Research Article

Received: 3 March 2021 / Accepted: 3 June 2021 / Published: 8 July 2021

Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters

Ahu Ergen

School of Applied Disciplines, Bahçeşehir University,
Yıldız, Çırağan Cd., 34349 Beşiktaş, İstanbul, Turkey

Ahmet Naci Ünal

Faculty of Engineering and Natural Sciences, Bahçeşehir University,
Yıldız, Çırağan Cd., 34349 Beşiktaş, İstanbul, Turkey

Mehmet Sıtkı Saygili

Vocational School, Bahçeşehir University,
Yıldız, Çırağan Cd., 34349 Beşiktaş, İstanbul, Turkey

DOI: https://doi.org/10.36941/ajis-2021-0111

Abstract

The increase in cyber attacks cause individuals and businesses to face financial loss and reputation damage. Most cyber security studies ignore human factor and focus only on technological measures although the cyber security behaviors of employees are vital for the organisations. This paper aims to explore and discuss the role of employees in cyber security. In-depth interviews with eight cyber security experts were conducted through semi-structured, open-ended interviews. This study gives perspectives regarding the cyber security behaviors of employees, the barriers and promoters of secure behaviors in cyberspace. The findings mainly stem reasons of unsecure behaviors and solutions for them, and provide implications to companies for effective training and recommendations to adopt secure behaviors in the companies.

Keywords: *cyber security, cyber security awareness, cyber security behaviour, cyberspace, information technology*

1. Introduction

Internet technology entered our lives in the 1990s and it was first called cyber environment. Today, the sensors with embedded systems can communicate with other sensors besides internet connection. This expanding network structure which is defined as cyberspace (Unal, 2020) provides many services and opportunities for the companies. It also includes many risks that the users are not aware (Kortjan and von Solms, 2014). Hence, cyberspace and internet include serious risks for information security breaches. Hackers have various technics to change confidentiality, integrity, and the availability of information in their interest. At this point, users become serious cyber victims because of their negligence, ignorance or sometimes unintentional behaviours such as sharing their

passwords with others, downloading any software from the Internet or using their social security numbers as passwords (Safa *et al*., 2015). Regarding risks in cyberspace, users are often described as the weakest element because technical precautions can not solely overcome cyber risks caused by human errors (Gratian et al., 2018:345, Anwar et al, 2017:437). Phishing accounts for 90% of all data breaches (HBR, 2020, p.17). Global spending on security awareness training for employees (predicted to reach US$ 10 billion by 2027) shows the importance of being prepared and defensive against cyber attacks (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016). So, there is higher need to understand human behavior from security perspective, since individuals and organisations become more dependent on digital data. This brings new challlenges such as protection of digital assets together with new opportunities. Personally, we may have different levels of awareness towards cyber incidents; however, as employees we also have responsibilities for our organisations.

In this paper, we present a study about the barriers and promoters of cyber security behavior of employees. The study is one of the first to examine how employees behave, from the cyber security experts' perspectives. Previous studies have mostly focused on technology dimension of cyber security. So, the objective of this research is to provide an overview and offer solutions to risky cyber security behaviors of employees. The next section presents the theoretical framework. The subsequent section outlines data and methods. The article concludes with final section summarizing the main findings of this study and gives implications for further research.

2. Literature Review

2.1 Risks in cyberspace and cyber security

In the book named "Spam nation" it is stated that anti-virus companies are fighting 82,000 new attacks every single day. Only McAfee detected 15 million new malwares in the first quarter of 2013. Target Corporation had a data breach incident in 2013 which affected 2.6 million consumers. This caused the company to lose business and reputation at that time. After that attack, Target improved its system, issued more secure chip-PIN cards and started to use advanced technologies. In June 2017, NotPetya cyber attack took place. As a result, Maersk group formatted and reinstalled 4.000 servers, 2.500 applications and 45.000 computers around the world (Eryaşa, 2020:89). Dominating cyber attack trends in 2019 is ransomware attacks (Check Point, 2020:6). According to McAfee In the first quarter of 2019, ransomware attacks grew by 118% and new ransomware families were detected. The increasing cybersecurity incidents especially in retailing, logistics, financial services and health services show the need for more effective solutions (He et al., 2016:99-100; Torten, 2018:77; Ghadge et al., 2020:224).

Moreover, Romansky (2016:121-122) analysed 12,000 cyber incidents including security and personal data breaches, and phishing to understand if minimising the costs and risks of cyber incidents is possible, and found out that a typical cyber attack costs approximately US$ 200,000. This amount also represented 0.4% of yearly income of a company. Financial theft through whaling has cost companies US$ 12.5 billion globally between October 2013 and May 2018 (Coburn et al., 2019:28). In 2019, enterprise businesses' devices were infected with malware costing US$ 2.73 million. Ransomware damages are predicted to cost the world US$ 20 billion in 2021(Morgan, 2019:5). WEF 2020 Global Risk Report points out that according to likelihood criteria, cyber attacks are in number seven after data fraud (The Global Risks Report, 2020). Every year, the losses associated with attacks on corporate networks and intellectual property theft, cost businesses billions of dollars. These facts and figures show us the vitality of cybersecurity in organisations.

