University of Twente

Master Thesis

DEVELOP AND ADOPT THE ORGANIZATIONAL CYBERSECURITY CULTURE IN THE COVID-19 TELEWORKING SCENARIO

Author:

Name:	Zhenrui Niu
Programme:	Master Computer Science
Specialization:	Cyber Security
Faculty:	Electrical Engineering, Mathematics and Computer Science (EEMCS)
E-mail:	zhenrui.niu@student.utwente.nl

Assessment Committee:

Chair and first supervisor:	Dr. Maya Daneva Services, Cybersecurity & Safety (SCS)
Examiner:	Dr. Faiza Bukhsh Data Management & Biometrics (DMB)

Abstract

Since the outbreak of the Covid-19 virus, governments throughout Europe have been implementing work-from-home (WFH) suggestions to prevent the spread of the virus and safeguard the safety of individuals. Meanwhile, cyber-attacks utilizing the virus outbreak as the bait has started to appear, which has had a detrimental effect globally on the overall functioning of businesses.

In the face of the Dutch WFH regulation and the prevalence of cyber-attacks world widely, Hanshow Netherlands B.V, an overseas branch of an international company that landed in the Netherlands in 2019, has gradually realized the importance of cybersecurity as well as teleworking management. With this, the company's top management initiated an assessment of the company's cybersecurity readiness, established a teleworking guideline, and a plan to foster an organizational cybersecurity culture. As an overseas small and medium-sized technology enterprise, it was a long and difficult challenge for Hanshow Netherlands B.V to develop employees' awareness of cybersecurity, improve teleworking initiatives, maintain customer endpoint information, and ultimately develop an organizational cybersecurity culture. This master's thesis aims to design and evaluate a model that helps small and medium-sized technology companies establish an organizational cybersecurity culture. The case of Hanshow Netherlands B.V served as the foundation for the design and evaluation of this model. However, we expect the model to be relevant and valuable for contexts well beyond Hanshow.

By collecting anonymous questionnaires from all Hanshow Netherlands B.V employees, this thesis first assessed the company's current cybersecurity readiness, teleworking attitude, and cybersecurity awareness. These three dimensions were chosen because of their importance for the empirical research on the topic of an organizational cybersecurity culture. It is noticeable that Hanshow was exposed to risks and cyber-attacks during the epidemic. After comprehending the current state of Hanshow, this thesis evaluates two previously published models (Huang & Pearlson, 2019; Alshaikh, 2020) on related topics to target two phases (1) The phase of establishing a cybersecurity culture; (2) The phase of enhancing and implementing a cybersecurity culture. After combining the cultural characteristics of Hanshow, a model for establishing a cybersecurity culture in small and medium-sized businesses is proposed. In order to verify the model's feasibility, operability, and practicability, this paper also conducts an expert evaluation.

The model presented in this thesis explains how to develop organizational cybersecurity culture and the components that contribute to its formation. The proposed model is based on Hanshow's cybersecurity culture status, which categorized five practical categories for building organizational and individual cybersecurity initiatives. In the long run, this model can help organizations go beyond minimum compliance standards to create functional cyber security cultures and serve as a reference for other SMEs seeking corporate cybersecurity culture advice.

These are the thesis’s contributions: (1) a cybersecurity culture application model in which SMEs can utilize the model’s categories and components to develop and improve their

corporate cybersecurity culture. (2) a UTAUT-based evaluation of the model with eight practitioners and a subsequent interview-based evaluation with two experts. The evaluation results indicate that the model is applicable, valuable, and usable in the context for which it was designed.

Table of Content

Chapter 1. Introduction

Since March 2020, because of Covid-19, people worldwide have been forced to isolate themselves, and get into the habit of homeschooling, shopping online, and communicating online. Work From Home (WFH) has been widely adopted by many businesses and organizations, which promotes remote working, telecommuting, and online communication. Many governments recommended the adoption of WFH to prevent the virus's spread and assure public safety. As a result, many employees were caught off guard by the abrupt shift in the remote working culture and exposed to information security risks.

Employers who had never taken cyber security infrastructure seriously or educated their employees about cyber risks, as well as these employees, found themselves in an unexpected situation. Because of remote working, employees of all sizes and types of businesses now have limited cybersecurity resources and are more vulnerable than before. Most employers and IT teams had neither a proper understanding of employee vulnerability nor an excellent cyber security plan for remote workers when the COVID-19 outbreak occurred (Borkovich & Skovira, 2020).

According to recent research (Yadav, 2021)(Mohsin, 2020)(Evangelakos, 2020), the new WFH approach has increased cyber security attacks and risks. On the one hand, malicious attackers are now taking advantage of people's fear of coronaviruses. Many cyber-criminals have used the theme of coronaviruses to launch social engineering attacks since the early days of the COVID-19 epidemic, distributing various malware packages and fraudulent emails. For example, recent research claims that 94% of computers corrupted by malware were infected by an email (Mohsin, 2020). The number of spam emails has increased 300 times, and 300% in malicious URLs since 2020 February (Yadav, 2021). Recent studies have shown that the success rate of phishing attacks during the epidemic has reached 30% or higher (Pranggono & Arabo, 2021). Until April 2020, phishing email attacks associated with coronaviruses increased dramatically by 600% (Shammari et al., 2021). During the pandemic, this resulted in a rapid increase in the number of cybercrimes (Obada-Obieh et al., 2021). On the other hand, the increase of corona cases and the popularity of telecommuting were cited as the main reasons for the rise in cybersecurity risks. According to the Deloitte report, people working from home did not have the same security protections and defences as those in the workplace, 47% of whom are duped by the increased risk. (*Impact of COVID-19 on Cybersecurity*, n.d.).

In other words, working from home inevitably affects the occurrence of cyber security risks. Additionally, there is a clear correlation between telecommuting policies and the occurrence of cybersecurity risks within businesses. Many businesses gradually realize that maintaining an organization's cyber security is no longer the sole responsibility of the information technology department. Cyber security concerns must be addressed through organizational measures, as internal threats posed by human behaviour are one of the most challenging aspects of security to control. Needless to say, telecommuting has gradually become a habit and a way of working due to the ongoing epidemic and is likely to be adopted in the long run. Raising

risk awareness among employees, implementing a robust cyber security policy, and fostering an appropriate organizational culture are the top priorities for long-term corporate security during telework.

This Chapter is the introduction to a master graduation project on cybersecurity and WFH. Section 1.1 of this paper outlines some of the definitions used in the thesis to establish and clarify the meaning of the concepts used in the study. Then, this Chapter discusses organizational culture, cybersecurity culture, telework, and cybersecurity performance in Sections 1.1.1, 1.1.2, 1.1.3, and 1.1.4. Finally, the paper will elaborate on the background of the study in Section 1.2. Based on the background and conceptual elaboration, the study's objectives will be further identified in Section 1.3. And in Section 1.4, this Chapter will further clarify how the research objectives should be deployed and achieved.

1.1 Concepts and Definitions

1.1.1 Organizational culture

Organizational culture (OC) is a topic that has been extensively studied in the literature., This thesis uses Schein's definition (2017) as it is known as the most widely recognized definition of organizational culture: an OC is "*a pattern of basic assumptions invented, discovered, or developed by a given group in the course of learning to cope with its external adaptation and internal integration problems, which has been valid enough to be considered effective and, therefore, is taught to new members as the correct way to perceive, think, and feel in relation to these problems*."(Schein, 1983). In short, it can be identified as "the way we do things around here" (Lundy & Cowling, 1996)

OC is based on cultural norms and represents a collective way of thinking and behaviours. Therefore, aligning employees with the same personal values and needs can develop great energy and help promote a thriving organization (*The Leader's Guide to Corporate Culture*, n.d.). Schein (2017) states that models, beliefs, and values constitute the three levels of culture. These values are transmitted and collectively accepted within the organization to enhance a sense of belonging and common good. (*Organizational Culture and Leadership - Edgar H. Schein - Google journal*, n.d.)

1.1.2 Cybersecurity culture

Cybersecurity culture (CSC) is a sub-component or integral part of organizational culture comprised of increasingly more observable layers (Corradini, 2020). A straightforward definition of cybersecurity culture is *"the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies"* (da Veiga et al., 2020). CSC is a sub-component of OC that encompasses a layer of models, values, and fundamental assumptions. However, many have referred to another layer as information security knowledge, which is critical for employees to comprehend the significance of specific rules, functions, and

behaviours (Corradini, 2020). A mature cybersecurity culture requires employees' awareness of security and risk to adapt quickly to changing threats.

1.1.3 Cybersecurity culture and organizational culture

According to the definition discussed above, CSC can be considered a subset of OC, as it is composed of elements belonging to different levels of the OC model. The tangible layer of models represents the requirement for CSC technical tools and awareness training. The unspoken layer of value is shared within organizations to foster a sense of belonging; in the case of CSC, this refers to papers and documents describing the organization's principles. While the most fundamental level of unspoken belief can be defined as the unspoken manner in which employees interact with and evaluate technology devices.

1.1.4 Teleworking/WFH

Teleworking or telecommuting is working remotely or from home with the help of online technology through the integrated use of Internet-connected communication systems, email, telephone, and other online digital applications. The term "working from home" is more widely recognized as "telecommuting" in the United States and "teleworking" in Europe. The term telecommunication indicates that WHF requires the utility of ICT devices, for instance, computers, internet, and mobile phones, to comprise the remote working at home (Dockery & Bawa, 2020).

Due to the contagious and novel infection aftereffect of COVID-19, the government and WHO have taken several public prevention and infection control measures, such as the restriction of mass gatherings to prevent public transmission. In response to the government's measures, many companies have turned to digital technology to continue their operations, and employees have adopted telecommunications software to work at home.

Recent uprising cybersecurity attacks and information leakages have proven the disadvantages of the massive adoption of teleworking. For instance, Tessian's Data Loss Prevention 2020 report (*The State of Data Loss Prevention 2020 | Tessian Research*, n.d.) reveals how the necessary shift to WFH poses security challenges for enterprises as many human factors in an organization are often ignored and not well prepared in strong cyber defence. According to 2020 employee statistics from Help Net Security, the number of remote working jobs in the U.S. has more than doubled in the last four years; meanwhile, data security is at a greater risk as the staff is more likely to send important and confidential company information to personal email accounts, with the usual intention of working on documents at home (*Employees Abandoning Security When Working Remotely - Help Net Security*, n.d.). In other words, teleworking significantly impacted an organization's cybersecurity performance.

1.1.5 Organizational culture & cybersecurity performance

Cybersecurity performance (CP), in general, can be considered as *"The security benefits anticipated by organizations due to readiness to combat cyber-attacks*"(Hasan et al., 2021). However, CP is a complex concept that includes many indicators and measurements to

illustrate a tangible value. To make cybersecurity performance measurable, this research will use cybersecurity readiness (CR) as the presenting indicator in showing the level of cybersecurity performance. Definition of cybersecurity readiness can therefore be defined as "The level of an organization's awareness, preparedness and commitment to prevent and combat cyberattacks"(Hasan et al., 2021).

Many scholars confirmed that OC significantly impacts information security performance (Tang et al., 2015). OC plays an irreplaceable role in guiding an organization's attitude and employee practice by defining guidance and beliefs for employee behaviours. According to Hsu et al. (2012), cybersecurity is influenced by the organisation's culture, which is shaped by mimetic, coercive, and normative pressures. In detail, Hsu et al. (2012) claim that OC impacts CP by encouraging employee contribution to increase their sense of belonging and responsibility toward the organizational cybersecurity. On the other hand, OC also defines employee training and risk awareness which enriches the security knowledge and operation of the organization. Hence, OC can positively affect the performance of organizational cybersecurity performance.

Based on the various variables mentioned above, this research develops a cyber security readiness model (Fig. 1.1 and Fig. 1.2) to illustrate the proposed relationship between the OC, CSC, teleworking, and organizational cybersecurity readiness.

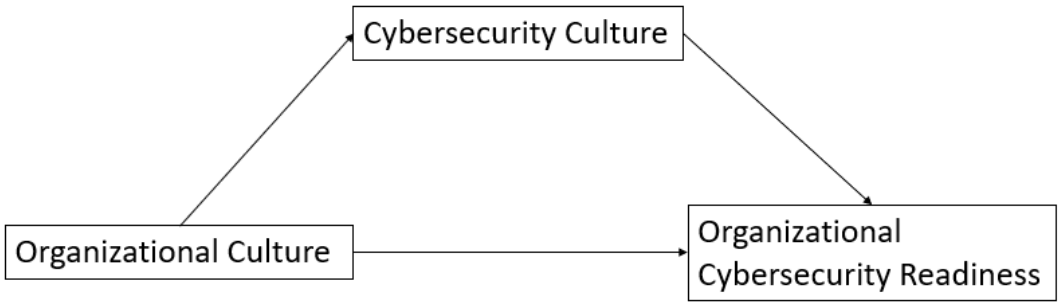


Figure 1.1: The relationship between OC, CSC, and OR

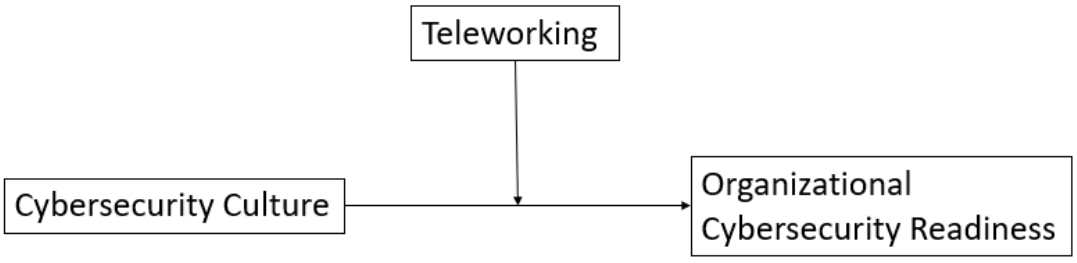


Figure 1.2: The relationship between CSC, Teleworking, and OR

Since CSC is a direct determinant of organizational network security performance in remote working situations, this study focuses on the relationships shown in Figure 1.2. The ultimate

goal of this master thesis project is to explain how to evaluate and build a complete CSC under teleworking principles. Furthermore, how to improve an organization's cybersecurity performance in the presence of a complete CSC to face future long-term teleworking scenarios.

1.2 Context

This master project has been done in the organizational context of Hanshow Technology, the world's leading provider of electronic shelf labels and omnichannel digital store solutions. Hanshow Netherlands B.V. was established in 2019 in Amsterdam, the Netherlands, and it has cooperated with major supermarket chains such as Ahold Delhaize, Jumbo, and Dirk in the Netherlands.

Hanshow's main line of products is electronic shelf labels, which are installed and utilized primarily in the retail industry. Electronic Shelf Label (ESL) is an innovative product that replaces traditional paper price tags in various retail scenarios. With the help of remote-control technologies such as NFC, remote operation software, and wireless communication protocols. Hanshow's ESLs can update inventory data, change prices remotely, navigate tag locations, and flashlights for flexible use in various retail scenarios. Other product chain includes digital signage, LCD ESL, Kiosk payment, and smart trolley.

All of Hanshow's products are very dependent on network security management. The products' selling point is to allow remote management of ESL, seamless data synchronization, and operational intelligence through the AIOT platform, OTA (over-the-air) technology, and IoT capabilities. To install any Hanshow product, an integrated access point is required in the store scenario. Hanshow claims that its products have a built-in AES chipset (AES128/AES256) and HTTPS for end-to-end secure data transfer to ensure the security of command communication. In other words, Hanshow needed to adapt to the general trend of local telecommuting in the Netherlands while ensuring its cybersecurity for its business operations.

1.3 Research Goal

In the Netherlands, facing the mainstream trend of WFH, developing a sound organizational cybersecurity culture, and having cybersecurity readiness for telecommuting are crucial for Hanshow. Therefore, the following research objective was developed:

To design and validate a model for Hanshow that addresses cybersecurity readiness in teleworking to develop a long-term cybersecurity culture.

1.4 Research Questions

In order to achieve the above research goal, this thesis addresses the following research questions (RQs) :

RQ1: What stage is Hanshow at in terms of forming an organizational cybersecurity culture during WFH?

RQ1.1: What is the current remote working possibility within Hanshow?

RQ1.2: What is the attitude of Hanshow's employees towards WFH?

RQ1.3: What are the current cybersecurity awareness and readiness state at Hanshow?

RQ2: What challenges and problems that Hanshow experienced during the WFH period so far?

RQ2.1: What measurement or method has Hanshow currently taken in response to the teleworking challenges?

RQ2.2: What consequences for Hanshow if the proper cybersecurity management can not maintain due to teleworking?

RQ2.3: What basic WFH recommendations can Hanshow use to keep and maintain teleworking secure?

RQ3: What method can Hanshow adopt to contribute to the creation of organizational cybersecurity culture?

RQ4: How useful and usable is the newly proposed model from the perspective of practitioners working in the field?

1.5 Outline

In the following Chapters, this thesis will be classified in this way. Chapter 2 will go into detail about the methodology used in this thesis. Chapter 3 corresponds to RQ1 and RQ2 which presents the results of the internal company interviews and questionnaires and the adoption of those basic recommendations that can address cybersecurity issues during WFH. Chapter 4 screens contextually relevant articles and theoretical frameworks based on the questionnaires of Hanshow employees and the current situation of WFH. This Chapter also discusses the relationship between cybersecurity culture and corporate cybersecurity readiness for RQ3 and how to build a model for Hanshow to foster and improve corporate cybersecurity culture and readiness from scratch. To further validate the feasibility and validity of the model, Chapter 5 outlines the expert evaluation to verify the validity of the model. Finally, Chapter 6 discusses the implication and limitations of this thesis. Chapter 7 concludes the thesis by summarizing the answers to the research questions and recommendations for practitioners and future research.

Chapter 2. Approach and Methodology

This Chapter describes the framework and the method of building the model of this study. Section 2.1 describes the model-building approach used in the article; based on the DSRM model, this paper will follow each segment for the methodological discussion. Next, Section 2.2 focuses on the methodology of the problem investigation. Then, Section 2.3 discusses how the specific treatment was created and implemented. Finally, Section 2.4 explains the practicality and feasibility of the concluding argumentation method.

2.1 Method

A proper method of developing a valid model in context must be chosen to fulfil the ultimate research goal. This article will use the Design Science Research approach developed by Peffers et al., 2007, shown in Figure 2.1.

The Design Science Research Methodology (DSRM) will be used to demonstrate and define the various phases of this research. The ultimate goal of DSR is to solve a problem by creating a model; the core steps of DSR are divided into two sections; the first section involves defining the model's requirements and problem areas in a realistic context. The second section is the validation and establishment procedure, which is responsible for establishing a feasible and practical solution to the situation.

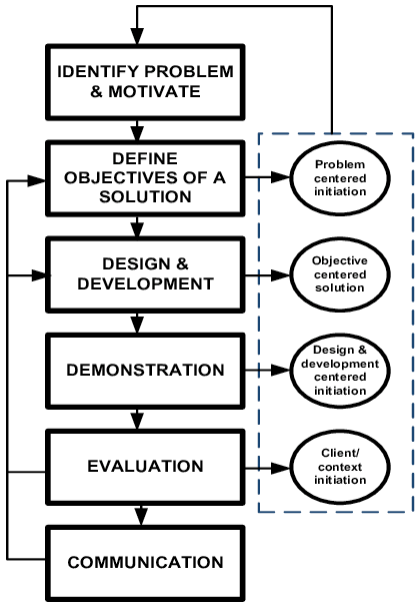


Figure 2.1: The Design Science Research Methodology (DSRM)

A complete design loop requires a clear identification of the problem and initiative in solving the solution. The ultimate step often requires a communication procedure for further improvement. In this research, initiative and motivation have been described as the thesis goal in Section 1. Because the proposed model in this thesis has not yet been implemented at

Hanshow, it is impossible to address the communication session. Therefore, the communication session will be omitted. Instead, this thesis will primarily focus on *the three steps* of the design cycle which is a cycle loop that can be iterated over many times. The *first step* is problem-centered initiation and means defining the research objectives and problems for investigation. The *second step* is the design and development step focusing on the objective-centred solution. The *final step* is to evaluate and validate the treatment.

First, an interview questionnaire will be prepared for Hanshow's employees as an internal investigation of how WFH was implemented from the cybersecurity perspective. This interview aims to define the problems and investigate the challenges that Hanshow faced in dealing with WFH regulation. Besides, it helps to understand Hanshow's current corporate culture and what stage in the cybersecurity culture Hanshow is currently at. To answer these questions, we will first investigate Hanshow's cybersecurity issues during the WFH period and what primary teleworking structure Hanshow adopted. What are the existing methods and initiatives that can be taken in a teleworking manner? And we will optimize the questionnaire base on Georgiadou, Mouzakitis & Askounis's (2021) method to address Hanshow's current standing in formulating organizational cybersecurity culture. The detailed methodology and interview aspects will be covered in Section 2.

For the *second step*, this thesis proposes an assessment method for measuring cybersecurity culture and cybersecurity readiness. Based on the current cultural situation in Hanshow, we will select the most applicable method from the previous literature review. After a throughout the investigation, we will decide which Hanshow can adopt specific frameworks or concepts. The selection and design approach will be illustrated in Section 2.3. And the proposed solution will be discussed in Chapter 4.

The third step includes an evaluation study, in which the proposed assessment method was reviewed with practitioners and their feedback was collected and analyzed. In order to verify whether the model proposed in this thesis applies to Hanshow and other international small and medium-sized enterprises. In this step, a group of experts will be invited to give their opinions on the proposed model and verify the initiatives' validity. The proposed validation treatment will be further described in Section 2.4.

However, the remaining circular step (see Figure 2.1) can hardly be addressed within this research. This thesis aims to provide an ultimate solution for Hanshow to deal with cybersecurity issues during the WFH period, which requires long-term observation and deployment. It is not easy to verify the cyclic process's effectiveness in a short time. Therefore, this research mainly focuses on the first three steps of the cycle to investigate and define the problem, design the solution, and the treatment evaluation.

2.2 Problem Investigation

2.2.1 Initial stakeholder analysis

For the purposes of this study, it is essential to recognize that a cybersecurity culture is an organization-wide norm and should be an internalized mindset and behaviour of all employees,

rather than something external or delegated. Numerous studies emphasize that a cybersecurity culture should involve every employee, not just IT professionals: regardless of position, everyone must know how to behave in a reasonably regulated manner in the digital environment (Corradini, 2020).

Therefore, this thesis will treat Hanshow employees as a whole without division into comparative groups to proceed with the research process. However, for this thesis, it is essential to address the following stakeholders.

- Hanshow Nederland B.V. – Sponsor
- Hanshow employees – End-users of the model

Hanshow Nederland B.V. is the hosting organization of this study as they are supporting the project to address local cybersecurity arrangements during WFH. Hanshow employees will be the research group and the beneficiary group of the proposed model.

The development of a safety culture is a time-consuming process influenced by a variety of factors. The Cybersecurity Culture Framework of Georgiadau et al. 2021 was chosen as the assessment and evaluation method for the security culture of individuals and organizations in this study. As shown in Figure 2.2, this framework categorizes organizational and individual security factors into different dimensions and domains. We use this framework as the foundation of our interview-based research step. The following sections capture the two-dimensional factors to clarify the current cybersecurity cultural status of Hanshow.

