Böckelman, P., Björkman, H., Eds. Martikainen M. and Lehner OM. (2019). Cybercrime in a Business World: Behavioral Perspectives. *ACRN Oxford Journal of Finance and Risk Perspectives, 8*(2019) Special Issue Digital Accounting, 98-110.

CYBERCRIME IN A BUSINESS WORLD: BEHAVIORAL PERSPECTIVES

BÖCKELMAN PETTER, BJÖRKMAN HENRIK[1]
MINNA MARTIKAINEN[1] AND OTHMAR M LEHNER[2] (EDITORS)

[1] Hanken School of Economics, Helsinki
[2] University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

***Abstract**: As we are living in a fast-growing digital age it is crucial to keep in mind risks related to digitalization. The current digital work environment enables cybercrime and the practice of cybercrime has become more and more common. Because of the fast digitalization of our society many people miss out on important parts such as cyber security and only focus on development. This means that social behaviour is a big issue when it comes to cybercrime and cyber security.*

This work explores cybercrime in a business world with a focus on social behaviour. It explains how big an impact social behaviour has on cybercrime and it also explains how you can protect yourself of becoming a victim of cybercrime.

***Keywords:** Cybercrime; Social behaviour; cyber security; Social engineering*

Introduction – What is Cybercrime and why is it relevant?

In today's society it is almost a prerequisite that we have smart devices and connection to the internet. In both the work environment and social environment, we can see that the digital age is evolving e.g. through artificial intelligence and autonomous systems. Because of these sorts of developments, it is also crucial to look at the security. As the technology and systems are evolving, the ways of taking control and hacking into these systems are also getting more sophisticated and these sorts of breaches are called cybercrime. Cybercrime is explained by Arief et al. (2015) that it is computer-oriented criminal activity to gain economic, psychological and/or personal benefits. Computer-oriented criminal activity means that, by using a computer or smart device with connection to the internet, the attacker can remotely access high profile information or confidential data, copy credit information, access different systems and a lot more.

There are many ways to access your private computer or your business computer and servers. When discussing about ways of exercising cybercrime, Schinder DL. et al. (2008) categorizes these types in their book as following:

- Pre-intrusion/attack activities
- Password-cracking methods
- Technical exploits (taking advantage of characteristics of the equipment or protocols)
- Malicious code attacks (Viruses, worms, trojans)

(Categorization taken from: Debra Littlejohn Schinder & Michael Cross (2008), "Scene of the Cybercrime", p.431 [Book] 2nd edition)

Even though there are many ways to exercise cybercrime, it is not always the actual cyberattack that is sophisticated and many times it can be a very simple virus or malicious code. Often the malicious code finds the information that the attacker is after, because of human errors or social behavior. This means that as the technology evolves, the need of education on risks related to this needs to be up to date. This is also something that Sabillon E et al. (2016) takes in consideration, "Technology by itself is not enough, the integration of other fields like training, awareness, social aspects, culture…".

Types of cybercrime

In the following chapter the different types of cybercrime are presented and shortly explained. The importance here is to get a view over how attackers are trying to reach out for your information. In this chapter the focus lies on social engineering.

Viruses – Worms - Ransomware

Viruses are malicious programs that infect other programs or applications by transferring its own code into theirs. Files that are thought to be legit are reprogrammed into something completely else. Once the code has been injected into the designated targets, the virus starts to spread. Usually in a rapid pace over networks. In most cases, the initial injection is affiliated with social engineering. The end-user is tricked into opening certain links or download files contained with the virus. One common way to create an entry is to attach malicious files to emails, once opened, the virus has been infused into the system. Viruses can also be classified into different categories depending on their characteristics. There are resident viruses which are embedded in the system memory and are activated every time the OS is started. Non-resident viruses are on the other hand executable viruses that does not store itself in the computer memory. As the anti-virus software evolves, so does the viruses.

Nowadays we can find the likes of Metamorphic viruses, Stealth viruses and Polymorphic viruses. Metamorphic viruses have the ability to change its own code after every new infection. Being able to rewrite the code leads to the functions of the code being the same but the detections of the virus really complicated. Stealth viruses can remove itself from inflicted files to then appear somewhere else to confuse the antivirus software. Once the Polymorphic viruses have infected the target, it can duplicate and at the same time slightly alter its' own code. What it achieves by doing so is making it very hard for the detection software due to a large number of slightly different versions of the same virus. (Symantec Corporation)