Cyber security, which has become the subject of global interest and importance (von Solms and van Niekerk, 2013:97), is defined as "*the precautions that have to be taken in order to prevent cyber attacks in information systems, unauthorized reach and harm to data and the fear and panic in public opinion*". The awareness of individuals and securing the personal computers to the building of

national cyber security teams who interfere with national cyber attacks can be some of those precaution (Cakir et al., 2017:154). Cyber security and information security are often used interchangeably. Figure 1 shows the relationship between these two terms. In cyber security, many assets such as individuals, household appliances, the society or the national infrastructure, that can be reached by cyberspace, need protection (von Solms and van Niekerk, 2013:97).

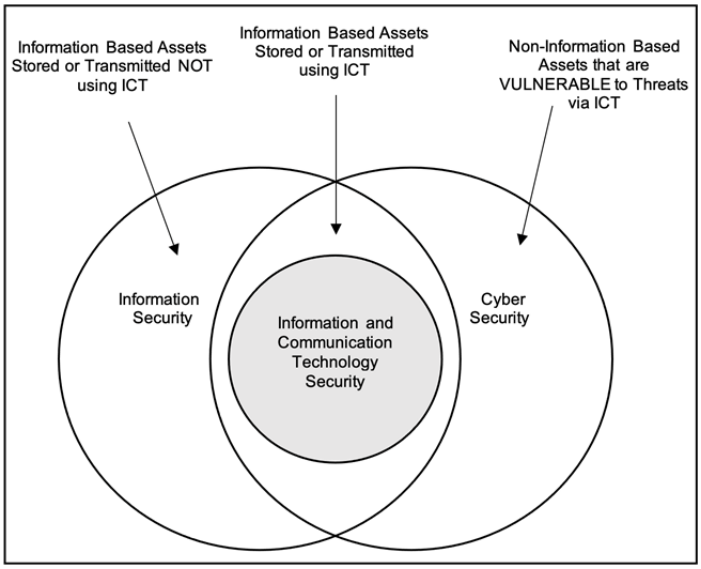

Figure 1: The relationship between information and communication security, information security and cyber security
Source: von Solms and van Niekerk, 2013:101

Today, cyber attacks that is part of national security, is becoming a threat for both developed and emerging countries. The cyber attacks to government web sites and strategically important internet sites affect the service quality and cause loss of reputation (Cakir et al., 2017:151). Since cyberspace doesn't have physical borders and it is not under the rule of a single country, together with the improvements in technology, malicious cyber initiatives have a tendency to increase. Although there is not a consensus in global society, in the close future, the possibility of increase in the complexity of malicious cyber initiatives may force the countries to give joined effort for legal preparations (Yayla, 2014:196). Commonwealth Telecommunications Organisation (CTO, 2015) points out that while many countries have designed cybersecurity strategies which are mainly "*structured documentations of the essential elements of an entity's cybersecurity journey*", only few have cybersecurity implementation frameworks (CIF) (Dedeke and Masterson, 2019:374).

According to Blythe (2013), the advance in technology enables the employees work from various devices and reach information from anywhere at anytime. This new situation increases user productivity and the efficiency of business processes. Companies provide their employees remote access and cloud-based storage, portable devices and mobile phones. Hence, this new technology also increases the risks stemming from cyber threats. Hekim and Basibuyuk (2013:156) state that despite all security precautions, cyber attacks may be successful due to human mistakes. According to the research findings of Dimensional Research in 2011, 43% of information systems experts state that their companies faced social engineering attacks. 48% also stated that each social engineering attack caused them to lose US$ 25.000 in average. In 2016, Cyence company stated that the United States

was the most targeted country by social engineering attacks and the estimated cost of these attacks in the US was US$ 121.22 billion (Salahdine & Kaabouch, 2019:1). Accenture (2019) report based on interviews with more than 2,600 security and information technology (IT) professionals at 355 organizations worldwide, found that the cost to companies due to malware increased 11 percent, to more than US$ 2.6 million per company, on average, and the cost due to malicious insiders such as employees, temporary staff, contractors and business partners, jumped by 15 percent, to US$ 1.6 million per organization, on average. Together with advanced precautions regarding hardware and software, a vital dimension of security which is the "human factor" must not be neglected by the companies.

2.2 Human factor in cybersecurity

The advances in technology including AI, IoT, big-data and cloud computing increase the responsibility of organisations to secure their intellectual capital and this brings the need to provide user-friendly designed information and cybersecurity procedures and policies for employees. He et al., (2019) recommends regular cyber security awareness training for all employees to prevent data breaches to intellectual capital. Cybersecurity awareness seems to be the starting point of this hard task, to fight with cyber attacks, although it is very challenging in organisations. Bada and Nurse (2019:404) focused on cybersecurity strategy of an organisation by proposing a cybersecurity education and awareness programme for small- and medium-sized companies in Australia, the UK and the USA. In Figure 2, five main steps of this programme are summarised as (i) initial engagement with SME's (ii) improving security practices and culture (iii) programme resources (iv) trusted third-party resources / services and (v) communication strategy.