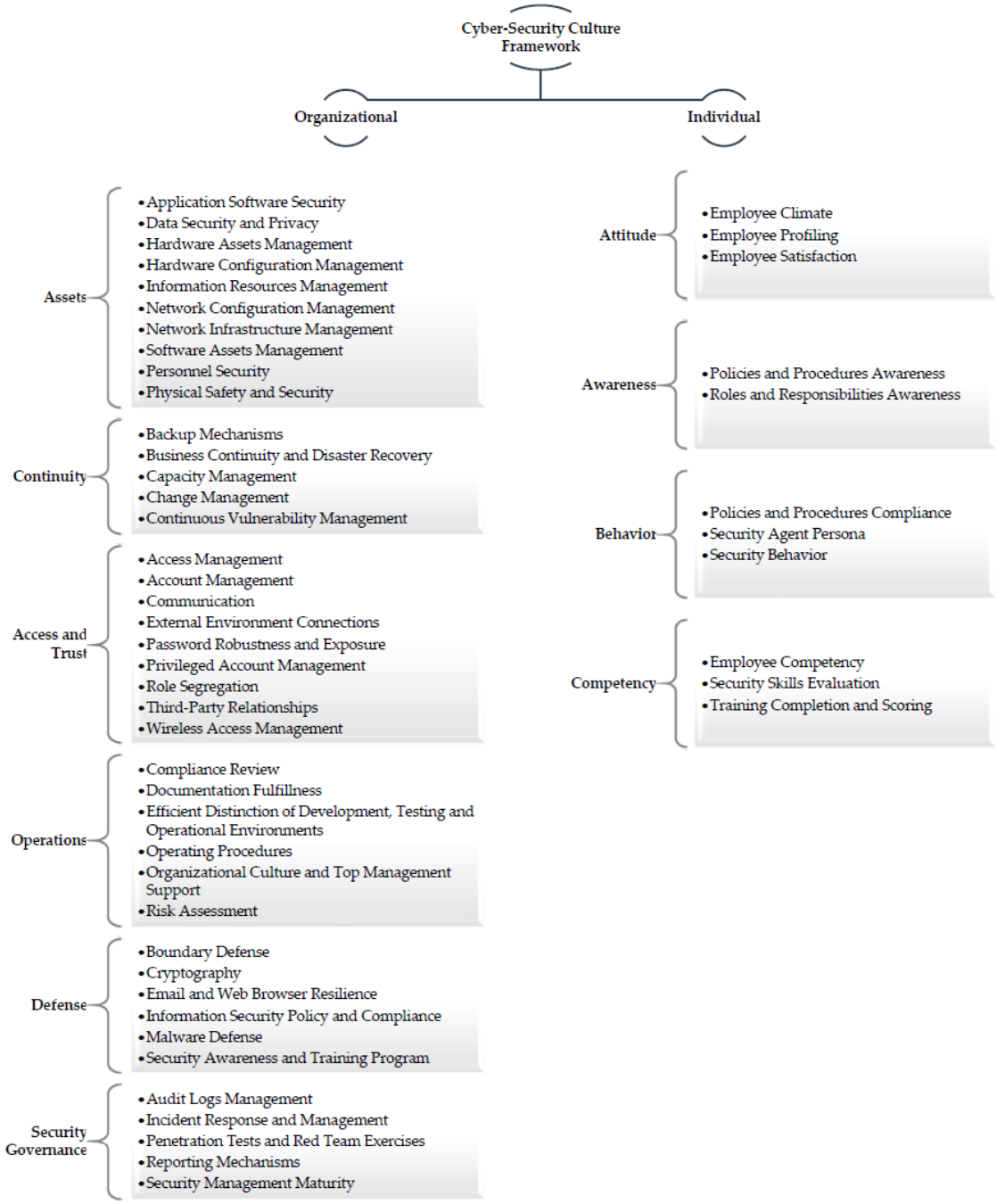


Figure 2.2 Cyber-Security Culture Framework

2.2.2 Interviews

The ultimate aim of the interviews with Hanshow employees is to find answers to some of our research questions and to generate an applicable model (i.e. an assessment method) for Hanshow to adopt internally. Thus, an interview questionnaire was created to answer the following research questions:

RQ1: What stage is Hanshow at in terms of forming an organizational cybersecurity culture during WFH?

RQ1.1: What is the current remote working possibility within Hanshow?

RQ1.2: What is the attitude of Hanshow's employees towards WFH?

RQ1.3: What are the current cybersecurity awareness and readiness state at Hanshow?

RQ2: What challenges and problems that Hanshow experienced during the WFH period so far?

RQ2.1: What measurement or method has Hanshow currently taken in response to the teleworking challenges?

RQ2.2: What consequence can Hanshow meet if the proper cybersecurity management can not maintain due to teleworking?

RQ2.3: What basic WFH recommendations can Hanshow use to maintain teleworking cybersecurity efforts?

The interview study will assess Hanshow's current cybersecurity culture readiness during WFH using the Georgiadou, Mouzakitis & Askounis (2021) questionnaire as its core. We implemented this questionnaire as a web-based survey that assesses the cybersecurity culture of global companies for employees WFH during COVID-19 on a global scale. This questionnaire proposes a cybersecurity culture framework based on a domain-neutral security model that incorporates key factors that influence and shape an organization's cybersecurity culture, which is divided into two levels, organizational level and individual level.

The Cybersecurity Culture Framework (Georgiadou et al., 2021) includes 10 security dimensions, with 52 domains assessed by more than 500 controls. In this thesis, the questionnaire narrows the questions to no more than 26 and provides a judicious distribution of organizational and individual levels. The questionnaire is attached as Appendix A.

Culture – as it describes the values, attitudes, goals, and knowledge outlined by the working environment, is crucial to identifying the organizational infrastructure and security countermeasure. Questions Q1-Q10 represent an organisation's overall technological and security readiness to assess the cybersecurity cultural status and readiness. Questions 11-12 attempt to identify remote workers' security behaviours, attitudes, and abilities by examining their emotions, thoughts, and beliefs. Moreover, probing any security incidents that employees encounter during the WFH period.

Questions Q18-Q22 refer to the generic information, including demographic indicators, stakeholder analysis, and work-from-home situations. Those questions allow us to categorize and analyze gathered results according to different dimensions and age groups. This questionnaire perfectly addresses the set of RQ1 because it can indicate the remote working possibility, current WFH attitude, current teleworking measurement, and states of cybersecurity readiness.

However, to answer RQ 2.2, an open-ended question is added, "What consequences do you think Hanshow will experience if proper cybersecurity management is not maintained due to remote work?"

To answer RQ2.3, we aim to clarify the WFH IT management suggestions for Hanshow to adopt. In this case, we summarize the "Measures for Mitigation of Cyber Security Challenges" completed in the literature review. See details in Table 1. We classified those measures at the organizational level as the multiple-choice options for employees to select in Q26.

Measures for Mitigation of Cyber Security Challenges	Source
1. User Education 2.Virtual Private Network (VPN) 3. Enable multi-factor authentication (MFA) 4. Ensure all devices firmware is up-to-date 5. Ensure that up-to-date anti-malware software is activated in all network-connected devices 6. Enable strong company online policy 7. Segmentation and separation 8. Physical security of home office 9. Intrusion detection system (IDS) 10. Security incident and event management (SIEM).	(Pranggono & Arabo, 2021)
the Due diligence of the organization, due care of the organization, due diligence of the end-user, due care of the end-user.	(Dumitru & Ion, 2020)
1. Avoid clicking on any UNKNunknOWN messages with links 2. Files should be backed up and stored in devices other than your system 3. Examine any URL or email address 4. Install legitimate and latest anti-virus software 5. Administrations' vulnerabilities of the system 6. Organizations are advised to reformat their BCPs and secluded working policies 7. Verify legit website before advancing personal info	(Pandharipande & Parashar, 2020)
1. Cybersecurity awareness 2. Cybersecurity governance frameworks 3. Cybersecurity protocols	(Chigada et al., n.d.)
1. Training protocol (organization level) 2. Education protocol (individual level) 3. Policy protocol (organization and government)	(Mashud et al., 2020)

1. Detective Control (Remote Monitoring; Incident Management) 2. Preventive Control (Employee training; Access controls; Backups and BIA-Recovery Plans; VPN, MFA: Vendor security controls; Endpoint security and Patching)	(Sebastian, 2021)
Introduced the OSI seven-layer model and introduced the eight-layer "education people."	(Chapman, 2020)
Introduce apprenticeship training and claim the cyber security industry must start valuing apprenticeships.	(Chapman, 2020)
1. Creating a security-focused culture 2. Device and account security 3. Safely using the cloud	(Sabin, 2021)
1. COVID-19 Malicious Websites Defense 2. COVID-19 Malicious Emails Defense 3. COVID-19 Malicious Mobile Apps Defense 4. COVID-19 Malicious Messaging Defense 5. COVID-19 Misinformation Defense	(Ahsan Pritom et al., 2020)

Table 1. Countermeasures for Mitigation of Cyber Security Challenges

2.2.3 Sample Size

The validity of the original questionnaire (Georgiadou, Mouzakitis & Askounis, 2021) was tested extensively with a global sample. The optimized questionnaire in this study added a few questions and applied only to Hanshow employees. Therefore, no additional pilot validity testing was conducted. Employees of Hanshow Nederland B.V. are chosen as participants, with a total number of 32 that participated in this survey.

The questionnaire was presented as a web-based questionnaire and distributed via Wecom, the work platform used by Hanshow. All Hanshow Nederland B.V. employees were asked to participate, with the company's administration assisting in confirming the number of participants.

The questionnaire consisted of 26 questions, including subsequent modifications and additions. The survey was conducted from April 15th to April 20th. The time limit was 5 days for all employees to complete the questionnaire. The questionnaires could be viewed by the users of the Wecom system and converted to Excel for further analysis.

2.2.4 Data Analysis

After data collection, all the questionnaire answers were encoded into Excel and were further classified into different demographic features. The indicators for the questionnaire questions are further categorized and refined for analysis. The main categories were created based on the questionnaire questions that correspond with the indicators. The following 10 categories were constructed:

- Remote working possibility
- Security awareness and readiness
- Hardware assets and security management
- Change management
- Remote working collaboration
- Security incidents management
- Employee WFH attitude
- Demographic Figure
- Consequence of mismanagement
- WFH recommendation

These categories are listed and analyzed in the result section (Chapter 3) in the form of sub-headings.

Since there were some open-ended questions, some answers required some explanation and summarization, but no extensive explanation was needed. The explanations were based on the context and the knowledge of the researcher.

The aim is to analyze the current state of cybersecurity culture within Hanshow, the opinions, and the difference between various departments and groups. The ultimate

solution for the comprehensive analysis is to clarify the current state of the culture within Hanshow and thus provide targeted suggestions for optimization.

2.3 Treatment Design

Our previous literature review identified several frameworks and models that can be viable alternatives or candidates for Chinese companies like Hanshow that are eager to adapt to foreign cultures and survive long-term teleworking remotely (Zhenrui, 2022).

The selected treatments are mapped and combined to match Hanshow's circumstances. The framework's concepts and components are extracted to address the identified challenges illustrated by the research questions. The survey results served as the basis for illustrating the current needs and deficiencies of Hanshow. Experts ultimately validate the mapping of the model within Hanshow. And some additional recommendations are made for Hanshow to improve its long-term cybersecurity performance.

2.4 Treatment validation

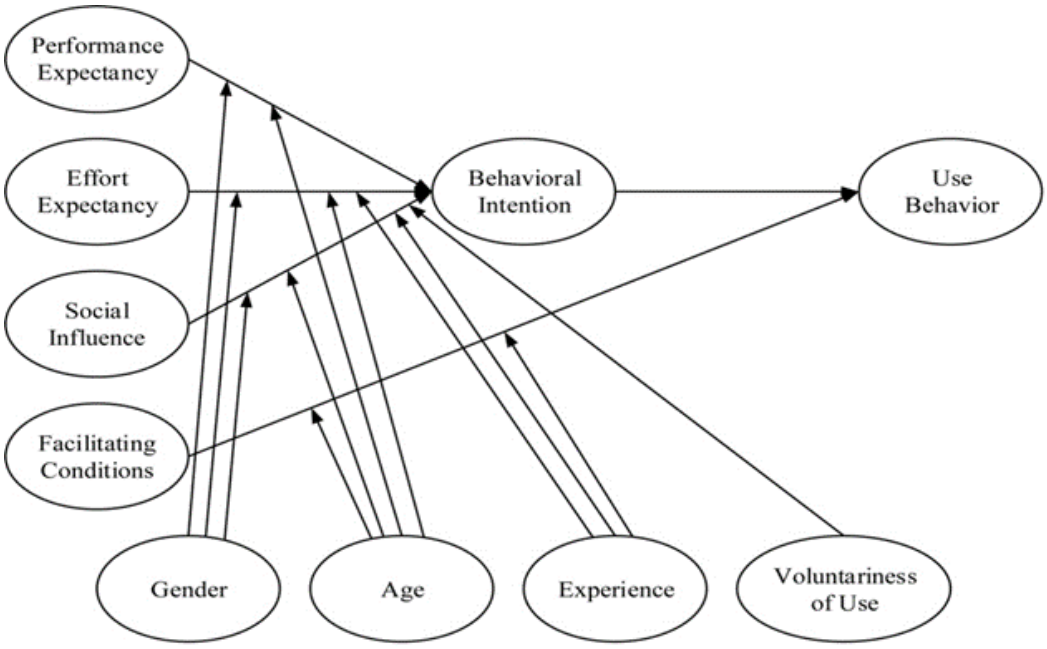


Figure 2.4. The adapted UTAUT model.

This thesis utilizes the UTAUT model to assess the validity and acceptance of the proposed treatment for Hanshow. The UTAUT model is an integrated model of user intention, which contains six primary constructs shown in Figure 2.4: performance expectancy, effort expectancy, social influence, facilitating conditions, behavioural intention, and usage behaviour (Venkatesh et al., 2003). This thesis selects four constructs from the UTAUT model and will evaluate those factors by conducting an expert evaluation. The selected constructs are performance expectancy, effort expectancy, behavioural intention, and social influence. The detailed evaluation section will be illustrated in Chapter 5.

The invited two experts are technical professionals from Hanshow, together with 6 subordinates of their departments. They will participate in a short questionnaire base on the constructs of the UTAUT model. They have all been with Hanshow for more than two years and have a deep understanding of the culture and technical aspects of the company.

To further understand the feedback and applicability of the proposed model, the two experts will participate in an expert interview to provide more focused and constructive, meaningful comments on the model proposed in this study.

One of the experts is the technical director in charge of SAAS. He has a professional technical vision of SAAS security. Another expert joined Hanshow from Huawei and is responsible for cybersecurity consultant in large project delivery. In particular, they can provide a different perspective but professional advice on the proposed Hanshow treatment.

Chapter 3. Result

The findings of the questionnaire-based study will be presented in this chapter to help determine the current state of Hanshow's cybersecurity culture and employees' willingness to adopt WFH in the long run. This section aims to locate Hanshow's current status to match the coherent model in forming long-term cybersecurity culture during WFH by analyzing the questionnaire results. Covid-19 was still aspiring within the Netherlands at the time of this thesis. As a result, the results of the survey can accurately reflect Hanshow's current situation and operations when it comes to teleworking. The following sections will be divided according to the sub-research questions and their corresponding indicators. Section 3.1 will show the demographics of all survey respondents. From Section 3.2 to Section 3.11, the different indicators of the questionnaire will be shown in order.

In detail, Sections 3.2 to 3.10 describe the attitude of Hanshow's employees toward WFH, their current IT assets usage, Hanshow's existing remote working management, and teleworking issues. Examining these questions sequentially can provide a comprehensive portrait of Hanshow's existing cybersecurity culture. Does Hanshow now promote a culture of safety? How far along is Hanshow in maturing their cybersecurity management? Which model can Hanshow employ to establish the required culture? In Section 3.11, a short interview invited four employees to describe cybersecurity attacks they encountered during Covid-19.

Furthermore, a concrete quantitative analysis is conducted in Section 3.12, in which a series of correlation and regression analyses are presented. That analysis aims to clarify in-depth Hanshow cybersecurity attitude and performance. Section 3.13 will eventually describe the findings in a manner that answers research questions RQ1 and RQ2. Eventually, after an interpretation, this chapter concludes with a summary in Section 3.14.

3.1 Demographic information

The questionnaire is sent to all Hanshow Nederland B.V employees with the management team's help. Therefore, the internal validity, completeness, anonymity, and privacy of the questionnaire are all ensured primarily.

In the end, 32 employees joined the survey and completed the online questionnaire at around 10 min as the average completion time. Around 35% of the Hanshow employees were aged between 25-34 years old, while 25% were aged between 35-44 years old and 18-24 years old (Figure 3.1a). Namely, Hanshow has a relatively young employee group. According to Figure 3.1b, the education level is relatively high that 69% of employees obtained a Master’s degree and 16% had a Bachelor’s degree. None of the employees has a degree lower than a Bachelor’s diploma. Employees provided feedback to our survey from the following department sectors Sales & Pre-sales,

including Project Manager (35%), Technician & After-sales (25%), Logistics (6%), Human Resources (6%), Accounting & Finance (6%), Legal Affairs (6%), Administration/operations (6%), Marketing (10%) (Figure 3.1c). 31% of technicians and project managers indicate that their work position is best described as IT professional. Of the remaining employees, 28% are Managers, and 16% are Specialists (Figure 3.1d).

It is important to emphasize that this job function and department classification is quite dependent on the corporate structure and identity of Hanshow. As described in Chapter 1, Hanshow is an information technology company with many IT department employees and IT professionals. Meanwhile, the organizational structure is relatively simple, as Hanshow is a B2B company that requires less employee support and coordination.

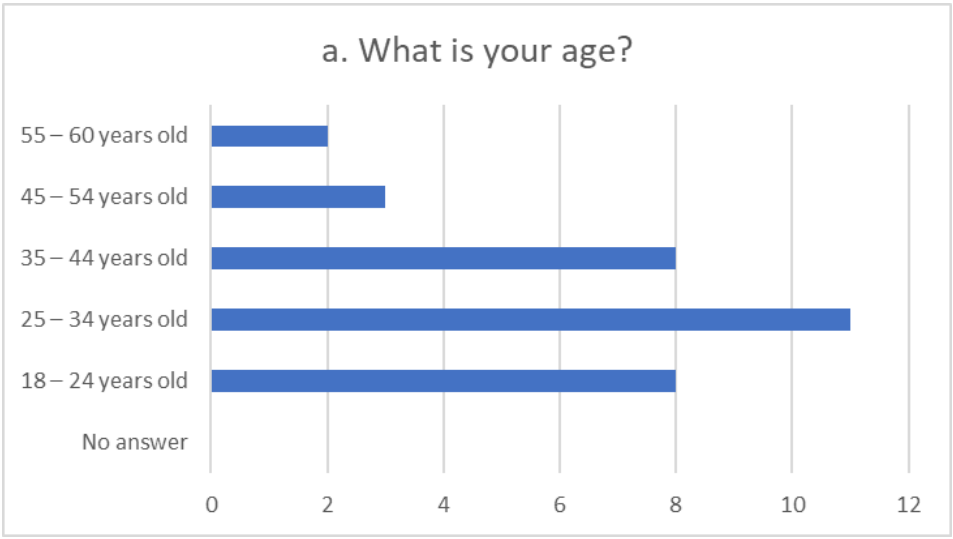


Fig. 3.1 **a**. Survey general demographic information(age)

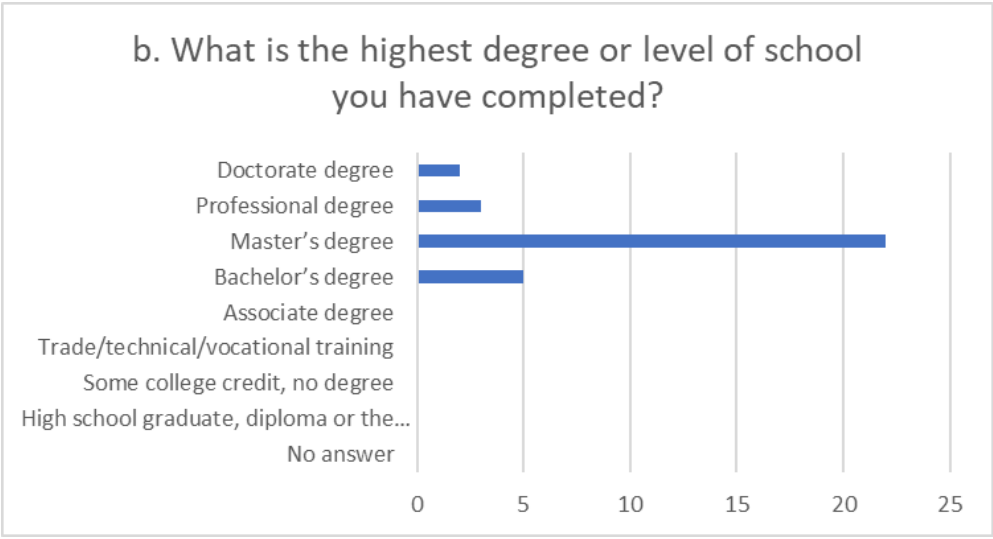


Fig. 3.1**b**. Survey general demographic information(education)

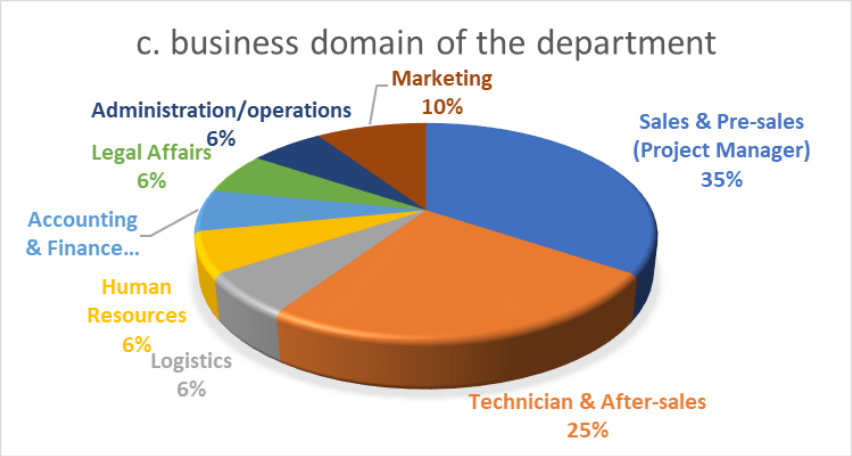


Fig. 3.1 **c**. Survey general demographic information(business domain)

Fig. 3.1**d**. Survey general demographic information(professional role)

3.2 Remote working possibility

This section aims to capture employees' possibility to adopt remoting working during Covid-19. By asking, "Before the COVID-19 crisis, were you able to work from home?", the survey aims to interpret the possibility for Hanshow to conduct extensive teleworking and the difficulty level for Hanshow to adopt teleworking management. Figure 3.2a indicates that up to 47% of employees could not work from home before Covid-19. Figure 3.2a also indicates that 81% of the Sales and Pre-sale employees were free to work from home before Covid-19. Collectively, they specify that *"the culture of Hanshow recommends Sales to contact and meet customers in person rather than stay in the office to operate paper works"*. However, almost all of the technical and After-sales employees (7 out of 8) reported they had no teleworking possibility before the pandemic. After a brief investigation, the feedback from the employees reveals the main reason is the product's functional and operational limitations.

Hanshow's products require real-time backend data interfacing and monitoring to ensure stable operations. In order to maximize the security of customer information, the after-sales and technical teams generally choose to work in the company's protected

network environment. In addition, the after-sales team often needs product samples in the office for repeated testing and confirmation when customers report a failure in the product operation. It means that after-sales and technical staff need secured network IP and product samples to embrace teleworking. The feedback confirms this from IT professionals, shown in Figure 3.2b, 8 out of 10 claim they could not help at home before the Covid-19 outbreak.