Worms are interchangeably used for viruses, but there are things that distinguish viruses from worms. The main one is the reproduction part. Worms are unlike most viruses able to duplicate and are not dependent on existing programs to spread itself. Worms are capable of leaving copies of themselves in every infected computer, without any assistance. Worms have their name for a reason. They are always looking to dig deeper. Worms are continually looking for new possible vulnerabilities to explore. The worms are often designed to either extract valuable information from the inflicted computer, or to take control over them and use them as bots. The purpose of creating zombie computers is being able to use them as proxies when engaging in activities such as sending spam emails or attacking governmental computer. Networks of bots - Bot nets - can then be sold or rented out to criminal organizations that have the intention to use it for different types of cybercrimes. The worms are often classified by the way they are spread. The four most common ways are through emails, networks and internet. (TechTarget)

According to O'Gorman et al. (2012), ransomware is a type of malware that infects your computer and denies access to your files. The malicious software is keeping your files hostage by encrypting your files and demanding a ransom payment for a decryption key. If the ransom

fee isn't met, the files will be deleted. The most common way for the ransomware to infect the computers is by phishing attacks.

Social engineering – The impact on businesses

Cybercrime has a very negative impact on businesses, for instance if a business is targeted by cybercrime there are different risks that the company faces. There are risks related to reputation & market, financial risks and risks related to processes. Social Engineering is one of the most common ways to commit cybercrime. Social engineering involves an attacker and a target, the attacker slowly builds up a trust through e.g. email or by phone with the employee. So basically, social engineering consists of psychological manipulation of the employee in intent to get confidential- or high-profile information or economical benefits. Abraham S. et al. (2010) verifies this by defining social engineering as "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks". So what Abraham S. et al. (2010) implies is that the employees in this case unintentionally help the attacker by assuming that the attacker is for an example a team member or a client for the company. Let's assume that an employee works for a big international company, this often means that the employee does not know every person that works for the company. Because of this the attacker can easily disguise as a team member and for example present a problem to the employee and ask if they can help them. After this the attacker can use this email thread to talk to the next person in line, slowly getting higher up on the corporate ladder until they reach the person/system the attacker really is targeting.

Krombholz et al. (2014) talks about the future and BYOD policies or bring your own device policies and emphasizes that as all sorts of devices are evolving, also the ways of how to attack these devices evolve. So Krombholz et al. (2014) suggests that "a detailed understanding of the attack vectors is required to develop efficient countermeasures and protect knowledge workers from social engineering attacks.". So, by knowing how the attack is done, you can more easily defend yourself from these sorts of attacks.

Social engineering is often done through something called phishing and phishing can be put into two main categories, spear phishing and whale phishing. An attacker that is concentrating on acquiring illegally passwords, credit information or other volatile information is a spear phisher or in other words it is called targeted phishing. On the other hand, an attacker that is targeting high profile targets such as government officials, CEO: s, CFO: s etc. is committing whale phishing. Whale phishing is also targeted phishing but on a more detailed level. According to Gupta B. B. et al. (2018) there has been many cases of phishing throughout 2005-2018, targeting large businesses such as VoIP (identity theft), Facebook (ad spams) and Sony (credit & debit information stolen) just to mention some. These attacks have had crucial effects on the businesses such as reputation and financial losses, for instance according to Gupta B. B. et al. (2010) the cost of the phishing attack towards Sony consisted of losses up to $1 - $2 billion dollars not to forget to mention the impact this attack had on their reputation.

The figure 1 below shows the phases of an email phishing attack and gives an overview of how phishing is executed through email.