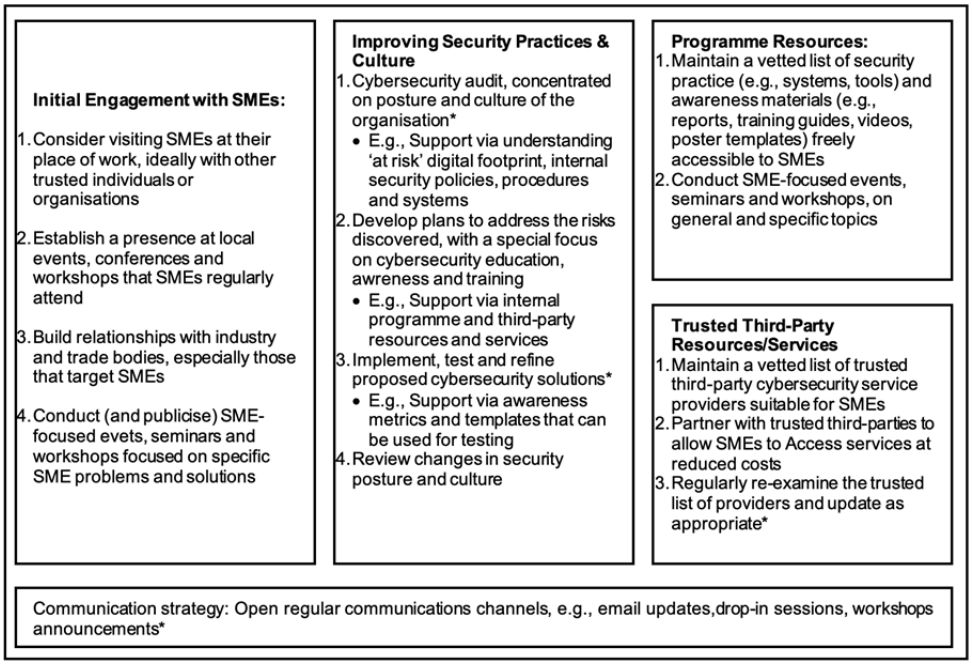

Figure 2: A cybersecurity awareness programme for SMEs/SMBs
Source: Bada and Nurse, 2019, 404

Being aware is an important element on the road to behavior change. Hence, it can not be enough to change behavior alone. For instance, the premise "for an employee who has high cyber security awareness will always behave securely in cyber space" is not right. There are many demographic, psychological and cultural factors influencing human behavior. According to Karaci et al. (2017), the threats rising from human factor are phishing, social engineering, malware, worm and spy softwares. Coventry et al. (2014) list ten main precautions regarding cyber threats: (i) having strong passwords and managing them securely (ii) using anti-virus programmes and firewalls (iii) running the latest version of a software (iv) logging out of web sites after finishing and before shutting down the computer (v) using only trusted and secure connections, devices (including Wi-Fi), sites and services (vi) knowing the risks and trying to avoid scams and phishing (vii) providing minimum personal information to protect the identity (viii) being aware of the physical surroundings when online (ix) reporting cybercrimes to the authorities. It is vital to make people adopt secure behaviors towards increasing risks in cyberspace; however, changing human behaviour in cyber space is not an easy task (Torten, 2018:77).

2.3 Cybersecurity awareness programs

Today, organisations have a new kind of threat, namely cyber threat. It is difficult to detect cyber threat and also hard to predict its long term effects. Although cyber security awareness is growing among executives, most organisations are still inactive. Being proactive would bring success to organisations in coping with the cyber risks. It would be useful to personalize the risks for managers so that they can realise the vulnerability and the effects (Johnson and Goetz, 2007). In a research conducted with 579 business professionals in the USA, the findings show that the employees who are aware of their companies' information security policies and procedures behave more securely compared to the ones who are unaware. In the same research it is also found that an organisational information security framework affects the employees' threat evaluation and coping skills positively which makes meaningful contribution to cyber security behaviors (Li et al., 2019:13-17).

By preparing cyber security awareness programs and measuring the results, companies may foster awareness and close the gap between secure behaviors and risk perception. Procedures are needed to motivate employees to learn security policies and act securely (Li et al., 2019:22). If a security policy consists of behaviors that none of the employees adopt, this will not bring secure cyber behaviors in the organisation (Coventry et al., 2014). Mass communication is necessary for the employees to be aware of the risks and act, however if the users perceive this as a fearful alarm and do not experience the results, it doesn't help. Today majority of the cyber security messages are massive. There is a need for customized messages with appealing formats designed yet for specific target groups (Unal and Ergen, 2018). Beyer et al., (2015:3) criticize this approach as follows: "*Security communication, education, and training (CET) is meant to align employee behavior with the security goals of the organization, but it is not always designed in a way that can achieve this. Currently, security CET is mostly delivered as generic web-based training with security quizzes, a "box-ticking" exercise that only indicates employees have read through pages and know the answers to questions. It does not mean they will adopt secure behaviors as they go about their daily tasks*". He et al., (2019) recommends to task some employees who will share cues, tips and reminders about information security and also hang posters of cyber security to enhance secure behaviors. Sedkaoui and Khelfaoui (2019) suggest the use of big data to understand the employees' needs and interests better, and to enhance personalized training and learning (cited from As vd, 2019). It is also recommended to develop tailored information security training programs for different demographic groups (Mittal and Ilavarasan, 2019:674). Torten (2018:77) emphasizes that the cybersecurity training must focus on countermeasure awareness rather than threat awareness and he proposes a model namely ACE (A: Awareness program implementation C: Countermeasure focused training E: Evaluate effectiveness) to the security training process.

