakness to exploit. According to Fan, Kevin and Rong (2017), I-E based model of human weakness for social engineering investigation framework considers kindness a significant internal weakness that makes individuals trust, sympathise and empathise with everyone, including strangers.

When the woman got into a conversation with Jill, she quickly noticed her "trust them all" weakness. The woman took advantage by pretending to be interested in joining the knitting workshop to exploit Jill and make her disclose more information. The deceptive technique of pretending to be interested in Jill's field of knitting and weaving was meant to manipulate her psychology and make her disclose all the sensitive information that the woman needed to launch the social engineering attack successfully.

Jill, who was unaware of the woman's deceptive technique, was easily manipulated and behaved in a manner that she was not willing to. She went ahead to disclose the organisation's work schedule to the woman, which was sensitive and meant only for the internal staff. The impact of sharing the work schedule was reflected later when the woman called and insisted that she wanted to speak to Jill because she was certain Jill was on duty that day. However, Jill had changed the shift with Pat; otherwise, the woman would have taken advantage to attain her goal.

Jill also disclosed to the woman how the firm was making profits and posting out orders frequently. Business profits and operation trends are sensitive information that only the organisation's staff should access. Pat was aware of Jill's kindness and willingness to build rapport with customers; therefore, she did not want to cut the conversation in a manner that could evoke anger. She used her patience to withstand the conversation for some time, but when she realised that Jill would not end the conversation soon, she interrupted in a friendly manner and sent Jill to collect her something from the store.

Under the framework used in this case, patience is an internal human trait that helps individuals resolve issues without evoking anger in others (Fan, Kevin and Rong, 2017). However, it's a weakness that social engineering attackers exploit to achieve their goals. For example, Pat's patience made her wait before interrupting the conversation. If Pat had taken quick action, Jill would not have shared the sensitive information about the company's work roster, trends of posting products and increasing profits. Similarly, the woman took advantage to continue with the conversation and maximise her information gathering process. The woman used a face-to-face physical technique as the medium to exploit Jill's kindness and "trust them all" internal characteristics. This, in turn, manipulated Jill's psychology, causing her to divulge the organisation's sensitive information to the woman.

A week later, when the woman returned, she pretended that she was enthusiastic about joining the workshop. As Jill was busy booking her into the system, she kept looking over her shoulder. Shoulder surfing is a form of physical attack vector that the social engineering attackers use to illegally note passwords or critical information that only the authorised staff should access (Fan, Kevin and Rong, 2017). The woman must have been trying to access the

administrative information about the workshop operations to carry out her social engineering attack.

Just a week after the workshop booking incident, the firm received a strange call from a woman who claimed that she had purchased a faulty spinning, worth £1,000, and was therefore demanding a refund. Jill was supposed to be on duty that day but exchanged it with Pat. The woman insisted that she wanted to speak directly to Jill but was informed that she was not available that day. Pat was shocked by the woman's plausible behaviour, manifested by her accurateness in mentioning names and other aspects of the organisation. It's apparent that the woman on the phone must have collected adequate information about the organisation, and that's why she was right in every deceptive measure she took.

Pat got suspicious because no such item had been sold recently and asked the 'customer' to bring a receipt or the faulty spinning wheel to be refunded. According to Fan, Kevin and Rong (2017), Pat's patience that made him address the customer in a friendly manner and appear willing to offer a refund was an internal characteristic that the customer could turn into a weakness. The alleging customer took advantage and insisted on being given a refund; otherwise, she would report the firm to the Trading Standards and give a bad review on Facebook. Issuing the threat was an exploitative technique to manipulate Pat's psychology and cause her to issue a refund for a non-existing item.

When Pat refused to give a refund and hung the phone, the 'customer' never called again. The woman also never showed up for the workshop course she had registered for, and there is no doubt that she was the actor. The 'customer' used the vishing medium (phone call) to perform the social engineering attack. According to Fan, Kevin and Rong (2017), vishing is a form of

social engineering attack that involves defrauding individuals using the phone communication to dupe them and divulge confidential information, as witnessed in this case.

