LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Cybersecurity engagement in a remote work environment

A study of employees' perspective on cybersecurity awareness.

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: César Vásquez
José González

Supervisor: Miranda Kajtazi

Grading Teachers: Saonee Sarker
Betty Saenyi

Cybersecurity engagement in a remote work environment.

A study of employees' perspective on cybersecurity awareness.

AUTHORS: César Vásquez and José González

PUBLISHER: Department of Informatics, Lund School of Economics and Management, Lund University

PRESENTED: June 2022

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Osama Mansour, PhD

NUMBER OF PAGES: 144

KEY WORDS: cybersecurity, awareness, employees, remote work, work environment, information security, cybersecurity program, cybersecurity learning, cybersecurity training, security policies, cyberthreats, cybersecurity guidelines

ABSTRACT (MAX. 200 WORDS):
The recent spread of COVID-19 pandemic encouraged organisations to facilitate a remote work environment for their employees. This work environment would most likely continue in the upcoming years. At the same time, this context has been followed with an increase in cyberthreats that could affect the optimal processes of organisations. Because of this, cybersecurity awareness must be cultivated to the employees of all levels. The success of the implementation of a cybersecurity program is associated with the level of engagement that it could generate in the participants. Thus, this thesis aims to explore what cybersecurity aspects are more relevant and/or relatable for remote working employees. A qualitative approach was used to collect experiences and perspectives from employees in different organisations. As a conclusion, this thesis found that emotional factors, trust in cybersecurity infrastructure, previous practices, training, security fatigue and improving the program with gamification are some aspects that might support to achieve success through a cybersecurity program in remote work.

Acknowledgement

We would like to recognize the invaluable collaboration of all the respondents who took part on this research due to their commitment, time, and insightful responses which allowed us to carry our study. Further, we would like to extend our deepest gratitude to Miranda Kajtazi who guided us during the development of this thesis and provided insightful recommendations to achieve high quality in our academic research.

César Vásquez & José González

Content

Figures

Tables

1 Introduction

This initial chapter introduces the subject of the thesis by explaining the background, the research problem, and the existing knowledge gap which implies an opportunity for investigation. The research purpose, question, and specific delimitations related to the thesis are presented to specify the focus and scope of the research.

1.1. Background

Organisations from different business sectors are constantly incorporating digital solutions that let workers augment their capabilities and optimise processes (Pagani & Pardo, 2017). In addition, the COVID-19 pandemic suddenly forced organisations to enable remote work. A key difference is that before employees only accessed systems inside the company's infrastructure (Borkovich & Skovira, 2020). In terms of numbers, an insightful report published by Eurofund (2020) showed that 48% of employees adopted the option to work remotely motivated by the pandemic measures (Eurofund, 2020). This is a huge increase considering that only 11% of employees worked remotely pre pandemic in 2019 (European Commission, 2020). As a result, many workers are using digital tools remotely to access sensitive information related to the business operations in their daily activities which implies a bigger exposure to cyberthreats (Ramadan, Aboshosha, Alshudukhi, Alzahrani, El-Sayed & Dessouky, 2021). This recent phenomenon has been referred to as the cybersecurity pandemic due to the high increase in cyberattacks worldwide (Ramadan et al. 2021). With this context there is a higher probability of risks such as financial loss and interruption of activities that organisations put resources into avoiding such risks.

Deeply related to this phenomenon is cybersecurity which is a discipline dedicated to assuring the cyber environment, organisation, and user assets (Von Solms & Van Niekerk, 2013). Further, some authors refer to the human factor as the weakest link in terms of vulnerabilities to be exploited by cyberattacks (D'Arcy, Hovav & Galletta, 2009). This is further supported by the idea that the absence of training and deficiencies in knowledge about cybersecurity might indicate an increase in data breaches, lack of compliance to important security policies, and intended and unintended violations from related users, in particular employees (Rubenstein & Francis, 2008; Vance, Lowry & Eggett, 2013). Because of this, different regulations, and frameworks such as National Institute of Standards and Technology (NIST), the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC 27001), and General Data Protection Regulation (GDPR) suggest implementations that contribute to having a protected environment (NIST, 2022; ISO/IEC 27001, 2022; GDPR, 2022).

One key practice that these regulations and frameworks have in common is building awareness and providing training (Chowdhury, Katsikas & Gkioulos, 2022). This practice comprises the effective transmission of policies and practises to all organisational levels (Siponen & Vance, 2010). However, according to the literature, not all the organisations are able to achieve the success of this endeavour due to at least two reasons. First, there is a lack of engagement of participants/employees (Chowdhury, Katsikas & Gkioulos, 2022); second, organisations are not fully prepared to make sure that cybersecurity programmes are regulated on how employees

should participate and perform (D'Arcy, Hovav & Galletta, 2009; Kajtazi, Cavusoglu, Benbasat & Haftor, 2018). On the first, the engagement is based on different factors such as cultural, motivational, learning preferences, and other behavioural-related theories that explain compliance and noncompliance behaviour in organisations (Chowdhury, Katsikas & Gkioulos, 2022; Bulgurcu, Cavusoglu & Benbasat, 2010). On the second, organisations often find it hard to cope with all the different factors that drive the human behaviour in organisations, as well as are often limited on financial resources to do so (D'Arcy, Hovav & Galletta, 2009; Sadok, Alter & Bednar, 2020). For that reason, some organisations are investing in a cybersecurity program strategy to proactively change the way cybersecurity is executed in an organisational context.

1.2. Problem Area

Due to the increased dependency of technology within organisations, cybersecurity is one of the most relevant topics of the field. Fenz, Heurix, Neubauer, and Pechstein (2014) indicated that this widespread usage of technology comes with unique challenges and dangers for users. They also argued that any device connected to a network can be compromised, and that software within devices can be used for a different purpose from which it was created for. In addition, COVID-19 has created disruption to common practices and well-established notions as well as increasing technology adoption.

Organisations now have an inherent need to provide a remote work environment for its employees. Soni, Kukreja, and Sharma (2020) commented that due to fast transition to a remote work environment, the best practices and policies for employees' environment would not be compliant. This lack of preparedness and wide use of technology put organisations and employees at a vulnerable position in terms of cybersecurity. This can be seen within the Global Risk Report of 2022 stating that in 2020 malware and ransomware increased in more than 350% for both categories (World Economic Forum, 2022). Furthermore, the same report stated that most cybersecurity issues are due to human error, for example insider threats which can be intentional or unintentional.

However, Veiga and Eloff (2007) stated that there are ways organisations can establish governance frameworks that are effective in mitigating risk associated with information security. Similarly, Spears and Barki (2010) pointed out that there are multiple controls and safeguards that organisations can enable in terms of cybersecurity. But most of these controls and policies would be in the hands of the employees to enforce. As a result, organisations have endeavoured to make aware of its employee's security policies and best practices to follow in a remote work environment.

The organisation's flexibility might remain in a post COVID-19 context (Gartner, 2021). Kane, Nanda, Phillips and Copulsky (2021) argues that the future of the work environment would have to be reconsidered to allow flexibility to adapt to the post pandemic reality, but the vulnerability surrounding the cybersecurity aspects will need to be addressed. As a result, this thesis finds it important to study what measures can be implemented to mitigate risk and build awareness among employees in a remote work environment.

Correia, Compeau, and Thatcher (2016) provides a compelling argument regarding the need to re-assess the validity of some practices and measurements from the IS community due to changes in conditions and new technology available. For that reason, this thesis will support re-

assessing the perception of employees regarding cybersecurity awareness which can be of vital importance to make sure the right tool is delivered for them. Moreover, the same reassessment can enrich the body of knowledge regarding the relevance of engagement and awareness within the cybersecurity field.

1.3. Objective and Purpose

There is a clear role of awareness within an organisation to increase employees' level of understanding and compliance for cybersecurity measures (Chowdhury, Katsikas & Gkioulos, 2022; Bulgurcu, Cavusoglu & Benbasat, 2010; D'Arcy, Hovav & Galletta, 2009).

Therefore, the objective of this thesis is to understand if the previous proposed awareness practices are still relevant or if new patterns are prevalent in a remote work environment.

Furthermore, the purpose of this thesis is to contribute to the body of knowledge on how to continue increasing cybersecurity awareness in organisations that are embracing the context of remote work.

1.4. Research Question

For this thesis, there are two views to be considered from a cybersecurity perspective within an organisation. First, ***relevance*** as an aspect viewed as important and appropriate to the current context of the employee. Second, ***relatable*** as an aspect implies a connection or engagement with a topic from the employees' perspective.

Question

What cybersecurity aspects are more relevant and/or relatable for remote working employees?

1.5. Delimitation

Firstly, it is important to define that the focus of this thesis is in the Cybersecurity area. There exist two important concepts in the literature which are Information Security and Cybersecurity. Specifically, Cybersecurity was chosen because its boundaries are beyond Information Security scope. Therefore, Cybersecurity also includes the study of technological assets which are vulnerable in the context of remote work environments.

The concept of remote working is also important to be defined. This thesis considers people as remote working employees if they frequently work from a place different from the organisation's physical offices. Therefore, the context analysed is not only the employee's home but also a different place such as a library or a cafe where an employee can perform their work tasks.

Cybersecurity training and awareness are components contemplated in the research due to their level of involvement with employees in their daily routines. By contrast, the component of

cybersecurity education is not deeply developed in this thesis as it is more related to the definition of a cybersecurity program content from an academic point of view that involves people whose effort is specifically focused on cybersecurity program creation. These people specialised in security are not the target of our research.

In terms of access to cybersecurity resources of organisations, this thesis did not have direct contact with the latest versions of cybersecurity policies, guidelines, or training of the participants' organisations. For that reason, the analysis was based on employees' perspective on their learning experience while interacting with the cybersecurity program. This could limit our capacity to verify the policies presented to employees in a more comprehensive way for the study.

Also, no Small and medium-sized enterprises (SMEs) were considered as part of the study. All the companies considered in this thesis were large corporations, so in terms of resources and experience would be considered more advanced.

In terms of the interviewees, relevant years of experience were required for participation in the qualitative study. This excluded all entry level positions, which have a unique perspective and who represent an important part of the workforce.

Anonymity was also chosen due to the timing of this study which would present a methodological delimitation. The reason was to avoid some of the organisation's ethical processes that would require extensive time to obtain permission and make the information from the interview’s public.

2 Theoretical Background

The following chapter aims to explain several themes that help to have a holistic view of the implementation of cybersecurity in organisations. Each of these themes have an extensive explanation and scope according to the literature so, particularly, the aspects that are more related to the engagement of employees are presented in a deeper way. At the end of the chapter, a table presents a summary of the literature review.

2.1. Cybersecurity

Terms such as Information Security and Cybersecurity are widely used as basic concepts in studies about issues related to the security implementation in organisations (Bulgurcu, Cavusoglu & Benbasat, 2010; Chowdhury, Katsikas & Gkioulos, 2022; Kajtazi et al. 2018). Thus, it could be interpreted that their meaning is evident due to their long adoption and use in the field. However, it is relevant to demarcate their scope for the purpose of this thesis (Von Solms & Van Niekerk, 2013).

Information Security has been introduced at least more than 20 years ago (Von Solms, 1998). Whitman and Mattord (2011) stated that the first concern to implement an Information Security process was during World War II where the focal point was to avoid espionage and physical theft of equipment that contains crucial information. Of course, the threats and assets to protect have tremendously evolved over time hand in hand with the sophistication of technology. For that reason, Information Security today could be defined as the processes, practices, and tools dedicated to protecting the information and its critical elements including software and hardware (Von Solms & Van Niekerk, 2013; Oscarson, 2003; Whitman & Mattord, 2011).

As a complementary idea, it is appropriate to consider the perspective of Von Solms and Van Niekerk (2013) who mentioned that the objective is to "ensure business continuity and minimise business damage" (Von Solms & Van Niekerk, 2013, p.98). Moreover, it is relevant to point out three properties such as confidentiality, integrity, and availability which must be preserved in the assets of information. These three properties are usually referred to as the CIA triad; however, other properties could also be included to set a broader scope (Von Solms & Van Niekerk, 2013; Oscarson, 2003).

Regarding Cybersecurity, Von Solms and Van Niekerk (2013) argued that the boundaries of this concept are beyond Information Security because it includes assets which exceed the scope of Information Security. NIST (2022), a well adopted security framework in the market, defined cybersecurity as the avoidance of damage to, preservation of, and restoration of technological components as well as the information contained there. Furthermore, ITU (2022) stated that it is the collection of tools, technologies, processes, and guidelines that are orientated to protect the cyber environment and organisation and user's assets.

Particularly, this last definition includes the threats that could affect user's assets which is one important difference with Information Security. A demonstrative example is the cyberbullying scenario where the confidentiality, availability or integrity of information is not affected but the personal or physical aspects of a person is damaged (Von Solms & Van Niekerk, 2013, p.98).

Consequently, based on this example, it could be confirmed that cybersecurity also protects society in general because people's feelings and belongings could also be affected by cyberthreats.

Additionally, to explain the differences previously commented, Von Solms and Van Niekerk (2013) introduced an extra concept named Information and Communication Technology Security which was originated to make an individualisation of the information-based assets that are transmitted using Information and Communications Technology (ICT). With that in mind, a useful diagram shown in Figure 1 works as a support to have a visual summary of the relationship between these concepts.

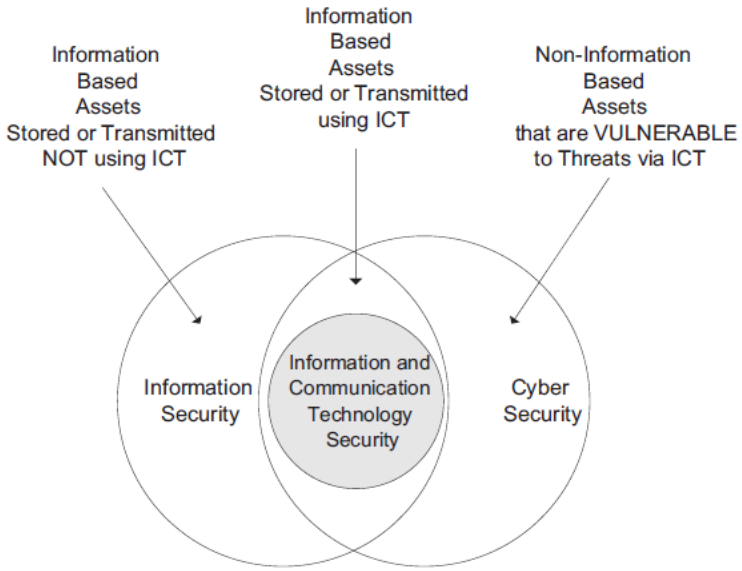

Figure 1: The relationship between information and communication security, information security, and cybersecurity (Von Solms & Van Niekerk, 2013)

Considering that the purpose of this thesis is focused on remote workers therefore the most adequate concept to use as a base for the investigation is cybersecurity. This is further supported because the elements that are vulnerable in a remote work environment could be more adequately studied from a cybersecurity perspective. Moreover, the terms employees or users will be utilised interchangeably to refer to the group of people who are the focus of the thesis.

2.2. Cybersecurity and Remote Work

COVID-19 caught society off guard, and it clearly disrupted many well-established conventions. In the case of organisations, they faced a set of specific challenges involving its users. One of them was to establish a remote workforce conformed by users that previously were office based. The term remote work would be used to define the activities that are outside of the physical spaces set by companies. Further, in one research by Pranggono and Arabo (2021), they stated that in the UK many of the organisations did not have a procedure in how to build a remote workforce.

The authors also observed that only around 38% of organisations had a policy in terms of security. Similarly, Naidoo (2020) indicated that within this unanticipated change the most important priority for organisations was to facilitate employees to work remotely in a short time. Consequently, the authors emphasised that the organisation did not have enough time to build and deploy the correct safeguard or awareness of this remote work environment. Pranggono and Arabo (2021) stated that in a lot of cases employees used their home systems to perform their jobs.

These systems were secure by the employer, but due to this new infrastructure it creates a clear security concern. Alexander and Jaffer (2021) suggested that the already available safeguards like Virtual Private Network (VPN) and other organisational tools still have some vulnerabilities embedded in them. The literature suggests an inherent vulnerability in the current remote work practices. In addition, there is a clear increase in dependency to technology from organisations. This technology dependence observed by Naidoo (2020) has not been overseen by cybercriminals and the number of cybercrimes has grown exponentially.

In some instances, authors state that cybercriminals are taking advantage of vulnerability of both the systems and the users. A global pandemic has caused emotional distress for users on a different level. For instance, Naidoo (2020) observed that emotional factors can be an important factor in users being compliant with security policies. It is important to mention that these attacks are not new, they have just been maximised in this era. For example, within the most used cyberattacks during the COVID era we find malware including phishing or ransomware, DDoS, and misinformation.

Moreover, the complexity of remote work can be utilised according to the Centre for the Protection of National Infrastructure from the UK (CPNI, 2020) to produce insider threats attacks. This is because of multiple factors like the lack of oversight from management, unfamiliar environment, stress, and poor screening processes when adding new employees to the organisations.

The success of malware and phishing emails for example resides in attackers using current relevant information, in this case related to the pandemic and using it to attract users with its malicious software (Naidoo, 2020). Further, as observed by Pranggono and Arabo (2021), DDoS attacks focused on infrastructure and organisations that were vulnerable or overwhelmed during the pandemic.

As an example of these organisations, Pranggono and Arabo (2021) claimed internet or healthcare providers. The reason for this is this type of organisation's focus was set on other priorities not in cybersecurity opening a window for vulnerability. Ultimately, we see that users with an increased engagement of technology left the door open for vulnerability which was exploited by criminals. Further, in terms of remote work it has been suggested that even when the pandemic is over this practice would remain.

As a result of this work environment change that would remain, it is important to consider some issues beyond cybersecurity. Galanti, Guidetti, Mazzei, Zappalà and Toscano (2021) stated that remote work presents some personal challenges for users. First, family conflict that impacts work. Second, social isolation, and third the distracting environment which users may be in. The importance of this is that as stated previously emotional factors may affect cybersecurity compliance from the part of the users. In addition, as envisioning a return to a previous work environment would not be correct it gives organisations an opportunity to explore different

options. Kane, Nanda, Phillips and Copulsky (2021) observed that organisations can take advantage of the effectiveness of remote work. The authors suggested a hybrid model which can bring the flexibility needed in a post pandemic reality.

2.3. Cyberthreats in a Remote Work Environment

Users within organisations rely on technology and cyberspace, and with more technologies available they continue to expand their adoption. Cyberthreats understanding is of vital importance for organisations and users to mitigate risk and assure their operations. Moreover, cyberattacks are increasing at an exponential rate and developing more sophisticated methods.

A cyberattack is a malicious attempt into the information systems of an organisation. The main goals of this type of attempt can be economic, political, destruction of data and others. According to Cisco (n. d.) around 53% of cyberattacks presented an economic damage of around $500,000 dollars. Further, there are different types of cyberattacks that are at the disposal of criminals. Moreover, there were some attacks that were used in the context of remote work that are important to review.

2.3.1. Social Engineering

Social engineering focus is breaching security by manipulating individuals to avoid best practices, by illegal or legal means. As a result, the main enabler of this type of attack would require human interaction. This goes in hand with previous literature that suggests the vulnerability of humans in terms of cybersecurity. However, it is important to mention that the success of this attack would rely heavily on the ability or technique used by the attacker to psychologically manipulate its victim (Syafitri, Shukur, Mokhtar, Sulaiman, & Ibrahim, 2022).

The attacker is someone that obtains access to sensitive data or financial resources. As an example of the information targeted by the attacker, we have passwords and users' names (Hijji, & Alam, 2021). Further, this attack has evolved and used multiple means like calls, text, mails, or face to face interactions. Along with the means, the methods found in social engineering can be impersonation, automated social engineering, attacks on online communities and others (Syafitri et al, 2022). One of the dangers of social engineering is that it can avoid hardware and software used in the prevention of attacks. The authors stated that it is fundamental users' awareness to avoid this type of attack.

Hijji and Alam (2021) based on the literature suggested 4 types of social engineering. First, is the physical type, here the purpose is to obtain information from a victim through physical materials. For instance, the attacker would use dumpsters to try to find physical materials containing sensitive information. Second, the social type, which according to the authors is the most common type. In this type of attack psychological techniques are used to breach security. As an example, the attacker would try to build a relationship, baiting or phishing for its attack. Third, the technical type, here the attacker uses social networking to collect relevant information from its targets. Finally, is the combination of the social and technical types that would increase the capacity of the attacker to succeed.

Moreover, Hijji and Alam (2021) stated that during the pandemic this attack posed a great security risk. One of the most used social engineering attacks used in this context was phishing. More in depth, the phishing attack takes advantage of the user by manipulation to collect confidential and sensitive information. In this case the attacker pretends to be a reputable organisation or individual on a message. This message would contain a link to what is referred to as a phishing website. One of the main characteristics of this threat is that the content which usually includes a message encouraging the user to perform a theoretically urgent action. Once the users access this website an attempt to compromise confidential information is in place. Further, these messages can be in the form of an email, text, social media, and others. In addition, one of the effective methods to avoid the risk of phishing attacks can be to build awareness among users to be informed of the different forms of attack (Stallings & Brown, 2018; FBI, n.d). Figure 2 portrays a cycle of a phishing attack.

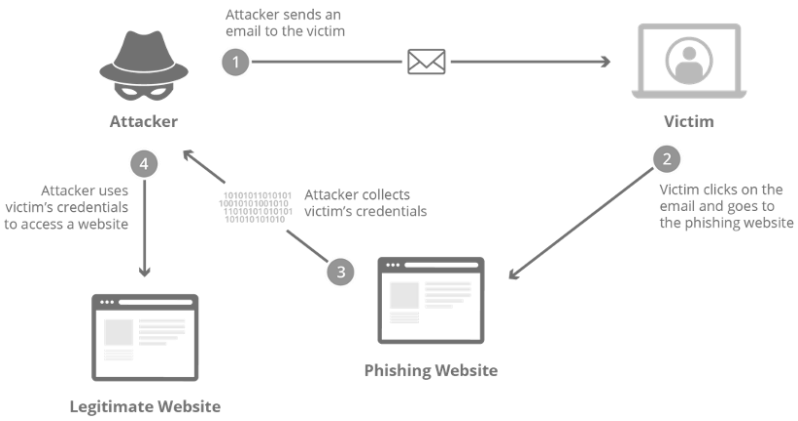

Figure 2: Phishing attack cycle (Cloudflare, n.d)

2.3.2. Insider Threat

One of the clear vulnerabilities from the interaction between users and technology is the insider threat attack. Insider refers to the fact that the attack comes from a user within the organisation. Roberts (2021) observed that in the US most of the data breaches come from human error. Moreover, the detection of this type of attack takes on average more than 200 days and around 80 days to resolve this issue. The employee or insider will have a valid access to the organisations systems which gives them a distinctive position to damage the information technology of an organisation.

Further, the target of these attacks can be customers, employees, or the organisation itself (Roberts, 2021). As observed by Warkentin, and Willison (2009), there is extensive coverage from the literature on this type of attack and categorise it as one of the most important threats for information systems. Furthermore, the authors stated that the complexity of this attack is that it comes from a trusted user. As a result, the damage to the finances, confidentiality, and integrity of the information systems can be significant.

In addition, there are some distinctions to be made regarding insider threats and the type of user doing the attack. This attack can have malicious and non-malicious insiders. First, the malicious insider's main characteristic is that they are making a rational decision to attack within the

organisation (Wang, Gupta, & Rao, 2015). Moreover, a malicious insider would have a greater level of complexity. This would be since a malicious action would require time from the attacker to familiarise with the system and make calculated attacks. What is more, it would require for the attacker to identify an opportunity to launch the attack and find the specific target (Wang, Gupta, & Rao, 2015). It is important to mention that this type of attack represents a minority of the work force and is less frequent (Roberts, 2021). However, the financial impact of these malicious attacks would be significant (Warkentin, and Willison, 2009).

Second, as stated by some authors, non-malicious insider refers to actions that include multiple factors like passive actions, a poor decision, ignorance, lack of training, laziness, or lack of motivation that produce an attack of the information systems of an organisation (Roberts, 2021; Warkentin & Willison, 2009). This attack takes a considerable percentage of the insider threats but are harder to keep track of. As an example of a non-malicious insider attack, we have visited insecure websites, malware introduction to organisation networks, not locking devices, victims of spam emails, password sharing and others (Roberts, 2021).

For all insider threats the literature suggests having a strong consideration for the behavioural aspect of employees. The same literature has studied this issue with multiple theories with the aim of physiological causes that might result in this type of action. Furthermore, it states that there are some indicators based on users actions those organisations could use to predict in some instances insider threats (Roberts, 2021; Warkentin & Willison, 2009). In addition, as a countermeasure for insider threats it is important to assess the users depending on the risk, they present for the information systems of the organisations. Moreover, have clear policies regarding the actions to be considered non-compliant and the consequences attached to them. Also, as suggested by Warkentin and Willison (2009) training and motivating users to act in a compliant way in terms of security policies can bring positive results in the fight against insider threats.

2.3.3. Malware

The main intent of a malware according to NIST (2020) is to compromise the integrity, confidentiality, and availability of a specific system. Moreover, there are multiple channels, methods, and tools for malware attacks, this can be seen in Table 1 which includes some of the most common types.

Table 1: Common types of Malwares (Stallings & Brown, 2018)

Name	Description
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Downloaders	Code that instals other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document or document template, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.

Spammer programs	Used to send large volumes of unwanted e-mail
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes it.
Virus	Malware that, when executed, tries to replicate itself into another executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, by exploiting software vulnerabilities in the target system, or using captured authorization credentials
Zombie, bot	Program installed on an infected machine that is activated to launch attacks on other machines.

Stallings and Brown (2018) proposed two important mechanisms to understand malware which are how they propagate or the actions/payload it performs. Firstly, in terms of propagation, it refers to once the malicious software has infected its target what mechanism they will use to propagate to other systems. To illustrate, some ways of propagation can be worms, users inadvertently installing the malicious software or infected program downloads.

The second mechanism according to Stallings and Brown (2018) would be payload actions. This would refer to some of the action malware performs once it infected a system. According to the authors malware can act on different fronts and points out five of them. First the corruption of systems or data, Second, theft of information from a system, this theft would include password, personal data, or logins, Third, creates a zombie agent to enforce an attack from a botnet. Fourth, spyware which is a software that would take sensitive information from a system and transmit them. Finally, stealthing which would make malicious actions while hiding its presents on the system.

By understanding these two mechanisms we can understand the reach and impact malware attacks can have. In addition, attacks are becoming more sophisticated because they also exploit new methods enabled by the evolution of technology. Previously, malware attacks would only use one method to propagate on the different systems. Current methods would show a blended approach where the attack would use different types of propagation and payloads to attack (Stallings & Brown, 2018). Thus, as more technology is being used the types and sophistication of attacks would increase.

During the pandemic popular malware attack was ransomware whose initial step is to block users from accessing specific resources that contain sensitive data. This can be in the form of encrypting the data from the user. Further, once the attack is established the purpose is to obtain

a ransom for the recovery of the data. However, there is a consensus of the effectiveness of awareness which can build cautiousness among users and as a result help in the prevention of these attacks. (Stallings & Brown, 2018; Microsoft, n.d).

2.3.4. Denial of Service (DoS)

The second type of cyberattack is Denial of Service. Multiple authors observe that DoS does not focus on creating a breach on the security but disrupting the access of users to systems or services. The objective for DoS in some cases can be political attacks to opponents, hacktivism, or some sort of financial extortion. Consequently, it becomes a great concert for cybersecurity and its users. DoS exploit the capacity limit of the different system resources for their attack. For instance, in the case of a website it will overload the site with multiple requests to make the service not function properly.

However, it is important to mention that DoS can also be used as a distractor for other types of attacks to the systems (Stallings, and Brown, 2018; Zargar, Joshi, & Tipper, 2013). Furthermore, there are multiple resources that can be targeted within a DoS. For example, Stallings and Brown (2018) mentioned the three specific categories. First, the capacity of the network to connect to a server on the internet. Second, the overload of the network that manages and specific software, this attack does not use massive volumes of traffic for the network but targets specific resources. Third, the attacks on an application which would be made by sending valid requests for the application that will at the end consume the resources to respond to the request and incapacitate the functioning of the application.

Distributed Denial of Service (DDoS)

A type within the DoS category used by attackers during the pandemic is Distributed Denial of Service (DDoS). The main characteristic of DDoS is the fact that they use multiple devices to carry their attack on a specific resource. Further, they utilise different techniques and tools, and they are carried remotely. For instance, some of the most useful facilitators of DDoS attacks and mentioned previously within the malware category is botnet. This is since they make the attack more effective and the defence mechanisms more difficult to act.