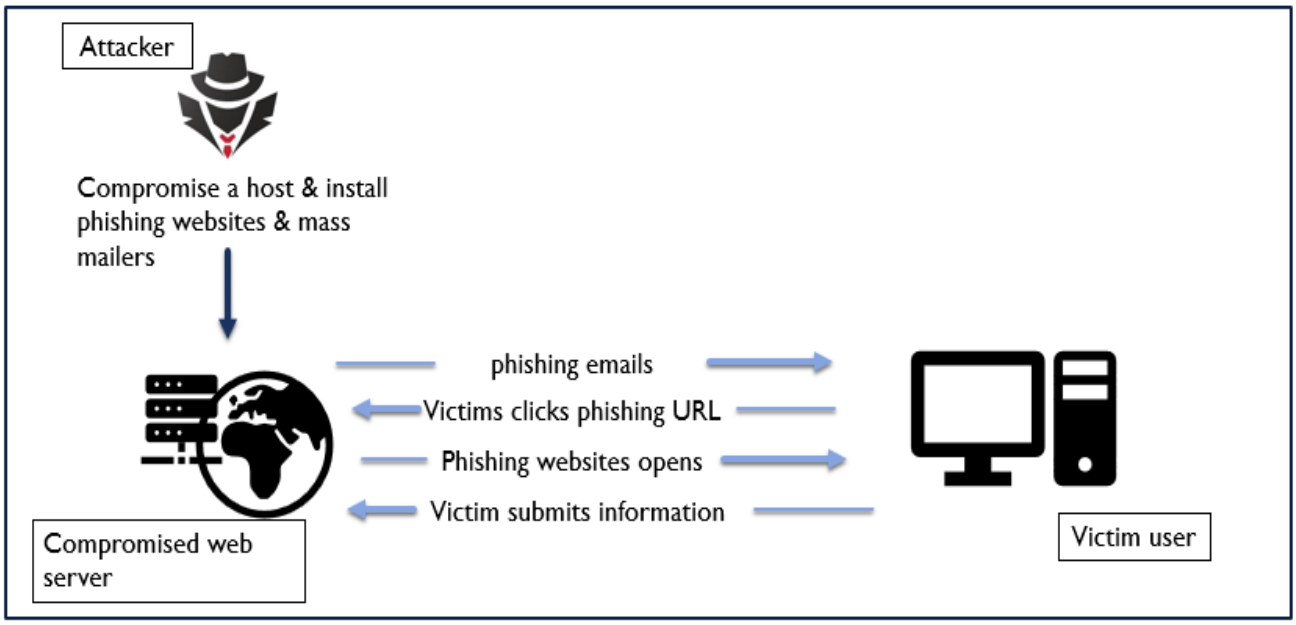

Figure 1. The Figure 1 is taken from B.B. Gupta, Nalin A. G. Arachchilage, Kostas E. Psannis (2018) article," Defending against phishing attacks: taxonomy of methods, current issues and future directions" (figure 11), but the figure design has been changed by the authors

Motives behind cybercrimes

Because of the constant growth of cyber criminality, it is important to understand the motives behind the people behind the screens. The different actors operating in the cyberspace can be distinguished from each other based on their motivations. The three main motivations are:

1. Financial gain
2. Political agenda
3. Intellectual challenge

Hacktivists are actors that are trying to achieve social changes or promoting a political agenda with the help of technology. It is important for the hacktivists to bring awareness and highlight a problem. The actions are often done in the name of freedom of speech, freedom of information or human rights. Hacktivists are often targeting governmental institutions or big corporations that are imposing censorship. Different methods are used in order to voice the activist's opinions. Examples of methods used by the activists are denial of service attacks on websites and stealing and publishing of sensitive and classified governmental information. Wikileaks and Anonymous is a prime example of an organization politically motivated (Ablon, 2018).

The largest group of actors are engaging in this type of activities of the sole purpose of money. Cybercrimes have been proven very profitable at the same time as the risk, if done right, is very low. Users of the peer-to-peer network Tor as well as people dealing with cryptocurrencies are basically untraceable, and because of the limited collaborations between countries' law-enforcement, it makes it even harder to get hold of the people responsible. There are a lot of different types of crimes than can be executed to make a profit. Stealing trade secrets, health information, intellectual property, credentials, bank details are a few of them. As most industries, the cybercriminals are differentiating their services to acquire as many new customers as possible. By customers, I mean people that are willing to either buy cybercriminal services or products. Monetizing on these activities are the top priority for the criminals and are

done via reliable black markets where payments are completed using cryptocurrencies. These black markets are both easy to access at the same time as they are very professional, both the likes of agents and intermediaries are found. The markets possess a hierarchy structure with the most knowledgeable administrators and subject-matter experts at the top. Because the lack of entry barriers, a lot of interested buyers find their way into these markets. Both services and products are provided here, some of the sellers are only providing certain exploit kits for the buyers to use themselves, where some provide a full-scaled cyberattack from initial hacking to the desired outcome. Extortion, stealing of intellectual properties and stealing of data is the most common types of services provided (Ablon, 2018).