2.2.2 Second Incident

The second incident involved a malware attack on Jill's laptop which she brought to the workplace for the first time. She was given the laptop by her grandson, a gamer, to help improve her skills in internet-related matters. When Jill asked Maggie if she could connect it to the firm's Wi-Fi, she agreed to show her that she was supportive of her staff. Maggie was empathetic and wanted to support her employee's development in every she could. Under the I-E based model of human weakness for social engineering investigation framework, being empathetic reflects an internal characteristic of kindness (Fan, Kevin and Rong, 2017). Social engineering attackers consider kindness an excellent internal characteristic and a weakness to exploit. Maggie's kindness created a channel that was later used to launch the attack.

After Maggie allowed Jill to connect to the firm's Wi-Fi, she offered to get the password for her from where it was kept. This was an act of generosity and helpfulness toward Jill. The framework used in this case classifies generosity and helpfulness under the charity trait. The social engineering attackers consider these two internal traits as weak points to exploit and manipulate the minds of individuals to divulge confidential information (Fan, Kevin and Rong, 2017). In this case, Maggie's generous and helpful traits paved the way for a subsequent malware attack. If she had taken time to think about the risks associated with connecting external devices to the firm's Wi-Fi, the attack risks would have been mitigated or prevented.

Writing the Wi-Fi password on a piece of paper and storing it in an open place was a poor cybersecurity practice. If the attackers found it, it would have been an easy way to gain unauthorised access to the firm's network and perform the desired activities without being

detected. Pat and Maggie, the owners, trusted all the staff beyond limits and decided to give everyone access to the password. According to Fan, Kevin and Rong (2017), trust is an internal characteristic that can be manipulated into weakness and defraud individuals into disclosing sensitive information.

When Jill and Maggie switched on the laptop, strange letters and numbers flashed on the screen, and Sam affirmed that it was indeed a malware attack. The attacker used the malware technical technique to perform the attack in this case. The attacker used the "Gotcha now, mate! Give us the password to your Minecraft account, and you can have your laptop back" message to lure the owner of the owner to provide the password for the gaming account to be able to restore control over the PC. Therefore, the quid pro quo technique was used to exploit the attacker by asking for the password to give the target her laptop back as a benefit. Quid pro quo functions on the "something for something" criteria, as evident in the case (Fan, Kevin and Rong, 2017).

2.2.3 Third Incident

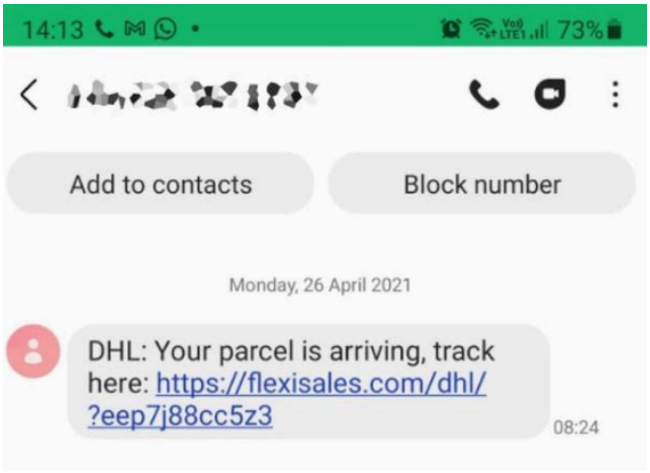

Figure 3: Deceptive pretext

The third incident came a few days after the second event when Katie and Jill were on duty. They received a text message with a link claiming that the firm was expecting a delivery

from DHL Company, as shown in *figure 3*. The message was very tempting, and Jill was just about to click the link when Katie stopped her. Katie suggested that it might be a scam message intended to lure them and cause harm to the organization. When Pat and Maggie arrived, they replied to Katie that the firm was not expecting any delivery that day.

In this case, the attacker used a pretexting approach to target the "All things fibre" company's staff (Katie and Jill). Jill had an internal weakness of curiosity that made her almost click the link if Katie had not stopped her. The attacker targeted to exploit Jill's internal weakness of curiosity to lure her into clicking the link, creating a weak security point to launch the attack and access the sensitive information about the firm. As stated by pretexting approach, the attacker intended to impersonate the DHL and use the luring package message to deceive the target.