DDoS attacks as mentioned by Zargar, Joshi, and Tipper, (2013) have as a focus to create a service unavailable. As a result, this impacts the financial side of organisations or an individual's due to the revenue loss or expenses necessary to incur after one of these attacks. In addition, preventing measures for this type of attack would mainly focus on the technical side of the attack. There is not a complete protection against these attacks as stated by Stallings, and Brown (2018). Some of the measure's focus is detecting the attack, filtering, traceback, reaction to the situation among others. Further, it is also important for users from an organisation to know how to respond to this type of attack and manage it in the best possible way.

2.4. Cybersecurity Governance

There are existing methods to manage the technological implications and cybersecurity risk for organisations and employees. These methods include policies, frameworks, and best practices that support the information and cybersecurity practices and come from both the literature and

practitioners. Further, these methods aim to target the technical and non-technical side of security for both employees and organisations (Guo, Wei, Huang & Chekole, 2021; NIST, 2022). This agrees with the literature that in recent years suggested that when managing information security, it is important to have a broad view beyond just the technology side (Soomro, Shah, & Ahmed, 2016; Siponen, Mahmood, & Pahnila, 2014). Also, most of these methods are created to be applied and enforced depending on the individual needs of the organisation. This is because the organisation's systems, employees and risk are unique (NIST, 2022).

Furthermore, there is suggested division between the plan for an organisation's security goals and the procedures and methods applied at the granular level. However, an important element and initial step for the management of security in the organisation is to build policies for guidance (Baskerville, & Siponen, 2002). There is clear consensus from multiple authors that suggest that having policies is highly effective for both managing cybersecurity risk and building awareness. Further, these authors state that policies must be clearly defined for their effectiveness to work.

Also, this type of policies should be customizable which would support the unique challenges for each organisation and its employees. Further it is of importance for these policies to include what is deem appropriate or not in terms of information security so users can have a clear understanding of what to do (Baskerville, & Siponen, 2002; Guo, Wei, Huang, & Chekole 2021; Singh, Gupta, & Ojha, 2014; Soomro, Shah, & Ahmed, 2016). These policies can include timing for password change, types of user access, security implementation for departments, physical devices management, internet usage and others (Baskerville, & Siponen, 2002).

Moreover, when referring to these policies according to some authors it is important to take into consideration the different views from the organisation. For example, there are three suggested views concerning security policies. First, top management view which can be labelled as corporate policy. Second, users' view or organisation's policy. Third, designer view or technical policy (Abrams, and Bailey, 1995; Baskerville, & Siponen, 2002). There is a clear focus supported on the literature of the importance to have a clear understanding on how users/employees perceived these policies.

Also, cybersecurity requires an organisation to have appropriate measures that cover multiple areas, and it is clearly supported by established frameworks. This thesis will explore some of these frameworks to further understand the areas of relevance for cybersecurity. Two of the most well accepted standards in terms of security for information systems are the ISO/IEC 27000 family and the National Institute of Standards and Technology framework (NIST). In the case of the ISO/IEC 27000 family there are multiple certifications organisations can obtain and it includes more than 40 standards to follow.

Further one of the aims of the ISO/IEC 27000 series is to maintain the integrity, confidentiality, and availability of the information for the organisation by applying best practices to multiple areas of the organisation. As an example of the ISO/IEC 2700 series, the ISO/IEC 27001 includes requirements that organisations can follow for the cycle of implementing an information security management system that goes from establishing to maintaining and improving.

In cybersecurity, the ISO/IEC 27001 includes a section regarding operational security which includes actions to take to protect against malware by monitoring and following other standards.

Further, the rest of ISO/IEC 27000 series includes cloud security, controls, incident investigation and others. Next, NIST is constituted by multiple guidelines and practices with the focus on managing and reducing cybersecurity risk. The core of this framework is built upon multiple well-accepted standards like CIS Critical Security Controls, COBIT 5, ISA, ISO/IEC, NIST SP 800-53 and others. These cybersecurity frameworks have processes and principles to cover multiple areas of the organisation. First, governance of cybersecurity risk which includes assessment, responsibilities, compliance, and implementation regarding security risk. Second, approaches on how to manage access of employees/users to systems and assets. Third, building awareness and training of employees. Fourth, detection and or monitoring of systems. Fifth, a response plan for anomalous activities. Both ISO/IEC and NIST have a strong focus on user/employee to implement successful cybersecurity measures.

This might be explained by the literature that suggests that a great part of the security issues is performed by employees or internal users. Users/Employees actions intentional or not can be the weak link from organisations Spears, & Barki, (2010) As an example, some employees seldom follow the policies that organisations have put in place for cybersecurity (Siponen, Mahmood & Pahnila, 2014). Just as the frameworks or best practices target users to improve security, the literature further supports how to strengthen the human vulnerabilities on cybersecurity.

Thus, an important tool within organisations is to build knowledge and awareness among its users. Siponen, Mahmood, & Pahnila, (2014) suggested that increased the perception of employees in terms of cybersecurity relevance can have a significant impact on compliance. Supporting this line of thought Moody, Siponen, & Pahnila, (2018) observed that employees having knowledge and believed on the severity of cybersecurity can keep issues down.

These authors also stated that it is important that employees perceive that their organisation does its part in complying with the same policies. This effectiveness of the connection between employees, cybersecurity has been studied with multiple theories. As an example, Moody, Siponen, & Pahnila, (2018) mentions Deterrence theory, Theory of planned behaviour, Theory of self-regulation, Protection motivation theory, Health belief model to mention a few. Thus, even when the efficacy of some of these theories as observed by Moody, Siponen, & Pahnila, (2018) needs more review, users' understanding and behaviours toward cybersecurity are fundamental. Frameworks and literature suggest training and awareness techniques for supporting employees. Spears, & Barki, (2010) suggest that employees can be a source of issues for cybersecurity, but they can also be the ones with the solution if they have the understanding and correct tools.

2.5. Employees' Cybersecurity Learning Process

As was previously stated, it is crucial that workers at all levels of an organisation are aware of their responsibilities to protect the resources they interact with. To implement a holistic cybersecurity program, frameworks such as NIST and ISO/IEC 27001 included the concepts of awareness and training in their handbooks and guides (NIST, 2022; ISO/IEC 27001, 2022). For this thesis, we will explain these elements following the structure introduced by Wilson and Hash (2003) who proposed the learning continuum process. This is shown in Figure 3 and includes three components such as awareness, training, and education.

Especially, training and awareness will be analysed in-depth as they are the core part of the phenomenon studied. This section will describe more about the implementation and common barriers faced by organisations while implementing these programs which is a valuable insight for this thesis.

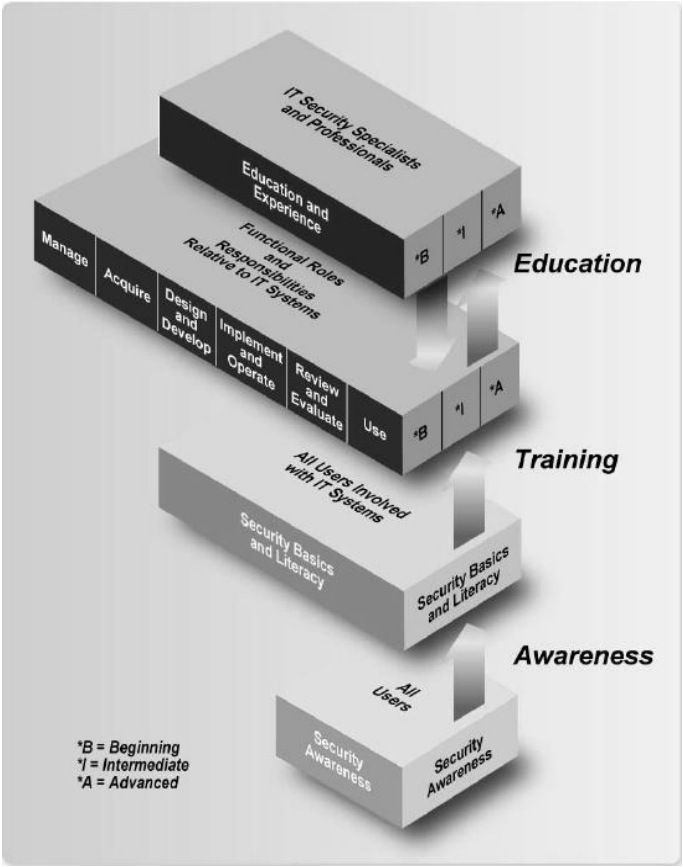

Figure 3: The IT Security Learning Continuum (Wilson & Hash, 2003, p.8)

2.5.1. Cybersecurity Awareness

Awareness is the capacity of individuals to identify a security concern and be able to respond adequately to them when a risky event occurs (Wilson & Hash, 2003). Previous investigations, books and reports in the literature defined with details the concept and mentioned aspects that could help to increase awareness in organisations (Bada, Sasse & Nurse, 2015; Stallings & Brown, 2018; Siponen, 2000). The motivation of these studies was driven by different objectives such as the reduction of user-related faults, the maximisation of the efficiency of the security procedures, and the compliance with regulations (Siponen, 2000; Stallings & Brown, 2018).

In terms of the process to increase awareness, according to many scholars in the field, the intention to provide information about existing risks and recommended behaviour to the people is one part of the process but not all (Siponen, 2000; Bada, Sasse & Nurse, 2015). In addition, the motivational aspect is an important element considering that the final objective of an awareness campaign is to modify the employees' behaviour and attitudes (Siponen, 2000). From an employee perspective, this requires different steps such as perceiving that the content is relevant, then accepting how they should respond, and finally being responsible to follow the

advice despite the existence of other demands (Bada, Sasse & Nurse, 2015). Therefore, an essential aspect is to design an awareness program that "support the business needs of the organisation and be relevant to the organisation's culture and information technology architecture" (Bowen, Hash & Wilson, 2006, p.31). One interesting observation obtained from these studies is the influence of the motivational factor in the success of awareness programs.

Moreover, an organisation which will start the implementation of awareness should realise a needs assessment to determine the status and justify the allocation of resources for this endeavour (Wilson & Hash, 2003). Because of this, different roles must be involved. Some of them are the organisational leaders whose function is key to promote full compliance, security personnel who are the experts with a good knowledge in best practices and policies, system users who perform business operations routinely, and others (Wilson & Hash, 2003). The main challenge of this approach is that a complete assessment of needs requires time and effort from different actors inside an organisation. What is more, these actors must have certain roles which sometimes are inexistent in some structures (Sadok, Alter & Bednar, 2020). Additionally, it could be interpreted that only the security personnel are responsible for this task; however, managers need to play a more effective role which is decisive (Soomro, Shah, & Ahmed, 2016). For that reason, some organisations could be obligated to realise trade-offs or abbreviated ways during the implementation which can lead them to lack of success.

Once the assessment is completed, the application of the methods must be executed. Wilson and Hash (2003) listed different tools and elements in their wide-ranging study. In terms of content, topics such as password management, unknown email, laptop security while on travel, software licence restriction issues, and desktop security are possible options to be included. The final decision to include one item or not is based on a discussion that considers the organisational context. Regarding the sources of material, several themes could be combined or one at a time in each material depending on what skills need to be transmitted to the audience (Wilson & Hash, 2003). For instance, e-mail advisories, security websites, periodicals, conferences, posters, flyers, courses, and seminars are possible options to expose the information to the employees (Wilson & Hash, 2003; Stallings & Brown, 2018).

One positive aspect to also consider in the current analysis of employee awareness is that today more people are aware of security risks. This not only happens because they receive the information as part of their organisation's policies but also because their constant interaction with digital products motivated them to proactively look for more knowledge in terms of personal protection (Öğütçü, Testik & Chouseinoglou, 2016). This could be a positive factor to increase the success of future awareness programs.

Furthermore, Stallings and Brown (2018) highlighted that it is relevant for organisations to share a security awareness policy document with the employees. This has three main objectives. Firstly, communicate the requirement to employees to participate in the awareness program on a mandatory basis. Secondly, inform that every employee will have enough time to be part of the activities. Thirdly, state with clarity who is responsible for the management and conduction of awareness activities (Stallings & Brown, 2018).

While the positive aspects of awareness have been constantly stated in previous publications, some of them also analysed the reasons that could potentially prevent the success of cybersecurity awareness endeavours (Bada, Sasse & Nurse, 2015). For instance, it is possible to see cases of employees violating information security policies even though they have received some security preparation (Kajtazi et al. 2018; Sadok, Alter & Bednar, 2020). Kajtazi

et al. (2018) conducted an insightful study with more than 500 participants of two banks in Europe. The insights showed that employees usually give more importance to the completion of a work task than to a possible exposition of confidential information (Kajtazi et al. 2018).

This is supported by the idea that the immediate benefit achieved with this specific task has a greater priority than the avoidance of a future security cost. (Kajtazi et al. 2018). Another relevant study performed by Parsons, McCormac, Butavicius, Pattinson and Jerram (2014) stated that employers could feel confident that an improvement in employees' knowledge about security rules will have a beneficial impact in their attitude. However, the results helped to conclude that generic courses do not influence the attitude as expected therefore training should be better contextualised (Parsons et al. 2014).

2.5.2. Cybersecurity Training

Training is focused on teaching specific and necessary security skills to employees depending on the role they perform (Wilson & Hash, 2003). It is relevant to state that the content of a training is designed based on the security basics and literacy material. Moreover, the idea is to provide tailored training based on the needs of each group of people inside the organisation (Wilson & Hash, 2003; Bowen, Hash & Wilson, 2006). For instance, training must be different for a System Administrator than for a Project Manager due to the different tasks they realise, and the security knowledge required. Additionally, recent papers have explained the positive results obtained when employee's learning preferences are also considered in the design of training (Chowdhury, Katsikas & Gkioulos, 2022; Pattinson, Butavicius, Ciccarello, Lillie, Parsons, Calic & Mccormac, 2018). More details about these ideas will be exposed in the following paragraphs.

Initially, a revision of the possible techniques used to deliver training material is illustrative to understand which are the possible options. Wilson and Hash (2003) recommended that when opting for a technology for training, aspects such as "ease of use, scalability, accountability, and broad base of industry support" must be evaluated (Wilson & Hash, 2003, p.34). This is supported by the fact that organisations are involved in an ever-changing environment where the ability to adapt and expand their training with continuous updates is perceived as a clear advantage.

Moreover, the different techniques for implementing training were mentioned by previous authors (Wilson and Hash, 2003; Chowdhury, Katsikas & Gkioulos, 2022; Pattinson et al. 2018). A list of them including a brief description is below:

- Interactive video training (IVT): Tool that supports audio and video facilitating the interaction in a synchronous way with the instructor.
- Web-based training: Popular option for distributed environments. The main characteristic is that the participants can study autonomously and work at their own pace. Some of these instances are integrating the possibility to interact with the instructor or other students.
- Computer-based training: It is considered an effective method in terms of distribution if the web-based approach is not feasible. Interaction with the instructor and students is not enabled.
- Onsite, instructor-led training: It is one of the most traditional ways to deliver training. The main advantage is the room for natural interaction. However, the disadvantage is

the inability to schedule enough classes for large organisations or remote work employees.
- Personalised training: Customised training format that considers human attributes which influence the outcome such as learning style, cognitive abilities, and meta-cognition of the participants

Furthermore, it is possible to combine different techniques in one session or implement more than one technique as part of the cybersecurity program of the organisation. With that in mind, Furnell, Gennatou and Dowland (2002) conducted a study about a company which implemented their own security training tool. One aspect of this innovative tool was that information about the suitability and the associated impact of each security issue was shared with the participant (Furnell, Gennatou & Dowland, 2002). Also, they were able to see a message explaining each possible decision they were able to make with teaching purposes (Furnell, Gennatou & Dowland, 2002). Thus, this demonstrated a good example of how different techniques could be adapted and tailored to needs.

A relevant aspect of personalised training was highlighted by Pattinson et al. (2018) who concluded that the extent to which a training is associated to the participant's learning preference is more important than the frequency of the training. This could be a strong reason to always consider personalised training as one of the most effective options. However, from a practical perspective, it would be impossible to tailor the training based on each individual characteristic. For that reason, a viable option is to design different training based on certain divisions inside the organisation such as business teams or groups (Pattinson et al. 2018).

Finally, it is important to note that nowadays, an organisation does not need to design an exclusive content for this endeavour which is sometimes complicated due to the probable absence of a specific security area in the organisation (Sadok, Alter & Bednar, 2020). Moreover, Furnell, Gennatou and Dowland (2002) argued that, especially for small organisations, this task is difficult to approach due to a lack of expertise. Moreover, Gartner (2021b) published a report containing several options of vendors offering computer-based-training. Some of these vendors offer the option of a free knowledge check and many of them could be accessed as Software as a service (SaaS) solution.

2.5.3. Cybersecurity Education

Education is the most thorough component which concentrates all the skills and competences of previous knowledge. This last one is more focused aiming to prepare security professionals who need expertise in the field to perform their activities (Wilson & Hash, 2003; Stallings & Brown, 2018).

The objective of education is to form IT security specialists with a broader vision that could contribute to the design of the internal cybersecurity program (Wilson & Hash, 2003). Nowadays, several options are offered in the market by colleges and universities to complement a deeper understanding of the cybersecurity area. These are viable options that might be considered by organisations to adequately develop this discipline.

It is important to acknowledge the existence of the education component and its relationship with the other components of the learning continuum process. However, Cybersecurity Education is not deeply investigated during this thesis. The reason is that this component does

not constantly participate in the daily routine of employees who are not specifically dedicated to security endeavours.

2.6. Employees' Behaviour

All the concepts previously explained have as main objective to provoke the attitudinal change of employees regarding cybersecurity threats. But it is also essential to analyse concepts that influence their behaviour during their security learning journey and the real application of the theories previously stated.

A useful resource to understand the employees' context is the security action cycle shown in Figure 4. The process starts when an abuser ignores deterrence which is the first try to restrain the risk represented by dishonest staff (Straub & Wekle, 1998; Willison & Warkentin, 2013). Then, the next step is prevention which includes countermeasures to enforce policy. If an abuser overcame the deterrence and prevention stages therefore the organisation needs to detect the misuse (Straub & Wekle, 1998). Finally, the last security program is remedies where the objective is to countermeasure the damage generated by the abuser or to apply punishment (Straub & Wekle, 1998). According to Straub and Wekle (1998), the ideal scenario for organisations is to prioritise deterrence and preventive efforts, while minimising detection and remedy actions.

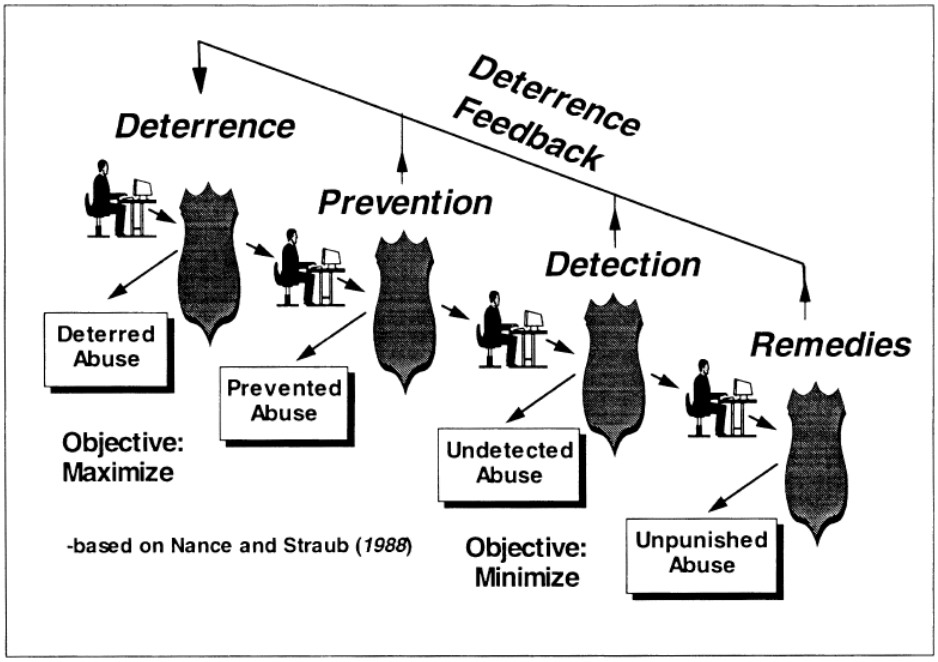

Figure 4: The Security Action Cycle (Straub & Wekle, 1998, p.446)

Despite the existence of frameworks and a strong literature background regarding how to implement cybersecurity training, there are also many studies that explain the causes of lack of compliance. There exist some factors such as neutralisation, deterrence, security fatigue, and others that let employees feel that a bad behaviour is justified or not (Willison & Warkentin, 2013). Bada, Sasse and Nurse (2015) argued that the implementation of cybersecurity awareness implies a challenge from the psychological perspective. The objective to change

people's behaviour implies that they not only understand the advice but also feel motivated to change their attitudes (Bada, Sasse & Nurse, 2015).

In terms of security behavioural research, several theories have been used as a reference in previous studies. As an insightful summary, Moody, Siponen and Pahnila (2018) consolidated 11 in a paper; some of them used by previous studies, and others with potential to be utilised, that could help to explain why the security behaviour of people is sometimes contrary to policies. Related theories collected during the literature review are described in next lines because they are considered part of the analysis of this thesis:

- Neutralisation: It is a distinguished theory in criminology. It states that rule-breaking people are aware of the norms and policies (Siponen & Vance, 2010). However, they justify incorrect behaviours by neutralising in their mind the existence of the rules during the deterrence stage. Some of the neutralisation techniques applicable to the security context are denial of responsibility, when an employee consider himself as lacking responsibility; denial of injury, when an employee justifies its act by minimising the harm caused; denial of necessity, when an employee views the rule-breaking action as necessary; and condemnation of the condemners, when an employee blames the target of the action (Siponen & Vance, 2010). Hence, all these techniques could be used from an attacker perspective to justify the failure of compliance.

- Security fatigue: This phenomenon occurs when security controls are perceived as a barrier by employees. One common reason is when a certain control is more frequently requested and has a long duration (Furnell & Thomson, 2009). As practical examples, we can find the reset password process as well as the firewall warning messages. Furthermore, three variables are relevant to determine the impact of security fatigue such as the effort needed to achieve the compliance, the difficulty associated with giving the specified effort, and the importance of the specific asset to assure (Furnell & Thomson, 2009).

- Self-efficacy: Explains the intention of a person to adopt a specific behaviour. This is based on subjective norms, attitudes, and perceived behavioural control (Bulgurcu, Cavusoglu & Benbasat, 2010). This concept is associated with the theory of planned behaviour. Moreover, the impact of cybersecurity training and awareness to influence these behaviours was also demonstrated in these studies (Bulgurcu, Cavusoglu & Benbasat, 2010). In summary, an employee's self-efficacy can certainly influence the intention to adhere to the policies.

In summary, it is important to analyse the thinking process followed by the offender through the security action cycle that could be studied from the perspective of these theories. What is more, many of the factors and reasons that support these behaviours include some aspects that the previous cybersecurity learning process could potentially help to modify.

2.7. Cybersecurity Program's Continuous Improvement

Some organisations possess a cybersecurity program plan already established but the actual work practices do not confirm their expectations in terms of a high level of security (Sadok, Alter & Bednar, 2020). For that reason, the inclusion of complementary processes and

methods must be evaluated to increase the effectiveness of the ongoing initiatives. Possible ideas to accompany the cybersecurity program endeavour are listed below:

- Gamification: An innovative way to increase the effectiveness is to include gamification as a complementary part of the educational process (Koutsouris, Vassilakis & Kolokotronis, 2021). Gamification integrated with the learning metrics might contribute to generate a more enjoyable and engaging journey for the participants including team competitions and awards (Koutsouris, Vassilakis & Kolokotronis, 2021). What is more, one way to prepare an employee to handle a security event is to emulate a similar hand-on experience. This could be achieved using interactive video game technologies (Nagarajan, Allbeck, Sood & Janssen, 2012).

- Evaluation and Feedback: The idea is to collect insights from the participants of the awareness and training programs. Different mechanisms could be used such as surveys, interviews, status reports, focus group, and benchmarking (Bowen, Hash & Wilson, 2006). Possible aspects that could be updated after the feedback consolidation are related to the scope, quality, usability, and duration of training based on what is more suitable for most respondents (Wilson & Hash, 2003). This could be also aligned with the earlier mentioned idea of implementing personalised training.

- Continuous Monitoring: The success of a cybersecurity program implementing all the aspects previously described should be supported by a continuous improvement process to avoid becoming obsolete (Wilson & Hash, 2003; Bowen, Hash & Wilson, 2006). To enable this, it is necessary to also activate a continuous monitoring process where information and metrics regarding security incidents, level of compliance, and level of effectiveness are available to drive decision making (Wilson & Hash, 2003; Sacher, 2020).

2.8. Summary of Literature Review

The literature review presented different themes that are part of a cybersecurity implementation in organisations. As these themes have different aspects, we consider the ones that are most relevant regarding the employee's participation. Table 2 shows all the themes, subthemes, and references in a consolidated way which is useful to have a holistic perspective of the literature review.

Table 2: Summary of Literature Review

Theme	Sub-Theme	References

Cybersecurity	- Information Security - Cybersecurity - Information and Communication Technology Security	(Bulgurcu, Cavusoglu & Benbasat, 2010), (Chowdhury, Katsikas & Gkioulos, 2022), (Kajtazi et al. 2018), (Von Solms & Van Niekerk, 2013), (Von Solms, 1998), (Whitman & Mattord, 2011), (Oscarson, 2003), (NIST, 2022), (ITU, 2022)
Cybersecurity and Remote Work	- Lack of preparedness and knowledge for a remote workforce - Vulnerability in remote work practices - Cybercrime increase - Emotional factors	(Pranggono & Arabo, 2021), (Naidoo, 2020), (Alexander, & Jaffer, 2021), (Kane, Nanda, Phillips & Copulsky, 2021), (Galanti, Guidetti, Mazzei, Zappalà & Toscano, 2021)
Cyberthreats in a Remote Work Environment	- Social Engineering - Insider Threats - Malware - DoS/DDoS - Awareness as a countermeasure	(Stallings, and Brown,2018), (Cisco, n.d), (Zargar, Joshi, & Tipper, 2013), (FBI, n.d), (Microsoft, n.d)
Cybersecurity Governance	- Security Policies, Frameworks and Standards - Flexibility on Implementation of cybersecurity plan - Key to focus on employees - Connection between employees' awareness and effectiveness of cybersecurity	(Guo, Wei, Huang & Chekole, 2021), (Soomro, Shah & Ahmed, 2016), (Baskerville & Siponen, 2002), (Singh, Gupta & Ojha, 2014), (Abrams & Bailey, 1995), (Spears & Barki, 2010), (Siponen, Mahmood & Pahnila, 2014), (Guo, Wei, Huang & Chekole, 2021), (Mirtsch, Kinne & Blind, 2020), (Moody, Siponen & Pahnila, 2018)

Employees' Cybersecurity Learning Process	- Learning continuum process - Awareness - Training - Education - Needs assessment - Motivation - Training types	(NIST, 2022), (ISO/IEC 27001), (Wilson and Hash, 2003), (Bada, Sasse & Nurse, 2015), (Stallings & Brown, 2018), (Siponen, 2000), (Bowen, Hash & Wilson, 2006), (Sadok, Alter & Bednar, 2020), (Soomro, Shah, & Ahmed, 2016), (Öğütçü, Testik & Chouseinoglou, 2016), (Kajtazi et al. 2018), (Parsons et al. 2014), (Chowdhury, Katsikas & Gkioulos, 2022), (Pattinson et al. 2018), (Furnell, Gennatou & Dowland, 2002), (Gartner, 2021b)
Employees' Behaviour	- Neutralisation - Security fatigue - Theory of planned behaviour	(Straub & Wekle, 1998), (Willison & Warkentin, 2013), (Bada, Sasse and Nurse, 2015), (Moody, Siponen & Pahnila, 2018), (Siponen & Vance, 2010), (Furnell & Thomson, 2009), (Bulgurcu, Cavusoglu & Benbasat, 2010)
Cybersecurity Program's Continuous Improvement	- Gamification - Evaluation and Feedback - Continuous Monitoring	(Sadok, Alter & Bednar, 2020), (Koutsouris, Vassilakis & Kolokotronis, 2021), (Nagarajan, Allbeck, Sood & Janssen, 2012), (Bowen, Hash & Wilson, 2006), (Wilson & Hash, 2003), (Sacher, 2020)

3 Methodology

The following chapter aims to describe the research methodology applied in this thesis. Firstly, it presents the connection between the literature review and the corresponding design of the research. Secondly, it explains the decision to use interviews as a research technique. Thirdly, the selection of participants and the interview guide are described. Finally, the data analysis process as well as the ethical considerations and scientific quality considered in this thesis are presented.