2.4 Who behaves securely in cyber space?

Coventry et al., (2014) summarised the reasons for insecure behaviors as follows: (i) the desire to be connected from everywhere at any time increases the risk of untrusted connection. (ii) People are used to click "I accept" button and get security related messages. They click directly, without reading what they accept and don't think about the results of their behaviors. They don't behave rationally all the time. (iii) The intention to choose the easy way always wins against security. (iv) Desirability (the desire to be connected, to download music, video, applications, sharing) wins against security. (v) Financial costs (the security software and update costs) do not always cover security gains. (vi) Attraction of immediate and insecure behaviors (desire for concrete gain vs. potential future risk). (vii) Effort needed to learn how to use different tools, to keep updated, to log in, and to remember passwords. (viii) The shortage of perceived benefit (the belief that secure behaviors will not bring security). (ix) No perceived risk (thinking that no attacks will happen or considering the personal data is not valuable and important, so this brings insecure connection). (x) No perception of the need for change and no belief regarding the negative results if the rules are not obeyed. For instance, if people use internet for a long time without any security problems, they believe less that they are susceptible to risk. (xi) Lack of knowledge regarding skills and information about how to detect fraud. (xii) Not knowing which information to believe (who is a trustable source when conflicting recommendations are done). (xiii) Forgetting to behave securely while one is active in cyber space and focused on internet activity. (xiv) Barrier of social etiquette (eg. sharing passwords or devices as a sign of trust) (xv) Wrong or incomplete mental models (the users may not have clear opinions about their own behaviors, security risks and from which points thay are open to threats). (xvi) Low sensitivity level (being sensitive leads to secure behaviors and people who believe that they are open to threats tend to behave more securely). (xvii) The risk of cyber attackers to use fear and threat to cause insecure behaviors (eg. e-phisher makes a user believe that he will lose his money or right to enter the web site unless he replies immediately to attacker). (xviii) Overestimating the understanding of threats (xix) Delegating the security responsibilities to others who are perceived as more knowledgeable.

When cyber security behaviours are analysed, it is seen that there are many demographic factors behind them. Gratian (2018:345) argues that understanding the individual differences in cyber security behaviors help the researchers, organisations and employees working in security sector to understand the sensitivity for potential security attacks. McCormac et al., (2017) state that individuals aged 30-65, have higher information security awareness than the ones aged 18-29 (cited from Hadlington, 2018:264). Similarly, Sheng et al.'s (2010) research showed higher possibility for 18-29 age group to lose phishing attacks compared to other age groups. Anwar et al. (2016:440) researched the role of gender in cyber security behavior and found out that self efficacy of women regarding cyber security was lower than men. Öztezcan and Cetinkaya's (2017:56) research conducted with the faculty and administrative staff of a university in Istanbul showed that the personal data protection awareness level of women is lower than men. On the other hand, Unal and Ergen (2018) state that software updating behavior of women were higher than men's. Halevi et al. (2013) point out that for women, there is a relationship between emotional instability and being more vulnerable to phishing. According to Gratian (2018:352) women have lower scores in password generating, pro-active awareness and updating dimensions of cyber behaviors compared to men. So, it was recommended for women to get additional training and support, concerning cyber security. Sheng et al. (2010) also state that women between the ages 18-25 and students studying social sciences are more open to phishing attacks. Whitty et al.'s (2015) research also supports this finding that young people are more vulnerable in sharing passwords with others (cited from Gratian, 2018:346). On the contrary, Mohebzada et al. (2012) state that the demographics don't have a role in predicting the exposure to attacks. In Unal and Ergen's (2018) research, it is stated that the more time individuals spend on the Internet, the more their pro-active awareness is. The individuals spending less time on the Internet show less cyber security behaviors but this doesn't mean that they will face less risks. Hadlington

(2018:271) states that risky cyber security behavior frequency of employees, who are working in companies with more than 250 employees, is much higher.

Not only demographics, but also attitudes towards risk taking and content of the training are related with different dimensions of cyber security. For example, Egelman and Peer (2015) indicate that risk taking is an important indicator of security behavior, while there is a negative correlation between taking health/security risks and updating behavior together with pro-active awareness. Similarly, Sheng et al. (2010) found that the users avoiding risks are less exposed to phishing (cited from Gratian, 2018:347). Donalds and Osei-Bryson (2020) state, not only security awareness and security self-efficacy, but also an individual's way of making a decision influences the cybersecurity compliance behavior and its other antecedents. For example, the Ponemon Institute's (2016) report shows that 68% of reported 874 security incidents were caused by employee or contractors' negligence and 22% of them by malicious individuals. Only 10% was due to external causes such as stolen credentials (Donalds and Osei-Bryson, 2020). A similar finding shows that 64% of reported incidents across all sectors were likely to be the result of human error (Evans et al., 2019:351). The authorities, who focus on human factor in cybersecurity, may also use perspectives and theories from social sciences such as Theory of Planned Behavior, Knowledge, Attitude and Practice Gap (KAP) and Protection Motivation Theory. Protection Motivation Theory (PMT) points out the importance of employees' past and automatic behaviors in enhancing the information security compliance behaviour. This theory also includes the coping skills with threats. These are response efficacy (the belief in the perceived benefits of the coping action by removing the threat), response cost and self-efficacy. PMT indicates that in evaluating the threats, rewards or benefits, the severity and vulnerability play a role. Almost all dimensions of the PMT, affect the intention of the employees' compliance with the information security policy of the organisation (Vance et al., 2012:190). Li et al. (2016:103-104) integrated PMT with Health Belief Model to test the effect of cyber security awareness on employees and found out that peer behaviours in the organisation and the employees' cyber security behavior enhances the cyber security behavior in the organisation. Baillon et al., (2019:5-11) tested the impact of information provision and stimulated experience among 10,000 employees of Dutch ministry and found out that these two factors and their combination reduce the risks of falling into a phishing attack. Also, the number of employees' giving away their password has reduced. The authors also point out cyber-risk beliefs as the most important barrier to phishing detection.