2.3 Analysis of Selected Framework

	Internal Characteristics														External Influences								
	Chastity	Temperance	Charity	Diligence	Patience	Kindness	Humility	Lust	Gluttony	Greed	Sloth	Wrath	Envy	Hubris	Strong affect	Overloading	Reciprocation	Deceptive Relationships	Diffusion of Responsibility	Authority	Integrity and consistency	Social validation	Scarcity
Physical																							
Dumpster diving	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	●	○
Shoulder surfing	○	○	○	○	○	●	○	○	○	○	●	○	○	○	○	○	○	●	○	○	○	●	○
Technical																							
Phishing	○	○	○	○	○	○	○	●	●	●	○	○	○	○	●	○	○	●	○	○	○	○	●
Waterholing	○	○	○	○	○	○	○	●	●	●	○	○	○	○	○	○	○	●	○	●	●	●	○
Baiting	○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○	○	○	●	○	○	○	●
Social																							
Persuasion	○	○	●	○	○	●	○	●	●	●	●	○	●	○	●	○	●	●	●	●	●	●	○
Pretexting	○	○	●	○	○	●	○	●	●	●	●	○	○	○	○	○	○	●	●	●	○	●	○
Quid pro quo	○	○	●	○	○	●	○	●	●	●	○	○	○	○	○	○	●	○	○	○	●	●	○
Reverse SE	○	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○	○	●	○	●	○	●	○
Hybrid																							
Tailgating	○	○	●	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Vishing	○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○	○	○	○	○	○	○	○

Figure 4: I-E based model of human weakness for social engineering investigation framework (Source: Fan, Kevin and Rong, 2017)

The I-E based model of human weakness for social engineering investigation framework was easy to use in analyzing this case because its models directly address the internal human characteristics that social engineering attackers use as weaknesses to attack (Fan, Kevin and Rong, 2017). The characteristics of the individuals at “All things fibre” fall under the internal characteristics listed in this framework. This made it easy to identify and analyze the traits of the individuals targeted by the attackers by the firm in the case study. The framework also provides external influences (*figure* 4) that make it easy to analyze the influences available in the case (Fan, Kevin and Rong, 2017. The framework presents the common techniques/vectors currently

used by social engineering attackers. This made it easy to identify the specific vectors used in the case.

PART 2

3. Solutions and Mitigations

Cybersecurity threats keep changing as technology advances; therefore, it is impossible to eliminate the risks. However, the risks can be reduced and impacts mitigated to minimize the severity of the attacks. The human weaknesses contribute to the social engineering attacks (Fan, Kevin and Rong, 2017; Mattera and Chowdhury, 2021). The mitigation strategies should thus target the human weaknesses to address the problem from the grassroots. The I-E model used in this context provides subjective and objective defence measures for the social engineering threats.

3.1 Objective Security Measures

The objective security measures seek to offer objective conditions by actively involving all the relevant people to address the social conditions and, in turn, address the threats (Fan, Kevin and Rong, 2017). The main objective measures that would be essential in this case include using standard security policies, updating facilities and detecting malicious data.

3.1.1 Standard Security Policies

"All things fibre" organization requires a clearly-defined and well-documented security policy to defend itself from social engineering attacks. An effective security policy would provide an excellent security training plan to train all the staff on the potential cybersecurity threats effectively, causes and risk mitigation ways (Fan, Kevin and Rong, 2017). The threats keep on changing; therefore, the staff must be continuously trained to keep them updated on the

emerging security risks. Pat and Maggie should invest in cybersecurity by implementing the information security management system (ISMS) to offer an effective risk management framework to respond to the threats. According to Fan, Kevin and Rong (2017), a well-established ISMS would present the specific policies for defining, constructing, developing and maintaining the computer systems at “All things fibre”. This would strengthen the security of the firm’s computer systems, thereby minimizing the risk of attack.

All things fibre currently lacks either ISO27K or Cyber Essentials certification. The firm should consider implementing any of these two cybersecurity certifications to promote the security of its network, computer, data, programs and other technological equipment. All things fibre can also implement other cybersecurity certifications that dictate how the staff uses computer resources. This would help to prevent dangerous uses that can cause the staff to fall into the traps of the attackers.