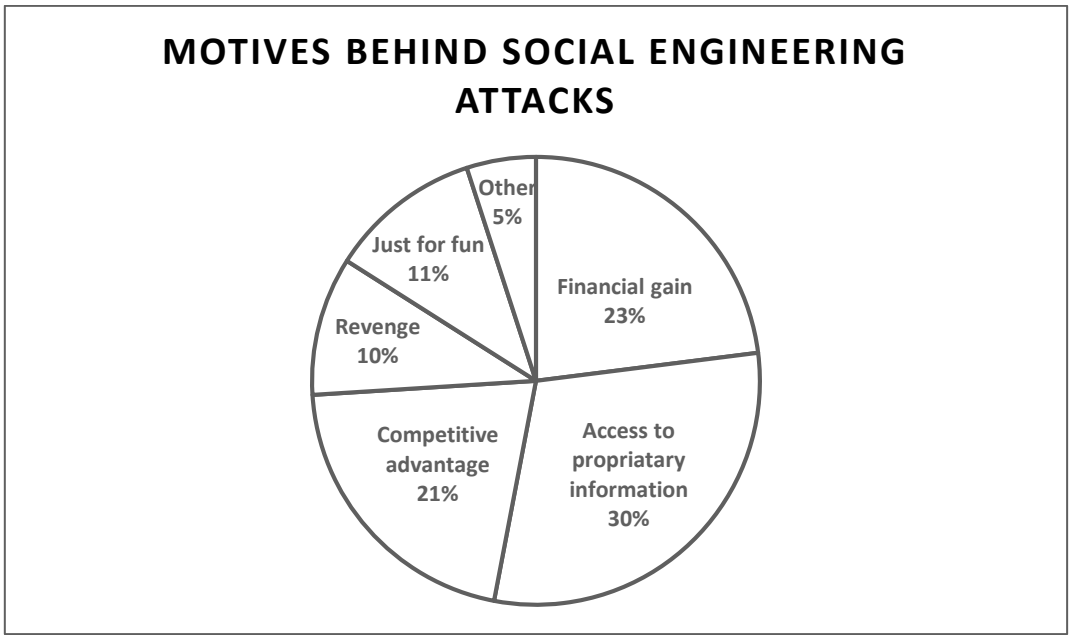

Figure 2. The Figure 2 is taken from Conteh, N. Y., & Schmick, P. J. (2016). "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks" (figure 2), but the figure design has been changed by the authors

Even though we present three main motives behind cybercrime, the above figure illustrates the distribution over the different motives behind social engineering attacks which was presented in chapter 1.4. Here we can see that the three biggest reasons are financial gain, competitive advantage and access to proprietary information.

Behavioral science

Up until this day, the approach for identifying and hindering cybercriminal maneuvers have been mostly technological. New computer software, advanced encryptions, password managers, multifaceted authentication are a few of the prevention methods used for stopping the cybercriminal threats. Considering that stolen data has become so simple to monetize from, cyber-criminal activities have grown into a profitable business of large scale. Seeing that the criminals easily can further financial gains from accessing data, new methods of exploiting vulnerabilities in businesses will always continue to be developed. Technological defense systems are of utmost importance, but the criminals have a tendency of circumventing these protection systems and instead focus on the weakest link in the security chain, the humans themselves (Eddolls 2016).

IBM's" Cyber Security Intelligence Index" from 2014 finds that 95 % of all security breaches include human errors. These numbers indicate that successful prevention requires a

shift from the technological approach to a more behavioral one. The technological systems will provide a protection for the organizations but are still vulnerable to human errors. A strong relationship between behavioral patterns and vulnerabilities need to be acknowledged. Cybercrime is in fact more about behavioral science than it is about computer science. Hence, we need to understand the relationship between behavioral patterns and cyber victimization.

Creating a cyber aware workforce and educating the employees how their personal cyber behavior is affecting the organization is an effective way of mitigating risk. The business leaders need to prioritize this matter and implement a cyber culture based on awareness. For this to become a reality, strong leadership is needed. The new corporate culture shall be implemented from the top and needs to permeate the organization as a whole. Cyber security shouldn't be an area that is left over for the IT-department to take care of. Instead, it should be embedded in all the processes of the business. By achieving that, and by focusing on the individuals instead, the businesses become sufficiently prepared and protected for threats. The business will still be a target for criminal activity, but now has a response plan in case it occurs (Eddolls 2016).

McBride et al. (2012) means that, by understanding employees' psychological profiles, companies act even more preventive. The reason for it being, employees with specific personality traits and behavioural patterns possess a bigger risk for being targeted by cyber criminals. Companies can therefore conduct personality tests and customize their education for those at bigger risk. The research made to this day has already helped us a bit on our way of understanding how different personalities possess different kind of risk. However, future evidence will most likely help us with how companies will be able to quantify personality traits and how they practically can implement this information in their cyber security training.

Existing research on the connection between cyber victimization and personality traits

In 1990 Gottfredson and Hirschi demonstrated through their general theory of crime that people with lower self-control are more likely to engage in criminal activities. The individuals with lower self-control are more impulsive, they take more risks and they are unmindful of future consequences. Numerous studies have applied the general theory of crime as a corner stone for further studies in the field of criminal cyber victimization. One study that uses the general theory of crime for cybercrime victimization research is Holtfreter et al. (2008). They have concluded that there is a connection between low self-control and victimization of several types of cybercrimes. These types are commonly scenarios where the end-user needs to provide the point of entry, for example opening an attachment in a phishing email. However, intrusions where no help from the end-user are wanted, the individual characteristics are less important. Schreck also found evidence in his study of a link between low self-control and being able to predict the risk of an individual falling victim for cybercrimes. The reason behind it is logical. Risk-taking and impulsiveness are not characteristics of a behavior that is known for its' preventive nature.