3.1. Research Approach

For this thesis a qualitative method was selected for furthering our understanding on the research question. Recker (2013) observed this method allows a researcher to understand a phenomenon within a unique context. Furthermore, Fossey, Harvey, McDermott, and Davidson (2002) stated that a qualitative method can help illuminate the context of the individuals used in the research study and provides a clear authenticity to the perspectives obtained. This supports the interest of this thesis of understanding the perspective of the employees regarding the aspects of cybersecurity awareness. Further, the understanding we want to obtain is within the remote work context which, as stated by the authors, a qualitative method can provide an insightful understanding of this phenomenon.

As shown in the literature review, there is a solid body of knowledge that supports the multiple themes of cybersecurity awareness to be studied within this thesis. Thus, by also applying a deductive approach within this thesis we can study this body of knowledge against the events that lead to a remote work context and what is the relationship or impact it has in terms of cybersecurity awareness.

On the other hand, in terms of the body of knowledge for cybersecurity there are multiple aspects involved, technical and non-technical. But for the purpose of this thesis and to clarify on previous sections we want to focus on the factors that are closely related to the employee perspective in terms of cybersecurity, and it further supports our selection for a qualitative methodology. This focus on the context for the literature review, data collection and the analysis would follow key principles of a qualitative approach (Patton, 2015). Therefore, guiding this thesis with a qualitative method will enable it to see individuals' perspectives and view the depth of the interactions of remote work and cybersecurity awareness.

3.2. Data Collection

3.2.1. Literature Review Process

As the foundation of the literature review, we followed Recker (2013) observation that a researcher needs to be informed about the current body of knowledge and how this can support our thesis. Also, we supported the literature review by scholarly articles, other credible sources

from practitioners, and official statistics (Recker, 2013). Thus, our literature review process focuses on four important points. First, we reviewed literature that is relevant for cybersecurity which includes background, definitions, threats, and practices. Second, we focused on cybersecurity through the lenses of the remote work that was instituted because of the COVID-19 pandemic. Moreover, it is important to mention that the literature regarding the impact of the COVID-19 as a trigger to adopt a remote work environment and expand technology used is still developing. Third, we focus on the relationship of cybersecurity and the employees and what the literature considers effective to increase awareness. Finally, we review the role of the cybersecurity learning process of the employee and the role to build awareness.

Multiple tools for data gathering were used as an example:

- LUBSearch
- LUBCa
- Google Scholar
- Senior Scholars' Basket of Journals for Information Systems
- Information Systems Conferences
- Journals for related fields

Within the terms used for the literature gatherings we have:

Cybersecurity, Information security, Remote work, Information systems, Information management, Security awareness, Information security training, Information security policy, Information security awareness

3.2.2. Interviews

The technique chosen to perform the qualitative study is interviews as it makes possible the conduction of an exploratory research where complex aspects of the phenomena and different perspectives could be brought to light (Recker, 2013).

3.2.2.1. Selection of Participants

The method followed to choose the participants was purposive sampling because the interviewees must meet specific criteria to tell a valid experience for the research (Recker, 2013). As mandatory requirements for the candidates we considered the following:

- Employees who use information systems and technology to perform their daily job.
- Their organisations must have a cybersecurity awareness and training program.
- The employees must have received cybersecurity training before the pandemic.
- The organisations must have offered cybersecurity training for remote working employees.
- Their job routine has changed due to the pandemic in terms of remote work.
- The participants must have relevant years of experience.

In terms of business sectors, IT, Financial Technology, and Business Process Outsourcing (BPO) were taken into consideration also known as information intensive organisations (Kajtazi

et al. 2018). These have been identified as industries where cybersecurity implementation plays an important factor. Further, the assumption is that some behavioural theories could be perceived in a different way by employees in different industries (Bulgurcu, Cavusoglu & Benbasat, 2010).

The people considered were identified in the professional network of the authors of this thesis. Specifically, a first conversation was realised to validate if they effectively meet the criteria indicated previously as was stated by the purposive sampling method. Once a participant confirms the precondition requirements then a brief explanation of the thesis objective is shared to ensure that they feel comfortable and open to help with the thesis purpose.

Further, there is an increase of cyberattacks within America, as a result we decided to target participants within this region (Statista, 2022). The locations of our participants were Peru, USA, and Guatemala. Furthermore, an important consideration was to obtain informed perspectives from employees. Therefore, the requirement of having relevant years of experience, this gave us employees within senior roles that would have a more mature perspective in terms of work experience.

Before conducting the interviews, an interview outline (Appendix 1) was shared with the interviewees. The main intention was to let them have an overview of the different themes that are going to be part of the conversation (Patton, 2015). We considered this activity essential as sometimes employees forget facts, details, and feelings experienced during their interaction with a cybersecurity program. Therefore, it was relevant during the interview to have this information on hand so different aspects could be described by the participants.

As a summary, Table 3 shows relevant information about the participants such as the organisation, industry, role, the country where they are based during their work and their years of experience.

Table 3: Participant details

Respondent	Organisation	Industry	Role	Country	Years of Experience
PR1	IT Consultancy Company 2	IT	Software Engineer	Peru	8
R1	Online payment company	Financial Technology	Risk Manager	Guatemala	14
R2	IT Consultancy Company 1	IT	Project Manager	Peru	15
R3	IT Consultancy Company 3	IT	Operations Manager	Guatemala	13

R4	BPO Company	Business Process Outsourcing (BPO)	Program Manager	USA	15
R5	Printing and digital products	IT	Project Manager	Guatemala	25

3.2.2.2. Pilot Interview

Our initial approach was to conduct a pilot interview where we can gain familiarity with the interview script planned and test the actual performance of the technological tools selected for our sessions. According to Majid, Othman, Mohamad, Lim and Yusof (2017), a pilot interview helped the researchers to get practical experience in conducting these types of sessions. What is more, it is useful to validate the suitability of the questions and get early feedback (Majid et al. 2017). This pilot interview was performed by the two authors of the thesis as interviewers. The interviewee was one person who meets the same requirements as the main interviewees. For that reason, this participant was randomly selected from the initial pool of participants available.

Moreover, it was important to complement the researcher's preparation as they did not have vast experience applying interview techniques. Therefore, we needed to have a high level of confidence in the tools we were going to use to replicate in a more realistic way an ideal but non possible real face environment. For that reason, the same tools were used in this pilot interview.

After the pilot interview was completed, a feedback session was facilitated by the researchers to evaluate positive and negative aspects found in this first stage. The objective was to improve these aspects before starting the main interviews stage.

Some of the feedback aspects obtained were:

- The length of the interview was appropriate.
- Some changes were applied in the questions related to cybersecurity training. The initial format could be observed at Table 4 in questions 3.3, 3.4, 3.5 and 3.6.
- After a conversation with the pilot interviewee, we observed that the questions applied for Cybersecurity Program's Continuous Improvement were a bit confusing. This happened because the participant did not have in mind what is the meaning of each one of the options discussed. For that reason, we decided to apply a different dynamic using a sorting exercise where we could present a slide with the three possible options found in the literature to improve a Cybersecurity Program such as Gamification, Evaluation and Feedback, and Continuous Monitoring. As a result, the participant will visualise in the videocall the meaning of all the options and have a better context to suggest which of them could help.
- We realised that Zoom was an adequate tool to conduct the interview given that the audio and the video were appropriately recorded.

- We realised that the Interview Invitation Outline that is in the Appendix 1 was useful because it gave the participant an idea of what is going to be discussed during the interview. As a result, a participant will be prepared given that sometimes the information about their experience with cybersecurity is not remembered so clearly.

In summary, all the feedback obtained helped us to define the final content of Table 4.

3.2.2.3. Main Interviews

Interviewing is the most outstanding technique to gather data according to Recker (2013). There exist different structured protocols to conduct an interview based on the objective of the study. For our research, semi-structured interview is the most suitable option because we can design a predefined script of questions but at the same time show openness and flexibility to vary the course of the interview based on what the interviewee says (Recker, 2013).

Additionally, it is essential to be aware that cybersecurity could be perceived as a sensitive topic therefore techniques like contextualising a question and the use of prefatory statements will be used to gain confidence with the interviewee by communicating the specific purpose behind a question if necessary (Recker, 2013; Patton, 2015). This is quite important to set up a trust environment where the interviewee is conscious that the information exposed will not be judged rather processed following a scientific method as an insight for this research.

In terms of the content that we could collect, one advantage is that we will not only obtain the answers but also the reason for the answers (Recker, 2013). To meet this expectation, it is a crucial task that the interviewer facilitates a conversation where follow-up questions are introduced to ensure a bidirectional discussion (Patton, 2015). These more specific questions could be generated spontaneously and in a natural style during the conversation (Patton, 2015). The objective is to look for details that are an important insight for the phenomenon studied.

It is important to consider that the interviews will be conducted remotely due to the geographical location of some participants. A remote environment could be an impediment to observe gestures and movements that were usually easy to capture in a face-to-face session. For that reason, the use of a video call platform will let the researchers view and hear online the reactions and participation of the interviewee. Moreover, the researcher will make an extra effort to perceive some subtle and non-verbal cues (Engward, Goldspink, Iancu, Kersey & Wood, 2022). Additionally, one advantage provided from this remote environment is that the participants will be able to take the interviews from a familiar location that they will decide. This aspect is positive for the development of the session as they will feel safe and comfortable.

3.2.3. Empirical Data Collection Process

The idea is to open a fluid conversation with an interviewee where specific sub-themes are not overlooked. For that reason, a semi-structured approach was followed during the interviews as was previously stated. The questions considered in the outline were based on the themes investigated in the literature review. Nevertheless, due to the casual line that a conversation could follow then the order of the questions may not be totally respected. For that reason, both researchers will be aware of the content provided by the participant. If information that needs to be addressed later during the analysis of interviews was not mentioned by the participant

therefore a follow-up question could be introduced to bring the topic to the conversation (Recker, 2013; Patton, 2015).

Regarding the development of the questions, both researchers collaborated to ensure that every theme relevant for the thesis that was mentioned in the literature review could be part of the interview outline. Furthermore, a validation with the thesis supervisor was performed to adjust details and have opportune feedback. Once this process was completed the pilot interview was conducted to validate if the number of questions was not so long to have an appropriate time and to know if some of the topics were overlapped. Therefore, it was possible to rewrite some questions before conducting the main interviews.

The basic structure of the final interview outline is described in Table 5. The questions are grouped under 5 themes where the first one is included for control purposes and the last one gives a chance to the participant to share some additional information or clarify an aspect that was revealed during the interview. The other 3 themes were formulated based on the themes collected in Table 1 as part of the literature review. Moreover, the order of them is specific. Firstly, the objective is to have an idea of what is cybersecurity from the perspective of the candidate. Secondly, it is relevant to get information about how the transition from work at the office to the remote context was.

Additionally, know if the employee has interacted with some cyberthreat before and its perception of them is also an insightful aspect. Finally, practical, and more personalised aspects such as their knowledge of the security policies, their interaction with the security training, and their engagement level with some areas of the cybersecurity program are brought to the conversation. Table 4 shows a summary of the interviews conducted for this thesis.

Furthermore, it is crucial to clarify that the structure of the question has as main objective to understand the sensations of the employees regarding each theme that are applied in the practice. For that reason, we did not directly ask to the participants what aspects of cybersecurity are more relevant and/or relatable while working from home. Particularly, the reasons behind each of the participant's comments helped us to deduct which are the aspects that are part of the answer to the research question.

Table 4: Interview Summary

Participant	Date	Duration (Minutes)
PR1	2022-04-20	33
R1	2022-04-21	48
R2	2022-04-22	43
R3	2022-04-26	37
R4	2022-04-27	51
R5	2022-04-28	33

Table 5: Interview Outline

Theme	Question	#
Interview Controls		
- Role **- Years of experience** **- Technology Dependence** **- Prior Remote Work** **- Emotional Factors**	What is your role at work? How long have you been there? How involved are you with technology to perform your job activities? Did you work remotely prior to the COVID-19 pandemic? What was the most difficult aspect of working from a remote environment? In terms of work dynamic, stress related to COVID-19 and work.	1
Cybersecurity - Conceptual		
Cybersecurity	What is cybersecurity from your perspective? What is your experience with cybersecurity?	2
Cybersecurity and Remote Work - Practical		
Cybersecurity and Remote Work **- Organisational perspective**	Have employees moved into a remote work set up because of the COVID-19 pandemic?	2.1
	Have employees had the opportunity to work remotely prior to the COVID-19 pandemic?	2.2
	Have employees received security policies provided from the organisation when the full remote work environment was instated?	2.3
Cyberthreats in a Remote Work Environment **- Individual perspective**	Do you think that the new remote work environment and tools you have can open new breaches for cyberthreats?	2.4
	Do you think your organisation has enough tools and infrastructure to protect your remote work environment from cyberthreats? Antivirus, VPN, Firewall, and others.	2.5
	Have you had contact with any cyberthreat in your remote work environment? Like suspicious emails, stolen passwords, or company systems down to an attack?	2.6
Cybersecurity Awareness and Training - Practical		
Cybersecurity Governance	Are cybersecurity policies easy to understand and relevant for your role in the organisation?	3.1
Employees' Cybersecurity	Have you obtained, from your perspective, enough knowledge from your organisation to avoid a cyberthreat?	3.2

Learning Process **- Awareness** **- Experience** **- Differences** **- Relevance** **- Personalised training**	What was the duration of the cybersecurity training you received?	3.3
	How often did you receive this cybersecurity training?	3.4
	What type of cybersecurity training was it?	3.5
	What do you feel was different from cybersecurity training facilitated while you were working at the office?	3.6
	Do you feel that the topics included in the training are relevant for your daily routine?	3.7
	Do you think training content should be individualised to each employee or the current standard practice is effective?	3.8
Employees' Behaviour **- Self-efficacy** **- Deterrence** **- Security Fatigue** **- Neutralisation** **- Work / Personal context**	Do you feel engaged to follow the cybersecurity guidelines provided?	3.9
	From your perspective, what are the possible consequences caused by not following cybersecurity policies?	3.1
	Did you feel overwhelmed trying to follow the cybersecurity guidelines provided by the organisation?	3.11
	Do you think you would prioritise to achieve a business goal even if this risks the cybersecurity policies of the organisation?	3.12
	Do you cover your webcam in your organisation's computer? What about your personal equipment?	3.13
Cybersecurity Program's Continuous Improvement **- Gamification** **- Evaluation and Feedback** **- Continuous Monitoring**	How do you think the employees' experience in terms of cybersecurity could be improved? New ideas to complement the current program are welcome.	3.14
	Sorting exercise about continuous improvement of training.	3.15
Final	Is there anything else you would like to add or something you would like to clarify further?	4

The last theme evaluated in the interview is Cybersecurity Program's Continuous Improvement. As was explained previously, one of the Pilot Interview points commented that one point of improvement was to modify the presentation of the question 3.15. As a result, Figure 5 shows

the slide shared by Zoom during the interviews to present visually the three possible options and start a closed card sorting exercise (Moore & Benbasat, 1991). Hence, the respondent has a visual support to remember the meaning of each concept and choose the order of priority in a friendly way during the session. The option selected in first place is the priority to be implemented to improve a cybersecurity program.

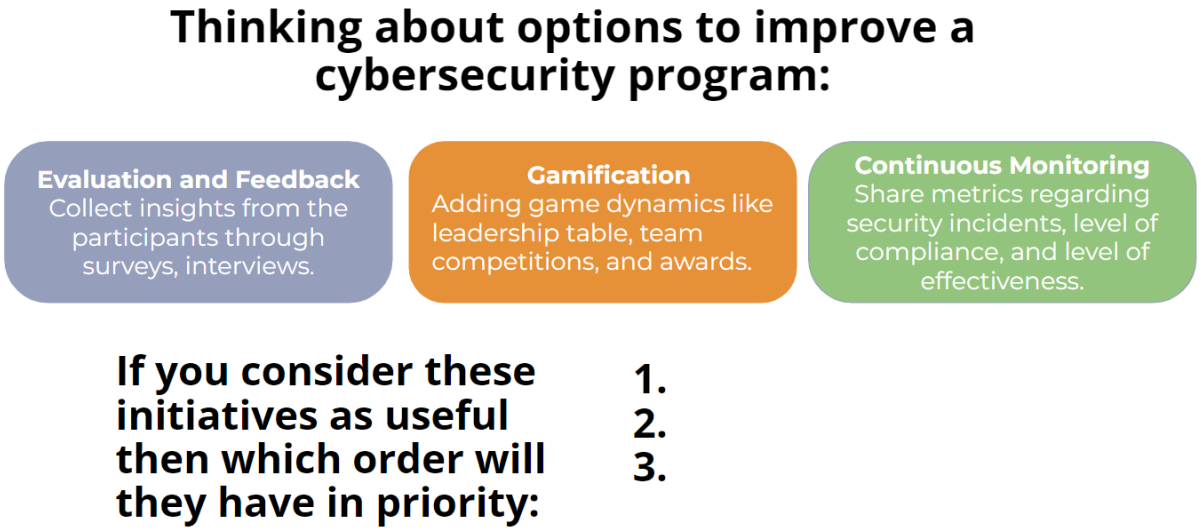

Figure 5: Sorting Exercise - Options to improve a cybersecurity program

3.3. Data Analysis

After conducting the sessions with the participants, we have content from 1 pilot interview and 5 main interviews. This implies a large amount of data which must be analysed using effective techniques to identify parts of them that are relevant for our topic. Coding is an appropriate technique to identify and organise portions of the data around concepts (Recker, 2013). This thesis categorised the data based on themes and subthemes exposed in the literature review. For this purpose, the structure of the interview outline is as it has already defined which themes are related to each question. Therefore, during the analysis, specific responses could be usually linked to an aspect of the phenomenon previously stated in the theoretical background.

In terms of transcription, after each interview was completed, we transformed the recorded audio content into text transcripts. Support tools were used to make efficient use of the time. For that reason, Dictate of Microsoft Word (Microsoft, 2022) and Otter AI (Otter, 2022) were selected to perform a speech to text transcription. However, these tools are not fully accurate, therefore a manual additional effort was made to make some corrections therefore the content matches the audio recordings of the interviews. Additionally, the Appendixes 4, 5, 6, 7, 8, and 9 show all the transcripts where the row indicates which is the order of occurrence of each intervention. This was a helpful method to quote specific parts of the interview during subsequent Chapter 4.

An important activity to avoid confusion in some parts of the transcript was to remove specific parts of the speech that are redundant. The purpose of this was to have clear content in the transcript that did not deviate the attention of the reader. For instance, repeated words found

usually in many answers and filtered words were reduced to a simpler way that expresses the same message. Furthermore, a copy of the transcripts presented in the Appendixes 4, 5, 6, 7, 8, and 9 were shared with the participants using the Appendix 3 format to receive their approval in case they need to update something that the researchers could misunderstand.

Moreover, we had meetings after each interview to comment on our understanding and interpretations of what was said during the session. This was useful to contextualise some of the answers and to confirm if some sensations perceived by the researchers effectively occurred during the interview.

Table 6 shows a categorisation of colours used to highlight specific portions of the participant's answers that express ideas associated to each theme and sub-theme. These colours are utilised in the Appendixes 5, 6, 7, 8, and 9.

Table 6: Interview Coding Outline

Theme	Sub-Theme	Colour	Code
Controls			
Cybersecurity			CS
Cybersecurity and Remote Work			CRW
Cyberthreats in a Remote Work Environment			CTR
Cybersecurity Governance			GOV
Employees' Cybersecurity Learning Process	Cybersecurity Awareness		AW
	Cybersecurity Training		TR
Employees' Behaviour	Self-efficacy		SE
	Deterrence		DT
	Security Fatigue		SF
	Neutralisation		NT
	Work / Personal context		WPC
Cybersecurity Program's Continuous Improvement	Continuous Improvement		CI
	Evaluation and Feedback		EF

	Gamification		GAM
	Continuous Monitoring		CM

3.4. Ethical Considerations

For any thesis that includes research within the information systems field, it is important to consider the ethical practices and implications. Recker (2013) made an important observation regarding the ethical considerations for research. The author stated that through all the steps of the research and activities involved it must maintain honesty and integrity. Moreover, it is a fundamental part of the ethical practices to show a perspective and conclusions that represent the most accurate representation of the topic in hand (Pimple, 2002). There is a clear consideration within this thesis to abide by ethical standards that would maintain the quality of our thesis.

The data obtained for the background of the thesis has been obtained from credible sources that allows authenticity to the information and allows the data to be guided by the right knowledge. Also, given the fact that this thesis will interact with interviewees, extreme care needs to be put in the ethical practices around it. Ryan, Coughlan, and Cronin (2009) observed that when dealing with people's perspective it is first important to obtain a consent from participants and maintain the rights of the participants along all the process. Thus, every participant within this thesis has previously agreed to participate voluntarily within the study with the condition of maintaining confidentiality for the process. Confidentiality is important for the participants as when talking about security practices within organisations is a sensitive topic that must be treated with the highest care.

Furthermore, when collecting, analysing, storing, and sharing the data and interviews this thesis will follow good practices to assure integrity and honesty (Recker, 2013). The interviews would be performed via Zoom which has an end-to-end encrypted platform to ensure the security and confidentiality. Moreover, the transcription of the interviews was approved by the interviewees to ensure accuracy and confidentiality. All this data and communications would be managed and stored with Lund University official accounts which already have security practices in place to maintain the security, privacy, and integrity. Overall, their ethical practices and considerations have been taken as a key part of this thesis.

3.5. Scientific Quality

There are some methodological elements that are necessary for every type of research to secure its quality. Recker (2013) stated that for qualitative research there are 4 methodological requirements to test the quality of a research and which this thesis has taken into consideration. First, Internal validity/credibility which refers to the thesis providing enough evidence for the interpretations that are being presented. For this requirement this thesis has taken special care on the patterns found within our data collection and interviews. Further on the data analysis we will present a detailed explanation on how we build the arguments for the findings. Second,

Construct validity/Confirmability which refers to ability of the thesis finding to be challenged or verified by a third party.

The body of knowledge for this thesis has been built with multiple reputable sources which includes peer review journals and conferences related to the field which are verifiable. As a result, finding is ground in the current state of events and knowledge available. Third, Reliability/dependability, this requirement specifies that when using the observations or data presented on the thesis that a third party would obtain a similar or same results as the one presented.

Given the fact that we did not use a specific case for this study we have provided enough information regarding the process for understanding and collecting our data. Further we have included an interview guide and what was the background of the interviewees to understand the social construct in which they interact. Fourth, Generalizability/Transferability which specifies that the thesis findings can be applied into other settings or cases for further study. As stated with the other requirement, the scholarly best practices and sources have created the foundation and guide for this thesis.

Due to this, the findings and data of this thesis can relate to other research to further understand the body of knowledge. As a result, we have included and followed methodological requirements from the design to the presentation of our findings to ensure the scientific quality of this thesis.

4 Results

The following chapter presents the thesis findings from the qualitative study. The findings are divided into seven themes with some having their own sub themes that go hand in hand with literature review and research process. The themes highlighted in findings are cybersecurity, cybersecurity, and remote work, cyberthreats in a remote environment, employees' cybersecurity learning process, employees' behaviour, and the cybersecurity program's continuous improvement.

4.1. Cybersecurity (CS)

Two questions were included to validate the knowledge of the participants in terms of cybersecurity. Firstly, we asked them about the concept of cybersecurity. It was interesting to confirm that all of them have an adequate idea of what is cybersecurity and what scope its practices can protect. However, their level of knowledge varies as reflected on their explanations. For instance, R2:12 explained several layers such as infrastructure, applications, network, and cloud. Particularly, this could be perceived as a valid insight given that this participant has previous experience implementing applications that involve security in IT companies. Additionally, many of the participants such as R1:14, R3:22, R4:14, R5:20 mentioned a general understanding of what is cybersecurity.

Secondly, the question to collect their experience about cybersecurity gave us some idea if they have implemented cybersecurity practices or experienced the risk of facing a cyberthreat. R5:22 mentioned explicitly the importance of training to learn cybersecurity concepts. R3:24 explained its experience receiving phishing emails that are under control because there is knowledge to figure out if they are really a threat. The rest of them (R2:14, R4:16, R1:14) show how the cybersecurity process or risk mitigation to avoid threats are included in the usual business process they work on.

4.2. Cybersecurity and Remote Work (CRW)

The set of questions for understanding cybersecurity and remote work practices included control and organisational questions. The control question was focused on knowing what practice or experience the interviewee had with remote work. Further, the next three questions were targeted to know the organisational practices and preparedness regarding this topic. Interestingly, respondents R2, R4, R5 mentioned they already had the remote work alternative for their respective roles. The remote work these respondents have was limited to a couple of days or hours a week and this practice was limited to specific roles. R2:17 stated the possibility for other employees to work remotely, but it would require an approval process and in just some instances.

A different view from respondent R1:8 mentioned that the reason they did not have remote work was that it would not be considered a social environment. Further, the same respondent stated that this had to evolve because of the way of work during the pandemic. Furthermore,

for the response from the organisation in terms of enabling remote work, respondents R1 and R5 had the same practices of signing an agreement about being responsible for the organisation's equipment. R2:21 stated that the response was the same policies that the company already had. Further, R4:25 mentioned that besides the general recommendation that is a common practice for cybersecurity, they also requested to have a VPN to simulate the in-office environment. In addition, respondents R4 and R5 mentioned the difficulty of setting a schedule and limit of hours for work related activities.

4.3. Cyberthreats in a Remote Work Environment (CTR)

The set of questions for analysis of cyberthreats was intended to confirm the increase of cyberattacks among organisations in a remote work environment and review the awareness from participants regarding these attacks. All responders except for R1 stated a form of cyberattack within their organisation. Phishing emails were reported in a remote work environment by R2, R3, R4, R5 and respondents R3:24, R4:33 stated a noticeable increase within this specific type of attack during the pandemic. Also, in the case of R2:27 the respondent stated that multiple employees did access the phishing email and log their information.

Further, R4 reported password related issues due to weak security infrastructure. All respondents mentioned a concern regarding the employees of the organisation using their equipment for other purposes beyond job related activities, and the threat it posed to the organisation systems. In the case of R2 the respondent mentioned that any non-related job activities need to be reported to the security team. Within the countermeasures for cyberthreats, R1 who was the only respondent with no episodes in cyberattacks explained that in their organisation they use a ***virtual desktop*** instead of the regular equipment to perform their task.

Along with R4, R1 also mentioned the use of VPN to build a secure connection and simulate the office environment. All the respondents mentioned the use of security updates or antivirus as part of their strategy against cyberthreats. In addition, R1 and R5, stated they believe their infrastructure is enough to protect them from cyberattacks. R2, R3, R4 mentioned a ***lack of good infrastructure*** against cyberthreats.

Furthermore, R4:29 stated that after two years of making mistakes it feels the infrastructure has improved. Moreover, respondents R3 and R5 mentioned that they would not have enough knowledge on how a cyberattack impacts the organisation and they would not know how to identify the attack. All respondents agreed that the remote work environment includes vulnerabilities in terms of cybersecurity. Furthermore, the vulnerabilities on the responses are highly related to the employees' usage of the systems. R5 in reference to this mentioned the lack of a ***control environment*** for employees.

4.4. Cybersecurity Governance (GOV)

The section targeting cybersecurity governance was aimed to test the relevance and comfortability of employees with the security policies from the organisation. The policies targeting the users within the organisations of the respondents seems to provide the basic knowledge about cybersecurity best practices. All respondents felt the policies regarding

cybersecurity were easy to understand. In terms of relevance for the roles in the organisation R4:36 mentioned that it still needs to be improved to make it relevant for the role.

Also, R2:32 made a comment that due to his ***extensive experience*** the content was easy and relevant. R2:14 was the only respondent that mentioned a security standard OWASP related to policies from the organisation. All respondents' answers show a strong correlation between training and learning about organisation policies. R3:43 stated that the policies were easy to understand due to the fact they have ***received training***, if not there would be terms that would not be easy to understand for a user.

4.5. Employees' Cybersecurity Learning Process

4.5.1. Cybersecurity Awareness (AW)

This section was aimed to review the intention of the organisation in providing relevant cybersecurity information and the perspective from the participant. The most positive answer regarding the awareness of cybersecurity information came from R1:30. This respondent stated that since the ***onboarding process*** in the organisation there is a whole initiative to make sure the employees are aware regarding the policies and best practices for cybersecurity. R1:14 stated also that the information received from the organisation has ***motivated*** them to follow best practices outside the work setting.