The organization should implement an ISO27032 security enforcement policy to address both human-based and computer-based risks. ISO27032 is an advancement of the previous 27001 and offers universal security policies that promote the safety of people in cyberspace (Fan, Kevin and Rong, 2017). This implies that implementing it would promote the safety of the staff at “All things fibre” during their normal computer operations. Since ISO27032 addresses all the baseline security activities for everyone within cyberspace, individuals like Jill would be protected from social engineering and malware attacks. The step-by-step guidance for addressing cybersecurity risks provided by the ISO27032 would be essential in training the staff to better their understanding of potential risks and ways of preventing them.

The key cybersecurity policies that would enable “All things fibre” to prevent and mitigate the social engineering attacks are as follows:

Implement Bring Your Own Device (BYOD) policy.

The firm should implement the BYOD policy to control how the staff use their personal devices to perform organizational tasks. Personal devices lack baseline security measures; therefore, they create a weak point for the attackers to launch their attacks (Campbell, 2018). If the employees are allowed to connect their personal devices to the firm's network or access business emails, the firm gets exposed to malware and social engineering attacks. For example, the attackers may use phishing strategies to deceive the staff into acting in a certain behaviour resulting in exposure of the organization's confidential information.

The BYOD policy should highly discourage staff such as Jill from connecting their devices to the firm's network to eliminate weak security points used by the attacker. The policy should also discourage the staff from storing the organization's sensitive information on their personal devices (Heffernan, 2021). If they do, and the devices are stolen, the BYOD policy should train them on how to clear the sensitive information remotely to avoid exposure. The policy must clearly outline to the staff how to use their devices to perform business tasks. Heffernan (2021) emphasizes that the BYOD policy should also describe the unacceptable behaviours when using personal devices on official duties. The policy should also inform the staff about the specific business software they can access from their gadgets to minimize security threats.

Implement the visitor's policy.

The visitor's policy should be implemented at the firm to restrict the visitors from accessing the business operation areas. Currently, the firm has no policy to regulate the visitors' movement. This justifies why the woman was too close to Jill to the extent that she had an

opportunity to perform shoulder surfing. According to Chung et al. (2021), the policy should restrict the visitors from accessing critical areas of the organization such as the data centres and restricted rooms because those areas harbour sensitive information about the firm. Campbell (2018) states that implementing the visitors' policy would enable the firm to prevent security breaches that can expose its proprietary information.

Individuals like Sam should be treated as visitors and should not be allowed to walk into every section the way he wants. He created the e-commerce platform; therefore, he is a threat to the firm's security if allowed to access every section of the business premises. The policy must apply to all visitors and must guide the staff on the measures to take when they encounter scenarios of trespass.

Implement password policy

All things fibre should implement the password policy. The password policy should require all the staff to create unique and robust passwords that cannot be easily cracked by attackers (Heffernan, 2021). In case of suspicious actions, the firm should guide the employees on specific measures to take. For example, the staff should regularly update the passwords of the business devices given to them to prevent insider and external security threats. According to Heffernan (2021), no passwords should be written on paper and placed in an area accessed by everyone in the organization, as evident in the case of Maggie and Jill. The password was written on a piece of paper and kept behind the till. The password policy would help the firm enforce its network and database security systems (Heffernan, 2021). This would help the firm minimize the risks that would create weak points for the attackers to gain illegal entry.

3.1.2 Update Facilities

The firm should regularly update its facilities to enforce weak security points. For example, the firm should update its network security system to make it strong enough to keep off the attackers. Updating the network security system would also enable the firm to strengthen the protection against social engineering attacks when the staff make risky decisions (Fan, Kevin and Rong, 2017). It is also important to improve the dumping strategies by introducing a paper shredder to shred all the documents that contain sensitive information about the organization. According to Fan, Kevin and Rong (2017), reducing the paper litter in the litter bins would help the organization minimize dumpster diving. All things fibre should replace manual password-typing with the biometric authentication approach to prevent shoulder surfing. If this had been available, the woman who shoulder-surfed on Jill could have no opportunity to do so.