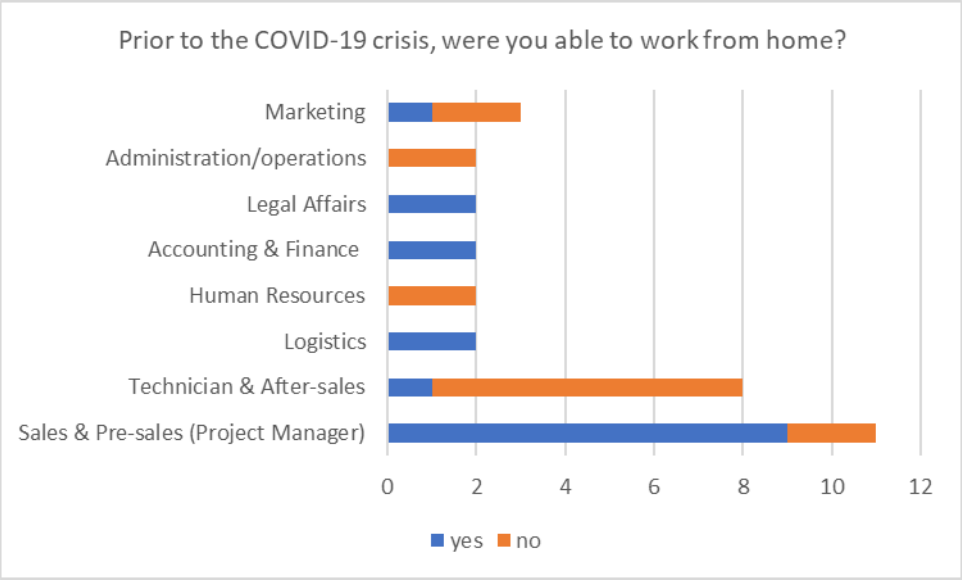


Fig. 3.2 **a**. remote working possibility per business domain

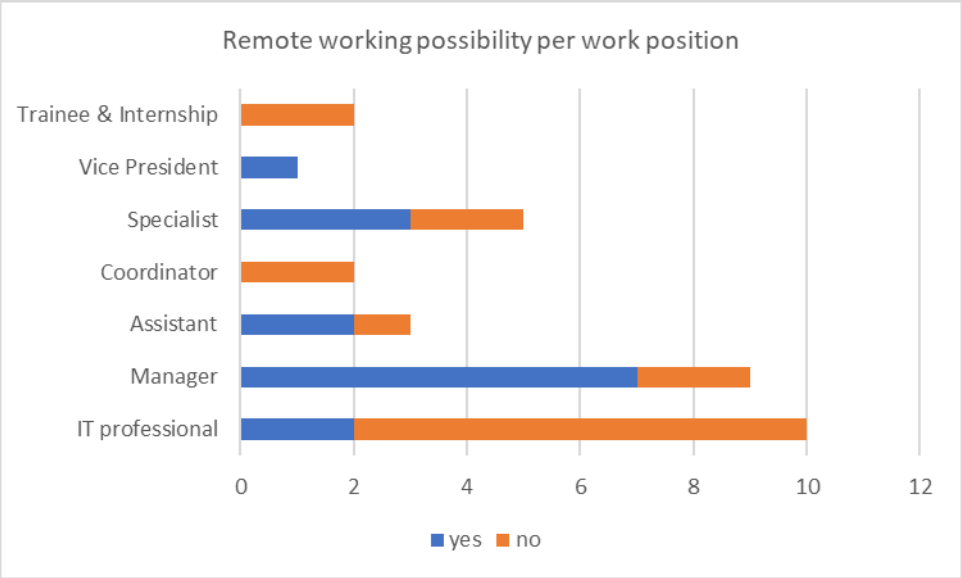


Fig. 3.2 **b**. per work position

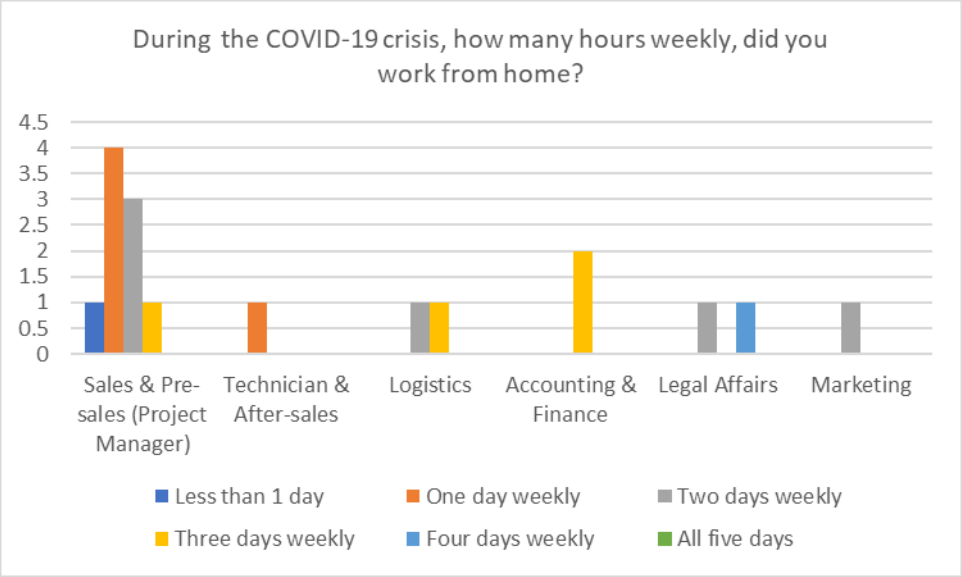


Fig. 3.2 **c.** hours WFH

3.3 Security awareness and readiness

Covid-19 pandemic has created a real breakthrough for the malicious hacker to invade the company's internal system. Research reveals many malicious malware is prevalent due to remote management (Mohsin, 2020). FBI 2020 reports indicate the U.S. has undergone 600% successful attacks skyrocketed and the global by 300% since the COVID-19 pandemic (Borkovich & Skovira, 2020).

Organizations must adopt security guidelines and defence against possible security risks. Fostering security awareness and readiness within the company's internal culture is the insurance for remote management.

At Hanshow, there were rarely any security guidelines regarding working from home. Figure 3.3b indicates that 75% of employees did not receive any training or protocol regarding remote working cybersecurity matters. Compared to others, the Legal Affairs department employees claim *"the security guideline can be found in the new employee training manual and courses."* They all helped monitor and develop the training content to remember the security protocol details. Some Technicians bears the importance of information security, so they also remember the guideline covered in the newcomer's training. However, Hanshow did not re-emphasize the security guideline before the WFH regulation. As a result, most employees did not recall an existent benchmark regarding remote working security management.

Organizational insider threat is one of the biggest threats to an organization's network security. The most common internal threat within every organization is employees who lack cyber awareness or have limited skills that unwittingly take actions that leak the company's information. In his 2021 research, Chapman emphasises that network security's eighth layer needs to become intertwined in building the company's security culture. A consumable dedicated training and policy updates (Chapman, 2021). The

policy should lay out the guidelines for computer network access and inform staff about the requirements for protecting corporate resources and underlining the risks.

Employee training and cybersecurity guidelines largely determine if employees can foster risk awareness and support making a key blow to the overall cyber security organizational culture. To generate a long-term cybersecurity culture, ensuring a robust corporate network access management is essential to cybersecurity readiness. Nevertheless, Hanshow did not foster a mature security guideline or updated policy regarding WFH (Figures 3.3a and b).

According to Table 2, the most common cybersecurity suggestion (28%) is to "Ensure password security and usage". In comparison, 22% of employees received a warning of "Be careful of phishing emails" and 19% of document disclosure. Namely, all those warnings are general rules and no specific guidelines regarding WFH regulation. The cybersecurity readiness of Hanshow can be considered weak and initial.

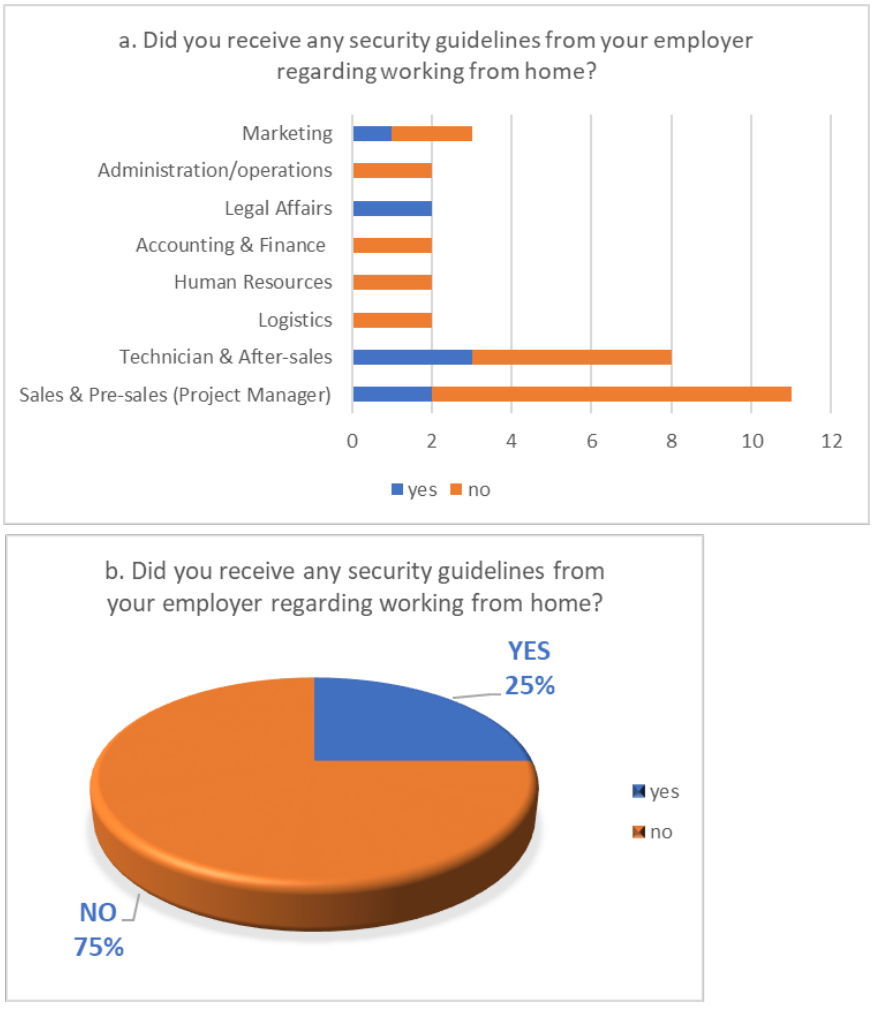


Fig.3.3. Security awareness and readiness **a.** per business domain **b.**overall

Top security guidelines	% of participants in our study that received the guidelines
Ensure password security and usage	28%
Be careful of phishing emails	22%
Internal documents and ppt cannot be disclosed	19%
Use the company's corporate email to dock internal information	13%
Lock Laptop when unattended	9%
Using company laptop for office work	9%

Table 2 The top security guidelines provided by Hanshow

3.4 Hardware assets management and security

Developing companies often do not have the time to provide timely remote network management in accordance with the system of working from home in the event of an epidemic. But companies that are aware of cyber risks often require employees to use company computers as their only office appliance. To enhance the severity of the previous Hanshow finding, around 37% of the teleworking assets were personal (Figure 3.4.1a), and up to 69% of devices are not fully controlled by the organization. The result indicates that only 63% of employees utilize corporate assets while WFH. But many of them use multiple devices while teleworking and 56% of devices are not fully controlled by the organization. To make numbers look worse, 13% of the devices used by employees have no control by the organization. In fact, 12 Hanshow employees mentioned they are using their personal desktops while teleworking. 4 employees also use their iPad or other tablets for corporate work. Not to mention, all 32 employees are using their personal smartphones to deal with daily work while WFH.

The entire staff of Hanshow is using China's corporate WeChat as a platform for daily company communication and correspondence. This has resulted in all employees using their personal phones to work from home. The concern is that file transfers are not monitored, and Hanshow does not remind employees to use VPNs to access the company's major platforms.

Figure 3.4.1b shows that these percentages vary significantly across business domains, highlighting the differences in their cybersecurity mindset and readiness. Employees from the Legal department also obey cybersecurity guidelines as they all use VPNs for accessing corporate resources. However, other colleagues, due to the flooding of work, 69% mainly use direct access to work at home.

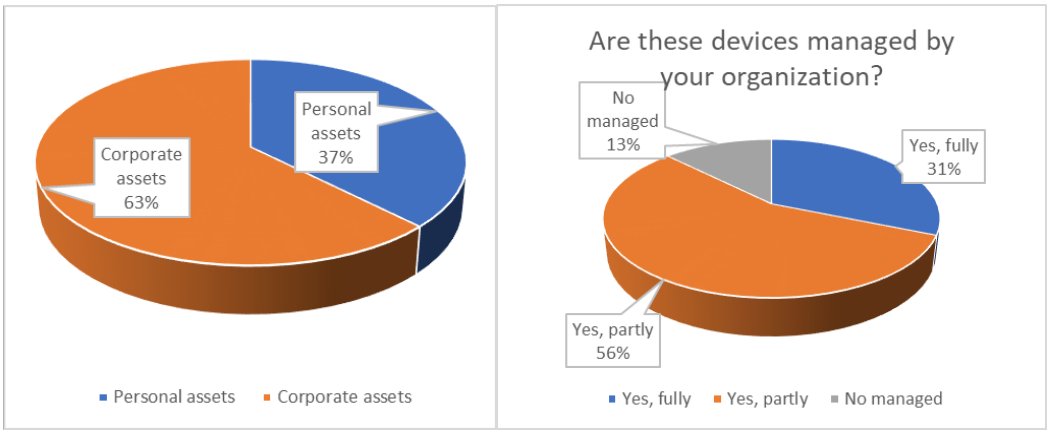


Fig. 3.4.1**a.** Hardware assets used for remote working

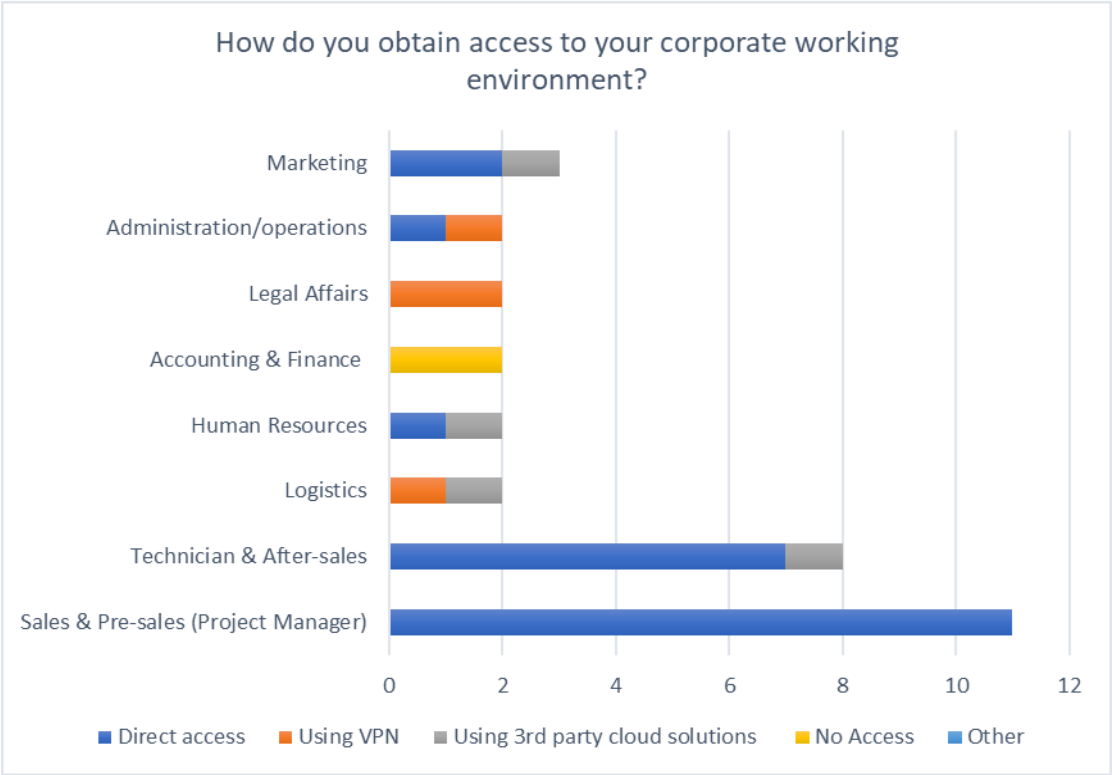


Fig. 3.4.1**b.** corporate access for remote working per business domain

The exact security features of the hardware assets used during teleworking time within Hanshow are presented in Figure 3.4.2a. This data (Figure 3.4.2a) reveals that 6% of employees lack the basic security awareness and readiness so to adopt none of the presented security devices. Up to 94% of employees adopt password protection, and 91% adopt automatic device screen locks. However, since Hanshow provides no strict security guidelines, the ratio of security software installation is extremely low among employees. It is worth mentioning that, although the result of password protection and automatic screen lock is reasonably good, there is hardly any antispam software installation or Antivirus software installation. In other words, Hanshow employees'

cybersecurity precautions are still weak in the face of hackers and cyber attackers with malicious intent.

Another notable phenomenon is that most employees have yet to adopt more advanced security technologies, such as two-factor authentication (38%) and hard drive encryption (9%). Figure 3.4.2b concludes that legal, technical and logistics are the most adaptive departments where IT appears to dominate among other departments.

Regarding the data storage and antispam software solution, it would be the case that Hanshow uses centralized Tencent mail and Wechat system to monitor and manage the background data. Therefore, the email and data storage solutions are bound together and transparent to the end-user.

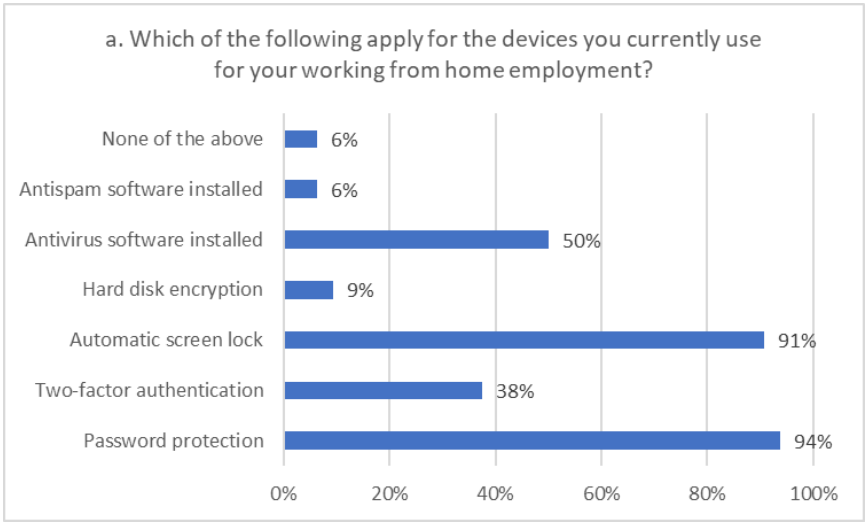


Fig.3.4.2 **a.** Hardware assets security features

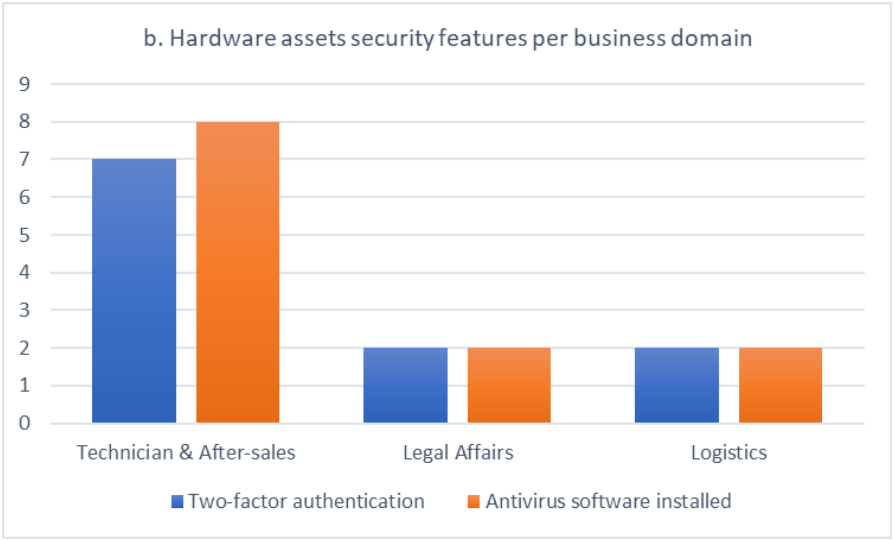


Fig.3.4.2 **b.** Hardware assets security features per business domain

3.5 Change management

Major companies have been forced to implement new cybersecurity policies in order to accommodate home office policies in the event of an epidemic outbreak. It is essential for companies to obtain new technological software and solution to facilitate remote management and teleworking environment. Consequently, many employees are also forced to get used to some unfamiliar remote working applications or services. Figure 3.5a shows that within Hanshow, 37.5% (12 out of 32) of employees are asked to use applications or services they were unfamiliar with. While 62.5% of employees did not utilize innovative applications but instead continued to use the same working service and application (Figure 3.5a).

According to the survey, Figure 3.5b shows that 69% of instructions are given via email. What follows is the user manual documentation provided, whereas the more interactive and fruitful method of training (9%) and instruction of the website (0%) are only adopted in 9% and 0%. While this is undoubtedly a good indicator of flexibility for companies, how they communicate these changes and facilitate employee adoption strongly affects the effectiveness of their change management strategies.

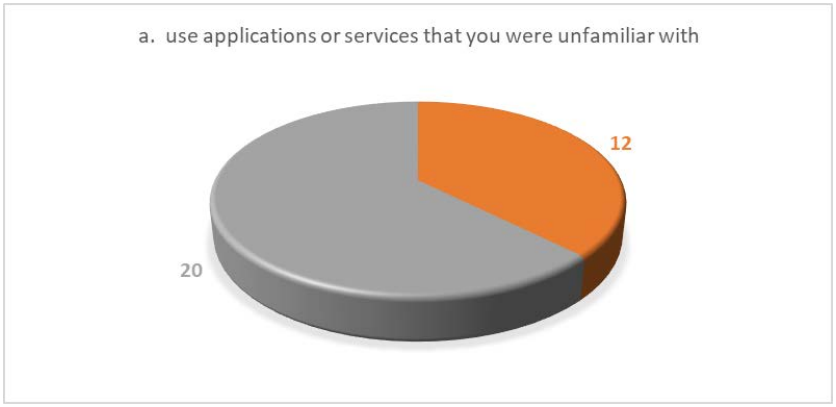


Fig. 3.5 **a**. Participants requested to use new applications or services due to remote working

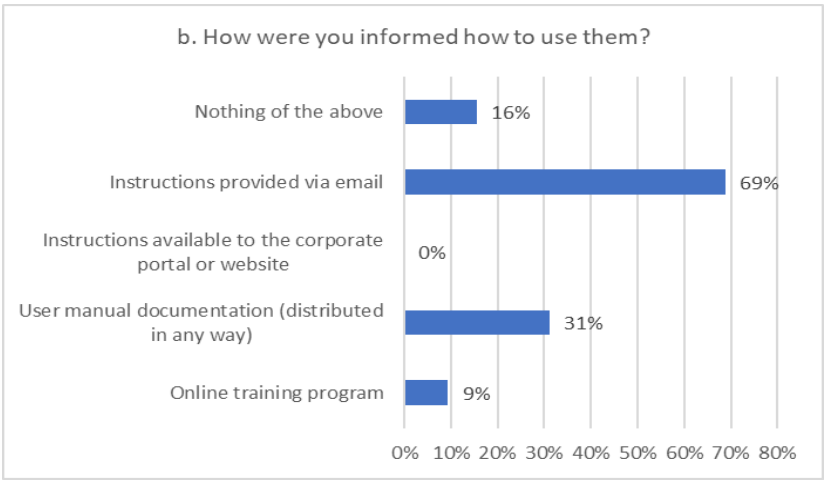


Fig. 3.5 **b**. the way they were informed

3.6 Remote working collaboration

While the government desires that companies implement the work-from-home proposal and drastically reduce outdoor activities, it also requires that companies implement the work-from-home proposal. However, working from home should never imply working alone. Collaboration and teamwork must be encouraged and fostered, particularly at this time when universal isolation is prescribed as the only means of preventing the spread of the virus. Companies have to provide increasingly practical and convenient communication platforms and channels. Ensure employees' productivity and effective communication. Today's collaboration solutions offer various options, from teleconferencing and real-time chat to document management and real-time co-creation, project management, and task scheduling. Hanshow primarily employs Chinese management platforms and software already encoded with many all-inclusive management functions.

According to Figure 3.6a, 72% of employees reported that Hanshow did not adopt a specific collaboration solution. Chinese communication platform like Enterprise WeChat is a well-established software combining online chatting, video, and live meeting altogether. There are several more integrated functions: daily report, check-in, clock-out, taxi travel, and travel reimbursement. Figure 3.6c indicates that 9 out of 32 employees mentioned new innovative collaboration solutions used during the teleworking period, but this phenomenon varies in different departments. This ratio, more or less, was validated in the following question, as displayed in Fig 3.6c. Marketing, Human resources, and logistics are the three business domains that had to adopt remote work arrangements, remote order following, client shoots, and face-to-face employee talks due to the epidemic. So their data shows that they adopted the latest online work arrangements.

Fig. 3.6 **a.** employees using a collaboration solution

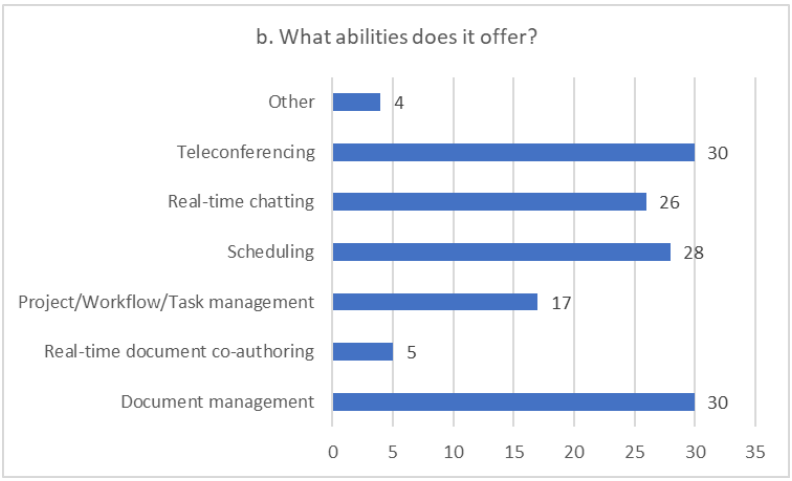


Fig. 3.6 **b.** collaboration possibilities offered

Fig. 3.6 **c.** Adoption of collaboration solutions per business domain

3.7 Security Incidents Management

To understand the cybersecurity situation at Hanshow during the Covid-19 outbreak, Hanshow employees were asked to reveal whether they encountered any cybersecurity issues and challenges during the outbreak. Our results (Figure 3.7a) indicate that one out of four reported having come up against some kind of security threat, with the number one malicious threat of phishing attacks (34%). This data might be due to the case that Hanshow did not provide a two-step authorization for the email access. Therefore, some malicious phishing emails are intended to steal information from employees.