In addition, R2 and R4 stated that they believe they have enough knowledge, but it is due to their work experience. In the case of R2:29 the reason is in some cyberattacks to the organisation there were multiple employees that did not have enough knowledge. R4:40 stated that the knowledge varies depending on the tier of the employees, for entry level employees the knowledge and engagement is low.

Furthermore, R3 and R5 stated having basic knowledge and some best practices but that from its perspective there is still a lack of knowledge. R5:46 further stated that due to its lack of proficiency in the topic, if something is not clear there is supported to obtain more information. From all respondents, there is a level of awareness regarding the cybersecurity policies and best practices, but it is not conclusive that it comes from their current organisation. Also, among all respondents the most common tool to build awareness is using ***web-based training***. Further, R3 and R4 stated that the organisation will send emails with cybersecurity information or policies to reinforce the practices with their employees.

4.5.2. Cybersecurity Training (TR)

A summary of the responses related to the duration, frequency, type, and content of the training is shown consolidated in Table 7.

Table 7: Cybersecurity Training Data from the Interviews

Respondent	Duration	Frequency	Type	Content
R1	4 hours	Yearly	Web-based. Interactive with accumulation of points to complete it.	Updated yearly and specifically based on new threats faced in a remote work environment.
R2	2 hours	Quarterly	Web-based. Interactive through videos. Questions must be answered in the middle and at the end of a video.	Periodically updated and aligned to the region. Not included new content about remote work.
R3	45 minutes	Yearly	Web-based.	Not included new content about remote work.
R4	40 minutes	Quarterly	Web-based. Interactive using questions to ensure the attendee is understanding the concepts.	The content was updated for remote work.
R5	2 hours	Yearly	Web-based. Interactive using videos and tasks.	The content was updated with some examples more specific for remote work.

Training is a relevant practice that was solidly considered in the interview guide. The respondents mentioned interesting facts and perceptions about their experience with cybersecurity training while answering questions.

In terms of type of training, all the respondents commented that they are using a ***Web-based*** option which opens the possibility to drive interaction between the participant and the content. For that reason, they do not only have to see and listen to the videos but also answer questions to confirm that the content was understood. This is a relevant insight confirming that all the organisations of this sample are using ***interactive*** ways to ensure the transmission of the concepts. What is more, according to R2:42, the diploma obtained from this training is tracked through the organisational system.

Regarding the content, R2:67 and R4:76 commented that it would be important to receive the training in ***native language***. Sometimes, the content is not fully captured by the participants

given that their training language's level is not ideal. Particularly, we should consider that they described that their organisations have sites in different countries.

With respect to the frequency, three of them (R1:30, R3:52, R5) commented that the training is done yearly and two participants (R2:36, R4:45) mentioned that they performed it quarterly. In terms of duration, there are different responses. Firstly, R1:32 stated that the training takes half a day to be completed. This was the longest training but maybe the requirement to do it in a yearly way could explain the long duration. Secondly, R2:32 and R5:50 pointed out that the training can take around two hours. Particularly, R2 mentioned that the training usually takes him usually less time, around 30 minutes, given that he has previous and extensive knowledge about cybersecurity. This could be an indicator that for people with more experience therefore a different training format could be a suitable option. Finally, R3:50 and R4:45 stated that the duration of their training is around 45 minutes.

What is more, an interesting aspect to consider is that some respondents (R3) mentioned that they needed to follow cybersecurity ***duplicate training***. One from their organisation and one from the client they are working with. This could be interpreted as a reason to generate security fatigue.

Furthermore, we tried to specifically ask about what was different in the training received while they were working remotely in comparison with the onsite traditional scenario. Participants R1:38, R4:51, R5:54 stated that the content of the new remote training included specific information about the new threats faced while working remotely or specific points such as the careful decision to use a public network. Moreover, all the participants felt that there is not a difference receiving the training remotely than in the office. Basically, R1:36 and R4:54 commenting explicitly that as the training is Web-based then they don't feel a difference.

In terms of the relevance of the content, all the respondents except R3 think that the content is relevant for their daily routine. Specifically, in the case of R3:60, this interviewee considered that as the topics in the training were not updated with specific issues regarding remote working therefore the relevance is not guaranteed.

Additionally, we asked the employees what they think about the ***personalisation*** of the training. All the interviewees expressed a positive attitude about this because the idea to have a personalised content could generate different benefits. Firstly, R1:42 explained that it could bring a ***sense of identity*** if an employee sees information more accurately of the information they manage. Also, R1:42 stated that the current division the organisation has implemented by department or region is working successfully. Secondly, R2:48 and R4:56 thought that this personalisation could be based on the ***access level*** of each employee because it varies depending on the role. Finally, R5:60 expressed its thoughts in a similar way to the previous respondents but also mentioned that it would imply a ***tremendous effort*** for some companies where the number of employees and the size is big. employees.

4.6. Employees' Behaviour

As was mentioned in the literature, to have a complete perspective of the cybersecurity learning process, it is important to analyse the motivational factors. For that reason, five questions were

strategically designed to get insights from the participants. The objective is to understand better how they feel about meeting the cybersecurity guidelines.

Self-efficacy (SE)

Firstly, in terms of ***self-efficacy***, the question was to know if the interviewees feel engaged to follow the cybersecurity guidelines provided. On one hand, three of the respondents (R1:44, R4:59, R5:65) answered that they are engaged mainly because they are aware of the possible risks and the importance of the topic. On the other hand, the participant R2:51 does not feel engaged due to the daily experience when other colleagues use their personal laptops for work activities which is counter indicated by the organisation. R3:71 explained that the lack of reinforcement of the content delivered in the yearly training blocks the participant from developing a real engagement.

Deterrence (DT)

Secondly, related to ***deterrence,*** we tried to figure out if the employees are aware of the possible consequences if they do not follow the cybersecurity guidelines. The interviewee R1:44 commented directly about the sanction given that is aware of dramatic consequences that are ***severe legally*** for the employees in those cases. R2:53 and R3:75 answered that they also feel stopped to break the guidelines but for two different reasons that are more associated with the public image of their organisations. One is the possible loss of ***company prestige*** and the second one is the leak of ***customer information*****.** Those insights are interesting because we can observe that some people follow the guidelines in a more organic way where they not only feel obligated due to the applicable sanctions. Finally, R5:67 follows the guidelines because this participant does not consider itself as technological savvy therefore could be considered as a possible aim of cyberthreats that want to avoid.

Security fatigue (SF)

Thirdly, regarding ***security fatigue***, we asked the participants if they feel overwhelmed trying to follow the cybersecurity guidelines provided by the organisation. The answers were interesting because the participants not only talked about their personal experience. What is more, they added information about their perception of other colleagues. In general, all the participants (R1:46, R2:57, R3:81, R4:61, R5:70) answered that they do not feel overwhelmed. However, R2:57 and R4:61 commented proactively that they know about other colleagues that feel overwhelmed.

Specifically, R2:57 mentioned that some members of the team express frustration because ***many approvals are needed*** for a ticket requesting access to a tool. Sometimes, this also happens because the access requested is to a client platform so the level of security could be even higher. In the case of R4:61, the perception is generated because for ***new employees*** like agents, the big set of rules already established could be overwhelming. This last perception is interesting because this participant worked as an agent in this company before also. Moreover, a particular lecture can be realised here because R1:25 mentioned the ***slow updates*** released in

the computers to ensure they are protected could be frustrating for the employees even though at the end it is very secure. In conclusion, it is insightful to know that some people feel comfortable but at the same time they know of other co-workers that do not feel the same.

Neutralisation (NT)

Fourthly, ***neutralisation*** was also evaluated, posing a specific scenario to the participants where they theoretically face a critical business situation to observe if they will achieve a business goal even if it risks the cybersecurity policies of the organisation. All the interviewees answered that they would not risk the policies. R1:48, R2:59, R3:83 answered that they would look for ***escalation***, ***negotiation*** with other people in the organisation looking for a viable alternative that does not break the policies. R4:66 participants will try to ***evaluate*** if the requirement came on time to be managed with all the compliance levels that must be considered. The participant R5:72 mentioned that will explain later why the task could not be completed. As a result, this is an important indicator that the participants prioritise cybersecurity even though the business routine could put them in compromising situations.

Work and personal context (WPC)

Finally, a practical question was included to know if the participants cover their web cameras while using a computer. This was asked to know more about the existing difference between the ***work and personal context.*** With respect to the work laptop, all the respondents affirmed that they cover their web cameras. Also, they said that this is not a security policy, so this is more for a privacy aspect just to avoid being seen if the camera is activated accidentally by them. In the case of the personal laptop, R1:52, R3:95 and R4:72 mentioned that they do not cover their webcam but R2:65 and R5:80 have the practice to cover it. In consequence, we can observe that the participants are more concerned for the work security context than the personal one.

4.7. Cybersecurity Program's Continuous Improvement (CI)

This section was looking for new ideas of how to improve the cybersecurity learning process of the employees. We gave participants an opening to share ideas or initiatives that could complement the actual program at their organisations. Some of the ideas collected are:

- R1 mentioned that being more specific about what personal staff could be done using the work computer would be complementary.
- R1 also mentioned that it would be interesting to know the correct way employees could portray themselves in social media stating that they belong to the organisation.
- R2 stated that the duration of the training videos must be concise and not too long.
- R3 and R4 mentioned that having periodical meetings to talk about cybersecurity might be helpful because people will pay more attention. What is more, these meetings could implement different formats such as conferences or focus groups.

- R3 also commented that to use different communication channels and not only email could contribute to ensure that the messages reach more people.
- R2 and R4 pointed to the importance of using the local language to ensure that the participants capture the ideas presented in the training.
- R5 said that try a different format for the training duration and frequency. For instance, to deliver one hour training each 6 months instead of 2 hours training once a year could be beneficial.

Furthermore, a sorting exercise was presented to the participants to know their feelings about the possibility of implementing Evaluation and Feedback, Gamification, or Continuous Monitoring to complement actual cybersecurity programs. The results are presented in Table 8.

Table 8: Cybersecurity Continuous Improvement - Sorting Exercise Results

Priority Order	**R1**	**R2**	**R3**	**R4**	**R5**
Evaluation and Feedback	3	2	3	2	2
Gamification	1	1	2	1	1
Continuous Monitoring	2	3	1	3	3

As the main conclusion, we can see that ***Gamification*** was considered as the most relevant option with the first level of priority indicated by all the participants except R3:111. Particularly, R3:54 is also the only one participant who commented that its company is using gamification in the training therefore this could be a reason to not place it as the first level of priority because it is already implemented. With respect to the rest of the participants, R2:70 referred to gamification as an interesting option to ***engage people***. Moreover, two of them (R4:79, R5:102) stated that it would be attractive for ***entry level positions*** and ***young people*** which are the majority at their organisations.

Evaluation and feedback were chosen as the second option by three respondents (R2, R4, R5). R4:79 and R5:102 agreed that employees' participation to improve the program could be a key factor. What is more, R5:102 commented that it could be beneficial that they feel as they are contributing to the company. R1 gave an explanation why this option was listed as the last one. Based on R1:58's experience, the collection of feedback is a hard activity if people are not interested in answering surveys or similar formats.

Continuous Monitoring was selected as the last option in priority by three respondents (R2, R4, R5). R3:111 placed it as the most important option arguing that it is highly relevant to know what the most impactful threats are so the employees could pay more attention to them. In the case of R4:79, the reason to put it in last place is that it will be ***more expensive*** and consume more resources to implement this initiative.

5 Discussion

The following chapter presents the thesis discussion which makes contributions to both research and practice. In theory, we have identified some factors, elements, challenges, and issues that are important to be noticed by the scholars. Whereas in practice, we have identified specific practical points that should be acknowledged by practitioners in the field.

5.1. Implications to Research

Cybersecurity

The empirical findings obtained when asking the participants about the concept of cybersecurity and their experience let us derive conclusions that have implications to research. Firstly, we can conclude that today, based on this sample, most people in an organisation are aware of the importance of cybersecurity and its general concept. What is more, some of them referred to the three properties stated in the CIA triad by Von Solms and Van Niekerk (2013) of confidentiality, integrity, and availability. Even though the terminology used by the interviewees differs, they commented about examples where it is important to ensure these characteristics.

Additionally, they also specified the scope of cybersecurity while referencing the systems, also technology that they use in their daily routine, or how it is connected to some business processes. This is aligned to the differentiation proposed by previous authors which is clearly stated in Figure 1 (Von Solms & Van Niekerk, 2013). Therefore, we could understand that for the respondents, cybersecurity is not the same as traditional security concepts because they know that it is linked to a certain division existing using ICT. With this in mind, we see the need to envision cybersecurity understanding from novel perspectives in the future and that traditional views might not capture the whole perspective.

Cybersecurity and Remote Work

The answers from the respondents support the literature about how the organisations facilitated all employees to work remotely due to the pandemic. Further, the literature suggested that many organisations did not have a procedure to have a remote workforce (Arabo, 2021). However, most of our respondents stated that a practice of working remotely was in place within their organisations for specific employees. Further, the same respondents stated a lack of proper infrastructure or control in a remote work environment which then would put in doubt the security practices the organisations had before the pandemic. This would need to be addressed within the governance the company has for these measures.

The inability to effectively scale up and secure the already in place practice of remote work in some organisations need to be also improved within the governance measures. The literature has also been vocal about the emotional factors within the remote work mixed with the pandemic and how it can affect the compliance to cybersecurity policies (Naidoo, 2020). In this case, among our respondents there are three cases we can mention. First, the lack of bonding among team members. Second, difficulty separating work with personal life due to increased

work hours. Third, difficulty getting support in terms of IT within the remote work context. Therefore, some practices along with increased employee support needs to be improved considering that the hybrid work environment is possible to continue.

Therefore, we suggest to researchers to consider emotional factors and its specific applications that could affect the remote work environment. This should be considered in planification of cybersecurity implementation in a remote or hybrid work environment.

Cyberthreats in a Remote Work Environment

In terms of cyberthreats in the remote work environment, the literature suggests an increase of specific attacks during the pandemic (Naidoo, 2020). This agrees with our respondents who stated the increase of interaction with these types of cyber-threats. Further, among our respondents the most common threat was phishing emails. In addition, even when non categorised as insider threats by our respondents, all of them stated the misused by employees of the company equipment and network for activities unrelated to their job. Even when some restrictions and policies were in place all respondents mentioned that compliance in that area was not as effective. As shown with these vulnerabilities, organisations still need to find a comprehensive way to address this issue regardless of the work setting.

Cybersecurity Governance

With all respondents we see a strong support of the literature which states that one of the most effective tools for managing the employee side of an organisation are policies, frameworks, and best practices for technical and non-technical users (Guo, Wei, Huang & Chekole, 2021; NIST, 2022). All the respondents showed ***basic knowledge*** among the policies for cybersecurity within their organisation and one of the respondents provided a security framework used. This further strengthens the effectiveness of these methods to start communicating with employees regarding cybersecurity information and practices.

Cybersecurity Awareness

Scholars stated that there are two main intentions regarding a cybersecurity awareness program. First, provide information to employees and second motivate for behaviours or practices to change (Siponen, 2000; Bada, Sasse & Nurse, 2015). Among our respondents even when a level of awareness of cybersecurity is clear, there is a discussion regarding how organisations are building this trait. There is a perception from some respondents in which they categorise the awareness and knowledge they have because of multiple years of experience or interactions with cybersecurity.

Further, the respondent mentioning within entry level or low tier employee's awareness is within low levels. The literature is vocal about the importance of the learning process in terms of cybersecurity to develop awareness and change. Only one respondent stated that due to the information provided was relevant for their operations it built a motivation to extend those practices to a personal level. This respondent also stated the effectiveness of engaging employees from the onboarding process. Therefore, it would be important to analyse if the awareness is built upon repetition or if there are other methods that would be effective in increasing awareness. Also trying to engage employees since the beginning of labour relations should be reviewed under the governance of the organisations.

Cybersecurity Training

The personalisation aspect as a possibility to improve training was an important point mentioned by several of the participants which promoted an interesting discussion during the interviews. The respondents showed positiveness about this aspect because it could increase the sense of identity of the employees or prevent overloading them with unnecessary concepts in a training which can be performed for instance on the access level of each employee. These answers confirmed the theory analysed in the literature review mentioning that the design of a content which does not consider the preferences of the participants can generate lack of engagement (Chowdhury, Katsikas & Gkioulos, 2022).

What is more, the studies we reviewed about personalisation are quite recent which indicate its appearance as a novel topic that is being implemented already by only some organisations as was also discovered in this thesis (Chowdhury, Katsikas & Gkioulos, 2022; Pattinson, Butavicius, Ciccarello, Lillie, Parsons, Calic & Mccormac, 2018). A possible reason to explain this was also mentioned in a paper stating that sometimes organisations do not have the sufficient capacities or resources assigned to the cybersecurity endeavours (Sadok, Alter & Bednar, 2020). This same motive was mentioned by the participant with the most working experience who mentioned that it could imply a tremendous effort for some companies. Therefore, we concluded that experienced employees might observe the personalisation effort as a difficult goal to be achieved even though they recognise it as an effective solution.

In summary, the findings demonstrated a good employees' perception about personalisation but there is still little empirical research that has studied the successful or not implementation of it in organisations. For that reason, we recommend the personalisation aspect to researchers as a worthwhile focus of study that might contribute to improving training experience. We also consider that there are already modern options in the market to realise these implementations (Gartner, 2021b). Therefore, more companies might be suitable for these types of studies.

Another interesting point mentioned by the participants was the duplicate training experience. This occurred when people must follow the security policies of their actual organisation but at the same time the guidelines provided by a client organisation they are working with. Thus, it is important to clarify that specifically this scenario will happen in organisations dedicated to the consultancy business. Furthermore, in the literature there were not many previous studies about this scenario. Hence, it would be insightful to conduct a study focused specifically on workers or organisations that work under this context to find if this could be a reason to generate security fatigue as was also mentioned during one interview.

Cybersecurity Program's Continuous Improvement (CI)

In general, this section helped us to confirm an idea previously mentioned in the literature review. Sadok, Alter & Bednar (2020) stated that in some organisations the actual practices do not demonstrate a high level of security. For that reason, the initiative to listen to employees and collect their feedback is a key activity. Chapter 4 summarised some of the possible improvements proposed by the respondents.

The main insight is that gamification is looked at as a beneficial tool to increase the engagement of employees, especially if many of them are young or at entry level positions. This finding is solid because one of the participants confirmed to us that the actual implementation of gamification in its company is helping them. For that reason, further research focused on the

use of gamification as a method to increase the success of a cybersecurity program would be beneficial for the literature.

5.2. Implications to Practice

Remote Work and Cyberthreats

From the respondents we found practices to improve the cybersecurity environment and to increase employee's confidence in their environment. Among the respondents, the one with the most positive experience in terms of security told us about some good practices. The first is the use of a cloud environment, a virtualization according to the respondent allows to provide a control environment that has better results in terms of cybersecurity. Second, the use of a Virtual Private Network according to our respondents creates the perception of a more secure infrastructure for all the employees working in a remote context and the literature would suggest this should be a practice in place for cybersecurity.

Further, the emotional factors seem to play an important role in the perception of the employees. The literature suggests a relation between emotional factors and compliance to cybersecurity. In the case of our respondents the impact was directed more in terms of teams and support. Interestingly a practice that was effective among one respondent was the inclusion of a well-being program within its employees. This created an environment of support where employees felt prioritised. According to the respondent this increases the engagement in job related activities and in following the policies.

Cybersecurity Training

Firstly, one of the main conclusions observed in the interviews was that Web-based training even before the pandemic setting is the predominant option chosen by all these organisations to implement cybersecurity training. This was previously stated by Wilson and Hash (2003) as an ideal option for a distributed environment that could encourage the interaction. All the participants mentioned that this training format is considered interactive because they need to pay attention to the messages to complete tasks during the process.

What is more, we found that the participants whose training frequency is higher, every three months, did not mention feeling uncomfortable with the periodicity. Moreover, they pointed out the importance of having relevant content in the training. This confirmed what was previously presented by Pattinson et al. (2018) who stated it is more important to have a training aligned to the participant's learning preference than the frequency defined.

In terms of training content, the literature suggested possible topics that could be considered by organisations (Wilson & Hash, 2003). Particularly, the empirical findings showed that employees feel more engaged when they interact with an updated content that included specific cybersecurity recommendations for the remote work environment. This could be insightful for practitioners who will follow the literature recommendations but also should be conscious of the importance of a new context.

Another interesting finding is about the importance of the language used in the training. According to two of the interviewees, a topic like cybersecurity which is vital to avoid risks

should have the option to be delivered in the employees' native language to ensure that the message is correctly acknowledged. As stated by one participant, even when the English knowledge is required for their jobs, this could add a relatability aspect to generate a stronger connection between the participant and the organisation. The literature review presented extensive information about the techniques and formats for delivering a training (Wilson & Hash, 2003). However, we think it could be complemented with the language availability which based on the empirical findings play a crucial role during the process.

Employees Behaviour

Firstly, in terms of self-efficacy, the way these concepts were evaluated was to understand the engagement respondents must follow the cybersecurity guidelines and how they feel about the consequences caused by not following the policies. We could find that effectively the behaviour of some employees is modified after the security training. Specifically, they mentioned that they feel engaged because they are aware of the possible risks that the topic involves which confirm the theory previously stated by scholars (Bulgurcu, Cavusoglu & Benbasat, 2010).

However, it should be important to emphasise that the respondents considered in this thesis have an accumulated level of experience which may influence the predisposition to modify their behaviour. Additionally, the lack of reinforcement and the effect provoked when one employee sees others not following the rules were pointed as possible causes of reducing the engagement. Both findings let us conclude that security training is effective but ensuring that most employees take them would be beneficial to not generate a contrary effect if some of them continue breaking the policies.

In terms of deterrence and neutralisation, the scholars mentioned that an employee could be restrained to realise a security fault if a sanction is clearly communicated by the organisation (Straub & Wekle, 1998; Willison & Warkentin, 2013). Even though, one of them mentioned that there are several legal consequences for them if the policies are not followed, most of them referred to other reasons. A possible loss of company prestige and a leak of customer information were pointed out as causes. This could be interpreted as a strong connection between the employee and the organisation assets.

Therefore, the deterrence effect is achieved through a more organic way where sanctions are not the main reason to follow the guidelines. With respect to neutralisation, a specific situation was proposed to the participants to validate if they will justify an action by minimising the impact (Siponen & Vance, 2010). The main conclusion obtained was that respondents in a critical situation will avoid breaking a cybersecurity policy. The respondents talked about re-evaluation, escalation, and negotiation as first options before deciding to not follow a cybersecurity policy. As a result, both theories were not confirmed as predominant in the behaviour of the employees. However, its relevance could not be discarded due to the size of the sample considered for this qualitative thesis.

According to the theory, some people could perceive the security controls as barriers, and this might generate a security fatigue sensation (Furnell & Thomson, 2009). The empirical findings confirmed that some employees feel that this occurred through the description of some events that they or their colleagues experienced. In the first instance, none of them said directly that they felt overwhelmed. However, they have a sensation that for novel employees who see for the first-time cybersecurity policies could be a hard topic. Additionally, the list of approvals needed for some tasks and the slow updates that work laptops experimented during the remote

work are clear evidence that might originate fatigue. In conclusion, the theory of security fatigue was present in these organisations and must be considered as a relevant variable for practitioners in the future as more policies are added.

Finally, we had a question to evaluate the work and personal context. The literature mentioned that today more people are aware of cybersecurity knowledge because their personal experience encouraged them to investigate more about the topic (Öğütçü, Testik & Chouseinoglou, 2016). According to the respondents, all of them cover their work web camera. However, they do not follow the same practice with their personal devices. What is more, some organisations are already including a physical restriction in the devices to ensure the camera is blocked by default. Therefore, the level of awareness and risk taking differ from the individual practices to the job environment.

6 Conclusions and future work

The following chapter aims to summarise the conclusions obtained in this thesis that are connected to the research question proposed initially.

6.1. Conclusion

From the literature, it is known that there are vulnerabilities in cybersecurity associated with the remote work environment. Furthermore, employees' awareness plays a vital role in supporting the cybersecurity strategy among organisations. This thesis found a strong relationship between awareness and training among the employees' perspective. In addition, since a remote work approach might continue for work practices, a focus on the perspective of employees in terms of awareness within this context is important. Thus, the research question that drove the study of this thesis is:

What cybersecurity aspects are more relevant and/or relatable for remote working employees?

Among all the themes explored within this thesis we have identified aspects that allow us to answer the research question. Specifically, we identify the ***relevant*** aspects as important and appropriate to the current context for the employees. Also, the ***relatable*** aspects in which there is a connection or engagement with a topic from the employees' perspective.

Cybersecurity and Remote work

There is a sense of vulnerability from the part of employees even though tools and some infrastructures are available. Due to the lack of control of the remote environment the perception of vulnerability increases. Thus, it is fundamental to address the perception of employees regarding the environment in which they work.

In addition, emotional factors play an important role in the adaptation of employees to a remote work environment. For instance, feeling the connection and engagement with their teams, and as a result the organisation. It is important to take a holistic approach in terms of the engagement of employees considering that emotional factors can play an important role in cybersecurity compliance.

Cyberthreats in a Remote Work Environment

Due to lack of control from the environment there is a misused from the organisation's equipment from employees. This can result in increased insider threats and widespread vulnerability. Also, one of the most important attacks from social engineering, phishing emails seem to be increasing. Thus, it is relevant to build awareness about best practices, policies, and actions in such cases.

Cybersecurity Governance

Cybersecurity policies and best practices should be replicable and scalable so organisations can respond in a more effective way to times of crisis. Moreover, in terms of policies and practices, it is important to effectively engage new employees at the organisation and in the workforce. This is since people with more experience feel more comfortable following and understanding the policies than new employees. It would be relevant to build connections among employees in this topic. Having this type of engagement would improve the compliance and effectiveness of cybersecurity.

Cybersecurity Training

Firstly, the training delivery technique chosen for a remote work context is of strong relevance for the employees. Web-based training is the predominant option nowadays and is positively perceived as was confirmed in the research. At the same time, the technique used could be also relatable for employees given that the interaction demanded during the process helps to increase the engagement.

Secondly, the language used to deliver the content is a relatable aspect. The main reason is that not all the employees have the same level of proficiency in a different language. For that reason, facilitating a native language option could be a key factor to ensure that the message is acknowledged.

For instance, the possibility to differentiate the content based on roles helps to generate a connection with the employee. As a result, they will feel that the content is useful for their daily activities. Moreover, a frequent update of the content indicates a feeling of reinforcement which is valued by the employees.

Employees' Behaviour

Security fatigue is a relevant phenomenon which is predominant for novel employees. Specifically, employees who experiment for the first time the understanding of cybersecurity policies could find it laborious. Furthermore, long processes required to obtain approval such as access requests to organisation's systems or assets can be felt as unnecessary. Therefore, special attention to the experience of novel employees can be a key factor to increase the success of cybersecurity programs.

Cybersecurity Program's Continuous Improvement

Regarding possible options to improve a cybersecurity program, gamification is the option most interesting for employees. It is relevant because it can help to enhance the user experience of the process and motivate participants based on possible rewards. Moreover, it is relatable for a sector of employees such as young talent or at entry level positions who are familiar with game techniques thus, they can establish an easy connection with the tool. For that reason, its inclusion in a cybersecurity program could play a crucial factor.

The Table 9 below concludes aspects that are relevant and/or relatable.

Table 9: Relevant and/or relatable aspects for remote working employees

Theme	Aspect	Consideration
Cybersecurity and Remote work	Emotional factors	Relatable
Cyberthreats in a Remote Work Environment	Exposure to cyberthreats	Relevant
Cybersecurity Governance	Previous Practices	Relevant
	New employees' engagement	Relevant
	Trust in cybersecurity practices and infrastructure	Relevant and relatable
Cybersecurity Training	Language	Relatable
	Training delivery technique	Relevant and relatable
	Content according to the role	Relatable
Employees' Behaviour	Security Fatigue	Relevant
Cybersecurity Program's Continuous Improvement	Gamification	Relevant and relatable

6.2. Future Work

This thesis can be further developed in at least two ways. First, studying employees' behaviour by using metric systems that captures their knowledge and awareness during an actual simulation of a cyberattack. This can contribute to a better understanding of whether preparedness makes a direct impact on how organisations succeed to keep good security in place during unprecedented times, like the COVID-19 pandemic.

From a methodological perspective, a sample with diversity in terms of tenure in the organisation would be an interesting input to see how young employees versus senior employees act in environments where they may be caught up by surprise. Particularly, the evaluation of employee behavioural theories to find which of them are predominant with different groups of participants would help to drive interesting contributions to the literature.

Finally, an aspect mentioned during the research but not being a focus of the study was the communication approach used by organisations to reinforce policies and guidelines. It would be complementary to study the experiences of leaders in organisations who are usually called to spread the cybersecurity guidelines and responsibility to employees in their teams.