The firm should install surveillance cameras to track the movements within and outside the premises. The surveillance cameras would hinder visitors from sneaking into restricted areas, thereby minimizing the threats (Fan, Kevin and Rong, 2017). The cameras would also record the behaviours of individuals within the premises, making it easy to track the criminals. If the firm has adequate financial capacity, it should implement call recording technology to record all phone conversations between the firm and external devices (Fan, Kevin and Rong, 2017). The phone recordings would be useful in tracking the social engineers that use the phone to perpetrate attacks. According to Fan, Kevin and Rong (2017), the recordings can also be used as evidence against the attackers. If the phone recording strategy were available, the firm would have used the recording to track the "customer" that claimed to have purchased the spinning wheel.

3.1.3 Malware Detection and Mitigation

The social engineering attackers mainly use technical and social techniques to exploit human weaknesses. Therefore, the firm should implement an automated security program that can detect and warn the staff about phishing emails and vishing phone calls (Fan, Kevin and Rong, 2017). If such a system were available, the system would have warned Katie and Jill about the deceptive message of the non-opposing package from DHL. Similarly, Pat would have received a warning about the person that claimed to be a customer, yet no similar purchase was made.

3.2 Subjective Security Measures

The subjective strategies seek to improve the subjective will of human elements in overcoming the effect of external conditions' influence on internal characteristics of human nature.

3.2.1 Training Awareness of Human Elements

Cybersecurity threats keep changing in nature and attack methods; therefore, it's necessary to update the staff security awareness. Offering ongoing cybersecurity training to all staff promotes their awareness and would help the firm enhance its cybersecurity protection (Fan, Kevin and Rong, 2017). For example, providing security training to Jill would boost her awareness of the risks associated with trusting everyone and granting them access to critical areas. When Jill was told about the woman's shoulder surfing behaviour, she calmly replied that she knew who to trust and who not to trust. Everyone is a threat to security; therefore, Jill and other staff must be trained on ways of keeping off unauthorized people from accessing the firm's sensitive information.

The firm should use the security training policy to offer adequate to all staff to boost human awareness of social engineering threats. The training would inform the staff on the right defensive measures to prevent social engineering attacks (Fan, Kevin and Rong, 2017). The firm's cybersecurity experts should be responsible for explaining to the staff various security matters and assisting them in responding to various cyberattacks when they are in close range. The firm should update the security compliance program to promote the employees' awareness of the new security enforcement measures (Fan, Kevin and Rong, 2017). This would promote the staff behaviours, thereby minimizing poor decisions that result in the exposure of the firm's confidential information.

The firm should also implement a comprehensive system that allows staff training, skill and knowledge testing, performance measurement and result feedback. The comprehensive approach would help to improve the staff's awareness and positively improve their behaviours in response to social engineering attacks (Fan, Kevin and Rong, 2017). For example, Jill would be fully aware of the scam texts and emails; therefore, she will not have to get the direction of colleagues to avoid falling into the traps of the attackers.

3.3.2 Human Emotion Detection

Typically, the emotional changes in individuals influence their cognitive functioning, thereby affecting their psychology. Such changes impact the awareness of the staff about sensitive and ordinary information (Fan, Kevin and Rong, 2017). Most people often behave abnormally when under pressure. For example, the staff under pressure would easily fall into the traps of social engineering attackers because the pressure would negatively affect their security awareness. Although it may be difficult to establish the emotions of individuals, detecting the observable emotions can help promote the cybersecurity of the firm (Fan, Kevin and Rong,

2017). The management can shuffle the duty roster to allow the emotional staff to take a rest and have the emotionally stable staff take charge.

All things fibre can also utilize the social engineering attack detection model (SEADM) to help the staff detect the SE attacks (Fan, Kevin and Rong, 2017). Social engineers mostly exploit psychological weaknesses to influence individuals' emotions and cognitive functioning. This tampers with their awareness and makes them vulnerable to social engineers. While the staff are in an unstable emotional state, the social engineers get a better opportunity to launch their attacks (Albladi and Weir, 2020). The SEADM, therefore, recommends a cognitive functioning psychological assessment that would help All things fibre to detect the emotional status of employees and reschedule their shifts to minimize the social engineering attacks.