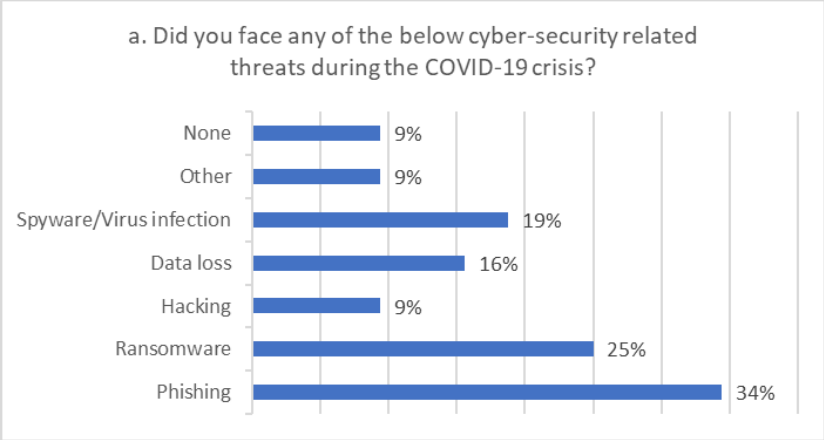
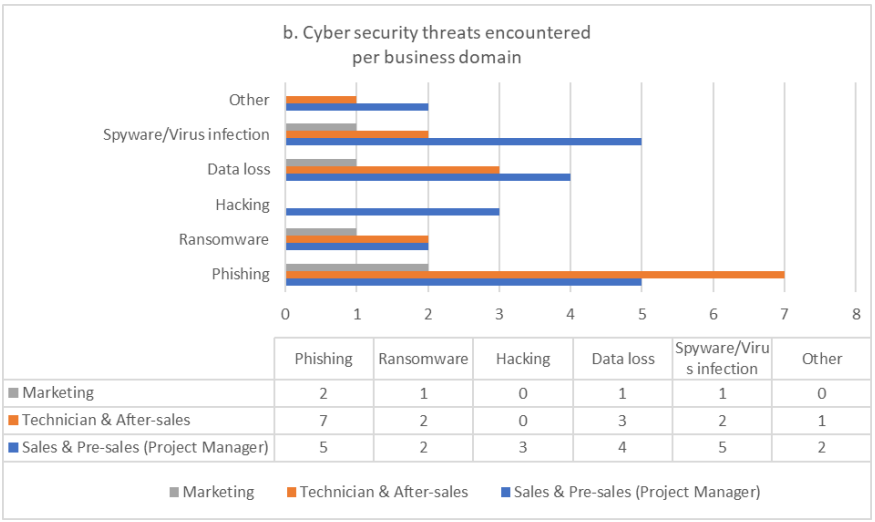


Fig. 3.7 **a.** Cyber security threats encountered by the employee

According to Figure 3.7b, there is a clear distinction between the indices of cyber attacks. As stated in the result, the security threat percentage drastically increased within the business domain of IT, Sales & Pre-sales, and Marketing. It is noticeable that variations, in this case, are significant. For example, hacking cases appear three times more often in the sales sector compared to the technical department, whereas phishing attempts are 1.5 times more often (Figure 3.7b). Technician & after-sales department reveals a significantly higher occurrence of cybersecurity threats, especially phishing attacks; 64% of phishing attacks are towards technical departments (Figure 3.7b). These observations were examined along with the hardware asset management and security results presented earlier, demonstrating the effectiveness of specific IT enterprise security policies and initiatives for other areas of engagement.

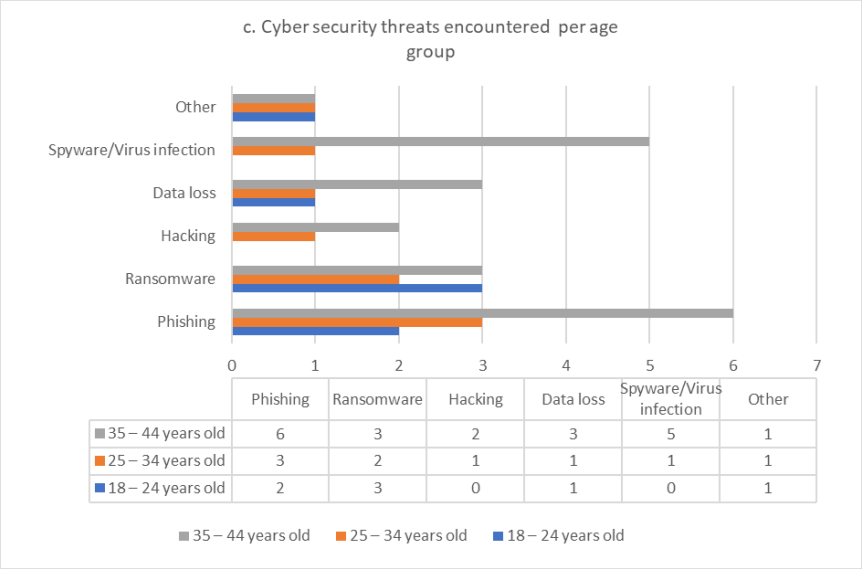


	Phishing	Ransomware	Hacking	Data loss	Spyware/Virus infection	Other
Marketing	2	1	0	1	1	0
Technician & After-sales	7	2	0	3	2	1
Sales & Pre-sales (Project Manager)	5	2	3	4	5	2

Fig. 3.7 **b.** Cyber security threats encountered per business domain.

According to Figure 3.7c, another worth-mentioned result is that cybersecurity threats increase when moving from younger to older employees. The result reveals that phishing and ransomware reach up to 55% and 37% for employees aged 35-44 years old, while the corresponding rates for 25-34 years old are limited to 27% and 25% (Figure 3.7c). Does this data represent a relatively strong awareness of cybersecurity

among younger employees? Or that younger people have more awareness and knowledge of cybersecurity software? Or do older employees have higher job titles and are more vulnerable to cybersecurity attacks? Such questions need to be further verified and substantiated in conjunction with the questionnaire indicators that address cybersecurity awareness and knowledge.



	Phishing	Ransomware	Hacking	Data loss	Spyware/Virus infection	Other
35 – 44 years old	6	3	2	3	5	1
25 – 34 years old	3	2	1	1	1	1
18 – 24 years old	2	3	0	1	0	1

Fig. 3.7 **c.** Cyber security threats encountered per age group

3.8 Employee climate

To find out if Hanshow is compatible with telecommuting policies and arrangements on a long-term basis. Eventually, succeed in generating a long-term cyber security culture. Understanding employees' attitudes and preferences towards the existing telecommuting policy is essential. A number of consenting 5 points Likert questions were included in our survey in an attempt to investigate participants' thoughts, emotions, and feelings, as these parameters are vital factors in an individual's overall safety behaviours and attitudes.

Interpreting the result shown in Figure 3.8, it is clear that employees have a preference for working from home rather than going to the office. The data indicates that employees have a higher preference for WFH indicators (20 out of 32). However, the preference varies in different business domains, and many employees indicate they can hardly collaborate effectively with colleagues when in the office. They appear to have no definite fondness for these distinct working circumstances and notice no radical differences in productivity.

On the other hand, there is a clear negative notion towards Hanshow employer and its reaction and support during this rather peculiar period. Most employees are not satisfied with their employers' remote working guidelines and support. And those data can be reflected by the previous findings as Hanshow management teams provide no proper guidelines. These figures verify most corporations' technological and security readiness

and flexibility, as noted in previous sections of the present study. However, most employees expressed their satisfaction regarding their working access and satisfaction during this pandemic.

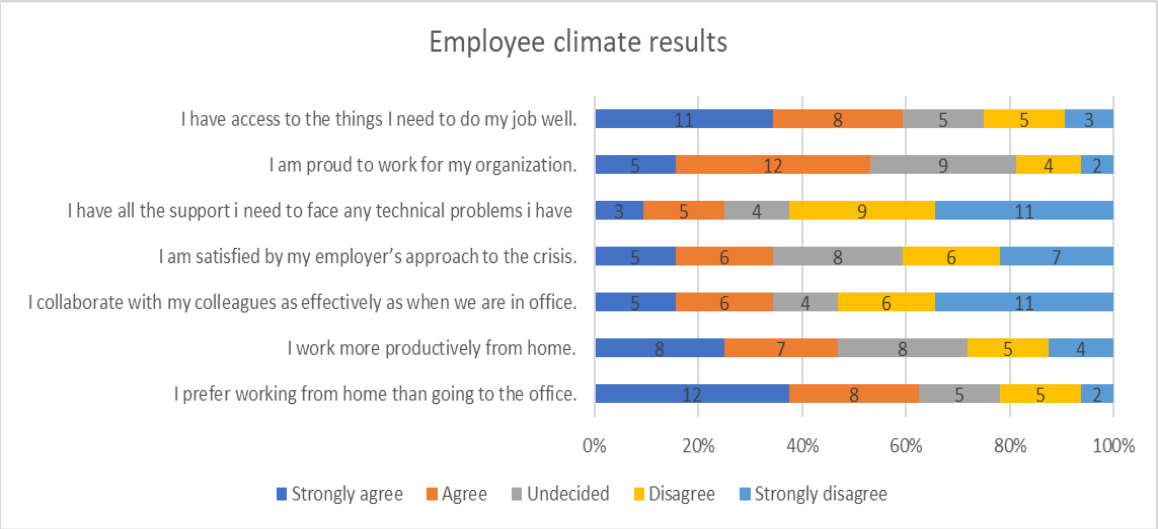


Fig. 3.8 Employee climate results

3.9 Consequences of poor cybersecurity management

To answer the research question, "What consequence can Hanshow meet if the proper cybersecurity management can not maintain due to teleworking?". An additional question is given to the Hanshow employees as an open question. After the surveys, all the answers are interpreted and summarized into the following answers.

According to Figure 3.9, 69% of employees mention that if there is no proper cybersecurity management, Hanshow may face a significant threat of data loss. Notably, Hanshow is an informational technique company that obtains numerous retail big chain clients like Ahold Delhaize, Jumbo, and Aldi. Therefore, malicious attackers may covet a company's core customer information to conduct cyberattacks such as ransomware extortion, resulting in the loss of information from Hanshow. All those malicious attacks might cause another severe consequence of lawsuits from Hanshow clients. Not to mention that productivity will be lost due to backend downtime. The scariest part is the reputational damage if it becomes a cyberattack victim. Eventually, suppose Hanshow leads to the theft or compromise of customer information. In that case, it can lead to a loss of customers, as trust in a company that fails to protect customer data can be shaken.

The technical department also mentioned another professional drawback of poor cybersecurity management. Some governing regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as the standards for data protection need to be obeyed by Hanshow. Failure to achieve compliant cybersecurity specifications by Hanshow can result in fines at the government level.

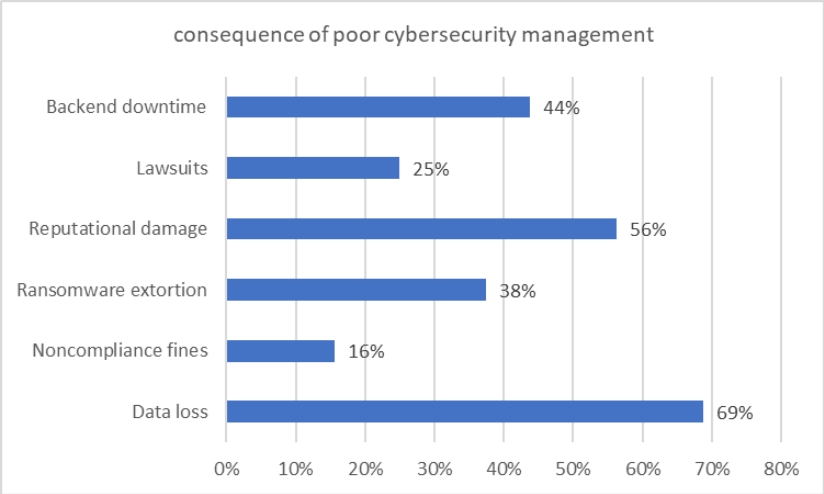


Fig. 3.9 consequence of poor cybersecurity management

3.10 WFH recommendation

This section demonstrates employees' suggestions on WFH policies. Also, to find out what employees want from Hanshow's teleworking management, an additional question 26 is injected into the questionnaire. The question describes, "which WFH recommendations can Hanshow use to maintain teleworking cybersecurity efforts?". The optional answers are summarized based on prior literature review and content investigation.

It is important to emphasize that mature cybersecurity management and a corporate cybersecurity culture require mutual cooperation between employees and employers. However, all those suggestions are given from the organizational perspective to reflect Hanshow employees' judgments about the effectiveness and importance of the suggested measures.

According to Figure 3.10, the result indicates that 94% of employees consider a proper training program about teleworking as the most efficient method to communicate the necessity of cybersecurity and guidelines. 81% of employees consider setting up an organizational Virtual Private Network (VPN) as another powerful means of remote office management and preventing information leakage. The remaining remote management recommendations received extra attention depending on the company's business domain. For example, multi-factor authentication (MFA) and constant data backup received the attention of the technical and after-sales departments. However, Access & Vendor security controls and online company policy received extra attention from the sales department. This result also reflects the fact that a sound corporate cybersecurity culture needs to incorporate the wishes and needs of employees from multiple departments and provide locally tailored management support policies.

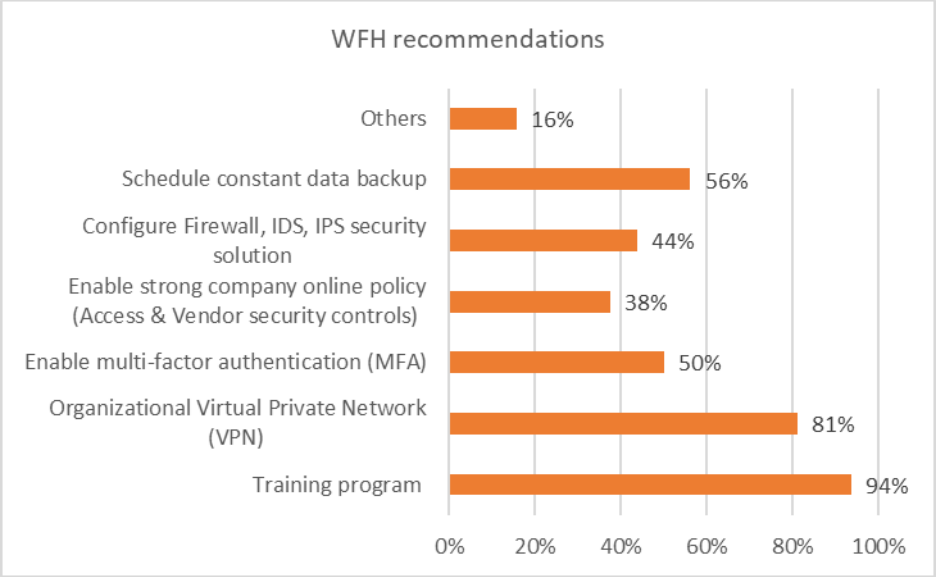


Fig. 3.10 WFH recommendations

3.11 Cybersecurity Threat Case

To further understand the cybersecurity risks experienced by Hanshow during the Covid-19 outbreak, several employees with technical backgrounds and knowledge of cybersecurity were selected for a short follow-up interview. The purpose of this brief interview is to understand the scenario of the cybersecurity threat outbreak and how Hanshow solved the threats internally. Ensure that the interviewees are unbiased and as objective and representative as possible. We selected four Hanshow employees. They are engaged in pre-sales, post-sales, sales, and technical engineer positions. There were one female and three male employees, ages 25, 31, 40, and 55, respectively. The following interview will be described one by one in the manner of cyber-attack cases.

Phishing 1： There were two phishing attacks that occurred in Hanshow during Covid-19. One phishing case was witnessed by one of the young girls from the Sales team. During the interview, she said, “Back in October last year, I received an email in the official sales matchmaking email inbox at Hanshow. The email was addressed in Dutch and said, " Nederlandse Covid-19 regeling". The title described the Dutch Covid regulation for foreign companies. I clicked on the email and read the preview, but the email did not have a signature or mention the Hanshow brand. At first, I did not read the exact content of the email because it was written in Dutch, and I do not speak Dutch. So I skimmed the content in general and found a link at the bottom of the email. I thought it was the homepage of a website showing the norms of the epidemic and almost clicked on it. But I asked the Dutch intern next to me to help me look at the content of the email. He immediately noticed that there was a problem with the email address. The Dutch government would update the data on the outbreak at RIVM but would not contact the company's email to send the data updates. The epidemic-related prevention norms are also viewed on the official website of NOS or RIVM. We clicked on the link

in the email, but the firewall immediately prompted us with the message, "The site is at risk. Do you want to continue accessing it". We then realized that the site was probably a Trojan horse or a site that stole information".

The above case is one of the phishing threats Hanshow encountered during Covid-19. This colleague was lucky to work with a Dutch local intern at the office, so she avoided the occurrence of phishing in the first phase.

Phishing 2: The second phishing attack was found by a 40 years old Pre-sales manager. He acquires years of technical and sales knowledge and is well experienced in the technical business domain. During the interview, he mentioned he was aware there was a dramatic increase in cyberattacks utilized the topic of pandemic during Covid-19. And he has a habit of reading, so he was also aware of the cybersecurity attack on Thuisbezorg and Zoom. To clarify, a phishing notification for a zoom meeting sent a fake COVID-19 alert to induce people to click on a link that triggers malware to take control of their system (Pandharipande & Parashar, 2020). So when he witnessed the phishing advertisement for the Tencent Meeting, he realized the threat immediately.

"It was during one of our international pre-sales communication meetings, and after I clicked on the Tencent Meeting software, I noticed that a plug-in advertisement appeared at the right corner of my desktop after the software opened. The ad showed the local epidemic data in the Netherlands, and the end of the ad said, "click for details". Since this conference software is not supposed to cause plug-in ads, I realized that this could be the same incident as the phishing ad that happened at the Zoom conference". These plug-in-ads did not cause any consequence because it happened to the manager who has cybersecurity awareness. But to prevent other colleagues from encountering the same situation. The supervisor fed this back to HR, who contacted headquarters and assisted IT in sending reminder emails to employees throughout the company. The email explained the phishing ad incident and reminded employees not to click on the relevant pages and ads.

Hacking: The overseas director of after-sales also reacted to one of the more serious hacking incidents during the outbreak. Hanshow has many core customers overseas, and Hanshow's business involves back-office data for retail customers. After-sale has always taken the security management of customer product information very seriously. "During the outbreak, I had found records of IP attempts to access from outside the whitelist in the history diary of Hanshow's product backend. The IP tried to access the backend of the product information more than once but was unsuccessful in the end. Suppose this malicious attack hacked into the backend of Hanshow and steeled customers' product information or planted a Trojan horse for extortion. The consequences would be unthinkable". This matter was directly reported to the overseas Vice President and the technical department of the headquarters and was given extra attention. The technical department of the headquarters upgraded the backend supervision system, and the leaders of each district also emphasized the importance of

network security in the management team of after-sales, hoping that the after-sales team would be vigilant about the security of personal information and customer information.

Malware: Another cyber-attack involving malware occurred late last year. A colleague in the technology department received an email in his corporate email inbox alerting him that someone on the same train as him was infected. "The email was sent to my corporate email. I originally thought it was because I was using the company's OV-chipkaart or the government had access to my personal data. But the end of the email asked me to download an APP that alerted people around me of the infection. This situation just reminded me directly of recent cases of cyber-attacks perpetrated by the outbreak. After Googling, I found that many people have posted these types of emails to alert them."

Thankfully, none of these events had a direct impact or consequence on Hanshow. But they further demonstrate to us the potential cybersecurity risks that Hanshow faces and the awareness of its employees about cyber security. Since the interviewees often had a knowledge base of cybersecurity or years of experience, we could not confirm whether the overall awareness of security risks among Hanshow employees was in place. This also reflects, from the side, the urgent need for Hanshow to implement a network security management policy, home office security training, and hardware management.

3.12 Quantitative Analysis

Correlation Analysis

To further analyze what the results of the questionnaire can indicate and present. To get a clearer picture of the attitudes of Hanshow employees towards teleworking and the current state of remote management. We imported all questionnaire results into SPSS and performed quantitative analysis.

The results of the quantitative analysis do present some valid and interpretatively meaningful findings. The focus of this thesis is not on age and educational background. Therefore, we do not include any correlation analysis between these two variables in the following analysis.

In the analysis, the two most important independent variables are "Profession" and "Department", which represent the background of Hanshow employees. To conduct a quantitative analysis, nominal variable “Department" is given values as: 1= Marketing; 2= Administration/operations; 3= Logistics; 4= Human Resources; 5= Accounting & Finance; 6= Legal Affairs; 7= Sales & Pre-sales (Project Manager); 8= Technician & After-sales. Another nominal variable “Profession" is defined as 1=Trainee&Internship; 2=Assistance; 3= Coordinator;4=Specialist; 5=Manager; 6=Vice President; 7=IT professional.

		Department	Profession	Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?	I have access to the things I need to do my job well.	I am proud to work for my organization.	I have all the support i need to face any technical problems i have	I am satisfied by my employer's approach to the crisis.	I collaborate with my colleagues as effectively as when we are in office.	I work more productively from home.	I prefer working from home than going to the office.
Department	Pearson Correlation	1	.603**	-.853**	.633**	.582**	.605**	-.442*	-0.166	-0.095	0.152
	Sig. (2-tailed)		**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.011**	0.365	0.605	0.406
	N	32	32	32	32	32	32	32	32	32	32
Profession	Pearson Correlation	.603**	1	-.590**	.683**	0.279	.573**	-.835**	-0.302	-0.231	-0.104
	Sig. (2-tailed)	0.000		**0.000**	**0.000**	0.122	**0.001**	**0.000**	0.093	0.204	0.571
	N	32	32	32	32	32	32	32	32	32	32

Table. 3.12.1 Correlation Analysis

According to Table 3.12.1, a series of correlation analyses are conducted. According to the Significant Score "Sig. (2-tailed)" shown in the 3rd row, the results show variable "Department" has a significant correlation with "Use of Unfamiliar Application" (shown in the 5th column) and four indicators for "Employee Climate" (shown in 6th to 9th columns). According to the Significant Score "Sig. (2-tailed)" shown in the 6th row, the variable "Profession" has a significant correlation with "Use of Unfamiliar Application" (shown in the 5th column) and three indicators for "Employee Climate" " (shown in 6th to 8th and 9th columns).

We can draw a few conclusions from the correlation analysis by interpreting Pearson's R. Firstly, both "Department" and "Profession" have a significant correlation with "Use of Unfamiliar Application" (p=0.0; p=0.0). And there is a relatively strong positive correlation between the "Department" and "Use of Unfamiliar Application"; "Profession" and "Use of Unfamiliar Application". This means that professionals with technical backgrounds and employees in high positions are less likely to use unfamiliar services and applications during teleworking. In other words, employees with lower job seniority were often asked to use unfamiliar services and applications during the epidemic period.

The same situation also presents in the case of the variable "Department". The results show that the more technically oriented employees (the IT and after-sales departments), the less they use unfamiliar applications. Conversely, Hanshow's failure to properly train non-specialized employees in teleworking resulted in employees in other departments needing to use unfamiliar applications and services when WFH during the epidemic. This could ultimately lead to an increase in human cyber risk.

The correlation analysis also demonstrates that employees with high seniority and the IT department have a significant positive correlation with "employee climate" indicators like "company access", "proudness", and "technical support". However, employees with high seniority and IT background claim they have a negative impression of "employers' approach to the crisis". In the correlation analysis, Pearson's R shows two significant considerable negative correlations between "approach to crisis". This situation means employers did not conduct sufficient and efficient tactics to solve the cybersecurity crisis.

Linear Regression Analysis

To further predict whether there is any significant linear regression between the variables "Department", "Profession", "Use of Unfamiliar Application", and "Employee Climate", another series of regression analyses are conducted. We want to predict if the dependent variables "Use of Unfamiliar Application" and "Employee Climate" are based on the independent variables “Profession” and “Department”.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	128.133	1	128.133	80.306	.000[b]
	Residual	47.867	30	1.596		
	Total	176.000	31			
2	Regression	148.921	8	18.615	15.811	.000[c]
	Residual	27.079	23	1.177		
	Total	176.000	31			

a. Dependent Variable: Department

b. Predictors: (Constant), Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?

c. Predictors: (Constant), Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?, I work more productively from home., I am proud to work for my organization., I prefer working from home than going to the office., I am satisfied by my employer’s approach to the crisis., I have all the support i need to face any technical problems i have , I have access to the things I need to do my job well., I collaborate with my colleagues as effectively as when we are in office.