Pham et al. (2019) conducted a research with Vietnamese employees to understand their experiences and perceptions of cybersecurity initiatives. This study is the first one that broadened the cyber security persepective with 7P's (marketing mix for services). The findings of the study show that user engagement, which means having shared objectives, localized communication, co-design of efficient processes and understanding the "pain points" of security compliance, is vital to develop secure systems.

3. Methodology

The aim of the study is to understand the barriers and promoters of the cyber security behavior of white-collar employees. The following research questions were investigated:

1. Is "human" the weakest link of the chain or is it only a stereotype?
2. What are the reasons of attitude-behavior gaps of employees regarding cyber security behaviors?
3. What can the companies do to foster cybersecurity behaviors of their employees?
4. Does the cyber security behavior vary according to the demographics?

Qualitative research involves interpreting the meaning, value, experiences, ideas and behaviors of the research subject by the researcher (Jaye, 2002:560). One of the qualitative research methods, in-depth interview was used in this study. The interview questions were structured to allow the researcher to explore a few general topics to uncover the views of the cyber security experts towards the employees' behaviors. Eleven open-ended questions were formulated as a basis for the interviews,

targeting cyber security behaviors of the employees. The in-depth interview is an effective qualitative method designed to reveal the participant's perspective on the subject of research, to get them to talk about their personal feelings, ideas, and experiences (Milena et al., 2008:1279; Patton, 2002: 4). It is a technique based on interaction that allows the participant to speak freely and to examine the subject in detail by asking a question to the participant about a topic, listening to the received answers, recording and asking additional questions (Stokes & Bergin, 2006:28; Corbin & Strauss, 2015:5). In semi-structured interviews, the researcher has a basic road map. It is usually organized around at a predetermined time and predetermined set of open-ended questions. Within this basic framework, different dimensions of the subject are tried to be revealed by asking different questions according to the course of the conversation, the interest and knowledge of the participant (Coşkun et al., 2017: 100). It is the most widely used interview format for qualitative research (DiCicco-Bloom & Crabtree, 2006:40).

Table 1. Participant details

Participant Codes	Age	Professional Experience (Year)	Position
P1	49	28	General Manager
P2	44	25	Technical Marketing Manager
P3	47	23	Coordinator
P4	45	21	Chief Information Security Officer (CISO)
P5	39	16	Cyber Security Group Manager
P6	45	10	Information Technologies Manager
P7	49	26	Sales Manager
P8	51	30	General Manager

The interviews were conducted with eight cyber security professionals working in different sectors and companies in Istanbul. The obtained results were analyzed with an inductive approach. To recruit potential participants, purposive sampling was used and participants were selected on the basis of their specific expertise in cyber security. The names are kept confidential and each respondent is given a code. The details of the participants are provided in Table 1.

3.1 Findings

3.1.1 Positioning human factor in cyber security: is it the weakest link in the chain?

Majority of the participants agreed that human is the weakest link in the cyber security chain. Although software programs can learn by themselves in an alghoritmic way, when human factor is involved, the errors may occur. Although white-collar employees who get security training are aware of the threats, especially the popular technics such as phishing and unconscious use of devices show the vulnerability of human. Moreover, one participant sees business owners, managers and IT staff as the weakest link as restrictions on the Internet access are specifically violated by them. However, one participant did not agree with this view: *"a well trained person may prevent security gaps that the most effective security devices may not catch"* and added that *"naming human as the weakest link in the chain would effect their risk perceptions negatively"*. So, for positive reinforcement, he proposes perceiving the human as the strongest link in the chain. With this approach, the employees may act as security ambassadors with high security awareness and be good partners of the company.

3.1.2 The barriers for cyber security behaviours

Majority of the participants state that the barriers for insecure cyber behaviours are due to lack of knowledge and low awareness of an important number of employees. On the other side, the

employees who are aware and have knowledge concerning cyber security behaviours think that these secure behaviours would disrupt or delay their work, bring them extra work load and make them feel that they are not free in access. For example, one participant stated that antivirus programs are not used since they slow down the computers; also, he has stated too many applications are used and the updates to them are postponed in order to save time.

From the employers' side, the main reason seems to be the high cyber security costs. In order to support the employees in adapting secure behaviours, mostly training and increasing awareness levels are shown as common solutions. One respondent brought a radical suggestion as *"one fatal error is better than thousands of advice"* which may be controversial when the topic is cyber security. Another respondent points out that awareness and training would not be enough for adopting cyber security behaviours. He proposes some measures like banning the employee from using the company infrastructure or access business data, if the employees are not careful enough about cyber security. Another statement regarding the barrier to security behaviour is as follows: *"in this technology age, password is a boring and nonsense layer and it is still not digitalised. The reason to leave these kinds of technologies to the initiative of the human is commercial concerns. He also states "the operating systems must automatically protect themselves without the user's purchase, installation and operation of these products. Also, parallel to the increase of mobile device use, the risks will decrease".* One participant points out that practicing an unannounced cyber attack towards the employees and training afterwards would show how crucial the topic is and would be helpful in the adoption of permanent secure behaviours. He also suggests teaching all the employees how to apply in case of a cyber issue.