Appendix 1 - Interview Invitation Outline

Thesis: Cybersecurity engagement in a remote work environment

Thank you for your time. Your insights will be quite useful for the research we are conducting as part of our master's Thesis.

The interview will cover different topics related to your experience with cybersecurity while working as an employee in a remote work environment. The topics are as follows. Some of the questions are presented so you can be prepared in case you don't have an immediate memory of your interaction during some cybersecurity events.

1. **Cybersecurity**

What is cybersecurity from your perspective? What is your experience with cybersecurity?

2. **Cybersecurity and Remote Work**

Did your organisation provide instructions when the new remote work environment was stated?

During your remote working journey, did you have an experience with cyberthreats?

Do you feel that you have enough tools to be protected against cyberthreats?

3. **Cybersecurity Awareness and Training**

Were cybersecurity policies communicated to you?

Did you receive cybersecurity training? Tell us about your experience (duration, frequency, type). What do you feel was different from cybersecurity training facilitated while you were working at the office?

The topics included in the cybersecurity training were relevant for your daily routine.

From your perspective, what are the possible consequences caused by not following cybersecurity policies?

While answering these questions, you can provide different details related to your experience. This will enrich our study. We ensure that all this information will be managed anonymously and confidentially. A transcript of the interview will be shared with you after the session so you can confirm that the content is aligned to what you answered.

Appendix 2 - Calendar Invitation

Hi XXXXXX,

Thank you for your time! Let's have a conversation about cybersecurity awareness. Your experience will be a great input for our master's Thesis. We are looking forward to meeting with you!

César / Jose

Appendix 3 - Transcript Information

Hi XXXXXX,

Thank you for your time! We were able to get valuable information based on the interview we had. As part of the scientific quality and ethical considerations of our thesis, we are sharing with you the anonymised transcript of the interview content.

Please let us know if you would like to edit or omit a specific part of this transcript if you consider it does not express accurately what you tried to communicate.

Thanks for your help!

César / Jose

Appendix 4 - Pilot Interview

Date: 2022-04-20
Interview length: 33:33 minutes
Language: English
Participants: Pilot Respondent 1 (P1), César Vásquez (CV), Jose Gonzalez (JG)

Row	Person	Text	Code
1	CV	What is your role at work?	
2	P1	In my current work I'm a software engineer in a tech company	
3	CV	how many years have you been there or in total your years of experience in the industry	
4	P1	Well, I started in 2015 so I guess I have eight years of experience in the industry, and in the beginning, I worked as an Android developer.	
5	CV	How involved are you with technology to perform your job activities?	
6	P1	Yes, I use many tools such as JIRA and some basic systems for management and for development.	
7	CV	Did you work remotely before the pandemic?	
8	P1	Well, I was in a kind of a mix up. I was working for three days in the office and two days at home.	
9	CV	Interesting, that is a good insight and from your perspective what was the most difficult aspect of working from a remote environment.	
10	P1	I guess my first concern when the pandemic started was how comfortable I will be to work fully remote at my home and how I can be both in a team. How could I interact with my team members? I was afraid that it wouldn't be the same as it used to be before the pandemic.	
11	CV	In the end how did you overcome that? Did you feel more comfortable?	

12	P1	Well at the beginning it was tough, I guess sometimes I wish I would be back at the office because I was bored in my Home Office but after one year of working remotely I started to get used to this and to a remote job and after that year I guess now I feel comfortable.	
13	JG	Now just to follow up the question in terms of the stress, do you think that the pandemic affected your work environment like were you stressed because of the pandemic and because of your work and did that affected you in any way?	
14	P1	Yes, it is really easy to be stressed and you know when people outside your home or your city are getting sick or also relatives got sick, but after the vaccines were released, I guess the stress were less and less and now I guess we are very safe.	
15	CV	Thank you for the answers. That's like an introduction so now our topic is cybersecurity training engagement in a remote work environment so we will have more questions regarding this theme. First, we would like to know from your perspective what is cybersecurity and what is your experience with cybersecurity.	
16	P1	well for me cybersecurity means how a company, or its employees protect sensitive information from digital attacks or maybe bad behaviour of the employees because they are not really trained in this matter. My experience about cybersecurity I can see that started at university when I had some courses that touch this IT or IT security or cybersecurity. I learned about cybersecurity, for example how to configure enough security in our local network, some applications about security and how to avoid SQL injection or SQL commands under web pages but that was the beginning. In my job experience I started to use these basic concepts of security to keep the sensitive data of our clients and our company safe.	
17	CV	thank you very insightful, JG you can continue.	
18	JG	Now we want to know some organisational aspects. You did mention that before the pandemic you had a hybrid model of working right, you have some days in the office some days remotely, so was that a case for everyone in	

		your company or only a few people have this benefit?	
19	P1	I guess only a few employees have this opportunity to work remotely some days but if I'm not wrong it depends on your seniority. I guess if you have a mid-level or more you were allowed to have one or two days at your home.	
20	JG	OK and when the pandemic happened everyone switched to remote right?	
21	P1	yeah so that's right.	
22	JG	OK thank you and from a company perspective when this change happened when everyone was remotely did the company provide any security policies that everyone needed to implement? Did you notice that the company provided you something?	
23	P1	Yes, the first level of security was to sign a form that you are not going to use your laptop or your machine for other things that are not related to your actual job, so that's the first thing. Also in this company we have some training each four or six months if I am not wrong and they explain to you how to behave in order to keep sensitive data safe. Also, how to avoid fishing, scamming, and other threads on the Internet. I guess they were really good because as an engineer maybe you think this is boring but I think it matters. It happened once to me that the company sent an email but this sender was not a trust sender it was a phishing email so I fill out all the information in this phishing page and after I click it continue they will say hey we want to let you know this was a training so you are good but be careful the next time. I realised it was really easy to get a phishing email so after that I realised how important this training is .	
24	JG	OK thank you, interesting, now specifically in remote work. Do you think that the work environment and the tools that you have are more vulnerable to cyber-attacks, do you think they open a window for cyber-attacks ?	

25	P1	Yes, in the IT environment we work with a lot of clients and with a lot of information. Well the company has many employees from different parts of the world and at some point you will have an attack. It's for sure, that is what I think. It happened to my company 2 months ago that all the passwords were changed and nobody knows how and why. But, I guess our environment, our IT environment is really affected by cybersecurity and all of their threats that are related to this matter.	
26	JG	OK thank you and that covers some of the questions that we have. You mentioned that you had training and the form that you have to fill out. Do you think that your organisation has given you enough tools and infrastructure to protect you from cyberthreats in remote work?	
27	P1	Well, I think it depends on my company right now. I guess I don't have a tool that I can use to report any kind of attack or any threat or any phishing email. But in a previous company that I was working at they had in outlook for our emails a button or plugging where if you receive an email that seems suspicious you can report to the security area so yes it depends. I guess I will be comfortable if I have more tools to report any threat like I don't know how to deal with that ransomware but as I told you it depends on each company.	
28	JG	Thank you for your answers so CV we can move to the practical.	
29	CV	Yes, this next part should be answered thinking in a remote work context, so our questions are about you. For you, are cybersecurity policies easy to understand and relevant for your role in the organisation?	
30	P1	Yes, I think so because as I told you before we have some training and also if I am not wrong we use OWASP which is a standard that we were studying on the training. We learned about applications security, network security, behavioural security, all this information was in our training.	

31	CV	yes, I found it, OWASP is an open web application for improved security information so I got the point. And well maybe this question was answered before as we would like to know if you feel that you have enough knowledge from your organisation to avoid a cyberthreat. But I think as you mentioned you have some tools, it could be better but still you feel comfortable with what you have.	
32	P1	Yes that is right, as I said to you it depends on the policies of the company and how they can improve the training that you receive from them in terms of security and how frequent the training is.	
33	CV	excellent so now move on to the topic which is cybersecurity training. So tell us about your experience with cybersecurity training, maybe about how much time you pass doing that, how often it is, and which type of training you receive in your organisation.	
34	P1	OK well in my actual job I only received one every six months which for me is not too good. In my previous job from around three years ago I've received like one every three months and as I told you they included the OWASP standard for security and it was really tough to solve because after each part you received some questions that you need to answer and 100% of the answers should be right if not you will repeat again the test. I guess it was not boring but difficult because you spend some time doing this training but I guess it is important because I don't think all the employees have a basic knowledge of security and as a company you need to care about your security.	
35	CV	Yes of course, and so if I understood it was like a web based or computer based training that you can take from the office and when you went to work from home you can take the same training it's that's right?	
36	P1	yes it was within a web page, and they give you a deadline if not your manager will talk to you and say just do it do it and so yeah I guess it was good.	
37	CV	So do you think something was different when you did the cybersecurity training at the office and then when you did it remotely, did you find a difference there?	

38	P1	I don't think so because as I told you it was only a webpage that gives you some classes about the OWASP standard and after it you need to answer some questions so it was not that different between doing this training at the job or at home.	
39	JG	Now just can I make a follow up, for example in terms of the content did you notice something different in the content like that mentions remote work on the training?	
40	P1	well I guess yes you're right because when we were working remotely I guess as we are using VPNs and we are outside the company so the security team of the company was always controlling , so I guess I received some information about some threats that can be trigger if I am working remotely so yes yes I barely remind some difference between training material when working at the office or working at home.	
41	CV	That's really interesting, thank you for that, and did your organisation ask you before the training which type of training is more suitable for you or they only send you the link to do?	
42	P1	well I guess it really depends the project that you are working on because if the client asked the the company that the employees that are working with client needs some specific training they will give you extra training but if the client doesn't care about how much information you have or about security then the company won't send you a training.	
43	JG	So we can say you have the training that your organisation provides you and the training that the client that you are working requested for, right?	
44	P1	Yes, there are two types.The ones that the client wants you to have and the ones that the company wants you to have. But all this training would also be on a web page, but it depends on the client.	
45	CV	Did you feel that the topics provided in the training were relevant for your daily work?	

46	P1	I think some training is something that I already know like how to log out from your computer each time if you are not in front of your machine or maybe if you just see a person that is not from your office inside and maybe report that. But other topics like all the threats that you can find on the Internet I don't know all the details about phishing email, ransomware so that for me was really important.	
47	CV	Thank you perfectly, and I think we can move on to the next section JG.	
48	JG	So now we're going to talk a little bit about the behaviour, so you have mentioned that like your company has provided you with trainings and you mentioned that there are some things that you already know like about policies now do you feel engaged to follow this cybersecurity guidelines that your organisation has provided, do you think you are engaged with that or you just see that as a rule?	
49	P1	Yes, I am a person that likes to follow the policies that the company gives you. I also know some cases where people do not care about these policies but in my case I try to follow all the policies. One policy says you can't open any social network on your computer but some do it because they really don't care about it. In my case I try to use another computer or maybe my cell phone to open my social networks.	
50	JG	OK thank you, and for example you mentioned social media and that in your work you cannot use it. So from your perspective do you understand or are you aware of the consequences that the company imposed on the employees if you don't follow those policies?	
51	P1	Yes, I'm aware of that. Because as I told you and on one of the training sessions in a previous job they sent me a phishing email and I and I sent some some personal information about me and it was really fun and scary at the same time but after that I guess I realised it is to follow the guidelines or any security policies that the company have. I'm aware that you know if I enter any social network I can easily share any information. Maybe not I'm not aware of what I'm sharing, maybe the background on social media collects some personal data and that's not following the	

		rules of the company.	
52	JG	Does your organisation make clear the sanctions they will give to you?	
53	P1	Yes	
54	JG	OK. Do you feel overwhelmed trying to follow all these cybersecurity guidelines that the company gives you? Do you think it's too much or do you think it's OK?	
55	P1	I guess each company has its own risks because maybe in the past they received some attacks and they are like just putting a strong policy because they already have an attack if not maybe they attack well sorry the policies are not too hard or are um easy to follow because maybe they develop a cybersecurity system that they can track all the things that end employee can do or cannot do so I guess depends on the in the company because some company gives you the the machine gives you the computer and the computer has some tools that they already are collecting information on how how you're using your computer so I guess it depends on on how the companies are developed in cybersecurity information and systems.	
56	JG	Thank you. Now, it's more like a case. Do you think that you would prioritise achieving a business goal even if that would mean that you will risk the cybersecurity policies of your organisation.	
57	P1	Well I guess I will talk to someone, maybe my boss or coworker before taking this business goal. Because maybe I'm not aware of all the policies or maybe I'm breaking a company policy.	

58	JG	OK thank you. One more question. you use a laptop right?	
59	P1	Yes	
60	JG	Do you have a webcam?	
61	P1	Yes	
62	JG	Do you cover your webcam?	
63	P1	No right now. Because I use it only for work so when I am in front of this computer I am only working. But on my personal computer I tried to cover my camera.	
64	JG	OK thank you, now you have mentioned the frequency of the training and some of the topics that you feel are missing from the training. Now in terms of the employee experience, how do you think it can be improved for employees from your perspective? How would it be better to train people or give more awareness?	
65	P1	I guess it depends how the training is presented to the employees. If they are little fun or a little bit of playing a role or or maybe you know if you complete the training you receive something in exchange like a day off maybe this will be a better option to the employees. because they will be more engaged like they will complete all the training differently because if you have a boring training with only decks or maybe just hearing a guy telling you about cybersecurity it will be really boring and you definitely won't want to hear anything.	
66	CV	Following the same line as with the previous question. We have some options that could improve the cybersecurity program. We would like to know your opinion about this. For example, do you think gamification concepts could help to improve cybersecurity programs? Gamification is like earning points with a leadership table of who comes first.	
67	P1	Definitely as we know gamification gives the user some type of challenge to reach the next level or or complete a challenge and I guess everyone wants to do that so yeah definitely it would be a good option.	

68	CV	How about having evaluation and feedback for example take the training and from time to time someone can ask you how do you feel with that or share with you a survey where you can feel information without do you think this could be helpful how do you see that.	
69	P1	Yes, maybe not for all the employees that take the training but just random surveys for all the employees that take the training to collect this information to improve the training it could be a good option too.	
70	JG	Why were you not collecting feedback from everyone?	
71	P1	I don't know I guess so I'm just thinking of maybe taking a training course and two or three days later you will receive this email, and it will happen the next time and again the same next time. In the end people won't take the survey because they know they already answered this survey so maybe random could be a better option.	
72	JG	It will become repetitive, that's kind of what you are saying.	
73	P1	Yes,	
74	CV	You mean something optional is better	
75	P1	Yes, I think it is a good option.	
76	CV	How about continuous monitoring, which has metrics about cyberthreats that occurred, level of compliance or some areas or so employees would be useful to improve the service security awareness.	
77	P1	Can you repeat the question please?	
78	CV	Yes, for example if I have the continuous monitoring concept which is metrics and information about how many threads were detected, which level of compliance the employees have, would that be useful for the cybersecurity program?	

79	P1	I guess this depends on the point of view of the employers or the company. Because for the company it will definitely be a good tool to have full dimensions of how people are following their policies. It may be sending an email monthly or or semestral to the employees how their policies are being followed could also be an option.	
80	JG	But from an employee perspective. Do you think it would be too much like it would be if I keep receiving that information? Do you think the employee will say this is too much or will you find it valuable?	
81	P1	Yes, I guess it's too much information. I think you may be every six months sending an email how the policies are been followed because if it is monthly or weekly as they will be bored about this information.	
82	CV	That's good feedback JG is there something you like to ask something else?	
83	JG	No, I'm good.	
84	CV	I think that's all the questions we have. R1 is there anything else you would like to add or something you would like to clarify further about the responses you have given us today?	
85	P1	I don't think that is everything that I know about cybersecurity.	
86	CV	Well thank you very much I will just stop the recording.	
87	CV	I think that's all the questions we have. R1 is there anything else you would like to add or something you would like to clarify further about the responses you have given us today?	
88	P1	I don't think that is everything that I know about cybersecurity.	
89	CV	Well thank you very much I will just stop the recording.	

Appendix 5 - R1 Interview

Date: 2022-04-21
Interview length: 48:37 minutes
Language: English
Participants: Respondent 1 (R1), César Vásquez (CV), Jose Gonzalez (JG)

Row	Person	Text	Code
1	JG	So, thank you for being here so the first question would be to get to know you a little bit So what is your role at work	
2	R1	My current role at work is a risk investigations team leader for financial institution and basically what we do is I manage a group of around 15 risk specialists that are focused to identify any fraud or good indicators from the customers that use this financial institution to be able to determine whether we want to continue doing business with them or not or we want to prevent any future losses for the company and basically put a stop to any fraud trends that we may have seen. Basically, we all work from home currently. We are also doing an organisational restructure to put a more effective process into finding fraud basically, so making sure that we have the correct steps and that we're not duplicating work throughout different organisations. That has been my latest project so far.	
3	JG	OK thank you and how long have you been there?	
4	R1	I've been working there for a year and a half	
5	JG	Thank you, so you mentioned that it's a digital environment and like some details about the job that you do, but just to confirm, you use technology to perform your job activities right?	

6	R1	Yes, so it's all based on computer systems that are developed by the company to review fraud Trent rules. We also work in a controlled environment using Citrix because of security. We don't use anything that is on paper or that we would have to print or anything that would not be encrypted.	CRW
7	JG	Alright, thank you and prior to COVID-19 did you work remotely, or it was office based.	
8	R1	Yes. it was not remotely the company I worked for had a strong value or belief of being social if you want to put it. Feeling like a community but obviously with the pandemic everything changed and we're evolving in our way of work.	CRW
9	JG	Ok, thank you and so now that we have established the remote work part. What was the most difficult aspect of working remotely would you say in terms of dynamic or usually stress related to COVID and work.	
10	R1	Yes, the dynamic is different because as a team leader it's hard to connect individually and to build that trust and bonding relationship and as well to make sure that we are being efficient at work and being focused on hand. We needed to have different IT systems to make sure that the work was being done correctly, fortunately we have them already. But it was tricky at first because it wasn't something that was set in place. One of the advantages obviously is that we have seen commitment increased with our teammates just because there are several benefits of working from home, like no commuting and all of that so they are committing themselves to the work just to keep that correct. So that is something that we take into consideration while we are being flexible and reopening and going back into the office.	CRW
11	JG	Do you think stress like the emotional part of all this pandemic affected your work?	

12	R1	Yes, I think not only mine, but it was a community sense. Fortunately, I can tell you with the company I work for, they have a strong sense of employees first, and in taking care of employees mental and physical well-being. They set in place several activities and guidelines that could help alleviate some of the stress and if needed any type of assistance you would have because of the pandemic. However there's still that aspect that is overwhelming in itself that you would have to get up every day and not be able to go outside, and remain in the same area just move within our houses and that in itself is just stress and pressure for one's mental well being.	CRW
13	JG	OK thank you for all your background and the details that you have provided. Now we're gonna move to a short section about the concept of cybersecurity. We would like to know for you what cybersecurity is and what is your experience with cybersecurity?	

14	R1	For me, cybersecurity is basically all encompassing anything that you could do with a digital device, like using the Internet with your computer, with your tablet, with your phone and making sure that it's secured. Also, making sure not to be scammed or have your identity stolen, victim to fraud. Also, related, that you can trust the sites that you are going into and that you don't have any concern. It has to do a lot with the platforms that one uses whether it's in a company or personally and then also the practices that I as a person have as well in the company or personally to keep my information secure. On your second question my experience is with a financial institution. We do have a very strict set of guidelines on what we have to do for the company itself and that has helped me personally as well. Because we can see as risk investigators what happens in the digital world of sharing information that is not being properly secured. I have not been a victim of any attack and I can tell you that since I started working in this company I have taken even more steps to secure my information.	CS,AW,GOV,CTR
15	JG	Right, what are the steps?	
16	R1	Well I don't wanna burn myself here but I used to have repeated passwords throughout several platforms. Now they're changed and they're not easy, before they were easy or something that I would remember. Also, making sure that if I go into the site and I have to put in any information that they have certain security measures and that you can see the trustworthiness of the site. And no use of a website that looks fishy, or not answering to fishy emails, deleting them right away.	
17	JG	OK so thank you, we closed the conceptual part of the interview and now we can move to the next part.	

18	CV	Thank you, well this is great because you provide many details about your work context and how is the organisation dynamic regarding remote work so we know now that during the pandemic you move toward remotely, so we would like to know if employees in the organisation receives security policies a about cybersecurity when they move to work remotely?	
19	R1	Yes, when we moved remotely it was very quick, in a matter of days. There was a reinforcement of the already security guidelines of how to manage information sent out. We sign the agreement and acknowledgement for the use of the equipment in a remote environment. There were online training sessions that explained what to do in case of a situation in which you were compromised with information, and even if it was something that was not done intentionally. There was also a process that they put in place to manage a security emergency .	CRW, TR
20	CV	Thank you, now the following questions are more you know about your individual perspective and your individual experience. Do you think that the new remote work environment and tools you have could open new breaches for cyberthreats?	
21	R1	I think I would have liked to see more from a personal perspective communication of what it's being done because obviously everybody was remote and the economy was suffering. There were new instances in which people were trying to take advantage of everything so I would have expected more from companies on what they're doing to secure the work setting, which I didn't receive from the company. In my personal perspective on going through the training, they are actually very good and dynamic but I'm not sure if going through an online training the people would have been putting the correct mindset to add and an attention.	CRW

22	CV	Thank you, do you think you have enough tools and infrastructure to protect your remote work environment from cyberthreats?	
23	R1	Yes, actually that's one of the things that amazed me with the company I worked for. They provide you the equipment and then a strong setup to secure the tools and accesses that you have available. If you wanna do something personal it's really hard and very limited. As I mentioned, we do use secure desktops through vendors like Citrix and there we have other settings even more secure than the computer itself. Even for sending an email or using outlook, we have several rules that it's very tricky if you are looking to do something that's not legal or trustworthy. I do think that the company has the correct infrastructure to prevent anything yeah yeah you mentioned a Citrix for virtual desktop.	CRW,CRT, AW
24	JG	Do you use VPN maybe or some firewall or other tools that your organisation is also implementing?	
25	R1	Yes, so it's antivirus and I can tell you that every three weeks we have computer updates coming into our system that are managed not only by our operating systems but by the IT department itself and they are global, they're not locally based . I would have to say we have to suffer through them because the computers sometimes get stuck but that only means that they are continuously developing new ways of updating our computers to make sure that they are protected. Sometimes it makes the computers a bit slow when they're updating but in the end it's very secure.	SF
26	CV	I think it's a common practice to run these types of updates and that's good to know. Also I think you mentioned that before but did you have contact with any cyberthreat in the remote work environment?	

27	R1	Not on my end personally, I'm not sure if this would be called out as a cyberthreat but we did have a case in which my mother was a victim of scam and she gave out information on a website and she ended up losing $25. Thankfully on my end no, neither for my work information or from my team.	CTR
28	CV	OK perfect, I think we can move on to the next section where is more about practical experience with security awareness and training	
29	JG	OK so we want to know your perspective about the current practices that your company has. You have mentioned for example that you receive training and that you have good infrastructure. Now do you think that the policies that your company has given you are easy to understand and relevant for your role in the organisation?	
30	R1	Yes, I do think so. Once you come in and are boarded into the company you are given a booklet on how to manage security and how to manage information and the equipment itself. [AW] That's being given to each employee upfront and you have to carefully read and then acknowledge before onboarding in the company even before having the physical equipment. Also, the training is very understandable and they are based on those policies and that booklet. The organisation makes it understandable, the training is dynamic and the way they pass on the information. Every year this policy and material is updated and it is something that I have not seen in any other company before. This dynamic training engages employees and helps them to pay attention. They give you a lot of videos and recordings and real case work scenarios of cyberthreats. For example, what has happened to banks or to major corporations when they have lost their information to fraudsters. So it is easier to identify this as is happening in the real world. [TR]	AW, TR

31	JG	Thank you for that information, now just in the training that you have, how long do you think it takes for you to complete that training or how much time do you have to invest to complete the training?	
32	R1	We have the period that it's given to complete the training. It's about two months and it depends on each organisation what is the timeline that they give to you. We do this timeline to organise and not affect the businesses volume or activities on a day to day basis. And all the training would take about half of a day to complete.	TR
33	JG	OK thank you and you did mention that it's only annually, I just want to confirm it. Any other besides that one?	
34	R1	No, besides that there are no other refreshers, unless there were any incidents they would send out any message but there's no other refreshers. If let's say you are hired after that annual training you have to complete the training as part of the onboarding. We can say that everyone in the company takes the training.	TR
35	JG	OK thank you. Now because you did have an experience in the office and now fully remote do you feel that there is any difference between the training that they gave you in the office and the training that you receive remotely. Do you see any difference?	
36	R1	That's the trick question no I didn't see it different because like I mentioned this is something that as a part of their learning department they have always had set in place of using that methodology of being dynamic and providing examples. I can compare it to my prior work experience where it was more of a click and click and click until you acknowledge and you didn't read anything of it. Looking at comparing work experiences now before and after the pandemic it's basically the same platform.	TR

37	JG	Now in terms of content so, for example, because it's remote, did you see any updates?	
38	R1	Yes, I can understand the question now. Definitely it was updated, now we have topics that talk about what new threats we have seen in remote work environments. The information was updated to reflect all of the situations that we were going through and obviously being able to know all the considerations that we have to take. So, the speech changes within the training how you manage cybersecurity from home.	TR, CRW
39	JG	OK, interesting and now just in terms of format?	
40	R1	Interactive, there's like several modules in between each training and the modules have questions for knowledge check which you cannot pass if you do not have a minimum points to pass. Besides having the questions you actually have to navigate by scrolling and then clicking on arrows in between the training so it's not just a video in which you have to pass on each slide you do have to navigate through a map and then you click on each section. when you watch the video from that section you go to the information and then you take on the questions so that's why it's more engaging because you actually have to pay attention to where you're at. In my previous work experience as I explained it was just kind of like a video slide in which you just had to click next . In my current company you have to put attention	TR
41	JG	Now you have mentioned that you have really good training and the information they provided is accurate. Now do you think that the training should be personalised for each type of role. Or do you think that the current material is those works?	

42	R1	Well I think the current material works but it could be beneficial to have it personalised just because it can give a sense of identity when you're completing the online training. For example, for your role as part of the risk department or as part of any department and give information of what you would be facing or the information that you manage. I think it could be done even by department or by region, for example Latin America. It is beneficial right now but it would be an added benefit.	TR
43	CV	OK thank you. We will move to a section about behaviour. Do you feel engaged to follow the cybersecurity guidelines provided by your organisation?	
44	R1	Yes and I can tell you I feel engaged. I have to lead by example for my team and also because the company itself that I work for has a strong legal department. It's not that I am afraid , but definitely it would have several negative consequences that would make you think twice about not following those policies. Also, I can see on a day to day basis what happens when data is not secured because we are in a risk department. [SE] I know that it's so important for the company and that if anything might happen the consequences for the employees including myself would be dramatic to put it or could be very severe legally. [DT]	SE, DT
45	CV	So I understand that you are aware of the possible consequences of not following the cybersecurity policies. Do you feel overwhelmed trying to follow all these cybersecurity policies provided by your organisation?	