Coefficients[a]

Model		Unstandardized	Coefficients	Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.300	0.282		25.845	0.000
	Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?	-4.133	0.461	-0.853	-8.961	0.000

a. Dependent Variable: Department

Table. 3.12.2 Regression Analysis “Department”

Table 3.12.2 indicates that the regression model predicts those dependent variables significantly well (p=0.00, $p < 0.0005$), and the independent variable “Department” statistically significantly predicts the outcome variables. The coefficients table indicates a result that for every unit increase in “Use of Unfamiliar Application”, a -4.13 unit increase in “Department” is predicted, holding all other variables constant. This figure confirms that the employees not from the IT department are more likely to be asked to use applications they were unfamiliar with during the Covid-19 outbreak.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.102	1	39.102	16.044	.000[b]
	Residual	73.117	30	2.437		
	Total	112.219	31			
2	Regression	95.574	8	11.947	16.509	.000[c]
	Residual	16.644	23	0.724		
	Total	112.219	31			

a. Dependent Variable: Profession

b. Predictors: (Constant), Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?

c. Predictors: (Constant), Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?, I work more productively from home., I am proud to work for my organization., I prefer working from home than going to the office., I am satisfied by my employer's approach to the crisis., I have all the support i need to face any technical problems i have , I have access to the things I need to do my job well., I collaborate with my colleagues as effectively as when we are in office.

Coefficients[a]						
Model		Unstandardized	Coefficients	Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	5.700	0.349		16.328	0.000
	Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?	-2.283	0.570	-0.590	-4.005	0.000
2	(Constant)	4.408	0.791		5.574	0.000
	I am satisfied by my employer's approach to the crisis.	-0.958	0.169	-0.714	-5.669	0.000

a. Dependent Variable: Profession

Table. 3.12.2 Regression Analysis "Profession"

The same significant regression relationship can also be found in the variable "Profession". Table 3.12.2 shows there is a statistically significant linear regression between "Profession" and the rest dependent variables ($p=0.00$, $p < 0.0005$). Coefficients Table indicates that for every unit increase in "Use of Unfamiliar Application", a -2.28 unit increase in "Profession" is predicted, holding all other variables constant. Besides, for every unit increase in "Satisfaction", a -0.96 unit increase in "Profession" is predicted, holding all other variables constant. In other words, employees without an IT professional background are more likely to use the unfamiliar application during Covid-19. And employees with solid IT professional backgrounds are not satisfied with the employer's approach to the crisis.

3.13 Answers of RQ 1 and RQ 2 and discussion of the results

Each question in this questionnaire addresses specific cybersecurity culture factors in an attempt to assess Hanshow's cybersecurity readiness and reveal deficiencies in existing security infrastructure and principles or even failures of existing security infrastructure and principles. In order to answer RQ1 and RQ2 posed earlier in this thesis, the results detailed in the previous paragraphs have been summarised and analyzed comparatively, leading to the following conclusions.

RQ1: What stage is Hanshow at in terms of forming an organizational cybersecurity culture during WFH?

Today, companies are becoming more agile thanks to advanced technological solutions that can adapt to the requirements of the business environment and even to drastic changes in it. This also fundamentally means that remote network management can meet the needs of employees working from home. Web conferencing, social media updates, video calls, remote access, and the use of a VPN can all meet the essential elements of WFH. This innovative behaviour also needs to be extended to the field of information security, where fundamental changes occur almost daily, in order to keep pace with developments and remain secure.

Based on the responses to the questionnaire, it is evident that the executives at Hanshow are eager to promote teleworking and implement effective cybersecurity management practices. Simultaneously, Hanshow's employees are enthusiastic about embracing the new changes and work patterns that teleworking entails. Hanshow lacks only a proper cybersecurity management protocol, employee training measures, and a method for establishing a cybersecurity corporate culture applicable to Hanshow. Quantitative data indicate that employees who are not from the IT department are very likely to be arranged to use unfamiliar services and applications, which may cause an increase in human risk in cybersecurity. Besides, Technology professionals are dissatisfied with the manner in which their leaders manage cybersecurity crises.

To sum up, Hanshow is still in the early stages of establishing a culture of cybersecurity because it did not set up corresponding initiatives for WFH or provide relevant training to its employees on cybersecurity before WFH.

RQ1.1: What is the current remote working possibility within Hanshow?

Due to the nature of the work, Hanshow has specific difficulties and decent requirements when it comes to teleworking management. For example, Hanshow's products require synchronization of back-end data, testing of samples, and a secured network environment. As a result, remote working is not always possible for all employees. Specific business domains seem more reluctant to accept this new working reality. At the same time, employees in other areas try to facilitate their establishment of remote collaboration and cooperation by adopting technological solutions.

Based on the possible distribution of job positions, the senior management at Hanshow, including vice presidents and managers, is happy to embrace teleworking as a management model and are pushing their employees to implement the new teleworking model. We can assume that there is no disagreement on the agenda to promote telecommuting among all employees at Hanshow. Only the technical and post-sales staff have remote access and work implementation difficulties. However, as far as the difficulties are concerned, once proper assets and guidelines are in place, it is not difficult to implement shift work or permanent telecommuting for technical and after-sales staff.

In a nutshell, the telecommuting possibilities at Hanshow are high. By sorting out the existing problems, establishing sound cyber security practices, and applying the right resources, Hanshow can still expect to build a long-term corporate cyber security culture.

RQ1.2: What is the attitude of Hanshow's employees towards WFH?

The answer to this part of the question can be found by looking directly at the indicators of "employee climate" (Figure 3.8). It is clear from the survey data that Hanshow employees have positive opinions and feedback about the company's top management's decision to work from home and about being a Hanshow employee itself. The data also shows that employees welcome the WFH policy, with 62% of employees stating that they prefer WFH and half stating that WFH is also very productive. Only in terms of remote interactive communication and the support given by management, Hanshow employees have shown slight dissatisfaction.

In other words, Hanshow employees have a positive attitude towards WFH and are satisfied with the feedback they receive from the company's top management. Quantitative data shows that employees with technical backgrounds tend not to be satisfied with the employer's approach to the crisis. Employees are open to the idea of working from home in the long term, but Hanshow needs to provide more favourable assistance and measures for working from home in the long term and building a secure corporate web culture.

RQ1.3: What are the current cybersecurity awareness and readiness state at Hanshow?

The most direct and effective way to avoid personnel errors in telecommuting is to advise, implement and train employees. The failure of Hanshow to implement organizational change management procedures and security training for employees before implementing the work-from-home policy is a worrying sign. As a result, this may have influenced employees to generate cyber security awareness and fail to be aware of the apparent increase in cybercrime. Regardless of the situation, Hanshow's poor performance in providing information and support to employees is a significant blow to the culture of cyber security organizations as a whole.

On the other hand, the readiness of network information security software is one of the essential elements reflecting the company's cybersecurity readiness. In order to establish a sound cybersecurity culture, the company should provide security technology solutions in terms of infrastructure and specifications, such as firewalls, anti-virus software, intrusion detection systems, and security operation centres. Nonetheless, the human element is not currently regarded as a central component of the cyber security protocol. This is evidenced by the reporting of cyber threat incidents and the absence of security guidelines and current information.

RQ2: What challenges and problems that Hanshow experienced during the WFH period so far?

The answer for this specific RQ can be captured in the security incidents and the interview in Section 3.11. By far, Hanshow has experienced several typical cybersecurity threats. The most typical threat is phishing attacks, followed by ransomware and spyware attacks. This data fits well with the data on cyber-attacks during the outbreak in various countries. According to Deloitte, 47% of individuals fall for a phishing scam while working at home (Deloitte Report, 2021). A similar result can also be found in the survey conducted by Sebastian; 60% of 109 WFH respondents claim there has been an increase in fraudulent emails, phishing attempts, and spam to corporate email since the start of the CovidCOVID-19 Pandemic (Sebastian, 2021).

According to the employee interview, a malicious hacker is trying to use coronavirus or COVID-19 as a header to lure Hanshow employees into conducting data loss. Outbreak management and infection data updates become good bait and excuses for aggressors. Especially for non-local companies, international employees are often unclear about the country's local updates and information sources, making it easier to get on the bandwagon. Although none of the network hacking cases had a substantial impact on Hanshow, the problem for Hanshow was that it did not summarize and circumvent these incidents, nor did it develop systematic norms and training. By reducing human error and information leakage, Hanshow can provide ultimate defence in the final battle of cyber-attack.

RQ2.1: What measurement or method has Hanshow currently taken in response to the teleworking challenges?

Hanshow has adopted password protection for almost all business laptops, and all employees except interns use their laptops with an automatic screen lock. Half of the employees use antivirus software and utilize two-factor authentication for the Hanshow backend system. However, all those measurements are biased in the different business departments. In general, Hanshow's existing prevention mechanisms are inadequate, neither training employees on cyber security awareness nor providing relevant instruction manuals. However, Hanshow provides every employee with a company laptop in terms of hardware. However, it is also clear from the questionnaire results that

70% of employees use their own hardware to handle their work in their home, and only 13% of employees choose to use a third-party cloud or VPN for their daily work.

RQ2.2: What consequence can Hanshow meet if the proper cybersecurity management can not maintain due to teleworking?

Hanshow needs to set up defences in network security. In the questionnaire, we asked about the consequences of Hanshow's inability to meet cyber security specifications. In conclusion, it appears that Hanshow would face a variety of severe consequences. For example, non-compliance fines from the government, corporate data or critical client data loss, and ransomware extortion. Due to the nature of Hanshow's work involving customer commodity information, even the back office management rights were subcontracted for remote management to the customers' IT department. Failure to manage network security when working remotely can result in reputational damage and even lead to complaints and lawsuits.

On a different level, telecommuting may also have the consequence of reduced productivity, poor employee communication, and reduced collaboration. Employee satisfaction and productivity will decrease if telecommuting arrangements are not based on persistent employee interactions. Ultimately, it is challenging to develop a long-term corporate cybersecurity culture.

RQ2.3: What basic WFH recommendations can Hanshow use to maintain teleworking cybersecurity efforts?

The final question in the questionnaire asked about the perception of the company's home-office initiatives within Hanshow's workforce. The primary purpose was to get a side-by-side view of how much employees need and value WFH initiatives. From the results, all employees know the importance of employee training, with 94% saying that adopting employee work-from-home training is necessary and practical. In addition, 81% of employees believe that the company's unified deployment of corporate VPNs for employees is an effective means of avoiding data loss and information leakage. Although adopting multi-element authentication and other means may reduce the timeliness of employees' work, nearly the majority of employees also indicated that they are willing to accept network security office arrangements such as multi-factor authentication, firewall, and data backup.

Indeed, specific remote working arrangements need to be systematically arranged, from staff training to WFH guidelines. Hanshow also needs to deploy appropriate codes of conduct and software assets within the company. Long-term synchronized monitoring and implementation to eventually develop into a corporate cybersecurity culture.

3.14 Summary

This chapter summarizes the results of the web-based questionnaire and small group interviews of Hanshow employees. Therefore, this section presents the analysis result

of the questionnaire and detailed answers to RQ 1 and RQ 2. Furthermore, through the analysis in this chapter, we gained a better understanding of the current status of cybersecurity, employees' WFH attitudes, and the corporate culture phase at Hanshow. As an inspiration and basis for Chapter 4, Chapter 4 will provide Hanshow with customized and cohesive models for the information gathered in Chapter 3.

Chapter 4. Proposed Solution

Chapter 3 provides an understanding of Hanshow's corporate culture and employee work-from-home policy. This chapter presents a solution for the cybersecurity and teleworking situation Hanshow is currently experiencing. The first section of this chapter, Section 4.1, describes the existing processing methods extracted from previous literature, the reason for selection and their application to Hanshow. The existing treatments help us to determine the current state of Hanshow's cybersecurity culture. Subsequently, Section 4.2 outlines how the approaches and components to promote a long-term corporate cybersecurity culture can be extracted from these treatments. What are the current status and the current treatments at Hanshow? What are the stages that Hanshow must go through and refine in order to establish a long-term cybersecurity culture? Furthermore, Section 4.3 discusses how these concepts and components can help avoid cybersecurity risks specific to Hanshow's operations. To clarify, Section 4.4 presents the methodology designed for Hanshow, which is based on existing literature and the questionnaire (Chapter 3). Finally, Section 4.5 will discuss the result of research question 3, illustrating the model as the proposed treatment for Hanshow to develop a long-term cybersecurity culture.

4.1 Available treatments

This section will choose existing treatments we discovered through our prior literature investigation to extract treatments appropriate to the Hanshow case (Ray Niu, 2022). When designing frameworks, overseas technology businesses such as Hanshow may be potential users. This investigation was preceded by a systematic review (Ray Niu, 2022) of 17 articles identifying viable approaches that could be considered ‘therapies’ for the problems discussed in this thesis. Ultimately, two articles ((Huang & Pearlson, 2019) are selected as references in this thesis.

The selection of these two models is motivated by the following concerns. The formation of culture is a lengthy process, particularly for multinational corporations like Hanshow, where the impact of the home country headquarters on overseas distribution is very long-lasting. In a short period, it is difficult for these companies to implement corporate cybersecurity culture regulations, enhance cybersecurity culture facilities, and motivate employees to follow and actively promote corporate cybersecurity culture. Consequently, to establish a cybersecurity culture under long-term remote management, businesses like Hanshow must complete two crucial phases. (1)The phase of establishing a culture of cybersecurity; (2) The phase of enhancing and optimizing the cybersecurity culture.

(1) The phase of establishing a culture of cybersecurity: Huang & Pearlson, 2019, describe in detail the three major constructs needed for employees to engage in cybersecurity behaviour to establish a cybersecurity culture. These three major

constructs, "external factors," "organizational mechanisms," and "cultural formation," lay the groundwork for the establishment of a cybersecurity culture; however, only when they are deployed and perfected can they ultimately promote cybersecurity behaviour.

(2) The phase of enhancing and optimizing the cybersecurity culture: When an organization recognizes external influences, deploys internal mechanisms, and implements top-down cybersecurity policies and management. Five key initiatives are outlined in the article by Alshaikh 2020 to assist organizations in transitioning from helping employees build cybersecurity awareness to proactively promoting and advocating a corporate cybersecurity culture.

This thesis ultimately modifies and optimizes the models of these two articles, thus creating the final model required for this thesis.

4.1.1 Establish Organizational Cybersecurity Culture

To foster a long-term cybersecurity culture, the primary condition is to clarify (1) the factors contributing to its creation and (2) how these factors can be measured. To this end, the model presented in Huang and Pearlson (2019) could be identified as a valuable aid that describes organizational cybersecurity culture.

According to Huang and Pearlson, organizational cybersecurity culture is *"the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organization from cyber-attacks"* (Huang & Pearlson, 2019). Therefore, in any organization, the ultimate goal of the manager in charge is to drive employees to conduct cybersecurity behaviour. Employees' behaviour helps reduce cyber-based vulnerability and protect the organization from potential cyber-attack. This article describes **three constructs 1. "External Influences" 2. "Organizational mechanisms" and 3. "Cybersecurity beliefs, values, attitudes"** for constructing a corporate cybersecurity culture encourage employees to engage in cybersecurity behaviours.

According to the authors, a cyber-secure culture's ultimate behaviours can be considered **in-role** and **extra-role** behaviours. In-Role Cybersecurity Behaviours refers to actions employees are supposed to take in their official role in the organization, e.g. comply with organizational security guidelines and follow employee training. Extra-Role Cybersecurity Behaviours refers to employees' actions that are not part of their job description, like cooperation and help. A detailed display of the model can be found in Figure 4.1.

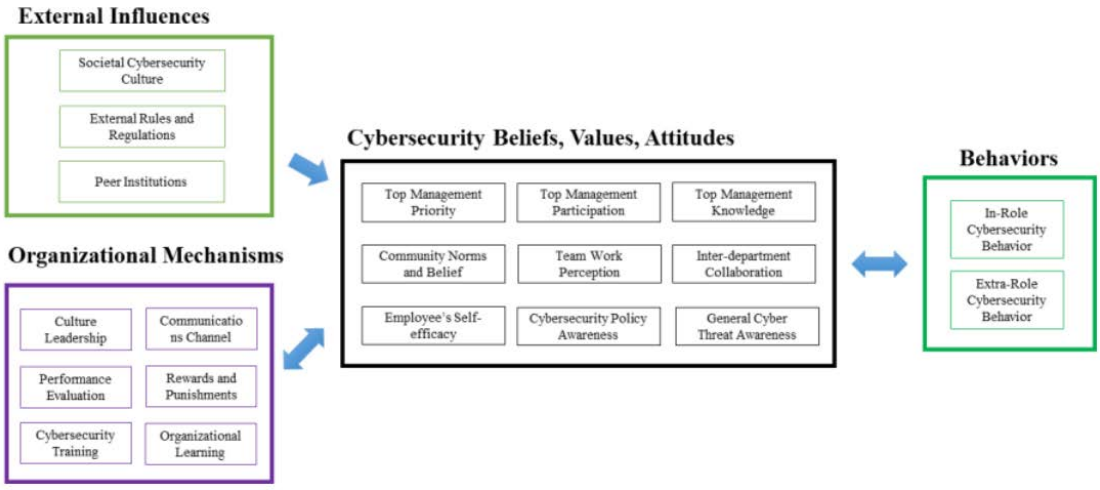


Figure 4.1 Organizational Cybersecurity Culture Model (Huang & Pearlson, 2019)

And culture is influenced by external factors outside managers' control and **internal organizational mechanisms** that managers use.

1. The model in Figure 4.1. illustrates some **external factors** that may shape individuals' attitudes, beliefs, and values: 1. **Social cybersecurity culture** refers to the culture of the society in which an organization operates. Differences between countries and societies can affect an individual's perception of cyber threats. 2. **External rules and regulations** are laws, guidelines, and regulations enforced by the government and other industry organizations. 3**. Peer institutions** refer to the pressure managers in an organization feel from actions taken by peer organizations.

2. For **internal organizational mechanisms**, culture cannot be developed without the supervision and training of the organization's leadership. Huang and Pearlson 2019 list six management levers that managers can use to influence the culture of cybersecurity. 1. **Cybersecurity culture leadership** refers to appointing an individual or team formally responsible for building a cybersecurity culture. 2. **Performance evaluation** is a formal evaluation process incorporating measures of cybersecurity compliance and employee behaviour. 3**. Rewards and punishments** directly represent cybersecurity behaviours' impact on management. Rewards and penalties must be matched to the severity of the behaviour. 4. **Organizational learning** refers to how organizations build and retain cybersecurity knowledge. 5. **Cybersecurity training** refers to courses and exercises that develop cybersecurity skills and knowledge. 6. **Communication channels** refer to the use of multiple methods and networks to communicate consistent, well-designed messages about cybersecurity.

3. For **Cybersecurity beliefs, values, and attitudes** of the business, the authors summarized three organizational levels of cybersecurity culture, which contain nine constructs that make up the organisation's culture**: leadership level, group, and individual level.**

The **leadership level** in an organization plays a significant role in creating and propagating the organization's culture. To refine the leadership dimension of corporate cybersecurity culture, the authors summarize three building blocks to assess the quality of cybersecurity culture in leadership: 1. **Top management priorities** happen when top management recognizes the importance of cybersecurity. They make it a priority for the organization. 2. **Top management involvement** refers to the personal involvement of top management in cybersecurity-related activities. Personal involvement is used to communicate policies and attitudes toward cybersecurity, such as involvement in funding and training. 3**. Top management knowledge** refers to leaders' knowledge, skills, and abilities that are relevant to cybersecurity. Having the relevant competencies and knowledge base is the only way to set an example and help employees develop a cybersecurity culture.

At the **group level**, the ultimate goal is to help employees build shared values and beliefs that are culture models. Three constructs identified the group-level attitudes, values, and beliefs: 1. **Community norms and beliefs** refer to the group's collective perception of cybersecurity and what people believe and evaluate. 2. **Teamwork perception** refers to the way teams work together within an organization to improve cybersecurity. In other words, whether employees are on the same page. 3**. Inter-departmental collaboration** refers to work between groups of individuals from different parts of the organization. For example, people within each department may need to divide work or participate in specific projects and training to find ways to increase cybersecurity throughout the organization.

The third level is employees' **individual level**. When employees learn how to act consistently with the corporate culture, they are more likely to act in a way that is consistent with increased cyber resilience: 1. **Employee self-efficacy** refers to the awareness of the extent to which individual employees can implement actions to improve cybersecurity. 2. **Cybersecurity policy awareness** is an individual employee's knowledge of the behaviour the company is pursuing. Employees know what needs to be done, what is right and wrong, and what is important. 3. **General cyber threat awareness** refers to an individual's awareness and understanding of the threat.

These three sets of constructs constitute a theoretical model that identifies the methods managers can employ to establish a cybersecurity culture within an organization and ultimately facilitates the cyber-secure behaviour of employees. The managers of Hanshow can refer to the model presented in Huang and Pearlson 2019 to gradually build a corporate cybersecurity culture ecosystem. The following sections will apply this model to Hanshow scenarios, and a summarized table can be found in Table 4.1.

4.1.2 Application of the Huang & Pearlson Model to Hanshow

To apply the Huang & Pearlson Model to Hanshow, we must first address the external factors of Hanshow's context. Chapter 1 describes Hanshow Technology as the world's leading provider of electronic shelf labels and omnichannel digital storage solutions. As a typical intelligent information enterprise, cooperation with big retail chains like Ahold Delhaize and Jumbo determines the severity of cybersecurity. Hanshow Nederland B.V. was established in Netherland in 2019. Therefore, Hanshow is an overseas company that embraces multi-national cultural background. As with many organizations utilizing intelligent technology, managing cybersecurity to protect their data and systems was a crucial success factor.

Therefore, regarding the external factors mentioned in Section 4.1.1., **(1.)** the society's cybersecurity culture for Hanshow is complex, as Hanshow combines both Chinese and European cultural backgrounds. China's cybersecurity system is centralized and authorized by the government but might be lases-faire at the organizational level. However, Europe is more stringent and concrete in maintaining the company's information security, customer privacy, and consumer information. Hanshow's product line, for instance, also includes camera face recognition and marketing screen interaction, neither of which are permitted for sale in Europe. Managers at Hanshow must emphasize the disparity between Chinese and European cybersecurity cultures and provide localized information to employees.

The second external factor is the (**2.)** external rules and regulations since Hanshow Nederland B.V. is based in the Netherlands. The direct rules and regulations are the General Data Protection Regulation (GDPR) regulations in Europe. The GDPR requires organizations to appoint a data protection officer. Companies subject to this regulation, such as Hanshow, will need to pay more attention than others to GDPR legislation and regulation. Hanshow shall request the legal department to investigate the local external rules and regulations like GDPR. On 22 March 2022, all European Union (EU) institutions, bodies, offices, and agencies will be required to have cyber security frameworks in place for governance, risk management, and control.

In the case of peer institutions, as the third external factor (**3.**), protection against cyber intrusions and other vulnerabilities is crucial for all industry players, including those in the intelligent technology and electronic technology sectors. Specifically, competing companies in Hanshow are all equally concerned with the security of retail customers' data, and no one wants to do business with a company that cannot be trusted or protect the information in the event of a breach.

The remaining internal factors of Hanshow will be demonstrated in Table 4.1as shown below.

Cybersecurity Culture			Application to Hanshow
External Influences	Societal Cybersecurity Culture		Hanshow top managers need to highlight the difference between Chinese and European society's cybersecurity culture and provide localized information to the employees
	External Rules and Regulations		Hanshow shall ask the legal department to investigate the local external rules and regulations like GDPR
	Peer Influence		Competing companies in Hanshow are all equally involved in the security of retail customers' data
Believe, Value and Attitudes	Leadership	Top Management Priority	Hanshow Manager needs to raise the WFH cybersecurity project to a Strategic-level priority or authorize a significant budget for security activities and software
		Top Management Participation	Hanshow's top management team needs to show personal attitudes and involvement the cybersecurity by attending training, rewarding and participating in other cybersecurity activities
		Top Management Knowledge	Hanshow's leader needs to know Hanshow's cybersecurity vulnerability. Provide training and regularly engage in the latest cybersecurity discussion
	Group	Community Norms and Belief	Hanshow needs to value and emphasize "info protection" regularly via email or weekly meetings
		Team Work Perception	Hanshow team needs to build cybersecurity consideration in their project and other exercises
		Inter-department Collaboration	The core team working with cybersecurity leaders needs to include members from different departments like logistics, legal, and marketing
	Individual	Employee's Self-efficacy	Through training and communication, Hanshow needs to make employees aware of how to identify and respond to phishing emails and who to communicate with
		Cybersecurity Policy Awareness	Hanshow needs to remind and notify employees about cybersecurity policy via meeting or email
		General Cyber Threat Awareness	Hanshow needs to train and summarize historical cyber threats as cases to build suspicious of unusual emails, attachments, and advertisement
Behaviours	In-role Cybersecurity Behaviours		The survey results indicated a positive attitude towards in-role cybersecurity behaviours. Hanshow employees need to obey WFH guidelines and security policy and avoid policy violation
	Extra-role Cybersecurity Behaviours		Hanshow needs to motivate employees to promote cyber security, speak up and improve self-knowledge
organizational Mechanism	Leadership	Cybersecurity Culture Leadership	Hanshow must assign a leader with an agenda covering cybersecurity guidelines and knowledge.
	Incentive	Performance Evaluations	Establish a performance review for employees. Those who repeatedly failed phishing exercises were subject to notations and low scores on KPI performance
		Rewards and Punishments	Employees who identify and avoid cyber-attacks need to be praised in the form of proclamations, certificates, or bonus
	Process	Organizational Learning	Hanshow needs to continually update on cybersecurity news and issue campaigns to facilitate long-term retention of cybersecurity practices and behaviours
		Cybersecurity Training	Hanshow needs to provide on-board training, periodic training, and WFH guidelines to increase awareness of cybersecurity
		Communications Channel	Hanshow needs to arrange marketing-like campaigns to encourage cybersecurity behaviours and spread the message via multiple channels like email, alters, events and training

Table 4.1Application of the Huang & Pearlson Model to Hanshow

Cybersecurity behaviour is driven by unwritten rules that are difficult to see. However, these unwritten rules are evident in the values, beliefs, and attitudes exhibited by management, teams, and individuals in an organization. To become a cyber-resilient organization, Hanshow needs to cultivate technology and organizational investment. Adopting Huang and Pearlson's model (Table 4.1) can help Hanshow managers to build a culture of cybersecurity and provide a blueprint for evaluating if the culture drives cybersecurity behaviours.