3.1.3 What are cyber security behaviours?

Below listed ten cyber security behaviours recommended by experts (Coventry, et al., 2014) were shown and what other cyber security behaviours would be added to this list were asked to the participants.

i. *Use strong passwords and manage them securely*
ii. *Use anti-virus software and firewalls*
iii. *Always run the latest version of software*
iv. *Log out of sites before shutting down the computer*
v. *Use only trusted and secure connections, computers and devices (including Wi-Fi)*
vi. *Stay informed about risks (knowledge, common sense, intuition). Try to avoid scams and phishing*
vii. *Use only trusted and secure sites and services*
viii. *Always opt to provide the minimal amount of personal information needed for any online interaction and keep your identity protected*
ix. *Be aware of your physical surroundings when online*
x. *Report cybercrime and criminals to the authorities*

In addition to these behaviors, participants added the following:

- Backups must be taken and data must be saved safely
- Risky mobile applications must not be downloaded to devices
- The sources of the e-mails must be confirmed and employees must be alert to spam e-mails
- Sensitive information must not be shared on the phone
- Secure methods must be chosen for sharing files
- "Clean table-clean screen" principles should be applied
- Portable devices such as USB's should not be connected to computers without being sure about their safety.
- Training of employees for cyber security
- The kind of personal information to be shared should be discussed with family members, especially with children.

- Legal sites must be used for information research and downloads.

3.1.4 The gap between cyber security attitudes and secure behaviors of employees

There are many reasons for behaviour gap according to the participants. One of them is the employees' opinions about taking security precautions. Majority thinks that it causes waste of time. Another reason is underestimating the risks *("it won't happen to me", "There are so many big companies, who cares about me and my accounts?")* and paying no attention to cyber threat. One participant states: *"The gap is due to the fact that employees see the risks far away from themselves. They think that the company must take measures, not the employees. Internet is freedom for the employees to the extent permitted by the company and measures taken.* Another reason is individual cyber addictions such as games, porn web sites or betting sites. One participant states that: *"The gain is directly achieved like fun, socialising, game scores etc. However, the losses are indirect or they come with delay like identity theft, data theft, use of the data without permission etc."*

One participant adds: "The employee may think that his device and office atmosphere is secure. He thinks that he has enough knowledge about cyber security or he trusts the antivirus software. The employee may download third party and crack software or applications. This situation is completely due to the fact that the employee thinks that he has enough and correct knowledge but in reality the knowledge may be incorrect". In order to close these gaps between attitudes and behaviours, almost all the participants think that the following measures must be taken:

- The security behaviors must be made easy for the employees.
- Ways for employees to adapt these "easy behaviours" must be found.
- Responsibility and security processes must be built. Audit and punishments can be applied.
- Training must be prepared with the content of cyber security gaps, their results and also exercises about these security incidents.
- Reminders are so important.
- The effects and results of cyber security problems must be visualised to employees.
- The ways to routinize the correct cyber security behaviours must be searched for the employees and act for it.

3.1.5 The ways to enhance cyber security behaviours of employees

When they are asked about their opinions regarding the companies' actions to create awareness and to foster cyber security behaviours among employees, almost all the participants focused on training, social engineering precautions and simulations. One participant states:

> *"The awareness and training for behaviour change should not be in the form of traditional texts sent by e-mail, hanging posters and boring online training. On the contrary, the content of training must be enhanced with technics such as phishing the employees, games, AR/VR applications, real life cases, stories and other creative contents to make them more effective and catchy."*

Another view is to give regular and interactive cyber security training for the employees. Then, the effects should be evaluated and shared with the employee to stress the effects of a possible cyber issue for the individual and for the company. He also recommends conducting mysterious surveys and phishing at intervals and again share the results with the employees.

3.1.6 The role of demographics, personality and attitudes towards risk taking in cyber security behaviours

All participants indicated that generational differences are important in cyber security behaviours. *"Experience and technology acceptance would be indicative in cyber security behaviours".* Access to

games and social media sites may cause security risks especially among young people. Advances in technology and the quick adaptation of young people to them may affect cyber behaviours in a positive way when compared with the elderly. Only one participant disagreed with that. According to him, being young or old does not determine the behaviours of the employees regarding cyber security. Majority of the participants think that gender is not effective on risky behaviours in cyber space.

Participants consider occupation as an important indicator of cyber security behaviour since occupations touching technology affect secure behaviour in cyber space positively. One participant said that *"the effect is not always positive... the one who knows too much is mostly wrong"*. According to him, this opinion is also valid for education level. All participants agreed with the importance of education in cyber security behaviour. One of them stated that "*the fast improvements in technology make the training obligatory". Especially the competence of the people responsible from cyber security processes is important. Also, all the employees who are not directly responsible from the processes must be trained well. Their awareness must be raised and control mechanisms should work."* Regarding personality, one participant stated that being a "responsible employee" matters in organisations and this is valid for cyber security behaviours. Another participant stressed the importance of discipline, adaptation and change in cyber security behaviours.

Attitude towards risk taking may also have an indicative role in secure behaviours. One participant states: *"The employees who don't like taking risks may behave more secure in cyber space. They may be more willing to take precautions about cyber security risks and have more knowledge about the cyber issues"*. Another opinion is stressing the skills of the cyber security professionals. The cyber security team members must rationally build security procedures and rules. They also have to analyse the effects of their actions. One concern about risk taking attitude of IT and top management is the possible negative consequences of risk taking if they behave irresponsibly. One participant didn't observe any relationship between attitudes towards risk taking and cyber security behaviours. Another participant also mentioned that regardless of the employees' attitudes towards taking risks, the risks should be clarified by the company.