Scholars have also extended their studies to include personality traits, which indeed is part of" self-control". One study that investigates the relationship between the Big Five model of personal traits and cyber victimization is van de Wijer et al. (2017). The Big Five personal traits are Openness to experiences, Conscientiousness, Extroversion, Agreeableness, Neuroticism. Using a large sample of 3648 Dutch individuals, the authors find evidence that people with lower conscientiousness and emotional stability and that felt more openness to experience have higher risk of falling victim for cybercrimes. This result is in line with previous literature since

the results gathered from the different traits reflects the characteristics of low self-control in the general theory described above.

McBride et al. (2012) has extended the research about the role of individual employee characteristics by including the role of sanctions and protection motivation theory. The findings of the current study are consistent with those of van de Wijer and Leukfeldt which are that there's evidence that employees with specific personal traits are more likely to violating cybersecurity policies and therefore becoming a victim. The interesting part about McBride et al.'s study is that it incorporates the Big Five personal trait model with deterrence methods and protection motivation theory. The researchers were interested in finding out how deterrence effects the likelihood of violating corporate policies and how this differs between individuals. For example, some employees will choose the benefit from policy violation over the punishment received from breaking the rules. McBride et al. (2012) also wanted to assess how employees reacted differently when they perceived threats. The survey was designed so the authors could assess employee's personality traits, and then how these people would act differently. The results from the study shows that people with different personal traits, act differently in the same situations.

These findings suggest that a new approach should be undertaken by the organizations. Instead of focusing on a "one fits all"- training method, the organizations should focus on how different personality profiles are more likely to violate cybersecurity protocol. Generic training methods should be put aside and customized training methods depending on employee profiles should be implemented. By utilizing the information about how personality traits affect the perception of deterrence and threat, the training methods can be designed to target specific personality traits and therefore be much more effective.

Framework for building a corporate cyber culture of awareness

In a business context, social engineering techniques are commonly used when trying to get the end-user to commit a mistake. A cooperation between the intruder and the employee is needed. For the employee to make a mistake, he is manipulated into making something he shouldn't do, a human error.

Cyber security is a part of risk management. By creating a corporate culture of cyber awareness, organizations will decrease the likelihood of human errors occurring. Changing the corporate culture is not happening overnight, but every little help. The way of safeguarding towards social engineering is creating a defence system built by multiple layers. If one layer is penetrated, there are several more to hinder it from leading to total havoc. Conteh et al. (2016) have in their research article provided a few measures against social engineering. By adapting these changes with the addition of a few other modifications, organizations are taking big steps towards a change in their cyber security culture.

Human errors

Firstly, Human errors will always occur, there is no getting by that fact. Changing the corporate culture, the way cyber security is looked upon, is a prevention method. Eliminating the risk of human errors will never happen, and the expectations should be aligned with reality. Individuals inside an organization are the most vulnerable link and should be treated like everything else in risk management. Be familiar with the vulnerabilities, the risk tolerance and have a response ready if something occurs.

Build a strong morale and don't punish errors

A strong morale inside an organization often leads to the employees appreciating their job more. Making them feel that they are a part of something, instead of just a corporate worker, will boost their eagerness to avoid threats. This happens both consciously and sub-consciously. Management should also remember not to punish human errors too harshly. Social engineering is in fact often conducted in new founded and sophisticated manners. And if errors are punished too hard, it can lead to the employees not being willing to report when they potentially have made an error. This can lead to the damage becoming far worse. (SecurityIntelligence 2018). Pleefeger et al.'s hypothesis is that if the employees are taught the importance of behaving responsibly, are given time to learn the computer systems and are trusted to behave satisfactory in terms of cyber security policies, it can lead to better cybercrime prevention.

Deterrence methods are frequently used to get the employees to follow security protocol (McBride et al.). Deterrence theory suggests that if the sanctions are severe and certain, it will lead to that the employees won't engage in activities that aren't allowed (Akers, 1990). The effect deterrence methods have on employees are based on an individual's rationality and morality. An individual's perception of the sanctions being too harsh, can lead to negative effects with respect to cyber security (McBride et al. 2012).

Constant education

Educating and making the employees aware of potential threats is key when it comes to cyber security. By educating the employees, they will learn how to recognize common social engineering techniques, how their private cyber behaviour like lax password management and risky handling of company files can put the company at risk. And finally, different response methods against intrusions. For this all to be accomplished, constant education needs to take place. The landscape of the cyber criminals is constantly shifting, new methods of exploiting vulnerabilities are founded. Therefore, the education should follow the same pattern, it should be ongoing. In order to get the employees to learn as much as possible, the education should be versatile. Both practical and informative education should be provided. The result from the practical exercises should indicate how the education methods can be adjusted (Conteh et al. 2016). The best way according to Luo et al. (2007) to prevent ransomware attacks is to show what implications risky cyber behaviour lead to in terms of loss of stock value or loss of important customers. When the employees understand the real-life implications it can lead to, the chances of them taking precautions increases. The awareness training should also begin directly from the employment. By doing so, the organization will automatically shift the employee's mindset in terms of how cyber security should be prioritized (Simpson, 2017).

