Human Factors in Cybersecurity, Vol. 53, 2022, 66–73
https://doi.org/10.54941/ahfe1002203

Exploring Human and Environmental Factors That Make Organisations Resilient to Social Engineering Attacks

Michelle Ancher[1], Erbilcan Aslan[1], and Rick van der Kleij[1,2]

[1]The Hague University of Applied Sciences (THUAS), The Hague, The Netherlands
[2]The Netherlands Organisation for Applied Scientific Research (TNO), The Hague, The Netherlands

ABSTRACT

In this explorative research social engineering attacks were studied, especially the ones that failed, in order to help organisations to become more resilient. Physical, phone and digital attacks were carried out using a script following the 'social engineering cycle'. We used the COM-B model of behaviour change, refined by the Theoretical Domains Framework, to examine by means of a survey how Capability, Motivational and foremost Opportunity factors help to increase resilience of organisations against social engineering attacks. Within Opportunity, social influence seemed of extra importance. Employees who work in small sized enterprises (<50 employees) were more successful in withstanding digital social engineering attacks than employees who work in larger organisations. An explanation for this could be a greater amount of social control; these employees work in close proximity to one another, so they are able to check irregularities or warn each other. Also, having a conversation protocol installed on how to interact with outsiders, was a measure taken by all organisations where attacks by telephone failed. Therefore, it is more difficult for an outsider to get access to the organisation by means of social engineering. This paper ends with a discussion and some recommendations for organisations to help increase their resilience against social engineering attacks.

Keywords: Cybersecurity, Cyber safe behaviour, Human factors, COM-B model, Cyber resilience, SME and cyber.

INTRODUCTION

Social engineering is the most common modus operandi of cybercriminals (Verizon, 2021). Social engineers aim at human vulnerabilities, convincing people to give them access to sensitive data through manipulation. For example, employees accidentally reveal their login credentials on a phishing website or physically give unauthorized individuals permission to enter their office, with severe consequences like data leakage as a result. This may lead to reputational or financial damage. Larger organisations often have the means to protect themselves from cybercrime. However, small and medium sized enterprises (SMEs) often have limited opportunities to defend themselves against cyberattacks. They have insufficient resources and basic security measures are not in order (Notté et al., 2019).

Organisations pay a lot of attention to technical measures in order to protect sensitive information, such as the use of encryption software, intrusion detection systems and firewalls. However, cybercriminals often cleverly circumvent technical security by manipulating the employee. Although we know how social engineering works (Ancher et al., 2019), less is known about measures aimed at increasing the resilience of people against it. In this study we focus on factors aimed at hardening the human target entity. We explore how organisations where social engineering attacks fail, protect themselves effectively against them. Our main research question reads: 'Which human and environmental factors play a decisive role in cyber safe behaviour when a social engineering attack takes place?'.

We started this research, by conducting an experiment of social engineering attacks at Dutch organisations, with their consent. These attacks were carried out by students of HBO ICT, the Hague University of Applied Sciences (THUAS). The students learn where (technical, organisational, or human) vulnerabilities lie so that they, as future professionals, will be better able to defend their employers' interests. After the attacks, we performed an analysis of the attack reports, conducted a survey at the participating organisations and performed a data analysis, using the grounded theory (Baarda, 2019).

SOCIAL ENGINEERING ATTACKS

In general, social engineering attacks appear in three ways: digital, physical and by telephone. The aim of social engineering is to provoke certain unsafe behaviour. There is a selected target, for instance an employee within a department, and the attack is often aimed at specific data like employee passwords or client information. The attacks follow the so called 'social engineering cycle': research, hook (how to 'catch' the target), play and exit. Preparatory research is often done by open-source intelligence (OSINT) like social media. Attackers rely on techniques such as Cialdini's principles of persuasion to manipulate their victims (Cialdini, 2007).

COM-B MODEL OF HUMAN BEHAVIOUR

Based on literature we identified several human and environmental factors that may be related to behaviour that keeps people safe from falling victim to social engineering. Cyber safe behaviour in regard to social engineering is defined as 'not giving sensitive data or access to this data to unauthorised persons when manipulated'. We will briefly explain the factors that relate to these types of behaviours below.

To acquire insights into the underlying causes of cyber safe behaviour when social engineering attacks take place, we use the Capability Opportunity Motivation-Behaviour (COM-B) model for behaviour change (Michie et al., 2011). This scientifically supported and promising model was originally developed for health interventions and has not yet been applied much in cyber security (Van der Kleij et al., 2020). The model states that people's behaviour can be explained by the components: Capability, Opportunity and Motivation and their interaction. Capability refers to whether employees have

required the knowledge and skills. Motivation to whether they have a positive attitude and intention. Opportunity to whether there are factors outside the individual that make certain behaviour possible, i.e., the physical (material) and social environment of employees. The theoretical Domains Framework (TDF) (Huijg et al., 2014), is used to map the COM-B components onto and is thus a refinement of the COM-B model.