4.1.3 Develop and optimize cybersecurity culture

Adopting Huang and Pearlson's model can help Hanshow to understand the **External influences**, the internal **Organizational mechanisms**, **beliefs, values, and attitudes,** which are the basis for developing a long-term cyber security culture. However, Alshaikh's model can help motivate employees to shift from passively obeying organizational management and guidelines to proactively cooperating and promoting a cyber security culture.

In the article Alshaikh 2020, Alshaikh explains the **five key initiatives** that three Australian organizations implemented to improve their respective cybersecurity cultures during the epidemic (Figure 4.2). The five key initiatives are**: (1) identifying key cyber security behaviours, (2) establishing a 'cyber security champion' network, (3) developing a brand for the cyber team, (4) building a cyber security hub, and (5) aligning security awareness activities with internal and external campaigns**. More effective cybersecurity culture is vital to prevent security breaches caused by employees' non-compliance with organizational security policies. Hanshow can draw on this model to further enhance its cybersecurity culture (Alshaikh, 2020).

With Huang and Pearlson's model, Hanshow could have implemented an initial work-from-home security policy, provided employee training, and progressively raised cybersecurity awareness. Hanshow, like many SMBs, will recognize that despite their education, training, and awareness efforts, employee behaviour remains a primary factor in the majority of cybersecurity incidents. Alshaikh's model, compared to Huang and Pearlson's, not only aids in establishing an organizational cybersecurity culture but also aids in implementing how to optimize and strengthen cybersecurity awareness and ethos in five directions. This model can assist Hanshow in optimizing the second stage of cybersecurity culture beyond security education, training, and awareness (SETA). Figure 4.2 depicts a representation of Alshaikh 2020.

Fig.4.2 Five key initiatives to transform SETA from compliance to culture (Alshaikh, 2020)

1. According to Alshaikh, 2020, the first step is **identifying key cyber security behaviours**. Establishing a security culture involves condensing existing security policies' direction and management intent into "five cybersecurity behaviours" that are simple to remember and convey. Hanshow was required to refine and simplify the guide's content after establishing and implementing a cybersecurity code for a period of time. Nobody has the time or desire to read a lengthy cybersecurity code. To facilitate a cybersecurity culture, the intent of these policies was condensed into four or five key messages that employees could comprehend and adhere to in order to avoid incidents.

2. The second important initiative is **establishing a 'cyber security champion' network**. One can understand it as selecting a representative or leader within different departments to promote cybersecurity behaviours. Due to the size of the organizations, cybersecurity culture and outreach teams cannot create awareness and build culture on their own. It must be a collaborative effort of the different stakeholders within the organization. The Cybersecurity Champion role can be defined as supporting the cybersecurity team in expanding security awareness messages. This champion helps employees in their department adopt the top five security behaviours identified in the policy, identify their department's SETA needs (skills, knowledge, and behaviours); and report progress to the security team (Alshaikh, 2020).

3. Developing a brand for the cyber team is one of the strategies implemented to create visibility for the cybersecurity team and SETA activities across organizations. When employees see this specific branding or logo, they are aware of these activities related to cybersecurity awareness.

4. Another tool to improve the implementation of a single training and policy into a security culture **is the creation of a "Cybersecurity Hub"** within the organization.

The cybersecurity hub is an internal website that puts all cybersecurity-related materials in one place and is used to support employees and improve their cybersecurity behaviour. The cybersecurity hub also serves as a single point of contact between employees and the cybersecurity team so that employees can raise issues with the cybersecurity team and get cyber risks resolved in time.

5. The final initiative is **to align security awareness activities with internal and external campaigns.** Building a culture requires teamwork to promote the importance of cybersecurity across multiple events and conferences, requiring a high degree of coordination between different activities and collaboration both internally and externally. Align cybersecurity messages with other campaigns in the organization across multiple company platforms—for example, marketing campaigns, weekly meetings, and training. From there, maximize the impact of security awareness to motivate employees' cybersecurity behaviour.

4.1.4 Application of Alshaikh's model to Hanshow

Alshaikh's model suggests five initiatives for the second phase of long-term cybersecurity culture: "The phase of enhancing and optimizing the cybersecurity culture". These five initiatives can help company managers move employees from passively adhering to the norms of cybersecurity culture to spontaneously exhibiting cybersecurity behaviours and promoting cybersecurity internally more efficiently. The tailor-made suggestion for Hanshow to adopt these five initiatives can be found in Table 4.2.

Key initiatives	**Application to Hanshow**
Identifying the key cybersecurity behaviours	Simplifies policy language and focuses employee focus from fundamental awareness to desired behaviours. Hanshow must outline five important alerts, such as "Think before you click," "Do not forget to auto-lock your laptop," and "Report anything suspect."
Establishing a cybersecurity champion network	Hanshow needs to select Opinion leaders in different departments. Define the roles and responsibilities of the "Champion" to create a network for the cybersecurity team
Building a Cybersecurity Hub	Hanshow needs to build a collective hub for WFH guidelines, security rules, training, VPN installation, and online Q&A for the cybersecurity teams
Developing a brand for the cybersecurity team	Hanshow needs to design a logo or brand for the cybersecurity teams. The security awareness and training logo should be used consistently in any activities related to security awareness, such as training sessions posters, alerts of new threats
Aligning security awareness with internal and external campaigns	Hanshow needs to align the cybersecurity slogan, alters, and team logo within all channels of communication like cybersecurity hub, training sessions, and monthly meetings

Table 4.2 five key initiatives to boost cybersecurity culture

4.2 Hanshow's present cultural situation

This section describes the current status of Hanshow's corporate culture. Based on Hanshow's present cultural situation, this section will outline the application sequence of the two models (Huang & Pearlson, 2019; Alshaikh, 2020) and the prerequisites for adopting each of them.

According to the questionnaire described in Chapter 3, we can identify the fact that Hanshow is at the primary stage of a cybersecurity culture. According to Huang and Pearlson 2019, the primary stage for building a cybersecurity culture is identifying **external influences** like peer influences and external rules. In this instance, Hanshow is aware of its exact position as they transition to the creation of cybersecurity management. It is because they are aware of the external environment and influences. For example, the work-from-home policy, the European government's management policy, and the pressure from competitors decided to adjust from within and gradually build a cybersecurity culture and a sound WFH cybersecurity management. We can assume that Hanshow has completed its previous preparations and reached an awareness of the external risks, which is the first step in suggesting a culture of cybersecurity.

While Hanshow's management team is aware of the significance of cybersecurity during telecommuting, the executive team begins to assist in establishing cybersecurity legislation and the development of relevant cultural norms. Nevertheless, according to the model of Huang and Pearlson 2019, another essential pre-request for building organizational culture, the **organizational mechanisms** have not yet been achieved. Namely, culture leadership, communication channel, and training are not settled. Reference the term from Alshaikh 2020; those organizational mechanisms are the "security education, training, and awareness (SETA)", which play as the fundamental asset for an organization to foster a decent culture.

In other words, the establishment of Hanshow's cybersecurity culture needs to start from the "organizational mechanisms" stage, only after the accomplishment of Hanshow's internal mechanisms and cybersecurity assets. The leadership norm, beliefs, values, and attitudes of the company can gradually penetrate the company and its employees. This is the foremost one of the three constructs of cultural formation according to the model of Huang and Pearlson 2019.

When Hanshow completes the "**cybersecurity beliefs, values, and attitude**" construct, Hanshow can adopt Alshaikh 2020's model to exceed minimal standards-compliance to create functional cyber security cultures as witnessed within employee behaviour.

4.3 Expected contributions to the risk avoidance

To respond to RQ2.2, the questionnaire for Hanshow Netherlands inquired about the potential consequences of Hanshow's failure to implement cybersecurity management.

In section 3.9, we have also enumerated the severe repercussions listed by Hansol employees. The concepts and models of available treatments are expected to help Hanshow avoid cybersecurity risks in the following way:

Data loss: Through organizational learning and training, employees will develop a better cybersecurity awareness to prevent human risks such as internal information leakage. Periodical data updating and building a cybersecurity hub can prevent historical data loss.

Noncompliance fines: Realizing external influences like Societal Cybersecurity Culture and External Rules and Regulations will help Hanshow detect the existence of GDPR. And the establishment of cybersecurity projects will prevent the consequence of noncompliance fines.

Ransomware extortion: The communication channel and the cybersecurity hub can help communicate the problem in time and prevent extortion historically from happening again to prevent unexpected ransomware extortion.

Reputational damage: Building an internal cybersecurity culture will help boost employees' self-efficacy and avoid cyber risks for the clients. The corporate culture will convey the importance and protection of customer data to enhance the company's reputation.

Lawsuits: A well-developed cybersecurity policy and a mechanism to monitor and reward employees for their cybersecurity behaviour all enable employees to remind each other and learn from history to avoid eventual court appeals.

Backend downtime: Continuous data retention, enhanced facilities and investments within the enterprise, staff training, and the appointment of cybersecurity champions will further avoid the chances of malicious attacks on the backend.

4.4 Our Proposed Model

Combining the two models' main categories (Huang & Pearlson, 2019; Alshaikh, 2020) resulted in the creation of the model presented in Figure 4.4. Figure 4.5 expands and develops the dimensions of each principal category presented in Figure 4.4, which can be regarded as the final model provided in this thesis.

The model present in Figure 4.4 refers to the four constructs (Figure 4.1) of cybersecurity culture establishment as defined by Huang and Pearlson 2019. The four building blocks are "External influences", "Organizational Mechanism", "Believe, Values and Attitudes", and "Behaviours" (Figure 4.1).

The five optimized initiatives (Figure 4.2) from Alshaikh 2020 are further combined to embed cybersecurity principles into the culture. The five key initiatives (Figure 4.2) "Identify Key Cyber Security Behaviours" "Establish a Cyber Champion Network" "Develop a Brand for the Cyber Team" "Build a Cyber Security Hub" and " Align

Security Awareness with External Campaigns" were combined into a phase called "Compliance Transformation to Culture." Employees can only take action to motivate the "Behaviours" stage after completing the motivating transformation phase. Therefore, those five merged main categories from both models (Huang & Pearlson, 2019; Alshaikh, 2020) represent the horizontal layer of Figure 4.4.

To compensate for the lack of company asset configuration, continuity policies, and governance arrangement in Table 4.1 "Hanshow application of Cybersecurity Culture Elements" and Table 4.2 "five key initiatives to booster cybersecurity culture". The proposed model also integrated Georgiadou et al. 2020's Cybersecurity Culture Framework (Figure 2.2) to improve the tailor-made model for Hanshow.

Figure 4.4 lists the five major categories in addition to the formation of a cybersecurity culture at Hanshow, and the lighter panels represent the relevant dimensions that Hanshow needs to deploy in each major category (Georgiadou et al., 2021)

Figure 4.5 further expands on the components that Hanshow needs to implement under each dimension. Following the order from left to right, from top to bottom, Hanshow needs to gradually follow the arrangement and deployment of each dimension to develop a long-term corporate cybersecurity culture gradually.

Step 1	Step 2	Step 3	Step 4	Step 5
External Influences	Organizational Mechanism	Believe, Value and Attitudes	Compliance Transformation to Culture	Behaviors
Societal Cybersecurity Culture	Leadership	Leadership	Five Initiatives	In-role Cybersecurity Behaviors
External Rules and Regulations	Incentive	Group		Extra-role Cybersecurity Behaviors
Peer Influence	Process	Individual		
	Asset			
	Continuity			
	Security Governance			

Figure 4.4 Model merging main categories

<table>
<tr><th>Step 1</th><th colspan="2">Step 2</th><th colspan="2">Step 3</th><th>Step 4</th><th>Step 5</th></tr>
<tr><td>External Influences</td><td colspan="2">Organizational Mechanism</td><td colspan="2">Believe, Value and Attitudes</td><td>Compliance Transformation to Culture</td><td>Behaviors</td></tr>
<tr><td>Societal Cybersecurity Culture</td><td>Leadership</td><td>Cybersecurity Culture Leadership</td><td rowspan="3">Leadership</td><td>Top Management Priority</td><td>key cybersecurity behaviors</td><td>In-role Cybersecurity Behaviors</td></tr>
<tr><td rowspan="3">External Rules and Regulations</td><td rowspan="3">Incentive</td><td>Performance Evaluations</td><td>Top Management Participation</td><td>champion network</td><td>Extra-role Cybersecurity Behaviors</td></tr>
<tr><td>Rewards and Punishments</td><td>Top Management Knowledge</td><td>Building a Cybersecurity Hub</td><td></td></tr>
<tr><td rowspan="3">Process</td><td>Organizational Learning</td><td rowspan="3">Group</td><td>Community Norms and Belief</td><td>branding cybersecurity team</td><td></td></tr>
<tr><td>Peer Influence</td><td>Cybersecurity Training</td><td>Team Work Perception</td><td>internal and external campaigns</td><td></td></tr>
<tr><td></td><td>Communications Channel</td><td>Inter-department Collaboration</td><td></td><td></td></tr>
<tr><td></td><td>Asset</td><td rowspan="3"></td><td rowspan="3">Individual</td><td>Employee's Self-efficacy</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td></td><td>Continuity</td><td>Cybersecurity Policy Awareness</td></tr>
<tr><td></td><td>Security Governance</td><td>General Cyber Threat Awareness</td></tr>
</table>

Figure 4.5 Model merging main dimensions

The following sections explain in more detail the meaning of each category (Top horizontal Layer) included in the models in the context of Hanshow (Figure 4.5).

4.4.1 External Influence

Regarding external influence (Figure 4.5), the key dimensions that need to consider are Societal cybersecurity culture, external rules and regulations, and peer influence (Huang & Pearlson, 2019).

As illustrated in Section 4.1, as a Chinese technology firm expanding overseas, Hanshow needs to have a precise positioning for itself. The first step in building a cybersecurity culture is to recognize your own surrounding conditions, constraints, and legal context. For example, as a Chinese company, Hanshow must survive in the European market. It must understand how European employees work, European cybersecurity laws and regulations, office software, cookie specifications, and government Covid-19 requirements for international outbreaks.

In addition, to keep up with the times, technology companies frequently have higher technological innovation and security maintenance standards. Due to Hanshow's products, business, and customer base, updates and maintenance of information technology and the protection of customer data are necessary for the company's survival. How to ensure safe survival while outperforming the competition, but also to provide protection for customers' information and reap the benefits of a good reputation, all

require Hanshow to pay attention to the external influences and environment. This also reflects the seriousness of forming a corporate cyber security culture for Hanshow.

4.4.2 Organizational Mechanism

Beliefs, values, and attitudes constitute the unwritten rules and, therefore, the culture of the organization. However, they are created by the actions of managers and leaders, which understand as management levers or organizational mechanisms (Figure 4.5) (Huang & Pearlson, 2019).

In order to popularize the concept and ecosystem of a cybersecurity culture within Hanshow, Hanshow first needed to appoint a leader who would spread the corporate cybersecurity culture. He has the responsibility and authority to communicate the culture's guidelines, measures, and importance to the entire Hanshow workforce. To accomplish this, he must possess a technical foundation in cybersecurity. As a KOL, he must also be familiar with every employee to effectively communicate with all internal stakeholders. Without a leader specifically responsible for fostering culture, these activities will be executed haphazardly and may even be neglected.

Alternatively, promoting employee attention to cybersecurity requires clear incentives and sanctions. Managers clarify which behaviours are required, acceptable, and unacceptable through the performance evaluation procedure. By incorporating employee performance on cybersecurity behaviours into performance evaluations, such measures can serve to remind employees of the organization's capacity to observe such behaviours, thereby influencing employee values.

All successful business communication requires that the right people hear the right message at the right time through the right channel. Consequently, it is necessary to help employees recognize, learn, communicate, and ultimately comprehend the significance of cybersecurity. Conscious application of the learning process at the individual, group, and organizational levels sustains organizational transformation to enhance stakeholder satisfaction. Similarly, Hanshow needs histology training to develop information security awareness among employees, educate users on the importance of information security, and train internal personnel to assume information security roles.

It is not only the managers' code of conduct that forms the prerequisites for culture but also the material, equipment, resources, and even financial investments needed to penetrate the corporate organization. Hanshow must invest in hardware configuration, assets, data security, cryptography, and privacy management. Data backup, disaster recovery, and capacity management are aspect Hanshow need to ensure continuity (Georgiadou et al., 2021).

4.4.3 Believe, Value and Attitudes

The values, attitudes, and beliefs (Figure 4.5) that form the core of a cybersecurity culture are unwritten rules that everyone knows but few can articulate. However, they can be observed in the actions of leaders, groups, and individuals in organizations. Hanshow's top management team need to raise cybersecurity training to the strategic level priority and involve managers from all department to engage with the project.

A culture can be fostered by coordinating teams of company employees and establishing shared values and beliefs. Organizations are comprised of individuals who collaborate to execute business processes. Teamwork provides a means to continuously process and update information in order to be situationally aware of a cybersecurity threat.

Hanshow must implement individual understanding of cyber threats, awareness of cybersecurity policies, and the impact of individual capabilities on corporate cybersecurity after reaching a collective understanding. Through training, the development of an employee handbook, and the scheduling of meetings, employees will be able to act in a manner consistent with increasing cyber resilience.

4.4.4 Compliance Transformation to culture

Hanshow had to implement Alshaikh 2020's five initiatives to transform employees from compliance to proactive action after achieving the three culture formation constructs outlined by Huang and Pearlson 2019. After the cultural background is formed, employees can easily develop the inertia to comply with the cybersecurity code of conduct. However, it is challenging to bridge the gap between awareness and behaviour. By adhering to Alshaikh's five key initiatives (Figure 4.2), The company can narrow the gap between thought and action. By creating communication hubs, team champions, and slogans, Hanshow may ultimately inspire and motivate employees (Figure 4.5).

4.4.5 Behaviour

After establishing a cybersecurity culture, organizations need to rely on the behaviour of their employees to prevent and protect them from potential cyber-attacks. Overall, employee behaviour is what creates or reduces cyber-based vulnerabilities. Therefore, it is only after Hanshow has completed all five stages (Figure 4.5) that Hanshow employees are willing to perform their in-role cybersecurity behaviours and spontaneously reach for cybersecurity advocacy and opinions outside their roles (Huang & Pearlson, 2019).

4.5 The Application Scenario of the Model

Table 4.5 explains how Hanshow can use the model proposed in this thesis to build a cybersecurity culture within the organization. The "Implementable Initiatives"

presented in the table are not unique; rather, they illustrate the initiatives that can be implemented at each stage.

The table's leftmost column summarizes the five categories derived from the 2019 models of Huang and Pearlson and the 2020 models of Alshaikh. The second column describes each category's secondary dimensions. The third column illustrates which components should be implemented in each dimension, while the fourth column demonstrates how to construct targeted initiatives utilizing the model proposed in this thesis.

Category	*Dimensions*	*Components*	*Implementable Initiatives*
External Influences	Societal Cybersecurity Culture		Hanshow top managers need to highlight the difference between Chinese and European society's cybersecurity culture and provide localized information to the employees
	External Rules and Regulations		Hanshow shall ask the legal department to investigate the local external rules and regulations like GDPR
	Peer Influence		Competing companies in Hanshow are all equally involved in the security of retail customers' data
Organizational Mechanism	Leadership	Cybersecurity Culture Leadership	Hanshow needs to assign a leader with an agenda covering cybersecurity guidelines and knowledge.
	Incentive	Performance Evaluations	Establish a performance review for employees. Those who repeatedly failed phishing exercises were subject to notations and low scores in KPI performance
		Rewards and Punishments	Employees who avoid cyber-attacks need to be praised in the form of proclamations, certificates, or bonus
	Process	Organizational Learning	Hanshow needs to continually update on cybersecurity news and issue campaigns to facilitate long-term retention of cybersecurity practices and behaviours
		Cybersecurity Training	Hanshow needs to provide on-board training, periodic training, and WFH guidelines to increase awareness of cybersecurity
		Communications Channel	Hanshow needs to arrange marketing-like campaigns to encourage cybersecurity behaviours and spread the message via multiple channels like email, alters, events and training
	Asset		Hanshow needs to invest in hardware configuration, hardware assets, data security, network infrastructure, and privacy management
	Continuity		Hanshow needs to strengthen its preventive mechanisms. Invest in backup mechanisms, disaster recovery, and continuous vulnerability management.
	Security Governance		Hanshow needs audit logs, incident response, email, and web browser resilience to enhance long-term governance
Belief, Value and	Leadership	Top Management Priority	Hanshow Manager needs to raise the WFH cybersecurity project to a Strategic-level priority or authorize a significant budget for security activities and software

		Top Management Participation	Hanshow's top management team needs to show personal attitudes and involvement the cybersecurity by attending training, rewarding and participating in other cybersecurity activities
		Top Management Knowledge	Hanshow's leader needs to know Hanshow's cybersecurity vulnerability. Provide training and regularly engage in the latest cybersecurity discussion
	Group	Community Norms and Belief	Hanshow needs to value and emphasize "info protection" regularly via email or weekly meetings
		Team Work Perception	Hanshow team needs to build cybersecurity consideration in their project and other exercises
		Inter-department Collaboration	The core team working with cybersecurity leaders included members from different departments like logistics, legal, and marketing
	Individual	Employee's Self-efficacy	Through training and communication, Hanshow needs to make employees aware of how to identify and respond to phishing emails and whom to communicate with
		Cybersecurity Policy Awareness	Hanshow needs to remind and notify employees about cybersecurity policy via meeting or email
		General Cyber Threat Awareness	Hanshow needs to train and summarize historical cyber threats as cases to build suspicious of unusual emails, attachments, and advertisement
Compliance Transformation to culture	Identifying the key cybersecurity behaviours		Simplifies policy language and shifts employees' focus from basic awareness to desired behaviours. Hanshow need to summarize 5 key notification like Think before you click; do not forget to auto-lock your laptop; report anything suspicious
	Establishing a cybersecurity champion network		Hanshow needs to select Opinion leaders in different departments. Define the roles and responsibilities of the Champion to create a support network for the cybersecurity team.
	Building a Cybersecurity Hub		Hanshow needs to build a collective hub for WFH guidelines, security rules, training, VPN installation, and online Q&A for the cybersecurity teams
	Developing a brand for the cybersecurity team		Hanshow needs to design a logo and brand for the cybersecurity teams. The security awareness and training logo should be used consistently in any activities related to security awareness, such as training sessions, posters, alerts of new threats
	Aligning security awareness with internal and external campaigns		Hanshow needs to align the cybersecurity slogan, alters, and team logo within all channels of communication like cybersecurity hub, training sessions, and monthly meeting
Behaviours	In-role Cybersecurity Behaviours		The survey results indicated a positive attitude towards in-role cybersecurity behaviours. Hanshow employees need to obey WFH guidelines and security policy and avoid policy violation

	Extra-role Cybersecurity Behaviours	Hanshow needs to motivate employees to promote cyber security, speak up and improve self-knowledge

Table 4.5 Application of Model

4.6 Answer to RQ3 and Discussion of the Treatment

RQ3: What method can Hanshow adopt to contribute to the creation of organizational cybersecurity culture?

The answer to this question is the models (Figure 4.5) proposed and empirically evaluated in this thesis. Namely, Hanshow can refer to the model presented in Figure 4.5. This newly proposed model outlines the culture-building components that must be implemented at both the internal employee and leadership levels. Hanshow can implement gradually each component of the corporate cybersecurity culture by following the step in Table 4.5. In detail, the management and initiatives within Hanshow can be implemented in stages according to the model's outlined categories. This thesis' model is intended to reflect the current state of Hanshow's cybersecurity culture. Hanshow has acknowledged the significance of cybersecurity and external factors.