PART 3

4. Ethical and Morality Issues

The staff at "All things fibre" are currently used to too much freedom to access any part of the organization. Implementing a restriction policy that restricts the staff from accessing some parts of the organization they used to access will likely cause trust issues (Christen, Gordijn and Loi, 2020). The staff may feel that the management no longer has faith in them, resulting in an unstable state of mind. The unstable emotions would adversely affect their security awareness, causing them to behave abnormally. The social engineers are likely to take advantage of the staff's unstable emotions to exploit their internal weaknesses. This would result in increased cybersecurity attacks at the firm instead of reducing them.

Detecting the human emotion was proposed as one of the key subjective strategies to mitigate social engineering attacks. Practically, individuals have their own emotions and personal

ways of coping with or recovering from emotions (Fan, Kevin and Rong, 2017). The staff may perceive the management's decision to measure their emotional state as invading their personal limits. The staff are likely to develop negative perceptions towards the management, thereby affecting their response to cybersecurity threats. For instance, the staff may intentionally ignore to report detected social engineering threats, thereby increasing the severity of the attack instead of mitigating it. Some staff may be depressed but pretend to have stable emotions to avoid being reshuffled. This can make them perfect targets for social engineers to exploit, thereby increasing the chances of attack instead of minimizing it.

The BYOD policy seeks to bar the staff from using their personal devices to access the organization's emails and critical software. The staff may perceive the move as too much restriction on staff, thereby developing a negative attitude towards the management. The negative attitude may deteriorate the communication between the staff and management, thereby affecting the flow of information about cybersecurity matters. In such a case, the cybersecurity level of the firm is likely to deteriorate, making the staff vulnerable to social engineering attacks.

The planned cybersecurity training may force the firm to increase the work duration for the staff to balance normal operations with additional training classes. The increased duration and activities may burden some of the staff who have a business that they operate after the normal work hours. This is likely to result in rejection of the program and trigger conflict between the staff and management (Christen, Gordijn and Loi, 2020). Some staff may even decide to resign if the management fails to reduce duties for them to allow the implementation of the training program. High staff turnover may damage the public reputation of the firm.

5. Conclusion

The All things fibre case analysis affirms that the social engineers exploit the internal human characteristics and weaknesses to influence individuals in a certain manner that divulges the firm's sensitive information. The I-E based model of human weakness and social engineering investigation framework perfectly suits the analysis of the social engineering attacks in "All things fibre" because it provides a clear picture of how the process occurs. The framework provides the internal characteristics, external circumstances and attacking techniques/vectors used by social engineers, making it easy for individuals to understand the behaviours to avoid to minimize the risk exposure. Implementing the security policies and improving the behaviour measures will help the firm minimize social engineering attacks and promote staff awareness about cybersecurity issues.

List of Reference

Albladi, S.M. and Weir, G.R., 2020. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), pp.1-19.

Campbell, C.C., 2018. Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*.

Christen, M., Gordijn, B. and Loi, M., 2020. *The ethics of cybersecurity* (p. 384). Springer Nature.

Chung, A., Dawda, S., Hussain, A., Shaikh, S.A. and Carr, M., 2021. Cybersecurity: Policy. *Encyclopedia of Security and Emergency Management*, pp.203-211.

Fan, W., Kevin, L. and Rong, R., 2017. Social engineering: IE based model of human weakness for attack and defense investigations. *IJ Computer Network and Information Security*, *9*(1), pp.1-11.

Heffernan, L., 2021. Bring Your Own Device (BYOD), Offsite Working and Password Policy Introduction.

Mattera, M. and Chowdhury, M.M., 2021, May. Social Engineering: The Looming Threat. In *2021 IEEE International Conference on Electro Information Technology (EIT)* (pp. 056-061). IEEE.

Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S., 2014, August. Social engineering attack framework. In *2014 Information Security for South Africa* (pp. 1-9). IEEE.

Saleem, J. and Hammoudeh, M., 2018. Defense methods against social engineering attacks. In *Computer and network security essentials* (pp. 603-618). Springer, Cham.