Common behaviour approaches to help prevent data leakage are security policies and awareness campaigns (Blythe et al., 2018). These are usually meant to increase employee's knowledge and ability on cyber security. However, they have limited success because procedures can be bypassed by employees, for example when under pressure. (Kirlappos et al., 2015) (Van der Kleij et al., 2020). In this study little attention is paid to Capability. We focused mainly on Opportunity in relation to cyber safe behaviour, because we are of the opinion this deserves extra attention.

The theory of Crime Prevention Through Environmental Design (Crowe et al., 2014) states that the proper design and effective use of the urban environment can lead to a reduction in the incidence of crime and thus has influence on the criminal's behaviour. An example of environmental design is the so-called 'safety spot'. This is a white semi-circle painted on the ground right in front of the ATM machine within which the user can protect his privacy because of the 'barrier' it creates for others to enter. This helps to prevent so called shoulder surfing, the practice of spying on the user of an electronic device in order to obtain e.g. their password. Based on this theory, we included the design of the physical work environment like open or closed workspaces and added aspects of the online work environment. Finally we assessed whether the organisation took basic information security measures (Notté et al., 2019), like a security architecture or password management and measures against social engineering (Gragg, 2002).

METHOD

During an annual semester at THUAS, students designed and conducted structured social engineering attacks to provoke unsafe behaviour by employees. They performed three types of attacks: physical, by entering the organisation's building or office areas without authority, by telephone, obtaining sensitive information by telephone, and the digital attack, by sending phishing links (mostly by email, but also via WhatsApp or Microsoft Teams). These attacks were done according to the 'social engineering cycle'. The students used a checklist with before mentioned variables: selected target, sensitive data to be collected and persuasion technique. They were free to give further interpretation to the design of the attack. Students adhered to the law, regulations and a code of ethics. They acted as if they were the attackers. A total of fifteen organisations volunteered for this experiment. They were recruited via the THUAS network and teachers' LinkedIn. Three organisations were public organisations (education, care, government) and twelve SMEs (metal, ICT, production). Five of the SMEs were small (<50 employees), the others were medium or bigger sized. To learn more about the different types of social engineering attacks that failed, the reports written

Table 1. Organisations and type of attacks that (not) succeeded.

Organisations	Attack NOT successful	Attack successful
A		D, P
B		D, P
C	D, P	
D	T, D	P
E	T	D, P
F	T	P
G	D	T, P
H	T, P	D
I	D	
J	T, D	P
K		D

Explanation: D = Digital attack, P = Physical attack, T = Attack by telephone.

by students were analysed. Both their observations and specific results for example the amount of clicks on a phishing link, were analysed.

Interviews were conducted after the attacks to learn more about the human and environmental factors that influenced the success of the attacks that took place. Eleven contact persons of the social engineering's targeted organisations participated: three of them were directors, the others ICT security professionals. They volunteered for a 45 minutes, qualitative, semi-structured, fifty-six items, interview. As we mentioned earlier, we adopted refinements of the COM-B components from the TDF (Huijg et al., 2014), and selected sixteen items from eight domains from the corresponding (initial) questionnaire. We asked respondents if they thought the components Opportunity, Capability and Motivation, that may have a positive influence on cyber safe behaviour of their employees, were present. We focused on Opportunity with the domains 'Social influences' and 'Environmental context and resources' of which we used eight items from the TDF. Two example questions: 'Is there any form of social control on cyber safe behaviour, present?' and 'Do other employees within the organisation consider cyber safe behaviour important and do they behave like it?'. We divided resources in: budget, staff, security policy and involvement of other departments. We also used eight items from the domains Beliefs about consequences, Beliefs about capabilities and Motivation and goals (Motivation), Knowledge and Skills (Capability) and Nature of behaviours (Behaviour).

In addition to the TDF questions, to find out if a physical and online environmental design plays a role in relation to cyber behaviour, we added questions about the use of devices, software and office design. We also asked about some characteristics of the organisation like, branch and size and the existence of protective basic security measures. Interviews were analysed using the grounded theory method (Baarda, 2019). Following the steps: data collection (interview transcripts) coding of the data (making word clouds and categorisation in mind maps) and drawing conclusions.