Through their performance and conduct, Hanshow managers can reinforce their employees' cybersecurity values, beliefs, and attitudes. The model (Figure 4.5) is divided into five major categories, including integrating the implementation of cybersecurity into employee performance evaluations and reward systems, promoting the repercussions of not adhering to cybersecurity behaviours, establishing a strong communication program, and providing ongoing training to learn about cybersecurity activities. Hanshow’s management team must actively participate in cyber resilience-enhancing activities and training. Additionally, the management of Hanshow must establish a position dedicated to promoting and supervising the implementation of a cybersecurity culture. The resilience and tenacity of the company's established corporate culture can be evaluated more accurately through integrated management.

The proposed model also explains how Hanshow evolved from a single obedience and participation training to voluntary cybersecurity maintenance behaviours. This is a crucial step in the transition of employees from compliance with norms to a culture of proactive cybersecurity advocacy. In addition, the model describes the significance of integrating cybersecurity activities with internal company events, where joint communication will significantly improve the effectiveness of cybersecurity awareness campaigns.

The models presented in this thesis not only present ways for managers to help Hanshow build a cybersecurity culture but further provide how Hanshow can assess whether its culture is driving cybersecurity behaviour. Behaviour is driven by unwritten rules that are hard to see. However, these unwritten rules are evident in the organisation's values, beliefs, and attitudes exhibited by management, teams, and individuals. Hanshow management can evaluate the stages of cybersecurity culture and the in-role and extra-role behaviours done by employees according to the model.

This model describes in detail the category and dimensions that must be considered when constructing a corporate cybersecurity culture. Consequently, companies can use this model as a benchmark for gauging their cybersecurity preparedness and readiness. Nonetheless, if quantifiable metrics are required to evaluate the development of a cybersecurity culture, one can consult the Cybersecurity Culture Framework (Georgiadou et al., 2021) assessment. We note that Georgiadou et al. originally designed their framework to examine an organization's security infrastructure, policies, and procedures with its employees' personal characteristics, behaviours, attitudes, and skills. Its elements are derived from a comprehensive and multidimensional literature review and research analysis of current cybersecurity realities. The methodology of Georgiadou et al. quantifies each component of its architecture to enable a viable assessment method. In addition, the methodology can be applied to design and develop applications for a security culture assessment tool that provides recommendations and alternatives for workforce training programs and techniques. This Cybersecurity Culture Framework (Georgiadou et al., 2021) can therefore be used to assess and quantify the security readiness of Hanshow employees.

Chapter 5. Expert Evaluation

To evaluate the proposed model's validity, consistency, and applicability, the following sections will propose an expert evaluation with Hanshow technical professionals to receive reflection and feedback. This expert evaluation chapter consists of two parts. One part of the evaluation includes a questionnaire adapted based on the UTAUT model and its constructs selected per Hanshow's situation. In order to have a more intuitive understanding and feedback on the model proposed in this thesis, the second part of the expert evaluation includes interviews with the two experts so to provide concrete feedback.

Section 5.1 will provide a brief summary of the experts' background, the reason why they are suitable for participation, and their position within Hanshow. Section 5.2 presents the description of the UTAUT model and its related factors. Section 5.3 describes the selected construct from the UTAUT model and the corresponding definition based on Hanshow's scenarios. Furthermore, Section 5.3 also provides a brief description of the proposed questionnaire. Section 5.4 concludes the result of the questionnaire. Section 5.5 provides detailed results from the expert interview and received feedback. Furthermore, Section 5.6 will briefly discuss the limitation of this expert evaluation chapter. Eventually, Section 5.7 will answer research question 3 based on the feedback from the expert evaluation chapter.

5.1 Expert Background

Since Hanshow is a small to medium-sized information technology company, at the same time, this thesis aims to create a cybersecurity culture model that can be used by Hanshow in the long term and applied to WFH policies. This meant that the experts must be selected from a group with a technical background and an adequate understanding of Hanshow's teleworking restrictions and the Chinese cultural context. Meanwhile, the experts selected had to have years of working experience in Hanshow to be able to comment on the feasibility of implementing the model's "Top Management Participation", "Establishing a cybersecurity champion network", and "Building a Cybersecurity Hub" in Hanshow.

After consideration, two experts with at least two years of working experience and technical background at Hanshow were selected to participate in the expert evaluation. One of the experts in the technical director in charge of the overseas SAAS operation and maintenance of Hanshow. He has been with Hanshow for three years and was promoted from a junior manager to technical director. He has a professional technical education background and capabilities, as well as exposure to several early major customer cases at Hanshow, such as the SAAS deployments of Ahold Delhaize and Aldi. At the same time, he has many years of overseas experience, which allows him to understand the differences between Chinese and foreign cultures and to neutrally evaluate the gaps and integration of Hanshow's European cybersecurity culture.

The other expert is a cyber security consultant in large project delivery who joined Hanshow from Huawei two years ago. He joined Hanshow mainly to deal with the delivery of large overseas projects, and he also had experience with key customers such

as Aldi and Carrefour projects. He has a technical background with a clear understanding of Hanshow's technology and backend operations. However, he also understands the more comprehensive areas of Hanshow's daily dealings with clients, project operations, and handovers. He is in frequent and close communication with both senior management and key clients. As a result, the feedback and comments from both experts were very comprehensive in terms of Hanshow's operations, staff work, client communication, and technical management.

These two experts will first lead their respective teams of six to complete the questionnaire based on the UTAUT model. Their team members are all elite team members responsible for SAAS and large project delivery, young and with overseas experience. After completing the questionnaire, the two experts will participate in an independent expert interview to provide more detailed feedback and opinions.

5.2 The adapted UTAUT model

To understand the feasibility of the model and the intention of use from an expert perspective, our expert evaluation study employed a questionnaire based on Venkatesh's Unified Theory of Acceptance and Use of Technology (UTAUT). UTAUT is widely used to determine the acceptance of new technologies (Venkatesh et al., 2003). In Section 2.4 of the article, the text briefly outlines the description, framework, and construction of the UTAUT model (Figure 2.4). UTAUT model is a well-known model testing the acceptance and use of new technology (Venkatesh et al., 2003).

For the expert evaluation, we selected four of the six constructs based on the treatment context of Hanshow. In the next Section 5.3, the variables and constructs of the model will be further explained and elaborated, while a specific definition based on Hanshow's situation will be provided.

5.3 UTAUT variables and constructs

In this section, this thesis provides an overview and definition of UTAUT variables and constructs, as well as their application to the Hanshow case. Also, this section will outline how the UTAUT model is incorporated into the expert evaluation questionnaire and in what form it is measured and assessed. In this thesis, some adjustments were made to the original questions of UTAUT model metrics. Thus, it fits more closely to the real situation of Hanshow to better fit this research project. The questionnaire and interview details can be found in Appendix B and Appendix C.

According to Figure 2.4, we select the following factors and constructs from the original UTAUT model: Gender, Age, Experience, Performance Expectancy, Effort Expectancy, Behavioural Intention, and Social Influence. The definition of each term in the current thesis’s scenarios can be defined as follows, shown in Table 5.3.

In addition to the two experts, six people from their respective teams participated in the questionnaire. In other words, a total of eight people participated in the questionnaire for the expert evaluation. The participants all had technology-related backgrounds but came from different age groups. Although the number of participants was small, they all had some knowledge and understanding of Hanshow's operations and maintenance

and cybersecurity controls, which could help to accurately assess the model on the topic of a corporate cybersecurity culture.

Constructs	Definitions
Performance Expectancy	The degree to which employees perceive that the model can improve the cybersecurity performance of Hanshow.
Effort Expectancy	The degree of ease associated with the adoption of the model.
Behavioural Intention	The degree to which employee perceive their intentions to adopt the model.
Social Influence	The degree to which employees perceive that the adoption of the model is affected by the people surrounding them.
Gender	Male, female
Age	18-24 years old 25-34 years old 35-44 years old 45-54 years old

Table 5.3 Definition of UTAUT Constructs

5.4 UTAUT Questionnaire Results

This section describes how each construct in the questionnaire was measured and its corresponding results. It also shows and discusses what each indicator represents, employing figures and features. All constructs' questions are measured using a 5-Likert scale ranging from "Strongly Disagree" (standing for 1) to "Strongly Agree" (standing for 5), and corresponding scores range from 1 to 5. Namely, this scale means that the higher the average score, the more positive feedback for the proposed model.

Gender and Age

The basic demographics of the participants are shown in Figures 5.4.1 a and b. As mentioned earlier, eight participants, two females and six males, ensured objectivity and diversity of views on the evaluation. They were from different age groups. Participants must have several years of professional experience, technical background in Hanshow, and diverse background characteristics to preserve the population's diversity as a requirement for selection. The average age of the participants is 35 years old.

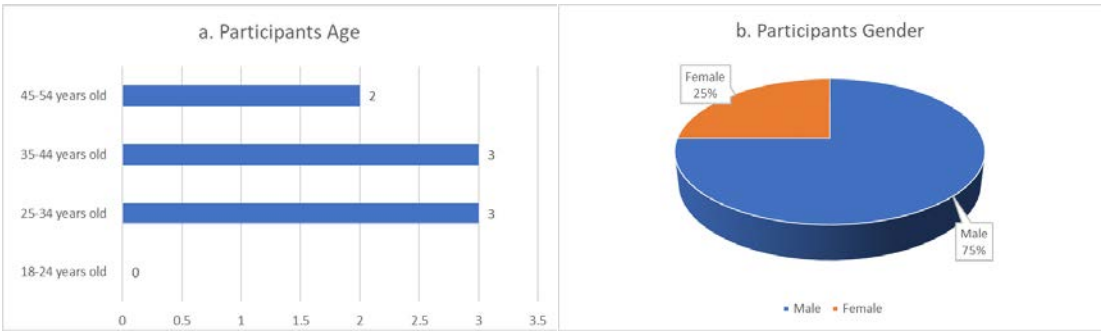


Figure 5.4.1 a. Participants Age b. Participants Gender

Performance Expectancy

The meaning of performance expectancy is to indicate the degree to which employees consider the proposed model can help promote a cybersecurity culture. In other words, if the proposed model can help boost employees' productivity. This construct utilizes a 5-Likert scale ranging from “Strongly Disagree” (standing for 1) to “Strongly Agree” (standing for 5). The result is shown in Figure 5.4.2. The overall evaluations and the general attitude of performance expectancy are very positive. The average score of “Performance Expectancy” is 4.06. This figure indicates that the proposed model is helpful in performance productivity and working efficiency.

Construct	Item
Performance expectancy	1. The use of the model can significantly ensure the cybersecurity of my work output. 2. Using the model would boost the efficiency of my work. 3. I would find the system useful in my cybersecurity performance. 4. Using the model increases the productivity of the department.

Table 5.4.2 Definition of Performance Expectancy

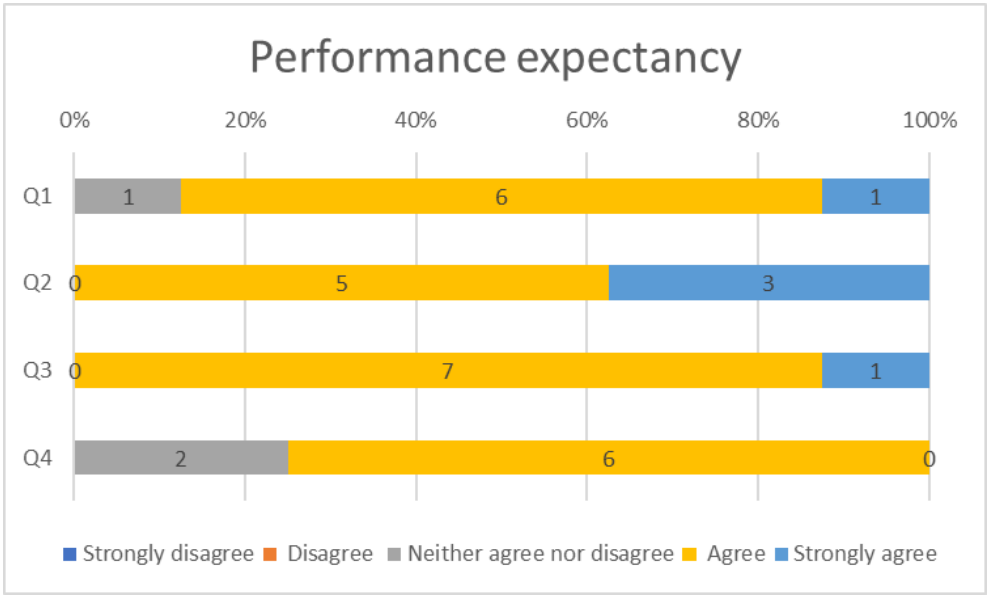


Figure 5.4.2 Performance expectancy

Effort Expectancy

To measure employees' effort expectancy is to define the ease of use for adopting the proposed model. In other words, if the proposed model is too complex to obey and follow. This construct is also measured using a 5-Likert scale ranging from "Strongly Disagree" (standing for 1) to "Strongly Agree" (standing for 5). The result is shown in Figure 5.4.3. As we can see, the average score is 3.88. Therefore, the simplicity of this model is relatively well understood and used. The mean scores showed that participants mostly agreed that the model is easy to use and follow.

Construct	Item
Effort expectancy	1. Learning to adopt the model would be easy for me. 2. The method mentioned in the model is practical to be applied. 3. The proposed method is easy to follow and does not too complex to obey. 4. The general procedure of the model is clear and understandable to be followed

Table 5.4.3 Definition of Effort Expectancy

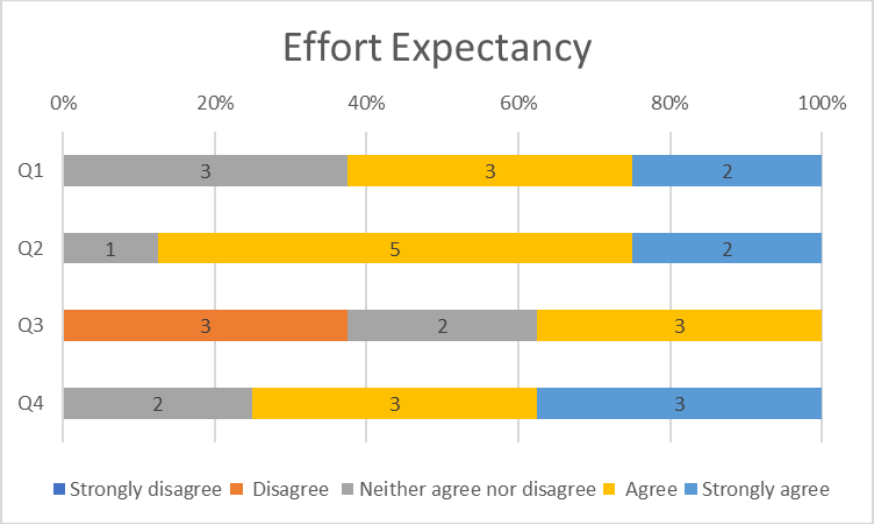


Figure 5.4.3 Effort expectancy

Behavioural Intention

Behavioural intention stands for whether employees have an intention and are willing to adapt and follow the model. This construct is measured with two questions. The average score on the 5-Likert scale ranging from "Strongly Disagree" (standing for 1) to "Strongly Agree" (standing for 5), shows a score of 3.69 (Figure 5.4.4). The participants remained enthusiastic and eager to adopt the proposed model. Most of them agreed to follow the model's advice continuously for six months.

Construct	Item
Behavioural Intention	1. I assume I will adopt the model in the next 6 months. 2. I would like to follow the model method in the following half years.

Table 5.4.4 Definition of Behavioural Intention

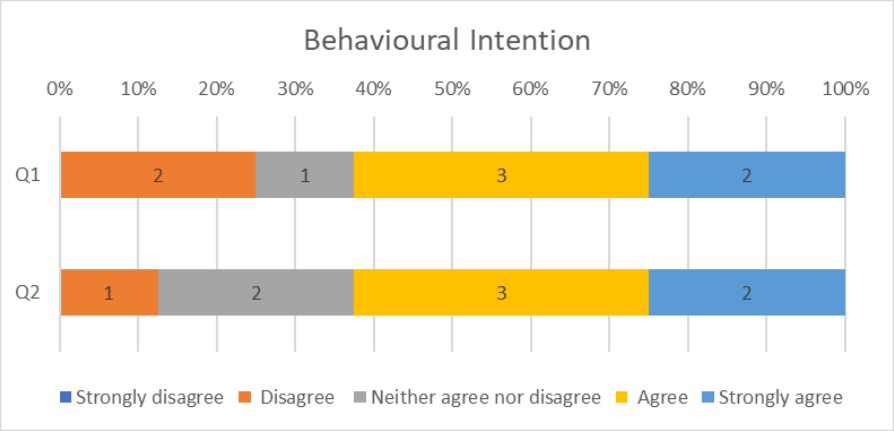


Figure 5.4.4 Behavioural Intention

Social Influence

Social influence is to show whether other employees of Hanshow have contributed to the use of the model. Whether the rest of the team supports and recommends implementing the model or not. This construct is also measured with a 5-Likert scale ranging from "Strongly Disagree" (standing for 1) to "Strongly Agree" (standing for 5) for 4 sub-questions. The detailed information is reported in Figure 5.4.5, where we can see that the average score is 3.19. The influence of other employees at Hanshow is not very high, and the employees mostly have their own opinions and judgments, probably also influenced by the Chinese culture. The average index shows that the social influence index of employees is not very high.

Construct	Item
Social Influence	1. Other employees think I should adopt this model. 2. Employees who are important to me think that I should use the method. 3. The internal employees support the advocacy of the proposed model. 4. The management teams support the promotion of the method.

Table 5.4.5 Definition of Social Influence

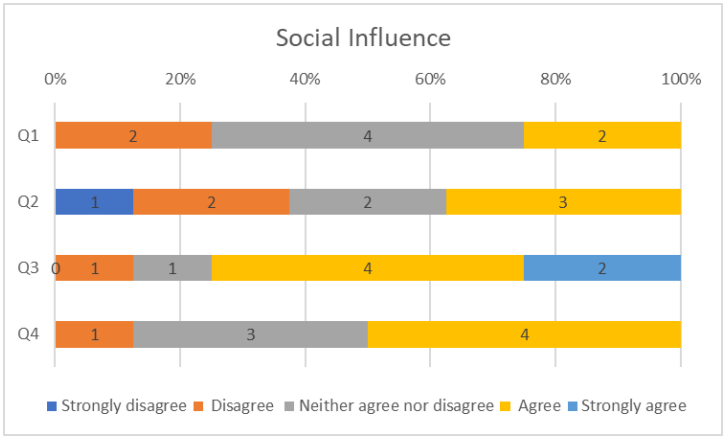


Figure 5.4.5 Social influence

5.5 The UTAUT Model Expert Interviews

This section presents the content of the interviews conducted with two experts. The detailed interview questions can be found in Appendix C. The interview questions are compiled based on the constructs filtered from the UTAUT model. The purpose of these two follow-up interviews is to provide a detailed understanding of the feedback and improvement from the expert's perspective. The description is presented in such a way that each construct is presented one by one, and the feedback and opinions of the two experts are addressed separately. Expert 1 is the technical director, and Expert 2 represents the cybersecurity consultant in big project delivery.

Construct	Interview Questions
Performance Expectancy	Do you think the model provided is specific enough? Will it help your employees improve efficiency and foster a long-term culture of cybersecurity? If not, what specifically can be done to improve it?
Effort Expectancy	Do you think the model provided is sufficiently actionable? Is it unambiguous enough for employees and leaders to implement and enforce? If it is inadequate, how can it be corrected?
Behavioural Intention	Do you think the proposed model will get the company's executives and employees motivated to implement it? Are you personally willing to follow the model's guidelines and implement them?
Social Influence	Do you think the model proposed in this paper can gain the solidarity and advocacy of employees and leaders? Are you personally willing to advocate for your subordinates to follow this model's plan?

Table 5.5.1 Definition of Interview Constructs

Performance Expectancy

Expert 1

On the point of “Performance Expectancy”, his view is positive. However, he also suggests some areas for improvement. For example, he mentions that *"the performance appraisal mentioned in the model, for example, can easily add some extra concerns and workload to employees (especially for non-technical colleagues), because performance appraisal is always related to personal development and motivation of employees. "*. Therefore, he suggests we need to focus on balancing criterion construction's negative impact on work efficiency to promote the formation of a cybersecurity culture more positively.

Expert 2

As a large project delivery manager, this expert said, *"The model is very well developed and comprehensive from a business perspective. Establishing a culture of cybersecurity*

is necessary for long-term customer relationships and back-office information privacy maintenance." In terms of his attitude, the validity of the model is confirmed. However, his opinion is that *"Hanshow is in the early stages of building a culture and is very unaware of cybersecurity. So for Hanshow, the pre-paving and training journey is much longer than for other overseas companies. Upfront training, security manuals, and hardware deployment took longer to penetrate and were not sufficiently detailed".*

The two experts recommend that in the pre-organizational mechanism phase, Hanshow needs to detail the dimensions and elaborate on each specific component in addition to the abstractive incentives, training, and hardware configuration. And each step needs to be put into a timeline with a specific running time. This is the most effective way to increase employee productivity.

Effort Expectancy

Expert 1

The expert expressed his views on “Effort Expectancy” from macro and micro perspectives. He believes that the model is clear regarding operability from a macro perspective but needs further refinement from a micro perspective. Taking "Emergency Response" as an example, he believes that it is not clear to build an emergency response system based on the model, and it needs to be clear which way we choose to build it (e.g., in-house or MSS service).

Expert 2

The expert’s attitude on “Effort Expectancy” is neutral, saying that the model provided is not practical enough to be implemented directly. He says, *"Of course, the evolution of culture is a long-term process, and this model is very specific in its views as a leading direction."* In this area, the expert gave more specific advice, saying, *"Hanshow will certainly encounter many obstacles when it comes to promoting the implementation of the model and its methodology in the early stages. The culture of Chinese companies may cause employees to prioritize work operations and performance over fostering a culture of long-term profitability. I suggest refining the detailed guidelines for each step in the early stages. And clarify the appropriate roles that leaders and employees need to play, even down to how everyone in each department needs to drive the cybersecurity culture."*

Behavioural Intention

Expert 1

As a direct stakeholder, the expert was very positive about “Behavioural Intention”, indicating that he was willing to build a cybersecurity system based on the model.

Expert 2

First, the expert's attitude was very positive in response to the “Behavioural Intention”. He said, *"I know the importance of a culture of cybersecurity, and that is why I'm committed to the security of my clients' information when delivering large projects. I will cooperate with the relevant arrangements and am willing to follow the approach proposed by the model."*

On whether leaders and employees have the intention to follow this model. The expert's attitude is also very positive. He says, *"The company's top management is also becoming aware of the importance of cybersecurity in dealing with European customers. The epidemic has also made leaders and employees realize that WFH and network security are very important for a long and secure working life. I think once this model is implemented, it will definitely be approved and obeyed by everyone."*

Social Influence

Expert 1

In "Social Influence", the expert expressed a relatively neutral opinion. First of all, he is very willing to follow and advocate the use of the model to build a cybersecurity culture. However, he also expressed concern on the issue of regional compliance. he mentioned that *"the model is reasonable and necessary in Europe where the cybersecurity system and regulations are relatively sound, but cybersecurity awareness might be underdeveloped in some other regions. Namely, following the model may violate local guidelines and affect the business development in some underdeveloped regions."* Therefore, he believes the model needs to be adjusted according to regional laws and regulations.

Expert 2

Regarding "Social Influence", experts say it could be difficult to get people's advocacy and promotion. The expert explains that *"as a Chinese company, the cultural impression of China is more solidified. Chinese people prefer to stay opinion independent. We are used to following rules and criteria, but it takes more motivation and initiative than Europeans to spontaneously preach and drive others".*

Chinese culture's influence is different in perception and cognition than Western culture. But in the case of the expert's personal opinion, he said, *"My profession and my team's profession are well aware of the need for cybersecurity. So, I believe we all agree on the importance of this model and we are all willing to contribute to the cybersecurity culture of Hanshow".*

5.6 Limitation

This section summarizes the limitations of the entire chapter on expert evaluation. First, only *eight* people participated in the UTAUT evaluation, which poses a potential threat to its validity. Nevertheless, there are only 32 employees at Hanshow in the Netherlands, and the eight participants carefully selected for this evaluation study actually represent 25% of the company's workforce. Therefore, we can assume that the eight participants can accurately reflect and represent the status and opinions of all Hanshow Netherlands employees and that their participation has no bearing on the evaluation validity.