46	R1	No, I can tell you, for my end personally I believe it's more of using common sense along with the proper use of your equipment and the platforms that we hold right. The platforms developed that we use in our company are very secure; there's really no loopholes that you would see. Also, the computer itself also reminds you of the policies for information security whether something has to be encrypted or not, whether the type of information that you were sending if it follows the policies. I believe that the infrastructure and all of the settings that are already built in our profiles help us to not feel overwhelmed with what we have to remember of the policies.	SF
47	CV	Perfect, that's a good thing to know. The next is a practical scenario, imagine that you're in a remote work environment and you need to complete a business goal but you realise that to complete the business goal on time you can risk the security policies of the organisation. Would you decide to complete the business goal even if that implies they can risk a policy or how would you manage that situation?	
48	R1	Oh no I would rather negotiate with the one that gave me the task and explain why I couldn't, why wouldn't I be able to deliver it on time. We had a situation with a question raised from one of my peers in which they had to deliver a certain project which had to do with managing a lot of information and presenting it in different ways and using a lot of excel formulas. They had the question whether they could seek outside help from people that knew how to build those dashboards, just so that they could finish that project. But it could not be done because it's internal information so even if it's delayed it's better to just communicate it and explain the reason why. It's very delicate.	NT

49	CV	OK thank you, there are no incorrect or correct question answers here so feel free to expand. Another question is if you cover your webcam while using your work laptop.	
50	R1	No, actually even if I wanted to there's no need because my computer has a cover with a switch and if you wanna cover the camera even if it's not turned on. But we are encouraged to use the webcam because of virtual work from home.	WPC
51	CV	What about your personal laptop, do you cover it?	
52	R1	Oh no I don't cover it, but personally I don't really like using my camera but I should maybe. That's something to think about right now because I do it in my work computer and it's in my bedroom but I don't do it for anything else so now I'm concerned because all the things they say that it could be activated from a website or any type of program but I hadn't thought of my devices.	
53	CV	For the last section we would like to know how do you think that the experience in terms of cybersecurity could be improved if you have some ideas maybe you can put this as their experience for my company or yeah thinking about your organisation	

54	R1	I think something because I was reinforcing that with my team the other day while we were building the expectations files. If they use the computers for any personal things that for example check their personal email. What are the things that you would need to take into consideration? I know we have the policies but they're not specifically part of the training, like social media usage from your device and all of that. Another thing would be that it might not be specifically cybersecurity but it could represent a threat. It's how we portray ourselves as employees of the company in social media because then we could be a target to people that would wanna take advantage. For me it is a point to consider they do have that policy again but uh it's not as reinforced as the other ones.	CI
55	CV	OK thank you. We have a last exercise here associated with the same topic, we have some options to improve the cybersecurity program. First we have gamification which means adding game dynamics, like a leadership table in competition, awards for people who completed the training or the policies. We also have evaluation and feedback which is more basic in the fact to collect insights from the participants to know what they think about the cybersecurity program. Another option is continuous monitoring which means presenting the metrics of how the company is doing, what is the level of compliance, how many incidents you found , or which level of effectiveness you achieved. You can take a time to think about which of these three or all of them could be options to improve on the cybersecurity program, and if they are options in which order will you order them?	
56	R1	I would actually put gamification first just because of the first user experience. As a team leader I would put second continuous monitoring because that's definitely something that I'm interested in. The third level would be evaluation end feedback	EF, GAM, CM

57	JG	Why would that be the last one, for any specific reason?	
58	R1	It was just because I've seen it, not only in cybersecurity but when we collect feedback on any other processes responses are hard to get in detail. You really have to push for that because otherwise they would just not be interested or don't wanna answer at this time. That's why it's the last one on evaluation and feedback yeah.	EF
59	CV	Yes, many people propose that but in the practices sometimes the practice itself is hard to do.	
60	R1	We already have those in our online training, we have feedback and surveys for each of them. But like I mentioned it might be better to personalise each of the training and not just general. Some of the feedback the survey collected is, have you felt this online training it's been helpful for your day to day activity, so it's very general right now. If it's more personalised to each other that could work to be more engaging for employees.	
61	CV	Thank you, that was the last point and we completed all the topics. Is there anything else you would like to add or something you would like to clarify further about your responses?	

62	R1	No, I think I portrayed the experience that I have in detail at this point. I'm thinking probably just to clear up that it does have to do a lot with the company workforce and it is how they take this matter. I believe it's important for a cybersecurity topic how the company higher management manages it and puts attention and importance to it . Because usually it's like the security area defines the policies but then you pressure the managers so they can pressure their employees to complete the training and this is a common phenomenon. Also it has to be like a conscious coherent message throughout the organisation. This is a topic of importance where they have to give its importance from top to bottom.	AW
63	JG	OK thank you, I think we covered all the topics and thank you for your time and for all the feedback you gave us now I will just stop the recording.	

Appendix 6 - R2 Interview

Date: 2022-04-21
Interview length: 43:46 minutes
Language: English
Participants: Respondent 2 (R2), César Vásquez (CV), Jose Gonzalez (JG)

Row	Person	Text	Code
1	CV	We would like to know first what is your current role at work?	
2	R2	I am performing right now as a Project Manager, I work in different projects mostly in Mexico, Colombia and Argentina. I will be on the top of the delivery of the project's to satisfy clients goals. Most of the time we are involved with security and concerns.	
3	CV	How long have you been there in the organisation and how is your overall experience in the sector, how many years?	
4	R2	So in my current organisation I have worked almost three years . But I have around 15 years of experience.	
5	CV	Great and we would like to know, How involved are you with technology, you use software and information systems during your daily routine?	
6	R2	Yes, absolutely that's part of the delivery team and management. We are currently involved with more security, for example when we need to onboard a new employee into the team we have to follow some rules for obtaining security permissions for access to repositories or workspaces, and also request whatever tools are required for development. Maybe the next questions talk about some examples of how I was involved in some security issues, because I received a lot of phishing emails, but we can talk later.	

7	CV	Absolutely we will go through that section in a few minutes. We'd like to know if you have the possibility to work remotely before the pandemic or it just started with the pandemic.	
8	R2	I've been working remotely for a couple of years. The companies that I have been working for promote the remote work office , this brings you good opportunities but also brings you security issues. Because mostly you are connected to your Internet access so it means you are not connected to the company Internet firewall . When you are in remote work you can go to any Starbucks and connect to the Wi-Fi and you can be attacked and maybe you will be showing confidential information for the company so it's complicated.	
9	CV	Yes that's true, from your perspective and personal opinion what is the most difficult aspect of working remote for the organisation may be in terms of stress word dynamic?	
10	R2	I think communication is the main issue. Communication and connectivity, for example in my computer I am not able to join or to connect my USB driver . but what happens if somebody grabs my laptop, and gains access to my permissions or takes the hard disk, see all the information.	
11	CV	OK, that is a good insight. Now we can move to the conceptual part of the interview. What is cybersecurity from your perspective?	
12	R2	Cybersecurity is all the practices related to systems, cloud hosting, programs, and user information that protect from malicious attacks. In my experience, we can split cybersecurity in different aspects. For example, the first one is infrastructure, the second one is for applications, network, and cloud which right now is widely used. Most of the companies are using the cloud, hosting their websites or applications. Cloud environment brings you new issues, but I think that is what cybersecurity is for me.	CS

13	CV	You bring some interesting points there about the definition of cybersecurity. Now what is your experience with cybersecurity?	
14	R2	Mostly with web applications, these applications were used for around 1,000,000 people so we have to align them to security protocol and follow the rules. Having a testing process that is not only about the functionality, but also about security. If you are only focused on your functionality and you don't care about the security side your website can be taken down for any reason. When you launch a new site people always try to test for security like password weakness, or try to maybe refuse several calls for the same API which is a DDoS attack. You need to be able to protect your site on release. This is my experience and I have worked mostly with OWASP which is an important protocol from a development perspective. Also with the release of the site the need to go pass an ethical hacking test.	CS
15	CV	Well, thank you it was a good description of your experience with cybersecurity and it's really useful for us. So now we can move on to our next part which is more about cybersecurity and remote work from a practical perspective and JG will have us with that.	
16	JG	Yes, thank you, you have mentioned that your organisation already provided remote work. But was that the case for each employee or was it specifically for some employees?	
17	R2	Good question, it was not for all employees because you needed to get approval. For my employees they need my authorization and after that the authorization of the security team.	CRW
18	JG	Interesting and with the pandemic everyone moved remotely?	
19	R2	Yes	
20	JG	When this change happened did you notice that your organisation provided any type of security policies?	

21	R2	Yes, policies were already there because mostly the policies are provided by clients. We work for an organisation but the client itself has his policies. When I am in a project I don't follow the policy from my current company most I follow clients policies.	CRW,GOV
22	JG	OK, that's interesting, in terms of the remote work you mentioned that can be more vulnerable because of communication and connectivity. Do you think that your organisation has enough tools and infrastructure to protect the remote work environment from cyberthreats?	
23	R2	To be honest no, because the organisation provides laptops to employees but most of the time those laptops are used for other purposes or by their children. Think about this situation so you are using your laptop as your son comes to you saying hey I need to play this game and you are opening up a web page that can have a phishing link or maybe your computer will be infected by viruses. This is the main complaint here because it happens that there are some cases where their kid uses the laptop nobody figured out where they clicked.	CTR
24	JG	Is there any policy for that situation or do you think this is still not?	
25	R2	Yes, you have to report to the security team also if you suspect that your laptop has been used you need to report it immediately. For these policies we have training, the company in online classes on how to follow any policies, also when the company launches a new security policy you need to do the training. To pass the training you need to watch the videos and answer some questions. It can be true or false questions and after that you get your diploma.	GOV
26	JG	OK, that's interesting and you mentioned previously about the cyberthreats that you have contact with with the phishing emails, can you expand on that?	

27	R2	There was a situation where a lot of emails were sent out from a bank to different employees in the company. It said that you have obtained a reward from your job, please open this link to see the full details. But, when somebody reported in the slack channel about this email it was too late because employees have already clicked on it. It was clearly a phishing attack because they requested company credentials. I did click on the link but it was obvious that it was not from the bank since it was clearly a fake url. The consequences for this case were pop ups showing up in the session of these people.	CTR
28	JG	Previous to that event do you think there was already knowledge about this type of attack or you think people didn't have enough information about it?	
29	R2	I think people didn't have enough information about these attacks. In my case because of my experience I have more knowledge about these kinds of attacks. But if you are new or if it is your first job you are not aware of what really happens inside the company in terms of security issues. If someone is new they cannot imagine that situation and what they will do.	AW
30	JG	Thank you for sharing that experience, and now we're gonna move to a section that is all about your perspective and CV will take this part.	
31	CV	From your perspective are they cybersecurity policies in the organisation easy to understand and relevant for your role?	
32	R2	Yes they are few, but they are mostly understandable. But I think it depends on the experience because when you are a new or when you don't have enough experience working I think the training can take almost three hours or two hours. For me it's only 30 minutes, it's very simple and it's relevant.	TR
33	CV	Do you think that from the organisation you obtain enough information to avoid cyberthreats?	

34	R2	I think yes, during our training we were provided with real examples and also how as mentioned we had real experiences. Now when I see an email I always double check the sender and for any link in the body of the email or any threat. Also despite all the anti virus, we have around 5 control policies for example some URLs are blocked, I think they are working for now.	AW, TR
35	CV	OK, good to know. We move on to talk about training, you mentioned before that you have taken some training within your organisation, could you tell us how your experience was?	
36	R2	Every three months we are demanded to take training that consists of new videos with new policies. These videos will talk about real examples of what happens in different situations. We are an organisation with around 20,000 people distributed in different locations around the world. The situation is not the same in South America as in Europe where they have different policies or in the United States, the policies presented are aligned to the region where you belong.	TR
37	CV	Would you say that the content is personalised based on the region?	
38	R2	Yes, I would say that. Imagine, government rules are mandatory to be included in the company policies. For example, Internet navigation and other use of division have different rules in the United States from here in Latin America.	
39	CV	Just to clarify that point, your company is giving you a different training if you are in South America or in Europe or USA?	
40	R2	Yes	
41	CV	That's a good insight. If I understand this, it is like a web based training that you can open in the browser and interact with the options, can you skip the options or you need to interact in order to get the right answer?	

42	R2	You cannot skip. You have to follow up some rules for the training to be completed. First, you need to complete the whole video. You cannot move the video back and forward. Second in the middle of the video they have some questions where you need to interact. Finally at the end of the video they have more questions to validate you understood all the video. Also, the questions aren't easy but they are open, it can be true or false or other options and after you finish you receive a diploma for that training. The diploma is mandatory and the system would keep track of it specially in the European team.	TR
43	CV	You explained it very well. Do you think that cybesecurity training is different for working remotely than when you were at the office? Did you feel something different while doing them?	
44	R2	To be honest no, since I started with the remote work I have received two training about cybersecurity but they were not different. [TR] For policies in terms of new subjects, it was about how to connect in your house network, and not to go to public places to connect your devices because you can be attacked. Also if you moved to another city you need to declare where you are moving because they are getting the IP address to give any permission. These were the only few and new policies added for remote work. [AW]	TR, AW
45	CV	Do you feel that the topics included in the training are relevant for your daily routine?	
46	R2	Yes, absolutely.	
47	CV	Do you think that training content should be personalised for each employee or the current standard practice is effective? For example, based on their preferences ?	

48	R2	Personalisation can happen maybe according to their access level, or based on products or programs. I think it will be more useful for my side to have a segmentation over a set of levels right. For example, people giving access or passwords to other employees have a different level than me. Beginner, intermediate or advanced could work, but you need to make sure all the employees have at least some knowledge about cybersecurity.	TR
49	CV	I think we can continue with the next part. JG will continue.	
50	JG	We are going to be talking about your perspective about the behavioural aspects of cybersecurity. Do you feel engaged to follow the cybersecurity policies that your organisation gives you?	
51	R2	I think no. For example, some employees don't use their laptops to work, they use other personal PC's or laptops that are not under their domain or they are not with the antivirus. I think this is a current behaviour that is not appropriate but I think people are using it. For me it's not allowed. If I need to use a computer that does not belong to the company, I need to declare and fill up forms.	SE
52	JG	Because you have mentioned employees don't always follow the policies, Do you think from your perspective that the consequences or the sanctions from the company are clear?	
53	R2	Yes, I think the consequences it's not only for you, but for the entire organisation and the prestige of the company. When you are aware that is not only for you but for your coworkers and your organisation. When you understand it you are committed to the security, this is a task for every employee we need to take care about security.	DT
54	JG	Do you know if you don't follow a policy about what your company is going to do or you think that's a little vague?	
55	R2	Yes you are aware and you are concerned about that.	DT

56	JG	OK thank you and you mentioned that it's important to be aware of these practices but did you feel overwhelmed trying to follow the cybersecurity policies that your company has given you? Do you think it's too much or it's easy?	
57	R2	I understand we need to follow the rules. For other team members it can be frustrating because when they open a ticket requesting access they need different approvals from different teams and it takes at least three days. I understand we need to follow the rules because if we skip any rule and are approved by any requirement we are compromising any assets for the company. Even when there is pressure from the client because the permissions shouldn't be started by the client.	SF
58	JG	OK thank you for that insight. Let's say that you have a task that you need to do for a business goal, but while working on this there are some risks of not following some security policies. Would you prioritise achieving this business goal even though it would break some of the policies for cybersecurity?	
59	R2	Absolutely no. I immediately need to escalate those issues because when you involve more people so they can help or maybe it is not for my team to do that task. I think communication between teams about if you know the different policies is a must. But I will not break the policies.	NT
60	JG	OK thank you. Now, like a practical question, do you cover your webcam in your computer from the organisation?	
61	R2	Yes, I cover it with masking tape.	WPC
62	JG	OK is that because of a policy or is it because of a concern from you?	
63	R2	It's not a policy. It is because I jump into the meetings with the camera open, so I would like to explicitly be allowed to show the camera. With the tape I need to move it for others to see.	WPC

64	JG	OK and what about your personal equipment do you cover your camera or not?	
65	R2	Yes, I cover it as well.	WPC
66	JG	OK, interesting. We have finished the part that deals with the behaviour and we would like to talk a little bit about the improvements. You mentioned the types of training that you have that you cannot skip the videos and so on. How do you think the employees experience in terms of cybersecurity could be improved from your perspective?	
67	R2	I think the language because most of them are in English and few of them are in Spanish. I think to be successful in fully understanding the policies it should be in our native language. Because maybe you speak English but you cannot understand all the words, so I think the translation should be improved. Another improvement can be that the video's time is appropriate and is not too long. Most of the time the videos have cartoons or there is a robot that is talking about but the subtitles are in the same language in English. I think it would be better if they are in the same native language.	CI, AW
68	JG	OK thank you now we're gonna move to a sorting exercise and CV will take that.	

69	CV	Thank you for your time until now. This last part is associated with the last topic on how to improve the cybersecurity program for employees. We have some options to improve a program like evaluation and feedback so the option to get insights from the participants through surveys or interviews with our focus groups. Gamification, which is adding some game dynamics like leadership tables, gives them the possibility to earn awards if they complete the training, or have team competitions. Finally, continuous monitoring which is the option to visualise the metrics regarding how well the organisation is doing about security incidents, detected level of compliance of employees, or the training. Given that these three options exist, what do you think about them so do you consider them useful to improve the cybersecurity program? and if you consider them useful can you sort them in terms of priority from your perspective?	
70	R2	I think we missed the first step about this cybersecurity program. I think it is about awareness. In marketing when you launch a new brand awareness is the first step on the top of the funnel. We need to start by what is the content, because maybe the content is not appropriate. It can be videos, blogs, or it can relate experiences or current examples of what happened in the company. I would like to improve the content first of the program itself. This is for me the first one, awareness. Once we have awareness, we need to engage the whole company so we do gamification in second place because you need some practice. Now evaluation and feedback but I don't understand, is this about what about the whole program? or it's about the content? or it's about the experience?	CI, CM
71	CV	Yes, how's employees view the cybersecurity program, how the employees feel regarding the communication of cybersecurity policies, and the training experience.	
72	R2	Got it , that's good so I think it would be number 3 and the last one is continuous monitoring.	CM
73	JG	Do you think it's necessary to add the last one?	

74	R2	Yes, I think because once you have your evaluation and feedback the next step is what you need to improve. You need to have an action plan after you have your feedback , you need to show metrics, continuous monitoring is part of evolution and feedback I think.	CM, EF
75	CV	OK thank you, is there anything else you would like to add or something you would like to clarify further?	
76	R2	No, I think that's OK.	
77	CV	It was a good conversation for all of us. Thank you very much for your time. I will end the recording now.	

Appendix 7 - R3 Interview

Date: 2022-04-26
Interview length: 38:02 minutes
Language: English
Participants: Respondent 3 (R3), César Vásquez (CV), Jose Gonzalez (JG)

Row	Person	Transcript	Code
1	JG	Okay, thank you for your time, to start the interview, I'll ask some questions regarding yourself. So what is your role at work?	
2	R3	I am a billing manager. I manage a group of customer building managers who resolve, let's say, escalations and problem solving.	
3	JG	Okay. Okay, and how long would you say your work experience?	
4	R3	Um, in my current role, or?	
5	JG	In total	
6	R3	Okay. So I've been working since 20..? I'm sorry, 2008? I would say how much of that?	
7	JG	14 years?	
8	R3	Yes. 13, I think 13 years.	
9	JG	Okay. And now for your role. Are you involved with technology to perform your job activities? Um,	
10	R3	well, I mean, if you are referring to,	
11	JG	Like, the tools that you use,	
12	R3	Oh, yeah, I mean, my computer. I mean, that's as much of tech that I would use for my day to day work.	
13	JG	Right. But like, for example, you will use internal systems email and right?	
14	R3	Yes, yes, I do. I use many application websites. Correct.	

15	JG	Okay, thank you. And now, prior to COVID 19 pandemic? Did you work remotely? Or office based?	
16	R3	No, I mean, no, I worked at the office, Monday through Friday.	CWR
17	JG	Okay. But now you have moved, completely remote. So what would you say is the most difficult aspect for you of working from a remote environment? In terms of work dynamic, or stress? What would you say is most difficult?	
18	R3	So, I think it's very impactful in human relationships. Because I think at this point, I know everyone that is on my team personally, because we've set up gatherings from time to time. But that interaction or bonding is, is a lot that gets lost in a bit, it gets lost a bit, right. And then also, what has impacted me the most is that whenever I need to have a conversation with someone, I can call them. But I mean, if I really want to have someone's time and attention, I need to check their calendar every time and set up a meeting so we can talk, so it's not as easy as it was in the office where I could just go to someone's desk, see that they were available? Having a small conversation and a question. I have to like, move into tools and everything before I even reached	**CWR**
19	JG	So in terms of emotional factors, like stress or something, do you feel like you were affected by that?	
20	R3	Um, no, no emotion? I don't think so. No, I mean, I like to work by myself. So I didn't have a large impact for not having that day to day interaction.	
21	JG	Okay. Okay. Thank you. So those will be like the first set of questions. Again, it was just to get to know you a little bit more. Now it comes to our conceptual part of the interview. So the first question will be what is cybersecurity from your perspective?	
22	R3	So cybersecurity, for me, is making sure that any employee in the organisation is responsible for ensuring that everything that they're working on is secure. Especially because we work with all of the information in our computer where overseas we don't see any paper pretty much. So we have to make sure that anything that we work on the customers, their information and our passwords, all of that is safe and will not go into the wrong hands.	CS

23	JG	Okay. So besides the interaction that you just mentioned about, like, the information for the customers and all that, Do you think there's any other experience that you have with cybersecurity?	
24	R3	Um, so yeah, actually, I think we do receive phishing emails, I would say at least once a month, from, or even emails asking like to meet with you, because they want to offer something to you to your working email, which is not common, because we don't give that information out to anyone, but the company, just their customers. But at times, we do receive phishing emails, like with attachments, or something that may look like that is coming from a customer to provide confidential information. And I have received those more often now that I'm working from home than before.	**CS, CTR**
25	JG	Okay, and what has been the response from your organisation for that?	
26	R3	Um, so all we do is forward that email to a security email address. But we elevated internally so that it reaches like the managers, everybody is aware. And then they forward it to the security email. So I haven't received any response to it. Personally, like we did it. And then recently, in one of my direct reports, he sent an email to a customer he wasn't supposed to, like he was sending confidential internal information. And by mistake, because of the last name, she sent it to the wrong person, it was a customer. So that one was for corporate security. And well, they just asked what was sent, they asked the employee to ask the customer to please delete the email, and then they closed the ticket.	**GOV,AW**
27	JG	Okay. Okay. And that, like you reporting that to the security team, is that like a policy? Was that indicated in a training or it was just an instruction that you received?	
28	R3	This time, it was, I mean, I know it's a policy that we should report every incident as such. Okay. Personally, I didn't notice. So until it reached me, someone else, they reported to another person and they instructed us to log a ticket to corporate security, so it wasn't coming from me or my direct report.	
29	JG	Okay. Thank you. So now, we move to a more practical part of an interview regarding cybersecurity and remote work. So just to	

		confirm every employee from your organisation moves into a remote work environment as a result of COVID pandemic, right?	
30	R3	Yes, in my team, we did. About 30 people or more.	
31	JG	Okay. Thank you. So, now CV is going to continue with the questions?	
32	CV	Yes, thank you. And just to complement the last question, or from Jose. So, were some employees able to work remotely for the organisation before the pandemic or everyone started at that moment?	
33	R3	No, everyone started in March 2020, when their pandemic started.	
34	CV	Okay, thank you. And in the moment where you passed to work remotely in March 2020, Did the employees receive security policies or information from the organisation?	
35	R3	Not really, we just signed an agreement, let's say to be responsible for the equipment we were taking. Everything had to be documented in terms of equipment, but no new training, like we didn't receive like online or presential training.	
36	CV	Okay, perfect. So, to have a context of the organisation. Now, we will move on to more individual questions. So do you think that the new remote work environment and tools you have can open new breaches for cyberthreats?	
37	R3	If it has opened new bridges for cyberattacks?	
38	CV	Exactly, yes.	
39	R3	Okay. I would say that I've seen it more often. And probably yes, it has opened more breaches because we do have internet policies, or there are pages that are blocked for security. But we cannot see if they're surfing the internet, and maybe pages that are not blocked, that they're downloading content. Not every page is blocked. Right. So yes, I think there are more opportunities for attacks.	**CTR**
38	CV	Okay, and just aligned to this last comment. So there exists more possibilities for cyberthreats, cyberattacks. So do you think your	

		organisation has enough tools and infrastructure to protect your remote work environment from these cyberthreats?	
39	R3	Well, I know we have the antivirus. I haven't seen any, like a run in my computer, like an app run scanning documents or anything like that. We just received the security patches from time to time. So I'm not, I don't think we have the tools to immediately identify them. Or the company knows that we have information that we shouldn't. So in that matter, I would say no, we don't have enough tools to protect the information.	**CTR**
40	CV	Good to know. In terms of cyberthreats, you mentioned that you have seen an increase. Could you tell us more about this? maybe describe some experience.	
41	R3	So what I receive now is more than before our emails from what they're called audit organisations, we work with many financial documents for the customer like invoices. And we have direct communication with customers. So we do exchange a lot of that information by email. So what I've seen occurring more now is, let's say, someone pretending to be an auditor for that customer requesting information for the customer stating that they have approval from the customer. But when we go to the customer, they have no idea what is being requested. So we don't provide it. But it could happen that an employee doesn't know that we're not supposed to provide that information, or do some checks directly with the customer. So those are the kinds of threats that I've seen more often now. And I would say like in the past year, I've seen it like, I don't know, seven times by now.	**CTR**
42	CV	Yeah, that's an increase and introduce it to have just an idea of how this type of cyberthreat. So thank you very much for the information. And now we will go to talk a bit more about cybersecurity awareness and training from a practical perspective. Okay, so Jose can start with these questions to have your feedback.	
43	JG	Yes. So in terms of the policies that you mentioned, your organisation has, do you think they are easy to understand and relevant for your role in the organisation?	
44	R3	Yes, I mean, I think they are easy to understand. There are terms that we don't know, unless we receive training, we wouldn't even understand like phishing or what is malware, or things like that.	**GOV,AW**

		But there are other things that they focus on like passwords, files, protecting your phone, protecting your computer, not connecting to external Wi-fi connections or public connections. Those are easy to understand.	
45	JG	Okay. And from your perspective, you have mentioned some of the information that they gave you, but do you think that you have enough knowledge to avoid a cyberthreat from your organisation?	
46	R3	I mean, the information that they provide in training is I would say very basic. So if I do get attacked, like, let's say by one of those phishing emails, and I open the file then I don't know what I would have to do next. Like, I don't know how it would affect me or the company. And all I would know to do is report it, look for someone else to look at it.	**AW**
47	JG	Okay. Thank you for answering that. So, you have mentioned a little bit of a lack of information from the training. So what do you think is your experience about the cybersecurity training that you receive from your company? Besides what you already mentioned? What has been your experience with?	
48	R3	So, online training, if nothing has been done, like in a meeting, like trying to draw people's attention? Or when we were in the office, was it always online? Like, like immediate? And they used to be very boring. Honestly, I think they've become more dynamic. Or they've tried to make them more dynamic since the pandemic started. But still an online training that A times just because it's a requirement, I will do it. [TR] But it does seem like it provides some information, but I wouldn't say I pay a lot of attention while I'm doing it. [SE]	**TR, SE**
49	JG	Okay. And how long does the training last? Like, when you're doing it one hour, two hours? How long would it take for you to complete the training?	
50	R3	Actually, that one is a pretty long one, I would say, Well, long one for online training, like 45 minutes.	**TR**
51	JG	Okay. And how often do you have to do that training? Like, monthly? yearly?	
52	R3	Yeah, yearly, once a year.	**TR**

53	JG	Okay. And you mentioned that it was online, and no other format has been used, right?	
54	R3	Email reminders, they have sent. Well, one of the companies that I've worked with, because I work with my employer, and I work with the client. So I have to do one for each. One training for each company at different times of the year. For my employer, we receive emails, reminders, a games like to try it in resolve our work puzzle, to earn some miles with our like, internal company points that you can exchange for something else. And they have Cybersecurity Awareness month in October. So they try to send more emails, but it's not like they do something else. They just do more activities and send some reminders or videos. So it's a site of the training, just that cyber month and emails.	TR GAM
55	JG	Okay. And so from the office experience in the training and now the training in the remote environment, do you feel that there's something different between the training like in terms of the information that they give you like, is there any different or is the exact same training?	
56	R3	They give more examples. In the new training, like before, there was just a scenario of two people speaking about cybersecurity. And now you get involved more in the mix to make it more interactive, like having a conversation on scenarios on cybersecurity, what would you do? That's what I've seen differently. More scenarios to put it in practice, maybe.	
57	JG	And in that scenario, is it about the remote work environment or is it just about cybersecurity in general?	
58	R3	Just cybersecurity.	
59	JG	Okay, thank you. And do you feel that? If this is the case, right, that they have not included something for remote work. Do you feel that the topics included in the training are relevant for your daily routine, then? Because you're in a remote work environment?	
60	R3	No. They focus on the day to day as they did before.	TR
61	JG	Okay. Now, do you think that training content should be individualised to each employee or the way it is you think it's effective?	

62	R3	I think that if it was individualised, at least by department or by operation, and they could focus more on maybe examples that they would run into. People would be more aware or would easily understand better if they do run into a security threat. It's like we do a lot of invoicing. So it's kind of easy to set some examples there. But there are other departments that don't see invoicing and billing, they don't see information that is as complex or have their strengths, or they don't have engagement directly with customers or outside parties. So it would be focused on something else, but we do manage critical information. So people will definitely pay more attention if it was focused.	**TR**
63	JG	And what do you say by organisation? What do you mean, from your perspective? For organisation?	
64	R3	Just that I can recognize we just have three organisations. We're at one that is all billing related. Second one is all that is sales related. And the third one is operations related.	
65	JG	Okay. Thank you for that information. Sorry, you were saying something?	
66	R3	Within each organisation, there are many different departments. But those are the top organisations.	
67	JG	Okay, I understand now. So now we will move to talk about the employees behaviour from your perspective in the remote work environment, and César will be doing the questions now.	
68	CV	Okay. I'll try to engage based on the last few answers. So do you feel engaged to follow the cybersecurity guidelines provided?	
69	R3	Could you repeat the question? Sorry.	
70	CV	Yes. Do you feel engaged to follow the cybersecurity guidelines provided?	
71	R3	No. I mean, I know we have yearly training, we have emails, but it's not that we get reinforced on that very often.	**SE**
72	CV	Okay, and that from both points of view from the organisation's perspective and the clients perspective, because sometimes you are taking like, two policies, two training sessions. Right?	