RESULTS

To learn more about what types of social engineering attacks failed and why, we analysed the attack reports of the eleven organisations who participated in the survey. There were in total twenty five attacks analysed (table 1). Physical attacks occurred nine times and were much more successful than the other types: only two physical attacks were not successful. Of the phone attacks five out of six failed, only one succeeded. The digital attacks appeared to be the most common (10). An employee did click on a phishing mail in one organisation and another employee gave his credentials. Five digital attacks were not successful. Looking closer at the organisations where digital attacks failed, they were all found to be small sized enterprises with less than (<50 employees).

EXAMPLES

Successful physical attack:

Students noticed that the organisation recently hired an interior designer. They replicated the e-mail address of the facility manager and send an email to the front desk explaining that the designer liked to take photos of the newly decorated rooms. Two students acting like photographers were let in without any identity checks. They walked around the office workplaces taking photos and gaining access to documents, open desktops, and rooms.

Unsuccessful Phone Attack:

Students found out that a company supplied the local hospital with equipment and installed the required machines in the operating rooms. They called the front desk asking for blueprints to the building and operating rooms. The front desk employee immediately told them that they always have specific representatives within partner organisations who handle questions and share information and that she couldn't share anything. The company had clear guidelines regarding this situation.

The grounded theory analysis of the interviews gave the following results about the COM-B components that could play a role in making attacks fail. No differences were found in COM-B elements for failure or success of a certain type of attack. Capability (Knowledge and Skills) seemed to be average present in the organisations. Motivation seemed to be present as well. All the respondents indicated that employees found it important to take measures against malware, viruses, and so forth. Half of the respondents indicated that employees consider paying attention to cybersecurity. A few (3) indicated that employees act automatically and are not alert. Respondents mentioned that capability and motivation differ a lot between individuals and the various departments within organisations. This comment is characteristic: 'People know about it and find it important, but whether they act accordingly, I doubt.

The Opportunity results are divided into Social influence and Environmental context and resources. Considering Social influence most of the organisations (9 out of 11) scored high; Organisations (9) indicated that

there is any form of social control present, they can count on support from colleagues to do work well (8) and, they think colleagues within the organisation consider cyber safe behaviour important (10). When asked about positive characteristics of leaders the following characteristics were mentioned: leaders take responsibility, monitor processes (6) and are always approachable and willing to help (11). Whether they play an active role in cyber security is doubted and it is assumed that they possess limited knowledge about the topic. Only in one organisation managers set a good example regarding cyber safe behaviour. It's even mentioned that 'employees pick it up faster than management'.

Considering the Environmental resources: nine organisations said that there is sufficient budget for information security, seven organisations said there are other departments involved, in only one it was the communication department. Five organisations have staff within their security department, and four have a clear policy regarding information security. With regard to the design of the physical environment, work is often done in open-plan offices including closed consultation rooms. The online environment, like communication software used, is diverse. Mostly there's no intranet.

All organisations take basic security measures and measures against social engineering to a greater or lesser extent. This varies from posters (2), awareness training (5) to red team assignments and the use of security toolkits (3) and protocols on how to interact with outsiders (5). Especially these protocols appear to be important in repelling social engineering attacks. In three of the four organisations where the physical attack succeeded there were no protocols in place. All five organisations where the unsuccessful attacks by telephone took place, had protocols. Seven organisations reported different issues when it came to information that is available through OSINT. Only three organisations did not pay attention to this, but there is no relation, because these digital attacks failed. Social engineering attacks of students have direct influence on behaviour: In three organisations there are more incident reports since then and one organisation arranged for a banner to pop up when an email arrives from outside the organisation.

CONCLUSION AND DISCUSSION

This study was set up to investigate which human and environmental factors play a role in organisations where social engineering attacks from external entities fail. We explored the extent to which the capability and motivation of employees, social influence, and environmental context and resources, play a role in strengthening organisations against social engineering attacks.

We found that the capability of employees to withstand social engineering attacks, was on average sufficient in most organisations. However, it appears that personal capability isn't such an important factor in withstanding attacks. The same is also true for the motivation of employees. We found that organisations where employees were motivated, e.g. find it important to take measures against malware, viruses and so forth, were not more resistant against social engineering. We do see however, that opportunity

factors play an important role in helping to keep organisations safe from social engineering.