In his research article, McBride et al. describes three levels of cyber security training. The first two levels are similar and is referred to as the status quo-levels where generic training protocols are used with only a few individual differences acknowledged. The third level represents a potential future approach to cyber security training. The training protocol both incorporates personality factors and in which way individuals perceive security threats and potential sanctions. By using the results of McBride et al's. study, it can help organizations to develop employee profiles based on their perception of threat, sanctions and their personality traits. Customized training would then be created for all employee profiles to specifically target the individual's need when it comes to cyber security training. The information needed would be obtained by letting the employees answer a questionnaire that would evaluate both their personal factors as well as the situational factors.

Security Policy

The organization should establish a well-made security policy. Both technical policies as well as policies that focus on the individual perspective should be included. To make the security policy as hard-hitting as possible, it must be promoted from the company's top management tier, embed all company's processes and back it up with awareness training (Zurkus, 2016).

One of the most important aspects of the security policy is a clearly defined line of conduct, how things are supposed to be done. The employees should understand the course of action when sharing any kind of information inside the company. If something is asked to be done outside this procedure, it's a red flag. In this case, the employer should simply ask its' manager about it, if given the green light, the demanded information can be shared. Social engineers are also specialists at making the target feel pressured in to making decisions, this is also seen as a red flag.

If the employees don't follow the security policy, it is useless. Therefore, organizations are required to actively check that the policies are adhered to. This is done by actively monitoring the employees. Such control methods can include analysing network logs, re-confirm employees' authentication and to carry out made up social engineering attempts on its' employees. In whatever it concerns when it comes to learning, people learn from their mistakes. For that reason, it's so important to conduct these controlled tests. People will most likely feel somewhat of embarrassment for falling victim, and results in them being more alert next time they are asked to share information (Conteh et al. 2016).

When developing the internal policies with respect to cybercrime prevention, Pfleeger et al. (2012) suggests that there are areas of behavioural science that should be taken into account. Previous research on behavioural science shows that individuals tend to perceive and act differently in specific situations. By understanding these concepts and acting accordingly, organizations give themselves the chance to get more protected. For organizations to be able to change the beliefs and behavioural patterns, cognitive dissonance should be something every organizations should be aware of. An example is, the system would point out when an employee is acting stupidly in terms of risky cyber behaviour and make them aware of it. This would lead to a feeling of discomfort, and to get rid of the dissonance, the employee would have to be forced to change its' cyber behaviour.

Understanding bias is also something useful when trying to promote a change in behaviours. Three biases that Pfleeger et al. presents are, Status Quo Bias, Optimist Bias Control Bias. Status Quo Bias shows how individuals usually stick to their current behaviour if they're not given a convincing incentive to do so. To reduce this, systems should be able to create incentives to detect threats and act on them, aswell as providing feedback of their actions. Optimist Bias is when employees are underestimating the risk of anything occurring. This often leads the employees to avoid security measures. Control Bias describes when individuals think they can control an uncontrollable situation. Since they think they have control over the risks, employees are less likely to use preventive care measures (Pfleeger et al. 2012).

Technical Guidance

For the behavioural changes to have any impact, a multi-layered technical system must be in place. To keep the data protected, the organization needs well designed software that are installed on every device. Software's such as; Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN) and Intrusion Detection Systems (IDS). The employers should also have good spyware and antivirus software installed on their private devices (Conteh et al. 2016). Leon (2008) promotes organizations to use password management software programs to

securely handle all network passwords. The software does this by encrypting and randomizing the passwords, leading to a drastic decrease in password thefts.

Future prevention of cybercrime

Firstly, as cybercrime is evolving, and we are moving towards an even more digital work environment, the best way to prevent cybercrime in the future is to give up information about how these different cybercrimes in the past have occurred. All affected parties should release information about the crimes committed to the society and the business community to give more transparency regarding these issues. The conclusion is, that this would work like an "opensource" community or in other words a free service where all businesses and other parties could protect themselves by checking past breaches and how others were breached. Abraham S. et al. (2010) also talks about a synergy between governments, ISPs (internet service providers) and end users to reduce future and current issues related to cybercrime.