3.1.7 Cyber security training

Majority of the participants proposed periodical applied training with real life examples and simulations showing the dangerous consequences of cyber issues. Except this general view, each participant has recommendations as follows:

- Employees must be trained according to their roles and responsibilities in the organisations. If possible, small groups would be better for such training.
- To measure the efficiency of the training, appropriate methods should be developed. In case of need, the training should be repeated.
- Pro-active training is better. The impacts must be evaluated and the results must be discussed with the employees. After the end of training, the employees should be able to understand the effects of cyber attacks to the organisation.
- "Right training to the right team with the right content and trainer" rule must be applied.
- They must have applied training showing the clear results.
- The training contents should be periodically updated and a competent trainer team must be built.
- The training must end with certificates after exams and this should be effective on employee's performance. The relationship between the company policy and cyber security actions should be clearly stressed to employees.
- Both internal training and international training programs with different trainers should be organised.
- The employee feedback should be collected immediately after the training and the new training program should be adapted accordingly.

- The education level of the employees should be determined as weak, medium and strong. Training should be organized according to these levels and the individual situation.

Contrary to the majority of the participants, one stated that no cyber security training should be given to employees.

3.1.8 Motivation of the employees to act securely in cyber space

One participant said: *"In today's high-tech world, the probability of living a cyber attack is very high for each employee. The consequences of such attacks cause irreparable damages for both the individual and the organisation. So, the employee must implement the things that he learnt in the training." Another* participant shared his observation: "*Explaining them that the things they learn are not only important for the organisation. They are also vital to protect themselves and their families. Starting the training with this idea helps them motivate*." Supporting this view, one participant said that employees should find a piece of themselves on this issue in order to provide motivation.

According to one participant, innovation and award systems may also motivate the employees. The employees would not only propose new ideas for their responsibility areas, they would also be able to share ideas for all the processes of the organisation in these systems. At the end of these new idea and improvement proposals in the innovation system, the employees may be awarded. One participant also added that "doing the things that are already obligatory is not an option for the employees. These obligatory secure behaviours must be fostered with discipline, routinised and controlled.

3.1.9 Other factors making the organisations vulnerable to cyber attacks

Apart from the human factor, all the participants agreed that using unlicensed software, neglecting the maintenance and update of security devices are among the leading factors for cyber security attacks. Two participants gave more details regarding this vulnerability with reasons from their perspectives:

- Not investing in technology and limited technology follow up
- Unclear responsibilities and job descriptions
- Not having a cyber intelligence team
- Unstandardised business processes
- Not following the effectiveness of control mechanisms
- Lack of cyber security items in company policies and procedures
- Not practicing cyber security simulations periodically
- Not informing the employees regarding company policies and limited controls
- The vulnerability checks must be conducted either manually or automatically in certain periods. The security certificates of the software and hardware should be controlled.
- Especially the software and design processes do not satisfy security needs. The focus is only on functionality. "DevSecOps" logic means thinking about application and infrastructure security from the start is not valid in development phase.
- Professional support should be taken from system installation to operation.

4. Conclusion

Creating high levels of cybersecurity awareness and employing highly skilled people about cyber security is one of the most challenging topics for many companies today. Many companies struggle to train and change the behaviors of employees to minimise cyber risks. While most studies on cyber security are focusing on technology or policy dimensions rather than human behaviour, a recent Harvard Business Review article (HBR, 2020, p.18) states that slight changes to employee training can bring better results.

In order to do research on the cybersecurity behaviors of employees in companies, data is collected from eight cyber security experts from different companies in Istanbul. It is seen that underestimating the risks, having the thought "it won't happen to me", lack of knowledge and awareness or seeing the cyber precautions as "waste of time", cyber addictions of some employees are some of the main reasons of risky behaviour in cyber space. The solutions to these issues are training, social engineering precautions and simulations. The nature of training seems a key factor for adopting the correct behavior to employees. Creativity, using AR/VR technology during the training, real life cases and interactivity are recommended for effective cyber security training. Repeating rule-based trainings does not always increase the resillience towards cyber attack. On the contrary, it can make employees insensible towards trainings and create a false competence feeling. So, designing the cyber security trainings with using tools like games would increase the awareness and make people internalize cyber security (HBR, 2020, p.18). From technology side, the companies must focus on unlicensed software programs, update the security devices and don't neglect the maintenance.

Finally, future studies could explore how employees feel and think about cyber security risks and precautions. There is still need for quantitative studies to support the findings of this study. This study used qualitative method, so the findings may have omitted factors that a quantitative method would have uncovered.

References

Accenture "Cost of Cybercrime Study" (2019), https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security.

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. PloS one, 14(12), e0224216.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper.

Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHItaly 2013 Doctoral Consortium, 1065, 92-101.

Check Point. (2020). Cyber Attack Trends: 2020 Mid-Year Report. Check Point Software Technologies LTD.

Coburn, A., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., & Harvey, T. (2019). Cyber Risk Outlook. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc.

Corbin, J., & Strauss, A. (2015). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory (Cilt Fourth Edition). USA: SAGE.