Regarding the environmental context and resources most organisations reported sufficient budget to cover information security and sufficient involvement of other departments. These are important factors in keeping the organisation safe from social engineering attacks. However, from all the organisations studied, only one had involved the communication department. Also, only a few organisations had a clear security policy and sufficient IT staff. These are missed opportunities regarding the protection of organisations (ENISA, 2018). Another interesting finding is that having a conversation protocol installed on how to interact with outsiders, may well help organisations in their battle against social engineering attacks. In all of the organisations where the telephone attack failed, it seemed that a conversation protocol helped the employees to counter the attackers' attempts at social engineering. More evidence arises from the fact that in most of the organisations where the physical attacks succeeded, no such protocols were in place to help employees in dealing with this kind of attacks.

When considering the design of the environmental context, we found that pop up email banners that appear when an email arrives from outside the organization, did help in preventing digital social engineering attacks from being successful. The explanation is that these pop ups better alerted employees to the potential threat of the situation. Another example is a report button for suspicious emails, which makes it easier to report a phishing incident. We can help organisations by translating examples from the theory of Crime Prevention Through Environmental Design (Crowe, 2014) into social engineering prevention measures in the (online) work environment. Another suggestion is to expand the TDF questionnaire with environmental design conditions.

Regarding social influence this study shows that social control is an important factor in countering social engineering attacks. All organisations where digital attacks failed, were small sized enterprises (<50 employees). The explanation for this could be a greater amount of social control; these employees work in close physical proximity to one another and if they need to check something suspicious, they are easily able to reach out to a colleague. The social norm is supposed to be a key factor in security behaviour (Glaspie, 2018). Advantage can be gained by employees who dare to address and warn each other about unsafe behaviour, transforming the common social norm into a cyber-safe norm. The social engineering attacks performed by students turned out to be an intervention in itself and the social norm (although perhaps only temporarily) positively changed, because people became more alert and reported incidents. Although managers are reported to be always approachable and willing to help, it's striking that only one organisation stated that the leader had an exemplary function when it came to cybersecurity. The leader is an important role-model for the employees (Bandura, 1986) (Gragg, 2002). Furthermore, everyone in the organisation carries a responsibility for cyber safe behaviour and in addition to the leader other motivated employees can act as security ambassadors in an organization.

In short we have shown that opportunity factors can be of importance in cyber safe behaviour. Resources like budget, enough staff and conversation protocols can provide solutions, especially within SMEs. Over the next years, we will continue our observational research on SMEs, paying attention to working on a cyber-safe norm and exploring elements in the design of the work environment that could prevent attacks from being successful.

ACKNOWLEDGMENT

We owe our gratitude to all organisations that volunteered to take part in this study. Thanks also to the students and teachers who made the social engineering attacks possible. We thank Glyn Giles and Renate Kenter for the English editing and Bart Alberts for his overall support.

REFERENCES

Ancher, M., Kleij, R. and Leukfeldt, E. (2019). Studenten treden in voetsporen cybercrimineel om meer inzicht te krijgen in social engineering. [online] IB-magazine, 2019-2, pp. 26–33.

Baarda, B. (2019). Dit is onderzoek!. Groningen/Houten: Noordhoff Uitgevers.

Bandura, A. (1995). Social foundations of thought and action. Englewood Cliffs, N.J.: Prenctice Hall.

Blythe, J.M. and Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in Human Behavior, 87, pp.87–97.

Cialdini, R.B. (2007). Influence, the psychology of persuasion. NY: Harper Collins Publishers Inc.

Crowe, T. and Fennelly, L. (2014) Crime prevention through environmental design. 3rd ed. London, England: Elsevier Science.

ENISA. (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.

Glaspie, H. (2018). Assessment of information security culture in higher education assessment of information security culture in higher education, Ucf.edu.

Gragg, D. (2002). A Multi-Level Defense Against Social Engineering. White paper, Sans Institute.

Huijg, J. M., Gebhart, W.A., Dusseldorp, E. et al. (2014). "Measuring determinants of implementation behavior: psychometric properties of a questionnaire based on the theoretical domains framework," Implementation science: IS, 9(1), p. 33.

Kirlappos, I., Parkin, S. and Sasse, M. A. (2015). "'Shadow security' as a tool for the learning organization," ACM SIGCAS Computers and Society, 45(1), pp. 29–37.

Michie, S., van Stralen, M. M. and West, R. (2011). "The behaviour change wheel: a new method for characterising and designing behaviour change interventions," Implementation science: IS, 6(1), p. 42.

Notté, R., Slot, L., van 't Hoff-de Goede, S. and Leukfeldt, R. (2019). Cybersecurity in het mkb Nulmeting. The Hague University of Applied Sciences.

Van der Kleij, R., Wijn, R. and Hof, T. (2020) "An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations," Computers & security, 97(101970), p. 101970.

Verizon.com. (2021). Data Breach Investigations Report.