Secondly, another issue to deal with is the constant maintenance of cyber security. The businesses/governments can't assume that the security is unbreachable or think that it is enough to have the latest security software's. It was David Bernstein president of The Bernstein Agency that said, "For every lock, there is someone out there trying to pick it or break in..". This highlights even more that these "security officers" of the entities needs to stay pessimistic, constantly maintain and test the system to prevent future problems and discover weak links.

Thirdly, education awareness of employees and end users is one of the key factors to prevent cybercrime. It is important to see that all employees know the risks and ways of cybercrime to minimalize the risk of getting targeted by cybercrime attackers. This was already verified by Fadi A. Aloul (2012) in his article that "While organizations expand their use of advanced security technology and continuously train their security professionals, very little is used to increase the security awareness among the normal users, making them the weakest link in any organisation.". So what Fadi A. Aloul (2012) means is that the pressure should not only be put on the "security officers" but also on the normal employee to get more coverage. These cybercrime educations could be done by having a monthly or quarterly workshop discussing new issues regarding cybersecurity and security breaches that is connected to that department and other related issues.

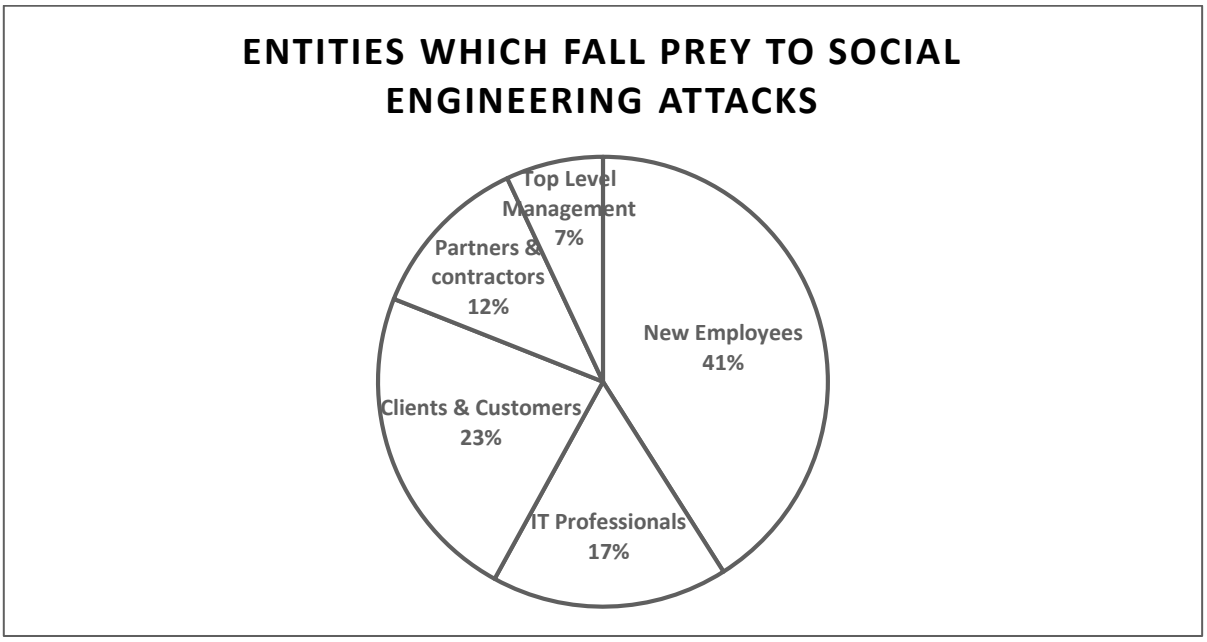

Figure 3. The Figure 3 is taken from Conteh, N. Y., & Schmick, P. J. (2016). "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks" (figure 3), but the figure design has been changed by the authors

The above figure from Conteh et al. (2016) article is a good example that shows which entities that are targeted regarding social engineering attacks. The biggest targets are new employees, clients & customers and IT professionals. This strengthen the view on future prevention of cybercrime which is discussed above, that businesses need to educate their employees, both new and old and of course do maintenance on current security systems.

Conclusion

The main conclusion in this paper is that we need to change the way we look at cybercrime and realize that it is spreading and getting more and more common. The ways and motives of committing cybercrime are various but social engineering is one of the most common ways and the motives behind this can be different depending on the attacker. In this article we have identified 3 main motives behind cybercrime:

1. Financial gain
2. Political agenda
3. Intellectual challenge

Behavioral science is one of the most important pillars after computer science regarding cybercrime and in many cases, it is not that the cybercrime itself is extremely sophisticated, but it is due to human errors and lack of education the cyber attacker can accomplish his intents. The main measures against social engineering was discussed from Conteh et al. (2016) article and five measures were discovered:

1. Human Errors
2. Build a strong morale and don't punish errors
3. Constant Education
4. Security policy
5. Technical guidance

In Das Sumanjits and Nayak Tapaswinis (2013) article they present a quote from Valerie McNiven, who is a U.S. Treasury Advisor and she indicates that the revenue from illegal drugs ($105 Billion) were less than, revenue from cybercrime and this was already in 2013. As we see an increasing trend in cybercrime we need to open our eyes and grab these issues when it is still possible. A combination of security information flow, education awareness and constant maintenance of security systems is a crucial and a good way of future and current cybercrime prevention for businesses and other end users.