Coşkun, R., Altunışık, R., & Yıldırım, E. (2017). Sosyal Bilimlerde Araştırma Yöntemleri SPSS Uygulamalı (Cilt 9. Baskı). Sakarya: Sakarya Kitabevi.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. gov. uk report

CTO (Commonwealth Telecommunications Organisation) (2015), Commonwealth Approach for Developing National Cybersecurity Strategies: A Guide to Creating a Cohesive and Inclusive Approach to Delivering a Safe, Secure and Resilient Cyberspace, 2015th ed, Commonwealth TelecommunicationsOrganisation(CTO), London.

Çakır, H., Yalçın, N., & Kılıç, M. S. (2017). İnternet Sitelerine Yapılan Siber Saldırılar: 2015 Yılı Türk Kamu Siteleri İncelemesi. Güvenlik Stratejileri, Yıl:13, Sayı:25, 149-192.

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. Information & Computer Security.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. Medical Education, 40(4), 314-321.

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management, 51, 102056.

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2873-2882). ACM.

Eryaşa, E. (2020). in Cyberspace Impacts on Maritime Sector. H. N. Keleş, & A. E. (eds.), What's happening in cyber space? An interdisciplinary approach. Berlin: Peter Lang.

Evans, M. G., He, Y., Yevseyeva, I., & Janicke, H. (2019). Published incidents and their proportions of human error. Information & Computer Security.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: An International Journal, 25(2), 223-240.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358.

Hadlington, L. J. (2018). Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom.

Halevi, T., Lewis, J., & Memon, N. (2013, May). A pilot study of cyber security and privacy related behavior and personality traits. In Proceedings of the 22nd international conference on world wide web (pp. 737-744).

HBR (2020). Boost Your Resistance to Phishing Attacks, Harvard Business Review September–October 2020, https://hbr.org/2020/09/boost-your-resistance-to-phishing-attacks

He, S., Lee, G. M., Han, S., & Whinston, A. B. (2016). How would information disclosure influence organizations' outbound spam volume? Evidence from a field experiment. Journal of Cybersecurity, 2(1), 99-118.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. Journal of Intellectual Capital.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikalari. Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135-158.

Jaye, C. (2002). Doing qualitative research in general practice: methodological utility and engagement. Family Practice, 19(5), 557-562.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. IEEE Security & Privacy, 5(3).

Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. Kastamonu Eğitim Dergisi, 25(6), 2079-2094.

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal, 52(1), 29-41.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016, December). Cyber Security Awareness and Its Impact on Employee's Behavior. In International Conference on Research and Practical Issues of Enterprise Information Systems (pp. 103-111). Springer, Cham.

Milena, Z. R., Dainora, G., & Alin, S. (2008). Qualitative Research Methods: A Comparison Between Focus-Group And In-Depth Interview. Annals of faculty of economics, 4(1), 1279-1283.

Mittal, S., & Ilavarasan, P. V. (2019, September). Demographic Factors in Cyber Security: An Empirical Study. In Conference on e-Business, e-Services and e-Society (pp. 667-676). Springer, Cham.

Mohebzada, J. G., El Zarka, A., BHojani, A. H., & Darwish, A. (2012, March). Phishing in a university community: Two large scale phishing experiments. In 2012 international conference on innovations in information technology (IIT) (pp. 249-254). IEEE.

Morgan, S. (2019). 2019 Official Annual Cybercrime Report. Herjavec Group.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151-156.

Öztezcan, B. A., & Çetinkaya, A. (2017) Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi Örneği, Ulusal Multidisipliner Hakemli Sosyal Bilimler ve Araştırmalar Dergisi, Sayı:1, 56-71.

Pham, H. C., Brennan, L., Parker, L., Phan, T. N., Ulhaq, I., Nkhoma, M. Z., & Nguyen, M. N. (2019). Enhancing cyber security behavior: an internal social marketing approach. Information & Computer Security.

Patton, M. Q. (2002). Qualitative Research & Evaluation Methods (Cilt Third Edition). USA: SAGE.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internet 2, 11(89), 1-17.

Saruhan, Ş. C., & Özdemirci, A. (2016). Bilim Felsefe ve Metodoloji (Cilt 4. Baskı). İstanbul: Beta.

Sedkaoui, S., & Khelfaoui, M. (2019). Understand, develop and enhance the learning process with big data. Information Discovery and Delivery.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 373-382).

The Global Risks Report (2020). World Economic Forum.

Stokes, D., & Bergin, R. (2006). Methodology or "methodolatry"? An evaluation of focus groups and depth interviews. Qualitative Market Research: An International Journal, 9(1), 26-37.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. Computers & Security, 79, 68-79.

Ünal, A.N. (2020). What's Happenning in Cyber Space? An interdisciplinary approach. Hatice Necla Keleş & Ahu Ergen (Eds.), Cyberspace and Chaos: A Conceptual Approach to Cyber Terrorism. Berlin: Peter Lang GmbH.

Ünal, A.N., & Ergen, A. (2018). Siber uzayda yeterince güvenli davranıyor muyuz? İstanbul ilinde yürütülen nicel bir araştırma. Celal Bayar Üniversitesi Sosyal Bilimler Dergisi, 16(2).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management, 49(3-4), 190-198.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networking, 18(1), 3-7.

Yayla, M. (2014). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. Hacettepe Hukuk Fakültesi Dergisi, 4(2), 181-200.

Yıldırım A., & Şimşek B. (2008). Sosyal Bilimlerde Nitel Araştırma Yöntemleri (6. Baskı). Ankara: Seçkin Yayıncılık.