On the other hand, the UTAUT questionnaire was administered to a diverse group of participants (see Figure 5.4.1 a and b) to ensure a healthy balance of viewpoints. While ensuring that each of the eight participants screened in this evaluation possesses professional cybersecurity knowledge, they differ in gender, work experience, and position level. Consequently, their feedback can provide alternative perspectives and

representations. Furthermore, in order to collect more detailed and constructive feedback, an interview was conducted with *two* additional industry experts. Therefore, the interview process mitigates the risk of missing an important feedback point in this evaluation study.

5.7 Answer to RQ4 and discussion of the model's feasibility

RQ 4: How useful and usable is the newly proposed model from the perspective of practitioners working in the field?

The answer to RQ 4 can be witnessed in Chapter 5 where the results of our empirical perception-based evaluation of the model are reported. To sum up, if the model proposed in this thesis can finally be implemented, it will enhance employee data protection, customer privacy, and the viability of teleworking for technical employees within Hanshow. As a result, human cybersecurity risks will be reduced, employee satisfaction in the IT department will increase, and overall employee productivity will be increased. Externally, Hanshow can cultivate a trustworthy image and customer relationship. As the participating experts stated, organizational cybersecurity culture will impact the efficacy of corporate cybersecurity resources, policies, practices, and employee efforts because it reflects the corporate office environment, employee perceptions, and behavioural guidelines.

In the context of the Covid-19 epidemic, WFH is gradually becoming a remote management trend for major companies. As a technology company, ensuring cybersecurity is a critical operational foundation. It is even more critical today when the epidemic is uprising and the management team has to implement remote management. Developing a corporate cybersecurity culture helps achieve growth through digital trust, enhances an organization's reputation with customers, and builds employees' sense of belonging and pride. They create an environment enabling the entire organization to operate more securely with less effort which boosts employee efficiency.

From Hanshow's perspective, network security management builds trust with core customers and creates an image of a trustworthy IT company. Hanshow will be able to face more environmental changes in the future and better integrate into the European management system and culture if it establishes a corporate cybersecurity culture. Moreover, as an international company expanding abroad, Hanshow will inevitably engage in remote communication and management with its headquarters; therefore, the establishment of a cyber security culture will be advantageous to Hanshow's long-term management.

Chapter.6 Reflection & Discussion

This chapter will summarize the findings of the questionnaire in Chapter 3, the proposed model in Chapter 4, and the expert evaluation in Chapter 5. Section 6.1 will discuss the whole process and the implications of this study. Section 6.2 will illustrate the limitations and shortcomings of this thesis.

6.1 Interpretation

In the third chapter of the thesis, we conducted an online, anonymous questionnaire for Hanshow Nederland BV employees. The purpose of the questionnaire was to answer the first and second set of research questions (RQ1 and RQ2) of this thesis. In other words, the ultimate goal is to find out how is the cybersecurity readiness of Hanshow during WFH in the situation of Covid-19. The questionnaire provided insight into Hanshow's telecommuting policy, employees' attitudes toward WFH, the facilities utilized, the cyber risks encountered, and the perceived ability and awareness of cybersecurity risks.

Combining the survey results and the quantitative analysis, we were surprised to discover that although employees have a positive and proactive attitude toward WFH, their dissatisfaction with Hanshow's response to the cybersecurity crisis increases with their technical expertise. During the period of teleworking, in addition to IT department employees with professional knowledge of network security, other employees were required to use applications they were unfamiliar with prior to the Covid-19 outbreak. All of these particulars exposed Hanshow to substantial human cybersecurity risks. According to the employees, the lack of cybersecurity precautions could expose Hanshow to lawsuits, reputational harm, loss of customer trust, and other tragic outcomes.

The investigation of these indicators in the questionnaire served to specify a WFH implementation guide for Hanshow in response to the pandemic-related cybersecurity risks. Long-term corporate cybersecurity culture is necessary to help Hanshow address remote management and cybersecurity fundamentals. With the web-based questionnaire coupled with the existing literature, this thesis proposes a model for Hanshow to help establish a long-term cybersecurity culture in dealing with WFH regulation. In order to verify the suitability and usefulness of the proposed model in this thesis, two experts and six of their team members were given a questionnaire based on the UTAUT model. The constructs of expectancy, complexity, and intention of usage were measured. Simultaneously, two experts were invited to conduct a separate interview to verify the applicability of the model. Ultimately, from the participants' feedback, we can conclude that the model proposed in this thesis is feasible and effective in enhancing corporate cybersecurity culture.

6.2 Implications for Practice

As a result of the Covid-19 pandemic, Hanshow employees were compelled to work from home without effective telecommuting management and the requisite resources. IT professionals were unable to adjust to a home-based setting and were restricted by the corporate office's network infrastructure. Other staff lacked risk awareness and were unable to obtain quick assistance in the event of cybersecurity issues. Hanshow was subject to years of Chinese cultural influence as a Chinese company with international operations. The Hanshow leaders could not alter the Chinese cultural climate and establish a sustainable culture of cybersecurity. Moreover, establishing the culture necessitates a lengthy period of penetration and propaganda. The leaders of Hanshow were unaware of how to bridge each stage of cultural development and what measures to implement at each stage.

Based on the current situation at Hanshow, the model proposed in this thesis describes the numerous stages that must be completed to develop a cybersecurity culture and the preparations and tasks that each individual must adhere to at each dimension. The thesis organizes the timing and criteria for each stage from large to small scale. From there, it can assist the company in establishing a long-term approach to cybersecurity management and assist employees in organizing their cybersecurity understanding. This model illustrates the strategy required at each level from the leader's and the employee's standpoint. With this methodology, Hanshow personnel can review in real-time the resources and activities the company should allocate at each stage. Leaders can also track the progress of their employees' culture-building efforts to appoint team leaders, recognize good behaviour, and create a cybersecurity ecosystem.

6.3 Implications for research

The model provided in this thesis organizes the stage and category needs from large to small size in a progressive manner. As a result, it can assist SMEs in developing a long-term cybersecurity management strategy and aid employees in enhancing their cybersecurity knowledge.

Future researchers can use the model's category and components to position themselves to target the company's existing culture (Figure 4.5). New culture management programs and measures can be added and revised based on the model's suggested components. In addition, this paper's model references a well-known cybersecurity culture framework (Georgiadau et al. 2021). Consequently, researchers that seek to quantify a company's cybersecurity culture can utilize the proposed model as a guide to developing quantitative measurements based on relevant articles.

While the model presented in this thesis currently includes categories, dimensions, and components for initiative implementation, experts at the expert validation session thought that more detailed behavioural requirements are necessary to increase cultural

readiness and overall cybersecurity performance. This means that the model provides simply the initial foundation for operationalizing the categories and the components into precise instructions that a company's employees can use to assess how well the model is being followed. Based on the model, future research can generate more specific initiatives that can be defined and operationalized. Figure 4.5. and Table 4.5. indicated how the model can be applied in Hanshow, however, we note that Figure 4.5. is a work in progress from a research perspective. More components could be added to the model based on future research. As Figure 4.5. shows not all dimensions have components and it would be interesting to refine the model by researching the components associated with the dimensions Asset, Continuity, and Security Governance (Georgiadau et al. 2021).

6.4 Limitations

As a technology-based business, Hanshow has more stringent requirements for the configuration of network security and oversight of remote management. To tailor a model to suit Hanshow's requirements better, the initial background questionnaire for this thesis included a number of questions specific to Hanshow. In order to prevent biased responses, these questions were formatted with multiple-choice answers. In addition, four representative employees were selected to conduct an interview after the questionnaire, so that objective feedback from Hanshow employees could be gathered more precisely and objectively to eliminate bias in the questionnaire.

The number of respondents to the questionnaire is an additional controversial limitation. There were only 32 respondents to the questionnaire, which may not guarantee the diversity and representativeness of the responses. However, the model proposed in this thesis is for Hanshow Nederland BV, which has only 32 local employees. Therefore, generalizability and representativeness issues are not considered to exist in the questionnaire responses presented in this thesis.

Another potential issue with the expert evaluation is that the evaluation session’s participants are not randomly selected. This may contradict the randomness of the questionnaire and the generalizability of the evaluation. However, as explained in Section 5.6, the experts who participated in the evaluation comprised 25 percent of Hanshow Netherlands' employees and had diverse backgrounds, so this did not affect the evaluation's representativeness and objectivity.

In addition, the model presented in this thesis does not generate any additional quantifiable metrics. Nevertheless, Hanshow is in the early stages of establishing a corporate cybersecurity culture; consequently, it will take a considerable time for Hanshow to gradually develop cybersecurity beliefs, values, and attitudes. The model proposed in this thesis is still a work in progress from a research point of view (Figure 4.5). Therefore, the model is not refined to a level that can be quantified and evaluated at the moment. However, because the model proposed in this thesis is based on a mature

organizational Cybersecurity Culture Framework (Georgiadau et al. 2021), small and medium-sized businesses such as Hanshow can incorporate quantitative assessment methods based on framework-related literature after the model proposed has been fully implemented.

Chapter 7. Conclusion

This chapter summarizes the contribution of the whole thesis, as well as recommendations for future work. Section 7.1 describes recommendations for future works. Finally, Section 7.2 will give a brief summary of the contribution of the whole thesis.

7.1 Future Work

Establishing a corporate cybersecurity culture takes a long time to penetrate, innovate and regulate. The model presented in this paper is only to help small and medium-sized ventures in establishing a cybersecurity culture on the stages and initiatives that need to be implemented in each segment. However, future researchers that wish to adopt this model will need to further determine its applicability based on the enterprise's context and positioning.

Furthermore, this thesis does not provide metrics that can be quantitatively measured and calculated for the model. In other words, this thesis does not provide corresponding completion and achievement assessment methods based on the model. Future articles that wish to further supervise the execution degree or completion status based on the model need to combine the Cybersecurity Culture Framework (Georgiadou et al., 2021) and related assessment articles to specify a supervisory method that can be quantified

7.2 Summary of the contributions

Against the backdrop of the Covid-19 epidemic, government policies for WFH have been introduced across Europe. Hanshow's Dutch subsidiary, in line with this government policy, has also started implementing telecommuting management. However, Hanshow's management gradually realized that the implementation of teleworking had encountered many difficulties within Hanshow. For example, the regional network limited Hanshow's products, and the after-sales team needed product debugging to solve customer requests. Meanwhile, many malicious attackers used the guise of the epidemic to steal core information from Hanshow or its customers. Hanshow's executives decided to implement remote management and establish a corporate cybersecurity culture to ensure long-term company operations.

This thesis proposes a cybersecurity culture model for Hanshow based on its current culture and remote management state. This model (Figure 4.5) and its empirical evaluation form the central contribution of the thesis. It helps Hanshow establish, popularize, and transition from compliance to building a cybersecurity culture. The study identifies five key categories that Hanshow should implement, along with corresponding dimensions and specific initiatives to improve its security culture and influence and change employee cybersecurity performance.

More in detail, the contribution includes the following components: (1) a survey with all employees that helped understand the security challenges pertaining to WFH; (2) an application of two selected models for analyzing and evaluating elements of security culture in the context of the company, which created the foundation for the design of the cybersecurity culture model on Figure 4.5. (3) the elaboration of the categories, the dimensions, and the components of the proposed model, and (4) the UTAUT-based evaluation of this model with eight practitioners and a follow-up interview-based evaluation with two experts. The evaluation results indicate the model's suitability, usefulness, and usability for the context for which it was designed. Of course, more research is needed for more complete validation of its components and applicability across contexts.

Appendix A

Questionnaire

Be assured that the survey is anonymous and the responses will be kept strictly confidential. We would really appreciate it if you could spend 5 minutes of your time to answer this short questionnaire.

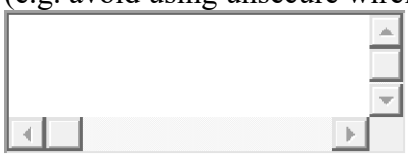
1. During the COVID-19 crisis, how many hours weekly, did you work from home?

- ○ Less than 1 day weekly
- ○ One day out of five, weekly
- ○ Two days out of five, weekly
- ○ Three days out of five, weekly
- ○ Four days out of five, weekly
- ○ All five days

2. Did you receive any security guidelines from your employer regarding working from home?

- ○ Yes
- ○ No

3.Please describe the main (2-3) security guidelines provided.
(e.g. avoid using unsecure wireless connections)



4.What kind of devices are you using to connect to your corporate working environment?
(You may select more than one answers)

- ☐ Desktop
- ☐ Laptop
- ☐ Tablet
- ☐ Smartphone
- ☐ Other

6. These devices are:

- ○ Personal assets
- ○ Corporate assets

7. Are these devices managed by your organization?
(using a Mobile Device Management system such as Microsoft Intune, G Suite, IBM MaaS360, etc. for security policies enforcement)

- ○ Yes, fully
- ○ Yes, partly
- ○ No

8. Which of the following apply for the devices you currently use for your working from home employment?
(You may select more than one answer)

- ☐ Password protection
- ☐ Two-factor authentication
- ☐ Automatic screen lock
- ☐ Hard disk encryption
- ☐ Antivirus software installed
- ☐ Antispam software installed
- ☐ None of the above

9. How do you obtain access to your corporate working environment?

- ○ Direct access
- ○ Using VPN
- ○ Using 3rd party cloud solutions (e.g. G Cloud, Microsoft 365)
- ○ No Access
- ○ Other

10.Please describe how you obtain access to your corporate working environment.

11.Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?

- ○ Yes
- ○ No

12.How were you informed how to use them?
(You may select more than one answers)

- ☐ Online training program
- ☐ User manual documentation (distributed in any way)
- ☐ Instructions available to the corporate portal or website
- ☐ Instructions provided via email
- ☐ Nothing of the above

13.Has your company adopted a specific collaboration solution? (for example, Zoom, MS TEAM, Google Doc).

- ○ Yes
- ○ No

14.Regarding the solution in Question 13, what abilities does this solution offer?
(You might be using more than one tool. Please indicate all services available.)

- ☐ Document management
- ☐ Real-time document co-authoring
- ☐ Project/Workflow/Task management
- ☐ Scheduling
- ☐ Real-time chatting
- ☐ Teleconferencing
- ☐ Other

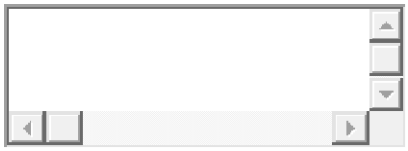
15.Did you face any of the below cyber-security related threats during the COVID-19 crisis?
(You may select more than one answers)

- ☐ Phishing
- ☐ Ransomware
- ☐ Hacking
- ☐ Data loss
- ☐ Spyware/Virus infection
- ☐ Other
- ☐ None

16. If you faced any of the cyber-security threats in Question 15, please describe the scenario in which it happened.

17. Regarding the cyber-security threat you described in Question 16, how did you deal with it? (for example, it was possible to solve it yourselfs; or you had to contact a colleague, or the security team in the headquarter)

18.Please name any other cyber-security threats you encountered during this period, not listed above.



19.To what extent do you agree with the following statements:
(during this specific period of the COVID-19 crisis)

	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
I prefer working from home than going to the office.	○	○	○	○	○
I work more productively from home.	○	○	○	○	○
I collaborate with my colleagues as effectively as when we are in office.	○	○	○	○	○
I am satisfied by my employer's approach to the crisis.	○	○	○	○	○
I have all the support i need to face any technical problems i have (eg. corporate access issues, infrastructure failures, etc.).	○	○	○	○	○
I am proud to work for my organization.	○	○	○	○	○
I have access to the things I need to do my job well.	○	○	○	○	○

20.What is your age?

- ○ 18 – 24 years old
- ○ 25 – 34 years old
- ○ 35 – 44 years old
- ○ 45 – 54 years old
- ○ 55 – 60 years old

21.What is the highest degree or level of school you have completed?
If currently enrolled, highest degree received.

- ○ High school graduate, diploma or the equivalent
- ○ Some college credit, no degree
- ○ Trade/technical/vocational training
- ○ Associate degree
- ○ Bachelor's degree
- ○ Master's degree
- ○ Professional degree
- ○ Doctorate degree

22. Please select the business domain of the department you work for.

- ○ Sales & Pre-sales (Project Manager)
- ○ Technician & After-sales

- Logistics
- Human Resources
- Accounting & Finance
- Legal Affairs
- Administration/operations
- Marketing
- Others

23.Please specify which is the business domain of the organization you work for.

24.Which of the following best describes your professional role?

- IT professional
- Manager
- Assistant
- Coordinator
- Specialist
- Vice President
- Trainee & Internship
- others

25. What consequences do you think Hanshow will experience if proper cybersecurity management is not maintained due to remote work?

26. Which work-from-home recommendations below, do you think Hanshow can use to maintain teleworking cybersecurity efforts?

- Training program
- Organizational Virtual Private Network (VPN)
- Enable multi-factor authentication (MFA)
- Enable strong company online policy (Access & Vendor security controls)
- ConFigure Firewall, IDS, IPS security solution
- Schedule constant data backup
- Others

Appendix B

UTAUT Model Questionnaire

Construct	Questionnaire Item
Performance expectancy	5. Use of the model can significantly ensure the cybersecurity of my work output. 6. Using the model would boost the efficient of my work. 7. I would find the system useful in my cybersecurity performance. 8. Using the model increases the productivity of the department.
effort expectancy	5. Learning to adopt the model would be easy for me. 6. The method mentioned in the model is practical to be applied. 7. The proposed method is easy to follow and does not too complex to obey. 8. The general procedure of the model is clear and understandable to be followed.
behavioural intention	1. I assume I will adopt the model in the next 6 months. 2. I would like to follow the model method in the following half years.
social influence	5. Other employees think I should adopt this model. 6. Employees who are important to me think that I should use the method. 7. The internal employees support the advocacy of the proposed model. 8. The management teams support the promotion of the method.

Appendix C

Expert Interview

Construct	Interview Question
Performance expectancy	Do you think the model provided is specific enough? Will it help your employees improve efficiency and foster a long-term culture of cybersecurity? If not, what specifically can be done to improve it?
Effort expectancy	Do you think the model provided is sufficiently actionable? Is it clear and unambiguous enough for employees and leaders to implement and enforce? If it is inadequate, how can it be corrected?
Behavioural intention	Do you think the proposed model will get the company's executives and employees motivated to implement it? Are you personally willing to follow the guidelines of the model and implement it?
Social influence	Do you think the model proposed in this paper can gain the solidarity and advocacy of employees and leaders? Are you personally willing to advocate for your subordinates to follow this model's plan?

Reference

Ahsan Pritom, M. M., Schweitzer, K. M., Bateman, R. M., Xu, M., & Xu, S. (2020). Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses. *Proceedings - 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020*. https://doi.org/10.1109/ISI49825.2020.9280539

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. *Computers and Security*, *98*. https://doi.org/10.1016/j.cose.2020.102003

Borkovich, D. J., & Skovira, R. J. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Issues In Information Systems*, *September 2021*. https://doi.org/10.48009/4_iis_2020_234-246

Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat? *Network Security*, *2020*(4), 8–11. https://doi.org/10.1016/S1353-4858(20)30042-8

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. Computer Fraud & Security, 2021(3), 8-13.

Chigada, J., Information, R. M.-S. A. J. of, & 2021, undefined. (n.d.). Cyberattacks and threats during COVID-19: A systematic literature review. *Scielo.Org.Za*. Retrieved January 6, 2022, from http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2021000100001

Corradini, I. (2020). Building a Cybersecurity Culture. In *Studies in Systems, Decision and Control* (Vol. 284). https://doi.org/10.1007/978-3-030-43999-6_4

Corradini, I., & Nardelli, E. (2018, July). Building organizational risk culture in cyber security: the role of human factors. In International Conference on Applied Human Factors and Ergonomics (pp. 193-202). Springer, Cham.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/J.COSE.2020.101713

Dockery, M., & Bawa, S. (2020). Working from home in the COVID-19 lockdown. *Bankwest Curtin Economics Centre Research Brief COVID-19*, *May*, 1–5. https://bcec.edu.au/assets/2020/05/BCEC-COVID19-Brief-4_Working-from-home.pdf

Dumitru, D., & Ion, T. (2020). CORONAVIRUS PANDEMIC - LEVERAGE FOR CYBERCRIME. In V. Dinu (Ed.), *2020 BASIQ INTERNATIONAL CONFERENCE: NEW TRENDS IN SUSTAINABLE BUSINESS AND CONSUMPTION* (Issue 6th BASIQ International Conference on New Trends in Sustainable Business and Consumption, pp. 1211–1217).

Employees abandoning security when working remotely - Help Net Security. (n.d.). Retrieved May 3, 2022, from https://www.helpnetsecurity.com/2020/05/29/abandoning-security-when-

working-remotely/

Evangelakos, G. (2020). Keeping critical assets safe when teleworking is the new norm. *Network Security*, *2020*(6), 11–14. https://doi.org/10.1016/S1353-4858(20)30067-2

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *0123456789*. https://doi.org/10.1057/s41284-021-00286-2

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. Sensors, 21(9), 3267.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102726

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-Janua*, 6398–6407. https://doi.org/10.24251/hicss.2019.769

Hsu C, Lee JN, Straub DW. Institutional Influences on Information Systems Security Innovations. Information Systems Research 2012;23(3):918–39.

Impact of COVID-19 on Cybersecurity. (n.d.). Retrieved May 3, 2022, from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Lundy, O., & Cowling, A. G. (1996). *Strategic human resource management*. 400. https://books.google.com/books/about/Strategic_Human_Resource_Management.html?hl=zh-CN&id=2Kg9AAAAIAAJ

Mashud, A., Prayudi, Y., Abukari, A. M., & Kwedzo Bankas, E. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond Related papers St at e of cyber securit y: t he Ugandan perspect ive Gilbert Gilibrays Exploring St at ic and Live Digit al Forensics: Met hods, Pract ices and T. *International Journal of Scientific & Engineering Research*, *11*(4). http://www.ijser.org

Mohsin, K. (2020). Cybersecurity in Corona Virus (COVID-19) Age. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3669810

Obada-Obieh, B., Huang, Y., & Beznosov, K. (2021). Challenges and threats of mass telecommuting: A qualitative study of workers. *Proceedings of the 17th Symposium on Usable Privacy and Security, SOUPS 2021*, 675–694.

Organizational Culture and Leadership - Edgar H. Schein - Google 图书. (n.d.). Retrieved May 3, 2022, from https://books.google.nl/books?hl=zh-CN&lr=&id=Mnres2PlFLMC&oi=fnd&pg=PR9&dq=schein+1985+organizational+culture+and+leadership&ots=opgpLj2qLj&sig=Y7R67cHDIDbiaLWCKZjWzMstIxA#v=onepage&q=schein 1985 organizational culture and leadership&f=false

Pandharipande, A., & Parashar, R. (2020). Repercussions of Coronavirus on Cyber-Security Threats. *BIOSCIENCE BIOTECHNOLOGY RESEARCH COMMUNICATIONS*, *13*(14), 45–48. https://doi.org/10.21786/bbrc/13.14/11

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

Pranggono, B., & Arabo, A. (2021). COVID -19 pandemic cybersecurity issues . *Internet Technology Letters*, *4*(2), 4–9. https://doi.org/10.1002/itl2.247

Sabin, J. (2021). The future of security in a remote-work environment. *Network Security*, *2021*(10), 15–17. https://doi.org/10.1016/S1353-4858(21)00118-5

Schein, E. H. (1983). The role o f the founder in creating organizational culture. *Organizational Dynamics*, *12*(1), 13–28. https://doi.org/10.1016/0090-2616(83)90023-2

Sebastian, G. (2021). A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. *IBIMA Business Review*, *2021*. https://doi.org/10.5171/2021.589235

Shammari, A. A., Maiti, R. R. R., Hammer, B., Al Shammari, A., Maiti, R. R. R., Hammer, B., & IEEE. (2021). Organizational Security Policy and Management during Covid-19. *SOUTHEASTCON 2021*, *2021-March*(IEEEE Southeast Conference (SoutheastCon)), 528–531. https://doi.org/10.1109/SOUTHEASTCON45413.2021.9401907

Tang, M., Li, M., & Zhang, T. (2015). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management 2015 17:2*, *17*(2), 179–186. https://doi.org/10.1007/S10799-015-0252-2

The Leader's Guide to Corporate Culture. (n.d.). Retrieved May 3, 2022, from https://hbr.org/2018/01/the-leaders-guide-to-corporate-culture#context-conditions-and-culture

The State of Data Loss Prevention 2020 | Tessian Research. (n.d.). Retrieved May 3, 2022, from https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly: Management Information Systems*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Yadav, R. (2021). Cyber Security Threats During Covid-19 Pandemic. *INTERNATIONAL TRANSACTION JOURNAL OF ENGINEERING MANAGEMENT & APPLIED SCIENCES & TECHNOLOGIES*, *12*(3). https://doi.org/10.14456/ITJEMAST.2021.59

Zhenrui, N (2022). A Systematic Literature Review : Security risks and remote working. (Master's thesis, University of Twente).