Future guidance and outlook regarding this topic are that business owners and governments should invest in education of current and new employees regarding cybercrime. When employees are educated in issues regarding cybercrime the employers eliminate many problems that are connected to social behavior and cybercrime, e.g. human errors.

References

Ablon, L. (2018). The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. RAND Corporation.

Abraham Sherly, Chengalur-Smith InduShobha. (2010). An overview of social engineering malware: Trends, tactics, and impications. Technology in Society 32(2010), 183-196

Aloul A. Fadi (2012) The Need for Effective Information Security Awareness. Journal of Advances in information technology, 3(3), August 2012

Arief, Budi and Bin Adzmi, Mohd Azeem and Gross, Thomas. (2015) Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1 – Attackers. IEE Security & Privacy, 13(1), 71-76. ISSN 1540-7993.

Akers R. (1990). Rational choice, deterrence, and social learning theory in criminology: the path not taken. The Journal of Criminal Law and Criminology. 81(3), 653–676

Bernstein David quote: http://www.pewinternet.org/2014/10/29/elaborations-more-expert-responses-3/. (2014) Elaborations: More Expert Responses. Pew Research Center – Internet & Technology

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31

Das Sumanjit and Nayak Tapaswini. (2013). Impact of Cyber Crime: Issues and Challenges. International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142-153

Eddolls, M., 2016. Making cybercrime prevention the highest priority. Network Security, 2016(8), 5-8.

Gottfredson, M.R. and Hirschi, T., (1990). A general theory of crime. Stanford University Press.

Gupta B. B., Arachilage Nalin A. G. & Psannis E. Kostas, (2017 First online). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems. February 2018, 67(2), 247-267

Holtfreter K, Reisig MD, Pratt TC. Low self-control, routine activities, and fraud victimization. Criminology 2008; 46:189–220

IBM. 2014. Available : https://www.ibm.com/developerworks/library/se-cyberindex2014/index.html

Krombholz Katharina, Hobel Heidelinde, Huber Markus and Weippl Edgar (2014). Advanced Social Engineering Attacks. Journal of information security and applications

Luo, X. and Liao, Q., 2007. Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), 195-202.

McBride, M., Carter, L. and Warkentin, M., (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International-Institute for Homeland Security Solutions, 5, 1.

O'Gorman, G. and McDonald, G., 2012. Ransomware: A growing menace. Symantec Corporation.

Pfleeger, S.L. and Caputo, D.D., (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & security,31(4), 597-611.

Sabillon Regner, Cano Jeimy, Cavaller Victor & Serra Jordi. (2016). Cybercrime and Criminals: A Comprehensive Study. International Journal of Computer networks and communications security, Vol. 4, NO. 6, June 2016, p. 165-176. Available online at: www.ijcncs.org , E-ISSN 2308-9830 (Online)/ ISSN 2410-0595 (Print)

Schinder Debra Littlejohn & Cross Michael (2008), Scene of the Cybercrime, p.431 [Book] 2nd Edition. Available: https://books.google.fi/books?hl=sv&lr=&id=fJVcgl8IJs4C&oi=fnd&pg=PP1&dq=cybercrime+types&ots=ezCtBdMJh2&sig=y_zT_qDjz5ew1PjcCWIgGzb8gmU&redir_esc=y#v=onepage&q=types&f=false

Simpson W., (2017). How to make your employees care about cyber security. Techrepublic. Available: https://www.techrepublic.com/article/how-to-make-your-employees-care-about-cybersecurity-10-tips/

Schreck CJ., 1999. Criminal victimization and low self-control: An extension and test of a general theory of crime. Justice Quarterly 1999; 16:633–654

Symantec Corporation. What is a computer virus. Available: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

TechTarget. Worms. Available: https://searchsecurity.techtarget.com/definition/worm

Van de Weijer, S.G. and Leukfeldt, E.R., 2017. Big five personality traits of cybercrime victims. Cyberpsychology, Behavior, and Social Networking, 20(7), 407-412.

Zurkus, K. 2018. How to build a corporate culture of cyber awareness. Security Intelligence. Available: https://securityintelligence.com/how-to-build-a-corporate-culture-of-cyber-awareness/.