73	R3	Right. Now, I have not seen much reinforcement from them on following the security policies.	
74	CV	From your perspective, what are the possible consequences caused by not following the cybersecurity policies?	
75	R3	Leak of customer information that could get to the wrong hands and impact the company. Because there's a breach of information. For us, I mean, there are many different customers with different pricing, different deals, and that would definitely be something that they could use against the company. Yes.	**DT**
76	CV	Okay. Yeah, good points. I think that is true that this could happen and it would be not beneficial for the company.	
77	JG	Just a follow up. Can I do a follow up question? Are you aware of the sanctions that they're your organisation would do if you don't follow those security policies.	
78	R3	No, I'm not aware of that. I mean, in the emails it is just said that there may be a disciplinary process, but I don't know if there are sanctions for the company itself. I don't know that.	**DT**
79	JG	Okay, thank you.	
80	CV	Okay, good complement and do you feel overwhelmed trying to follow the cybersecurity guidelines provided by the organisation?	
81	R3	Um, no. I mean, I'm careful. But no, I wouldn't say I feel overwhelmed.	**SF**
82	CV	Okay, so this is like a particular scenario that I will propose now. So let's think that you need to achieve a business goal. So you're working on a task. And you realise that to complete the task on time, you will risk some cybersecurity policies of the organisation. So the question is, would you prioritise achieving the business goal, even if it risks the cybersecurity policies? Or how would you manage this situation?	
83	R3	I would say I would question myself as to what risk I will be taking? I think it would depend on the risk. But I would prioritise security over the goal, because I would have to, I would have an explanation for the delay. If that makes sense.	**NT**

84	CV	Maybe would you talk about this with a manager or someone who is also in charge of these tasks, so they can be informed about the possible solutions that you can take?	
85	R3	Right. Yeah, I would definitely ask if there's something else I can do, or maybe some. I mean, I think it would just depend on what type of task right because let's say if it is something password related that I don't have access to, then I would ask someone that has access to it. That could pull the information for me. But if I don't have access, because I'm not supposed to see it, but I need it for the purpose that I'm following. I would still ask for the information.	**NT**
86	CV	Yeah, good insight, thank you. This is an open question. Do you cover your webcam in your organisational computer?	
87	R3	In what? Sorry.	
88	CV	If you cover your webcam in your organisational laptop?	
89	R3	Actually, I know not all of them do but my laptop has. I don't know what you call it. I can hide it. Because it has a panel for me to move it. So I can hide it. I can block the view.	
90	CV	Okay, and do you usually have it blocked? Because some people try to work by default and reopen it for meetings?	
91	R3	I do . I usually have it blocked. Just because sometimes it may turn by itself. I don't know. So I do have it locked at all times. And only when I'm supposed to be sharing my camera I unlock it.	**WPC**
92	CV	Okay, good to know. And what about your personal laptop?	
93	R3	My personal?	
94	CV	Your personal computer or laptop?	
95	R3	So our personal computer, you can hide the camera by pushing it. So we don't usually hide it. Maybe we leave it on? Not on but like I don't hide it. Yeah. I don't hide it all the time.	
96	CV	Okay, no, perfect. Thank you. So well, this is an open question. Maybe to bring some ideas to the table from your side, how do you think the employee's experience in terms of cybersecurity could be improved?	

97	R3	Like for them to truly be aware of what they should be paying attention to. I would say that when there's a meeting, even if it is just a short one, it's live, like people tend to pay more attention to what they're seeing. And we don't have any of that for cybersecurity, like, all of the communication that we have is email communication. So, and if there were meetings from time to time, even if it wasn't monthly, I think that would make people be more aware.	**CI**
98	JG	So you have mentioned the email communication. So is there any way that the organisation or you can know that, like, the employees acknowledge that they have seen that, that they have read that or just saying that no?	
99	R3	No, just emails, and if you don't read it, nothing happens. Okay. The only thing we need to acknowledge is the online training.	
100	JG	Okay. Thank you.	
101	CV	Okay, so to summarise that, like, meetings in person could be useful from your perspective to improve the experience. Right?	
102	R3	Right. Because, I mean, it is truly a threat, and it's happening. And like they could share scenarios that have happened and like for you not to run into that, like if they share real threats that they've run into.	
103	CV	Yeah, that's true. And you mentioned during the interview, that sometimes the organisation is not reinforcing. So they do the training, but then they don't reinforce the same message that they gave during the training. So, do you think there is a possible way to do a better reinforcement of this? Or what should be a method that could possibly help you in that aspect?	
104	R3	Yeah, so they don't reinforce it like monthly, they just do that in the Cybersecurity month in October. But after that, I don't see many, so I did some searching, and we don't receive many reminders of it. So I don't know if reminders may work. But I mean, in our day to day, I just would say we have a lot of email communication. So not even emails are like, we may just leave it and read and go on with our day. Right. So I don't know how good that would work. But we don't receive that either.	**CI**

105	CV	Yes. Okay. Good idea. Finally, would you like to present the exercise Jose?.	
106	JG	Yes. Just one question. Just to have maybe a little more context. Is your company a global company?	
107	R3	Yes, it is.	
108	JG	And we know, around how many employees does the company have? Like an estimate or you don't know? It's okay, if you don't know.	
107	R3	Honestly, no, I mean I don't do it on top of my mind. But both companies, my employer and the client that I work for are large companies worldwide.	
108	JG	Okay. Thank you. So right now we're going to do a sorting exercise. So, from the scholarly point of view, there are three ways that are suggested to improve the cybersecurity program. First, we have evaluation and feedback that consists of collecting insights from the participants through surveys, or interviews about the program. We have gamification which is like adding a game dynamic. Like for example, presenting leaders or leadership tables, team competitions and awards. So a cybersecurity program will have something more dynamic. Or we have continuous monitoring, which is shared metrics regarding how many security incidents. If the company has the level of compliance or the level of effectiveness that the company has, like, I know you have mentioned that you have seen an increase, but maybe like, let's say your company is going to say how many incidents they have had. So considering these three initiatives, can you rate them from one to three? And also you can say, maybe I think this shouldn't be so there's no right or wrong answer, like, but can you rate them? Which one would you put first, second, and third?	
109	R3	Okay. For me, I would put continuous monitoring as number one. Okay. Do you want me to explain why?	**CM**
110	JG	Yes.	
111	R3	Okay. So for me, continuous monitoring would be for me to know that it's something that I need to pay attention to, because it is an actual threat. Like maybe we were talking a few moments	**CM EF GAM**

		ago? If this is a business that may be what type of threats we are most impacted by so that I would pay more attention. Right, I think that's how it will help me personally. Gamification I would place as number two because I think that's more engaging for employees and especially if there's a reward in like I said, they do do that here. So that's kind of one thing that I think would likely work for people to pay attention to. And then evaluation and feedback, I would put as number three, just because I think it's not as easy to collect feedback and information. If someone doesn't understand what could be an actual threat and how to handle it.	
112	JG	Okay, thank you so much. So we have completed all the set of questions that we have. So is there anything that you would like to add or clarify?	
113	R3	No, I am okay.	
114	JG	Thanks. Okay. So, César, is there anything you would like to add?	
115	CV	I think we have recorded all the answers. So thank you very much for your time.	
116	R3	Thank you.	
117	JG	Fine, stop the recording right now.	

Appendix 8 - R4 Interview

Date: 2022-04-27
Interview length: 54:20 minutes
Language: English
Participants: Respondent 4 (R4), César Vásquez (CV), Jose Gonzalez (JG)

Row	Person	Transcript	Code
1	CV	Thank you for your time. First, we have a set of introduction questions to get to know you better. We would like to know what is your role at work?	
2	R4	Okay, sure. Well, currently I work for a BPO. So is an outsourcing company and I am in charge of business intelligence and analytics. I am a Program Manager there in charge of identifying business value added for our customers, finding improvement opportunities, and also process evaluation that we can do for our customers. And my role is directly related also with sales. So if we find an opportunity to offer another system, another service to our customer, that's where we will make a study and we will present ideas. I also work with a group of robotics with RPAs (Robot Process Automation) for the same reason to offer solutions to our customers, and I work with another team that is in charge of speech analytics. So we pull the calls from the customer, we put it into text, and then we translate to insights. In a nutshell, I will say that's my current role.	
3	CV	Really interesting. How long have you been there?	
4	R4	I've been with this company for two years. This is my second time with this company. I was with them for seven years when I first started working when I was an agent. I mean a customer service agent. And I got several promotions until I left back in 2014. And by July 2020, I came back as the role that I just mentioned to you.	
5	CV	Sounds like a good experience to come back. And in general, in total, how many years of experience do you have?	
6	R4	Total, I have 15 years of experience since I started as a customer service agent.	

7	CV	Excellent. Thank you. And we would like to know, How involved are you with technology to perform your job daily activities?	
8	R4	I am involved. I will say probably right in the middle. I've had opportunities to go a little bit deeper due to what I'm doing business intelligence. But I'm more in the middle from the user through the path. I've had a little experience with developing but I've had to and evaluate probably some new technologies, but when more as a user, so if the company needs to purchase new technology for something that is related to me, I will evaluate it. I provide my opinion, but just as I mentioned, probably not as an end user, but in the middle like an administrator through users. I don't know if that makes sense.	
9	CV	It answers the question because you also before mentioned that you're working with RPA and speech recognition. So yes, to have the complete picture of how your daily activities are. Okay. And now talking about the remote context due to COVID pandemic, did you work remotely prior to the pandemic?	
10	R4	No, I was working remotely, probably just a couple of hours a day if it was necessary, or whenever we needed to do overtime, but just maybe like, over the weekends or or after hours but not on a regular basis.	**CRW**
11	CV	Thank you. In terms of remote work, what was the most difficult aspect of working from a remote environment for you?	
12	R4	Well, I had a particular challenge. And it was when I started with this company, it was already working remotely. So I started working with them knowing no one. And I needed to move around. And I couldn't tell who will be able to help me because I guess that interaction really helped before, like walking and knowing people and then having their names in mind, like, oh, that's the guy from IT. So you just walk to the IT Office and you talk to whoever is there. But it is for me, like knowing no one, like I had an IT issue, I will have to look for a peer and get that feedback. That's because as I mentioned, that's my particular case. Prior to that probably being with my previous company, I started the pandemic transition. And the challenge was that I couldn't really separate how many times I needed to be sitting in the computer, even if I had my work done, if I needed to just continue there. If I go take a break. What will happen if they call me and	**CRW**

		I don't answer. I mean, I felt that because I wasn't home, I needed to demonstrate that I was really there that I was working. So that transition really was a challenge because at the office student didn't sit in all day, you move around, you have meetings, so no one is expecting for you to be at your desk, but I felt like in this case, that transition for me was was difficult because I wasn't being I was not being very productive. Like even if I was at the computer. And yeah, I would say that was the main challenge from the transition part.	
13	CV	Thank you for the feedback. Now we move to the conceptual part to start the conversation about cybersecurity. So from your perspective, what is cybersecurity?	
14	R4	I will see, it is the practice that takes care of protecting everything that is in the system, all the technologies. It is like a virtual gate. Like we will have our gate in our house to protect from the outside is the same but virtual gate and virtual guardians that will protect what is inside from the outside. And I think also that it's internal as well, like, even within the organisation. Not everyone should have access to everything.	CS
15	CV	Okay. It's a good explanation to know that and in terms of how much experience you have with cybersecurity. So, if you have some interaction with this topic, on your daily activities, you may have some examples maybe.	
16	R4	I do, I've helped to implement new customers. So, whenever a customer decides to work with my company, they sign an agreement and we start working on all the logistics from zero to day one of operation. So, in this path, there is a part where we need to consider what are the requirements for our customer, what are my company requirements, and where we can find risk points. So, we do a risk evaluation through the whole process. And with these three elements: customer requirements, risk evaluation and our requirements, we put together what are the control points and what are the measures that we will take for cybersecurity. So, to give you an example, some of our customers, who like being on site, already requested a VPN in order to access their systems. So, we were covered with that, but some others do not request that the software installed in the computer is not web based. So we need to identify what is required on that part, and also, because some of the customers	CS, AW,GOV

		right now will still request a group to be on site and some to be at home. So, I will also need to determine what the control points there we will have for each customer.	
17	CV	And just a follow- up question, in the organisation, you have a specific area responsible for cybersecurity that interacts with you when you make this preventive evaluation of a customer.	
18	R4	There is an organisation but I do not interact with them. I only interact with local IT or regional IT. And this group is more worldwide. So they delegate. Let me add this a little bit of context. The company where I work has the majority of the presence in Latin America. There are some sites in the United States and in Europe. It was initially a European company but it expanded through Latin America most of it. So there are some of these countries that are so big, they have very big organisations for everything they do. So in the last two years, they have been working to make everything more global, more regional. So there is a specific case for a Latin American country, which is that these companies are huge there that they had these roles for longer. So I understand that the cybersecurity director is located there. He's been doing his role for some time now. And in the past two years, they've decided to replicate these in every country. So it has been expanding. So to go back to your question I deal with local teams or regional teams, and they are the ones who will go to the cybersecurity direction if it is necessary. But basically, the local team has been working with the role from the beginning in the country where I work, and in the region. I don't know if that makes sense.	**GOV**
19	JG	So maybe like the division that you're mentioning is like there is corporate security. And there's like, regional or local security, which are the teams that you interact with, right?	
20	R4	Yes, and they have other roles. They are not dedicated to that right now. At least locally. Okay. Thank you.	
21	CV	Yeah, yeah, there's the point. Thank you for all the details. Now, we will move on to the next section which is about cybersecurity and remote work more from a practical perspective. And so we can continue Jose with this part.	
22	JG	Yes. So you have mentioned previously that before the pandemic, you had some hours that you can do remotely. So for your	

		organisation, do the employees have the opportunity to work remotely or was it just a specific employee that can do that?	
23	R4	For my current organisation, just very few specific employees. The entry level position supervisors. Basically, anyone related to the actual operation, they were at the site.	
24	JG	Okay. And you also mentioned that you transition to this new company already in a remote work environment. But are you aware if the organisation provided any security policies regarding, like the work, remote work environment cybersecurity policies, when this change happened, do they have to do something?	
25	R4	Well, because I am now in charge of, as I mentioned, implementing these new projects. When I got on board with the company, I collected all of the documentation and all of the processes that were in place in order to get an agent on board. And I found them at work from the home manual for the agent. And from what I saw, what they delivered was very basic information that I will say it's related to cybersecurity. First, they had to introduce a local VPN in order to simulate being on site, that was part of the instructions. Then, there were general recommendations, like, do not write down your passwords, do not leave your computer locked, work in, in a place where you are alone. But I know as a fact that that was probably it. I don't think they did a lot more.	**CRW, AW**
26	JG	Okay, thank you for those details. Now. We want to know specifically your perspective right now from the organisation, or what your perspective is like, so do you think that this new remote work environment opens new breaches for cyberthreats?	
27	R4	Yes. And the reason I mentioned that is because, okay, I'm going to refer to this company. So in order to accommodate everyone, fast, like, because there was little previous planning, to, to going home, so in order to accommodate everyone, they had to open. Okay, so I don't know the terms, I'm going to say open, for example, the email accounts. So previously, the email accounts could be only accessed on the site. But in order to make sure everyone had what they needed, outside of the VPN, and on the site, they opened it to be a public website. And I know that because of this, and because of the previous work, like previously, anyone willing to come to the office, or open their	**CRW, CTR**

		email there, it was being tracked by the computer, it was being, like, tracked by physical security cameras and guards. So it was very difficult to do something they shouldn't be doing. They didn't have cell phones there. So by doing this, anyone will only be able to access their email. But not only that, because the previous work was so low that some of the agents have generic passwords. This was not okay, this was I don't know, the platform, and I won't mention it. But this was an email server, kind of generic. I don't know who developed it. So this platform will allow you to have generic passwords, so let's say I will tell you, your password is your first name and the year you were born to give you an example. And this platform will not allow anyone to change their password. So by just knowing a little bit about one person, you will be able to know their password and you will be able to access. So by doing this, we do have some threats of fraud by people entering some, some other people's emails, and then changing some of the other credentials they had in another platform. So when you recover your password, and it goes to your email, they have access to that. And so it was a threat, because in order to make everything happen so fast, they opened a lot of the permissions they had.	
28	JG	So you have mentioned some of the vulnerabilities on the infrastructure. So do you think your organisation provides you enough tools to protect you from the cyberthreats in remote work based on the one you have already mentioned? Do you think you have enough?	
29	R4	I will say by this point, yes but I'm talking it's been two years of experience and bad practices they've been dealing with? But yeah, at this point, yes.	
30	JG	And have you had any contact with cyberthreats, like suspicious emails, stolen passwords, or the company systems were down or something?	
31	R4	Um, I've had some alerts from my manager, like, hey, this email is coming through, do not enter any information because it is a threat. I know this is sort of a case. The one I mentioned that passwords were kind of generic. And in order to avoid that, they migrated to Microsoft, and to the two step authentication process. On my end, I will say that that's it.	**CTR**

32	JG	And have you seen an increase in the remote work environment versus when you were in the office from the cyberthreats? Do you think you have seen that more? Or is it kind of the same?	
33	R4	Yes, I've seen more. One of the reasons is that the call centre works with capacity. So I'm giving you this background just to follow my answer. They see that when they install a computer, and they use it for two or three different shifts. So it's the same computer for different agents. And I decided that's not a risk because the agent will go away and will block or turn off the computer and the next agent will need to open with their own credentials. However, in order to go home quickly, they required some of the agents to bring their own device. So they brought the computers to decide, they got installed everything they needed there, or they created their credentials for web access. So basically, what they did is that they gave access to a computer that didn't have the security compliance guidelines they had before. And all of these computers by then, if they left the company, they didn't ask: Okay, bring back your computer, we'll fix it. So they just have access to their computer. So it'll become like, like a situation like how, how do we guarantee they won't be able to access or even if they have another user and all of that. So going back to your question. That's why I've seen an increase because they needed to duplicate or even three times more of the equipment available to to work in an operations environment. And the more equipment they had, there were more probability and more chances for something to happen.	**CTR**
34	JG	Okay, thank you for that information and with this we close the part for cybersecurity and remote work. And now we want to know a little bit more about your perspective about awareness and training and César will work on that.	
35	CV	Okay, well, to continue. Next questions are more from an individual perspective. So it's what you think about these points that I will comment on. We would like to know if cybersecurity policies in your organisation are easy to understand and relevant for your role?	
36	R4	Yes, I will say yes, when I got onboard, I got the policies overview. And relevant? I will say, sorry, let me see if I understood correctly, for my role. I mean, okay, yes, they're	**GOV**

		relevant, but probably not the policy that I got on day one from my organisation, but more specific ones. So to give you an example, this statement is, as I mentioned before, I am in charge of a process that will pull the calls from one of our customers. And I need to transport, save like that. This goes from my country to a Latin American country, where we have the software and the vendor that will translate from voice to text. So in order to do this, I have to read the contract from the customer and see what we can do. And if it is necessary to get an approval letter stating that I can take those calls, put it on a SFTP. And then give it to my peers in other Latin American country. So the policies that I got on the one do not cover this port, but because they are more general, but in my role being more specific, like what I can and how I should be handling it. It's more specific. So the guidance will come from our legal team and from IT. And I don't have a policy that will tell me specifically how to handle those calls, I need to work them case by case with every different customer. But in general, they are relevant for everyone. For my role, I will say I will need more guidance to say like that. I don't know if that answers your question.	
37	CV	Yes, because I feel that you have a set of policies that are relevant, but it would be better if they were more personalised, maybe based on a specific role. That's something that usually happens. My next question is related to this. From your perspective, have you obtained enough knowledge from your organisation to avoid a cyberthreat?	
38	R4	Yes, well, right now we receive more information over emails or more requests for e-learning than in the past. So I recall I've received quarterly elearning to be completed with a test. In the end, I will probably receive emails. I'm seeing it right now, probably once a week with a friendly reminder like, hey, know what to do. You shouldn't be like password guidance, credential management, if that's the word. Probably, once a week or twice a month. That's the previous year. How often I received the emails.	**AW**
39	CV	Okay, so you consider that with this periodicity of information sent to you is enough knowledge to manage in case the cyberthreat appears.	
40	R4	No, and the reason I say no, is because I work with my email all day. This is my main source of communication. But for the	**AW**

		agents, they need to, well, they barely see their email. And if they miss the email where someone is telling us: “Hey, do not open this email because it is a threat”. If they miss it for some reason, because it came at 8am. And then it's already the afternoon, they might miss the email where it says: “Hey, don't this email”. And they might do it. Because they are not constantly checking for their email. Their email is just another tool of the several tools they have to handle. So I will say that it will need to be different for every role. The way that we communicate about cyberthreats, the way that we remind them, like Hey, do not write your passwords or do not leave your computer or lock or whatever is required. There might need to be more channels of communication to them more aligned to the role that everyone has. And yeah, that's what I think.	
41	JG	So just the follow. So you think if for example for your role, you have received enough knowledge but like from lower tier roles, you think the knowledge is not enough? Would that be accurate?	**AW**
42	R4	Yes.	**AW**
43	JG	Okay, thank you.	
44	CV	Okay. So let's go to the next question. These questions are more related to cybersecurity training. So, we understand that you have taken some cybersecurity training as part of your organisation policy. So we would like to know, for you to tell us more about your experience with that. Maybe the duration of them? How often did you receive them? What type of training was it?	
45	R4	Okay. If I recall correctly, the duration is around 30 to 40 minutes. It is e-learning. There is some interaction inside of the training in order to test the content to know if whoever is taking the test is understanding the concepts. So it's an interactive training and it goes from basic, like I mentioned the credentials, through not discussing some topics with anyone else like more privacy and confidential information. If I recall correctly, I have seen it once a quarter and something I've seen is that they do not update it very constantly. For example, I recall last year seeing the same training twice, or even three times. And then, this year, I saw a different one. But I don't feel they have a lot of impact. Probably the first time it was like, Okay, I'm going to take it very consciously. But then the second time, three months later, you get the same training, the same questions and it is more like a routine.	**TR**

		You asked me about the duration? Sorry, am I missing something from your question?	
46	CV	No for the question, you completed them, because you mentioned the frequency, the time you need to take to complete the training. It's e-learning training. So it's web based, you open in a browser, and you can follow the content with some interactions, right? So if I understood, the interaction implies that you cannot play the video and do other things. Instead, you need to listen to the audio, and then try to answer some questions to verify that you're currently understanding the concepts.	
47	R4	Correct, it is not like a set of videos, or even one video. It is very interactive. So you need to click several times in order to continue.	**TR**
48	CV	Okay. Yeah, good to know. That's the feedback we were looking for. And so this question is, what do you think was different from the cybersecurity training facilitated while you were working at the office? So did you find that the content was different for the training when you were working remotely, than when you were working at the office?	
49	R4	I don't think it was different for my role, but I do know that for some of the other roles, it wasn't even required. Like it was training at the beginning of the onboarding process and then that was it. And I do know now that agents have the same requirements as I do, like, one quarterly but my role, it was, I will say very similar.	
50	JG	And in terms of the content, so you mentioned already the onboarding material that everyone received about VPN? The content of the training has been updated to reflect the remote work environment, will you say that? Or is the same content?	
51	R4	Yes, it has been updated for home environment.	**TR**
52	JG	Okay, thank you.	
53	CV	Okay, and this is more related to your personal opinion or feelings? Did you feel something different while you were taking the training remotely than at the office? Did you pay more attention remotely than in the office? Or vice versa? Or something like that?	

54	R4	No, I will not consider there is a difference. Because both were e-learning. I don't recall a physical training for cybersecurity ever, at least for me. So I will say it's the same. Like at work, you can not pay attention. I mean, at the site, you can click, click, click if you want to or pay good attention. And the same at home.	**TR**
55	CV	Perfect and a final question to finish this cybersecurity training section. Do you think that training content should be individualised to each employee or the current standard practice is effective?	
56	R4	Yeah, I will say yes, it needs to be individualised. And because as I mentioned, I have a different greater responsibility than than an agent may have. But they have access to almost a lot more tools that I wouldn't and they seem like for an IT analyst they have access to servers or to the back end of applications. So it needs to be more into each role, or even to have layers of training, if it's required.	**TR**
57	CV	Okay, thank you. Well, we have a lot of information about cybersecurity training. We can move on to explore more about the behavioural aspect of following the cybersecurity awareness and training program. So Jose you can continue here.	
58	JG	Yes. Do you think that you feel engaged to follow the cybersecurity guidance that your organisation has provided to you?	
59	R4	Yes, and the reason I say yes, is because I feel like at this point, everything I do can be tracked. So if I, if I'm not responsible with what I do, I might get in trouble, or I might open the opportunity for someone to do it for me, so I do feel.	**SE**
60	JG	Okay, and so because, you know the consequences that might happen if you don't follow these guidelines, do you feel overwhelmed trying to follow the cybersecurity guidelines that you have?	
61	R4	No. I feel like they are aligned with our regular process and it's like part of the process now. I don't feel it's a lot of more work. I might think, like for an agent who is new to working then might be overwhelming, I can see that. Like, if it's their first work and they have like this big set of rules like, that might be overwhelming. But in my role, I consider that due to the tenure	**SF AW**

		I've been working, I'm more used to it. So probably that is the difference in the tenure of working with some of the guidelines.	
62	CV	Just to follow up that comment, do you think that for a new person, maybe a new agent, that is like his first or second job experience would be overwhelming? Because maybe you hear from them some feedback previously? Or is it your feeling?	
63	R4	I think it's a little bit of both. So let me give you an example. So I do focus groups with agents in order to obtain feedback and eventually have insights for my customers. So whenever I get with them, I might get a comment like, "Oh, there are so many different passwords that I need to know. So I use the same password for everything" and as I mentioned this in this specific case. I mean, it wasn't even like the topic, but this agent mentioned it because he was like showing his computer and taking me through some of his system. And like, oh, yeah, I use it. And I think he even shared the password while we were on the call. So that's probably why I have this feeling. And also from feedback from the managers like the same case, they have so many passwords that they forget. And then they can wait for a couple of hours because whoever is responsible for resetting them is not at the office. So in order to avoid that they will give the password to the supervisor and then the manager is excited about it like, no you shouldn't take that password. So it becomes that type of little issues that might make me think like that	**SF**
64	CV	It is really interesting feedback. Thank you for that.	
65	JG	Okay, and now we're going to do like a little case. So let's say that there is a business goal that you need to prioritise. But by doing this, you might risk some cybersecurity policies from your organisation. So do you think you would prioritise to achieve the goal, even though it means breaking some cybersecurity policies?	
66	R4	No, I wouldn't do it. Well, thinking that this business goal is with my customer, for example, I don't know if that's the case. But let's say this, this calls with my customer. And I knew that I would be putting the company's reputation at risk by doing that. Maybe I'm thinking, Oh, I'm doing great, because I'm attending to this responsibility or to this task. But they may come back later saying: "Hey, your company did that. Like, we noticed that happened". So I will say, I will go back, does this requirement came on time for me to prepare and have everything compliant?	**NT**

		but by the time the event happened, I didn't have enough time, so it wasn't me, I needed to take action. Like, I need to prepare better to ask for permissions on time. And I'm planning better, or maybe it came quickly, or they need to tell whoever requested it "Hey, you need to give me some time in order to get all the approvals or right environment in order to accomplish this".	
67	JG	Okay, thanks for the details. And now, it's like a very simple question. Do you cover your webcam on your work laptop?	
68	R4	Yes, I do. Especially because sometimes I'm typing or doing something else. And I might accidentally activate it. So if it gets activated, at least they don't see me.	**WPC**
69	JG	Do you think? Is this like a policy or is it like a personal choice?	
70	R4	It's a personal choice.	**WPC**
71	JG	Okay, and what about your personal computer? Do you cover your webcam?	
72	R4	No, I don't use my personal computer.	**WPC**
73	JG	Okay, thank you for that. And now we're going to move to talk a little bit about the improvements of the cybersecurity training program. Right. So how do you think the employees experience in terms of cybersecurity could be improved? You have mentioned about making it more personalised to the role? Is there any other suggestion that you might have for improving?	
74	R4	Yeah, I think that, probably making it, I don't know, very formal once a year will be okay. And whenever they get on board. But, but the same way, every quarter, I don't think it works. Because it gets repetitive and they know what to answer. So, probably having different ways of communicating this to everyone like, Okay, we did an e-learning for quarter one, then we can have a conference for quarter two, a focus group for quarter three, and some other ways, like so having different channels, different ways to make sure everyone is aware, because an e-learning is interactive, but it's interactive with the computer, not with whoever is is overlooking cybersecurity. So they are not receiving the feedback, in my opinion.	**CI**
75	JG	Right. Okay. You mentioned that, for example, you are working with people in a Latin American country and a European	

		company and in the US, so, in terms of Language, do you think this is relevant? What language is the training provided? Or do you think it's okay in English?	
76	R4	No, it needs to be under local language in order to make sure they are capturing the idea and we do have several languages on this company. So they do in Spanish, Portuguese, English and, I think, I'm not sure if they do mayan languages as well, because there are some of that as well. Okay.	**CI**
77	JG	Okay, thank you for that information. And now we're going to do a little exercise and César will show you that.	
78	CV	Okay, yeah, this is the final part of the session. So Jose if you can go to the next slide, please. Well, here we have some possible options to improve cybersecurity programs for organisations. For example, one possible idea is to use evaluation and feedback, which is to collect insights from the participants, from the employees, through surveys, interviews, and focus groups. Another possible option is gamification, having game dynamics like leadership tables, team competitions, awards, where you can see how your progress is versus your colleagues, and also from different areas to compare them to push you to continue doing this. And finally, continuous monitoring, which is the ability to visualise metrics about how many security incidents occurred, the level of compliance, the level of effectiveness of each area. So, we would like to know if these options look interesting, from your perspective, to improve cybersecurity training programs. And if you consider them as useful, maybe you can order them in priority, how would you add them to the program? How would you implement them?	
79	R4	Okay, sure. Well, now that I see gamification, I will say that will be the first one and the reason I'm saying this is because as I mentioned the roles that we have the majority are entry level positions and younger audience so I will say this might attract the majority of people in the organisation. Then, I will say evaluation and feedback as number two because what I mentioned you can get feedback and improve with whatever they're saying and continuous monitoring, I will leave it as last, because the way I see it, you will require more resources to do this. So if you don't have the right resources, handy, it might be more expensive. This is one in my opinion.	**GAM** **EF** **CM**

80	CV	Thank you for that. I think with this we finished the set of questions and had so we would like to know if there is anything else you would like to add or something you would like to clarify that you answered previously.	
81	R4	No, I think I'm good and I expect my experience is relevant for your study.	
82	CV	Absolutely. Well, thank you for your time. We'll stop the recording here.	

Appendix 9 - R5 Interview

Date: 2022-04-28
Interview length: 33:14 minutes
Language: English
Participants: Respondent 5 (R5), César Vásquez (CV), Jose Gonzalez (JG)

Row	Person	Transcript	Code
1	JG	The first set of questions is just to get to know a little bit about your experience. So can you explain what your role is at work?	
2	R5	Yes, absolutely. Right now, I'm a project manager in a large technological company. And I oversee projects regarding technology, like automation, or sometimes also projects that are not technological, just learning processes, etcetera. So we have different clients, and we foresee all the project management regarding those requests that they have posted or requested from us.	
3	JG	Okay, thank you. And how long have you been in that position?	
4	R5	In this position? As a Project Manager, it's been seven years so far.	
5	JG	Okay. And in total, like all your job experience, how many years would you say you have?	
6	R5	Oh, well, that's a long time as a project manager, I have 15 years of experience at different companies. And working in total over 25 years of work experience.	
7	JG	Okay. Thank you for that information. And because you mentioned automation, we can assume that you are involved with technology to perform your job activities, right?	
8	R5	Yes, that is correct.	
9	JG	Okay. Did you work remotely prior to the COVID-19 pandemic? Are you office based?	
10	R5	At times, due to the nature of my job, it is feasible to work from home at times. So I did work at times from home, but never as during the pandemic situation, right? in the pandemic situation that it's 24/7. For over two years now.	CRW

11	JG	Right. And was this flexibility of working remotely was for every employee of the organisation, or it was just for a specific role prior to the pandemic?	
12	R5	Just for specific roles prior to the pandemic.	CRW
13	JG	Okay. And we can assume that once the pandemic started everyone moved remotely in the entire organisation, right?	
14	R5	That is correct, yes. As of the day after the local president said that everybody should be working from home and staying at home, the organisation asked all the employees to go.	CRW
15	JG	Okay, thank you. And because you have already experienced working with this flexibility, and now you are, like all the time, remote. What would you say is the most difficult aspect of working from a remote work environment in terms of work dynamic or stress? Or what would you say is the most difficult aspect?	
16	R5	Well, there are several right? or at least many. I would say the first one is network wise. It is in my country, it fluctuates a lot. So sometimes, even now, I am left without the internet, or we have power outages and stuff like that. So that causes a bit of stress because you're in the middle of a call and, suddenly, you're left. However, that's one of the things. The other one is stress wise, when you're working from home, you work more, a lot more than when you're working at the office. Because at the office, you know that you have to leave at a certain point in time. While at home, if there's something pressing, you just keep going and going and going. So it's hard for me to at least stop when I'm required to stop working. It requires an effort from my side to just say, “Okay, I'll continue doing this tomorrow”. So that's another cause of stress. And sometimes also, the systems don't work properly because we don't have, for example, we have to call IT a lot more than when we're at the office. So, for example, something doesn't work and at the office, it would be fixed. If not immediately, very fast at home, you have to get in a line to wait for IT to be able to assist you. So I'm sure that the IT guys are having a tougher time than before.	

17	JG	And this system that doesn't work. Is there any reason in particular like a cyberattack?	
18	R5	No, these are updates. Sometimes, updates to the machines that sometimes you even have to go to the office during the pandemic to have those updates pre installed in your computer automatically at the office. Because they aren't at home so that's also something that causes a little bit more stress while working from home.	CRW
19	JG	Thank you for all the details about that. And with this, we will close the first set of questions. And now we will just want to move to our conceptual part of the interview. So from your perspective, what is cybersecurity?	
20	R5	To me, cybersecurity is just protecting all the exactly what I just mentioned, right? All the systems, all the network, the information that is kept within a company, just protecting all the data and the information and that's it. I'm not an expert. So I'm just telling you what I think it is.	CS
21	JG	Yes, exactly. That's, we want your perspective. So that's a perfect answer. So what is your experience with cybersecurity? What would you say for that?	
22	R5	Well, my experience with it goes back to when I started working in this company, where we had to undergo several training. First of all, when joining the company, and then I got to understand the importance of, you know, keeping all the controls and systems and virus protections, etc, on the tools that are used for work. And so with those yearly courses that we have to mandatorily take and provide assurance that we did take them and we do understand. That's mainly the experience that I've had with cybersecurity.	CS, TR
23	JG	Okay, thank you. So that was the small part of the conceptual part of the interview. And now we will talk about little practical questions and César is going to take those questions.	
24	R5	Sure, sure.	
25	CV	Thank you. You mentioned that you had the possibility to work from home before the pandemic sometimes. And just to have the complete picture here. Also, in this IT company, other employees	

		had this option, this availability to work from home before pandemic?	
26	R5	Yes.	
27	CV	Perfect. And when the pandemic started and their full remote work environment was instated. Have employees received security policies provided from the organisation?	
28	R5	Yes.	
29	CV	Yes, could you describe more about these guidelines or policies that they mentioned to you?	
30	R5	Yes, they asked us to be very attentive, I would say, to how we used the computers, because back then there was a problem but not a problem. But we had an image that was put in our computers. And as I said before, I am not technical savvy. So this is what I understand. We didn't have in our computers all the security measures for working from home, not all of us did. So we were asked to go home and make sure that we used the computer properly and that we didn't use it for other means that were not working purposes. In time, I know that they started sending emails saying that they had found out through some systems that they have at the office, that people were using the computers for other purposes than work. So we started getting a lot of information from our technical teams. And in that sense, we also had to take courses on the company platform, I would say, regarding security measures to take when we were working from home. Because of the pandemic.	CTR, TR
31	JG	These training sessions were updated training, or was it the same training that was before?	
32	R5	Oh, no, they were updated.	TR
33	JG	Okay, thank you. I just wanted to clarify.	
34	CV	Thank you. And now, the next questions are more from the individual's perspective of you as an employee of this organisation. So do you think that the new remote work environment and tools you have can open new breaches for cyberthreats?	
35	R5	Could you repeat the question, please?	

36	CV	Yeah. Do you think that the new remote work environment and tools you have can open new reaches for cyberthreats?	
37	R5	Absolutely, yes. I do, because you're not in a controlled environment. So I don't have the knowledge to use the computer other than for work, but some people do. And that could pose a risk. Yes.	
38	CV	Okay. Thank you. And aligned to this last comment. Do you think that the organisation has enough tools and infrastructure to protect your remote work environment from cyberthreats?	
39	R5	Yes, they do up to a limit. As everybody, I think they do. They are constantly asking us to update our computers and to, you know when it says, restart your equipment right now, for some updates. So we do that constantly. But there's always a space right there where people don't abide by the company's requests or rules, I would say, and that poses a risk also.	
38	CV	Okay, yeah, of course. One question, more here, Did you have contact with cyberthreats in your remote work environment?	
39	R5	No, I haven't. Not that I know of.	
40	CV	Okay. Perfect. Thank you. And now we will talk more about cybersecurity awareness and training from a practical perspective about your experience. Jose could help me with this next question.	
41	JG	Yes. And this specifically will be in the context of remote work. Right. So do you think that cybersecurity policies are easy to understand and relevant for your role in the organisation?	
42	R5	Yes, they are easy to understand. They have it designed in a way that everybody can understand it. And with the periodical courses that we are mandated to take. It helps us see the importance of, you know, being attentive and protecting our networks and devices, most likely because we're using the company devices at home. Right.	GOV
43	JG	Right. So will you categorise them as relevant?	
44	R5	Yes.	

45	JG	Okay. Thank you. Have you obtained, from your perspective, enough knowledge from your organisation to avoid a cyberthreat?	
46	R5	Hmm, that's a good question. I think that they do all that they can in this company to make sure that everybody understands. Sometimes as I said before, the Project Managers that are not technological like myself, have a hard time understanding but if I do have questions or concerns, I can always reach out and those would be addressed and explained.	AW
47	JG	For example, Do you know what to do in the case you face a cyberthreat, like an attack or a cyberattack? Well, do you know what to do in that case?	
48	R5	What I would do is to immediately contact it, stop using my computer.	AW
49	JG	Okay. Thank you. So, now we will talk about the specific training that you have mentioned. Exactly how much time do those trainings that you've mentioned that you have been receiving periodically? How long does it take for you to complete that training?	
50	R5	It is basically two hours, in some cases, one hour and a half to two hours. Okay. And it's every year, it's yearly, once a year,	TR
51	JG	And what type of format is this training on a webpage or video? How is it?	
52	R5	It is videos, its company videos, and powerpoint presentations with tasks required to be passed before each of the topics are presented. So you have to pass the prior one in order to access the next one. So it's PowerPoint presentations with videos.	TR
53	JG	Okay. And is there any difference? You mentioned that they were updated to reflect the policies from our remote work environment, right? So is there any other difference between this training when you were in the office and when you were remote? or is it basically the same? and if they just updated the content?	
54	R5	They use some videos, repeatedly, videos that can be used again. However, when they were updated for working from home because of the pandemic, they did use new formatting and new information in them. For example, now that you're going to be	TR

		working from home, make sure that you don't go out or you don't use a network that is not secure, etc. So they did update it to make sure that we would be very careful when using the company computer.	
55	JG	Right. So these topics that were updated, do you think they are relevant for your daily routine? The topics?	
56	R5	Yes, I do.	TR
57	JG	Okay, because of all the things that you can mention about.	
58	R5	Yeah, right	
59	JG	Now, from your perspective, do you think that the training content should be individualised to each employee, or the way it works? So for example, should it be individualised by department? Or what would be your perspective about that?	
60	R5	That would be ideal if they did it. But honestly, in such a large company as the one I'm working, it would be a monumental effort because there are so many roles. But it would be great if it would be set up for the different positions, because some of them have more risks regarding cybersecurity than others.	TR
61	JG	Okay. Thank you. And now, we will move to a set of questions about behaviour and César I will take this part.	
62	CV	Okay. Thank you. Yes. Do you feel engaged to follow the cybersecurity guidelines provided?	
63	R5	Yes, I do.	SE
64	CV	And this is a curious question, maybe if you had the opportunity to have feedback sessions with other people in the organisation, Do you feel coworkers are aligned to this, or some people have reported like, not feeling engaged due to the type of training they are receiving?	
65	R5	Mainly, we get that from a time usage perspective, they are mandated to take those courses and it takes them two hours of their work time. And that is the reason why they reject these courses because of that, mainly, one. The second one is that some of them complain about, “Oh, we have to take this again. And it's going to be the same thing again”. That type of comment, but they	SE

		do know that they have to be very careful when using their laptops and that they could be subject to an attack from hackers or from people outside the organisation.	
66	JG	And, of course, just to follow up. You mentioned you feel engaged, right? So is this engaged because of the consequences of not following these policies? Or why would you say you're engaged to follow this?	
67	R5	I am engaged because since I am not technological savvy, whatever they post, there is an eye opener for me. And it makes me just be more aware, because having no training and the technological background makes me a good aim. So when I take those courses, or I just really take note then I'm more careful.	DT
68	JG	Okay, thank you.	
69	CV	Thank you. And we would like to know, also, if you feel overwhelmed, trying to follow the cybersecurity guidelines provided by the organisation?	
70	R5	Now, I don't know, I think it's provided me a path to follow, right? So no, I don't.	SF
71	CV	Okay, good to know, thank you. And this is where I will try to set up a scenario. So you can give us your perspective. Let's imagine that you are in a working day, and you need to achieve a business goal, to complete a business task. But you realise that, to complete that on time, you will risk some cybersecurity policies of the organisation. How would you manage this situation? Will you prioritise the business goal instead of the cybersecurity policy?	
72	R5	No, I wouldn't put at risk the security of the company information or anything. I would simply explain later.	NT
73	CV	Okay. Thank you. And this is more from a practical perspective. Do you usually cover your webcam in your organisational computer?	
74	R5	Do I use it? You say?	
75	CV	No, if you cover the webcam.	

76	R5	Yes. I do and mainly because it's working from home, right? When you're working from home, you're in your pants suits, or you're wearing sneakers or a t-shirt or you're informally dressed. So that's why. But if I have a call that needs to have the camera on, I simply dress up a little bit as if I was going to work at the office and then I open the camera.	WPC
77	JG	So you don't have any policies about this.	
78	R5	No, we don't.	WPC
79	CV	Yeah, that's totally interesting and for a good reason. What about your personal laptop?	
80	R5	It's the same. I hardly ever use my video camera unless it's a friendly conversation with, you know, school friends or family.	WPC
81	JG	And do you think that it can be used for a cyberattack?	
82	R5	Absolutely yes, it could.	WPC
83	JG	So how will you balance that? I have why not cover that in your personal one?	
84	R5	Oh, I have. I don't know if it can be done with all the Norton antivirus and stuff that I have in my personal computer. I don't know but I have everything installed there. Hopefully preventing a cyberattack close to my personal computer.	
85	JG	So you think, because of all the measures that you have taken, you are in a way secure, right?	
86	R5	Yes.	
87	JG	Okay. Thank you.	
88	CV	So the next question is open. So any answer is valid here. How do you think the employees' experience in terms of cybersecurity could be improved?	
89	R5	At home, right?	
90	CV	Yes, thinking in a remote work context.	
91	R5	So how would employees?	

92	CV	Employees' experience could be improved. Like the interaction with the program, with the training, with the awareness initiatives that the organisation is pushing.	
93	R5	I think that mainly, it's not having certain updates in your computers that allow you to interact smoothly, I would say with the company training and stuff. So something in that sense. Having more connection with the company systems, perhaps, but I can't answer more than that. Go further down, I can't. That's it.	CI
94	JG	And, for example, you mentioned to like, when talking about the engagement, you mentioned the timing complaints, and how you think you can improve that situation for those types of employees?	
95	R5	I don't know. Maybe designing, you see, cybersecurity is such a broad topic, a broad one. It covers such a broad area that I don't see training becoming shorter in time because of the contents, right? It has so much content. Perhaps, instead of doing two hour training once a year, try to do two training of one hour during a year. But I wouldn't be the right person to find a solution to the timing of the training.	CI
96	JG	Right. Okay. Thank you.	
97	R5	Sure	
98	CV	Okay, and we can move now to a final exercise, I will share my screen here to present a scenario. So Jose you can help me maybe with this explanation.	
99	JG	Yeah. So this is a sorting exercise. So there are three options that the literature suggests for improving a cybersecurity program. The first one is evaluation and feedback, which consists of collecting insight from the participants through surveys, interviews to see what they think about the cybersecurity program. We have gamification, which adds game dynamics, like for example, a leadership table, or team competitions or awards as part of the cybersecurity program. And we also have continuous monitoring, which is sharing the metrics regarding how many security incidents the company has, the level of compliance that employees have, or the level of effectiveness that employees are weighed about in the cybersecurity program. So	

		would you consider these options useful? And if so, how would you rate them in order?	
100	R5	Okay, the order to rate those okay. I would say probably that gamification would be number one. I would think.	GAM
101	JG	Why is that?	
102	R5	Because we have Millennials mostly in the company and they like games, dynamics, and competitions. Then number two would be. That's a tough one. Yeah, number two would be evaluation and feedback because it keeps users informed and also participating. They feel like they can contribute to the company. So I would say that would be number two.	EF
103	JG	Right. And, for example, you mentioned the millennials part. Do you think it is easier to get feedback from them?	
104	R5	I think it is easier for a millennial to provide. I think it is easier for a millennial to be part of the solution whether it be by surveys or interviews or providing their feedback.	
105	JG	Okay, thank you. So the last one would be continuous monitoring? Or you don't feel that?	
106	R5	Yeah. That's important too.	CM
107	JG	Would that be important from a company perspective or from an employee perspective?	
108	R5	Company.	
107	JG	Why do you think employees wouldn't be engaged by that?	
108	R5	Well, I do think they would, but not all of them, I think it provides good information to the company on how many incidents have happened before or after a certain training. So, I think it serves both employees and company but because that would be interesting to know right, but maybe not everybody.	
109	JG	Right. And you mentioned that you have not had contact with cyberthreats. But are you aware if your company has been attacked by a cyberthreat, like a virus like suspicious email, or stolen password? Is that something you heard from your company?	

110	R5	Yes, yes. A virus.	
111	JG	Okay. And does that happen a lot or?	
112	R5	No, it was, I remember it because it was once. And then suspicious emails we do get, but we've been trained to spot them and alert the IT team.	
113	JG	Okay. So you will not consider that as a threat. Because you have the knowledge, let's say you know what to do.	
114	R5	This. Yes, I do, because of these training sessions.	
115	JG	Okay. And that virus did that happen within a remote work environment or?	
116	R5	No, no, it happened while working at the site a long time ago. By the way, it got up all the way to the CEO.	
117	JG	Okay, okay.	
118	R5	That's why I remember it.	
119	JG	Yeah. Okay, so this is the sorting exercise that we had. And this will cover all the sections from our interview. So just as a final question, is there anything else that you would like to add or something that you can clarify further about this interview?	
120	R5	No, I appreciate that you took me into account to help out. Ff I did, I don't know. But I did try. And I wish you the very best with your thesis.	
121	JG	Okay. Thank you. César, do you have anything else?	
122	CV	No, thank you for your time. It's really useful information for us.	
123	R5	Super. Thank you very much, guys. You have a wonderful rest of the day.	
124	JG	Thank you. Bye	

7 References

Abrams, M.D. and Bailey, D. (1995), "Abstraction and refinement of layered security policy", in Abrams, M.D, Jajodia, S. and Podell, H.J. (Eds), Information Security – An integrated Collection of Essays, IEEE Computer Society Press, New York, NY.

Alexander, K. B., & Jaffer, J. N. (2021). COVID-19 and the Cyber Challenge. The Cyber Defence Review, 6(2), 17-28.

Bada, M., Sasse, A. & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? *International Conference on Cyber Security for Sustainable Society*

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. Logistics information management.

Borkovich, D. J. & Skovira, R. J. (2020). Working from Home: Cybersecurity in the Age of COVID-19, *Issues in Information Systems.*

Bowen, P., Hash, J. & Wilson, M. (2006). Information Security Handbook: A Guide for Managers, *NIST Special Publication 800-100*

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*.

Cisco. (n.d). What Is a Cyberattack? Available Online: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html [Accessed 25 March 2022]

Cloudflare. (n.d) What is a phishing attack? Available online: https://www.cloudflare.com/learning/access-management/phishing-attack/ [Accessed on May 1, 2022]

Chowdhury, M. F. (2014). Interpretivism in aiding our understanding of the contemporary social world. *Open Journal of Philosophy*, 2014.

Chowdhury, N., Katsikas, S. & Gkioulos, V. (2022). Modelling Effective Cybersecurity Training Frameworks: A Delphi Method-Based Study, *Computers and Security*, vol. 113.

Correia, J., Compeau, D., & Thatcher, J. (2016). Implications of technological progress for the measurement of technology acceptance variables: The case of self-efficacy.

CPNI (2020) Personnel Security Guidance on Remote Working – A Good Practice Guide

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, vol. 20, no. 1, pp.79–98.

Engward, H., Goldspink, S., Iancu, M., Kersey, T. & Wood, A. (2022). Togetherness in Separation: Practical Considerations for Doing Remote Qualitative Interviews Ethically, *International Journal of Qualitative Methods*, vol. 21.

Eurofund. (2020). Living, Working and COVID-19 [pdf], Available at: https://www.eurofound.europa.eu/publications/report/2020/living-working-and-covid-19 [Accessed 29 March 2022]

European Commission (2020). Telework in the EU before and after the COVID-19: where we were, where we head to [pdf], Available at: https://joint-research-centre.ec.europa.eu/system/files/2021-06/jrc120945_policy_brief_-_covid_and_telework_final.pdf [Accessed 29 March 2022]

FBI (n.d) Ransomware. Scams and Safety. Available Online: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware [Accessed March 24,2022]

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security.

Furnell, S. M., Gennatou, M. & Dowland, P. S. (2002). A Prototype Tool for Information Security Awareness and Training, *Logistics Information Management*, vol. 15, no. 5/6, pp.352–357.

Furnell, S. & Thomson, K. L. (2009). Recognising and Addressing "Security Fatigue," *Computer Fraud and Security*, vol. 2009, no. 11, pp.7–11.

Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., & Toscano, F. (2021). Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement, and stress. Journal of occupational and environmental medicine, 63(7), e426.

Gartner. (2021). Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021, Available online: https://www.gartner.com/en/newsroom/press-releases/2021-06-22-gartner-forecasts-51-percent-of-global-knowledge-workers-will-be-remote-by-2021 [Accessed 30 March 2022]

Gartner. (2021b). Security Awareness Computer-Based Training Reviews and Ratings. Available online: https://www.gartner.com/reviews/market/security-awareness-computer-based-training [Accessed 9 April 2022]

Guo, H., Wei, M., Huang, P., & Chekole, E. G. (2021). Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard. In 2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) (pp. 1-6). IEEE.

GDPR. (2022). General Data Protection Regulation, Available online: https://gdpr-info.eu/ [Accessed 30 March 2022]

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. Ieee Access, 9, 7152-7169.

ISO/IEC 27001. (2022). Information Security Management, Available online: https://www.iso.org/isoiec-27001-information-security.html [Accessed 30 March 2022]

ITU (2022). Definition of cybersecurity, Available online: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed 4 April 2022]

Kajtazi, M., Cavusoglu, H., Benbasat, I. & Haftor, D. (2018). Escalation of Commitment as an Antecedent to Noncompliance with Information Security Policy, Information and Computer Security, vol. 26, no. 2, pp.171–193.

Kane G., Nanda, R., Phillips, A., Copulsky, J. (2021) Redesigning the Post-Pandemic Workplace. MIT Sloan Management Review.

Koutsouris, N., Vassilakis, C. & Kolokotronis, N. (2021). Cyber-Security Training Evaluation Metrics, in Proceedings of the 2021 *IEEE International Conference on Cyber Security and Resilience, CSR 2021*, July 26, 2021, Institute of Electrical and Electronics Engineers Inc., pp.192–197.

Majid, M. A. A., Othman, M., Mohamad, S. F., Lim, S. A. H. & Yusof, A. (2017). Piloting for Interviews in Qualitative Research: Operationalization and Lessons Learnt, *International Journal of Academic Research in Business and Social Sciences*, vol. 7, no. 4.

Microsoft (n.d) Protect yourself from phishing. Available Online: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44 [Accessed: March 24,2022]

Microsoft. (2022). Dictate your documents in Word, Available online: https://support.microsoft.com/en-us/office/dictate-your-documents-in-word-3876e05f-3fcc-418f-b8ab-db7ce0d11d3c [Accessed 5 May 2022]

Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. IEEE Transactions on Engineering Management, 68(1), 87-100.

Moody, G. D., Siponen, M. & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance, *MIS Quarterly: Management Information Systems*, vol. 42, no. 1, pp.285–311.

Moore, G. C. & Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, *Information Systems Research*.

Nagarajan, A., Allbeck, J. M., Sood, A. & Janssen, T. L. (2012). Exploring Game Design for Cybersecurity Training, *Proceedings - 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, *CYBER 2012*, 2012, IEEE Computer Society, pp.256–262.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 29(3), 306-321.

NIST. (2022). Cybersecurity Framework, Available online: https://www.nist.gov/cyberframework [Accessed 28 March 2022]

Öğütçü, G., Testik, Ö. M. & Chouseinoglou, O. (2016). Analysis of Personal Information Security Behaviour and Awareness, *Computers and Security*, vol. 56, pp.83–93.

Oscarson, P. (2003). Information Security Fundamentals, *Graphical Conceptualisations for Understanding.*

Otter. (2022). Meet the New Otter, Available online: https://otter.ai/ [Accessed 5 May 2022]

Pagani, M., & Pardo, C. (2017). The impact of digital technology on relationships in a business network. *Industrial Marketing Management*, 67, 185-192.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q), *Computers and Security*, vol. 42, pp.165–176

Pattinson, M., Butavicius, M., Ciccarello, B., Lillie, M., Parsons, K., Calic, D. & Mccormac, A. (2018). Adapting Cyber-Security Training to Your Employees, *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*.

Patton, M.Q. (2015). Qualitative Evaluation and Research Methods, 4th ed, Thousand Oaks: Sage Publications

Pimple, K. D. (2002). Six domains of research ethics. *Science and engineering ethics*, 8(2), 191-205.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), e247.

Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A. & Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic, *Journal of Advanced Transportation*.

Recker, J. (2013). Scientific Research in Information Systems: A Beginner's Guide, Berlin, Heidelberg: Springer Berlin Heidelberg, Imprint: Springer.

Rubenstein, S., & Francis, T. (2008). Are your medical records at risk? *Wall Street Journal—Eastern Edition*, 251(100), D1–D2

Sacher, D. (2020). Finger pointing False Positives: How to Better Integrate Continuous Improvement into Security Monitoring, *Digital Threats: Research and Practice*, vol. 1, no. 1.

Sadok, M., Alter, S., & Bednar, P. (2020). It Is Not My Job: Exploring the Disconnect between Corporate Security Policies and Actual Security Practices in SMEs, *Information and Computer Security*, vol. 28, no. 3, pp.467–483.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information management & computer security*.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, 51(2), 217-224.

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, Source: *MIS Quarterly*, vol. 34, no. 3, pp.487–502.

Soni, V., Kukreja, D., & Sharma, D. K. (2020). Security vs. Flexibility: Striking a Balance in the Pandemic Era. In 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-5). IEEE.

Soomro, Z. A., Shah, M. H. & Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review, *International Journal of Information Management*, vol. 36, no. 2, pp.215–225

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Statista (2020) Annual change in incidence of computer viruses in Latin America and the Caribbean from January to March 2020. Available online: https://www.statista.com/statistics/1117225/computer-virus-latin-america/ [Accessed 5 May 2022]

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, vol. 22, no. 4, pp.441–469.

Stallings, W., and Brown, L. (2018): Computer Security: Principles and Practice. 4th Ed, Global Ed. Pearson Education Limited, Harlow, United Kingdom.

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. IEEE Access.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29(4), 263–290.

Von Solms R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*

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

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. Information systems management, 24(4), 361-372.

Walsham, G. (1995). The emergence of interpretivism in IS research. *Information systems research*, 6(4), 376-394.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse, *MIS Quarterly*.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition.

Wilson, M. & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program, *NIST Special Publication 800-50*

World Economic Forum (2022) The Global Risks Report 2022 17th Edition. Insight Report

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), 2046-2069.