CYBER INSURANCE ADOPTION IN SMES AS A RISK MANAGEMENT TOOL IN DIGITALIZATION

ASLI ÖZKELEŞ YILDIRIM

BOĞAZİÇİ UNIVERSITY

2022

CYBER INSURANCE ADOPTION IN SMES AS A RISK MANAGEMENT TOOL IN DIGITALIZATION

Thesis submitted to the

Institute for Graduate Studies in Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

Business Information Systems

by

Aslı Özkeleş Yıldırım

Boğaziçi University

2022

Cyber Insurance Adoption in SMEs as a Risk Management Tool in Digitalization

The thesis of Aslı Özkeleş Yıldırım has been approved by:

Prof. Bilgin Metin
(Thesis Advisor) _____

Assist. Prof. Nazım Taşkın
(Thesis Co-Advisor) _____

Prof. Aslı Sencer _____

Assoc. Prof. Ali Coşkun _____

Assist. Prof. Arafat Salih Aydıner
(External Member) _____

July 2022

DECLARATION OF ORIGINALITY

I, Aslı Özkeleş Yıldırım, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature…….....

Date …….....

ABSTRACT

Cyber Insurance Adoption in SMEs as a Risk Management Tool in Digitalization

Small – medium sized enterprises (SMEs) create the backbone of the Turkish economy. Digitalization is a key advancement for SMEs in order to create efficiency and open up new opportunities for innovation. However, digitalization makes SMEs vulnerable to cyber threats by opening an outlet to other systems. The lack of awareness of cyber protection and the increasing advancements in cyberattacks puts SMEs at risk of data breaches which in turn causes damage to the company. Cyber insurance is considered a risk management tool for the coverage of costs in the event of an unexpected cyber incident. Even though the coverages are beneficial for the insured, the cyber insurance market is far from reaching its full potential. The study aims to find the factors of cyber insurance adoption for SMEs and the effects of cyber insurance on digitalization through cyber readiness, organizational security performance and information and communication technologies (ICT) adoption. The model created for the study was based on technology-organization-environment (TOE) context extended with individual context and the post adoption effects of cyber insurance. A quantitative survey aimed towards SMEs was conducted to test the model. Methods for increasing adoption of cyber insurance among SMEs were suggested based on the model outcomes.

ÖZET

Türkiye'deki KOBİ'lerin Dijitalleşmede Risk Yönetimi İçin Siber Güvenlik Sigortası

Küçük – ortak büyüklükte işletmeler (KOBİ) Türk ekonomisinin bel kemiğini oluşturmaktadırlar. Dijitalleşme de ekonomik olarak KOBİ'lerin verimliliklerini arttırmaları ve inovasyon ile işlerini büyütmeleri için önemli yer arz etmektedir. Ancak dijitaleşmenin beraberinde getirdikleri siber saldırılara karşı zarafiyet durumu KOBİ'ler arasında yetereince bilinmemekte olup siber güvenlik farkındalığının az olması ve siber saldırı teknolojilerinin gelişmesi sebebiyle KOBİ'ler siber saldırılara daha açık konuma gelmişlerdir. Beklenmedik siber olayları kapsamaları sebebiyle siber güvenlik sigortaları siber risk yönetim aracı olarak görülmektediler fakat henüz siber sigorta pazarı olgunluğa erişmemiştir. Araştırmada KOBİ'lerin siber sigortayı almalarındaki etkenler ve siber hazırlılık, güvenlik verimliliği ve teknoloji edinimi aracılığı ile siber sigortaların dijitalleşmeye etksi araştırılacaktır. Araştırma kapsamında oluşturulan modelde teknoloji – organizasyon – çevre modeli bireysel bakış açısı ile genişletilmiş ve siber güvenlik sigortasını edinmenin etkileri eklenmiştir. Modeli test etmek amacıyla KOBİ'lere yönelik nicel anket hazırlanmıştır. Modelin sonucunda siber güvenlik sigortasının KOBİ'ler arasındaki edinimini arttırıcı metodlar önerilmiştir.

DEDICATION

I dedicate this thesis to my mother Demet Özkeleş, who is the sole inspiration for all my work and accomplishments. I would not be here today if not for countless sacrifices she has made. I am so proud to call myself your daughter.

I also dedicate this thesis to my husband and the father to our two cats, Göksu Yıldırım. Thank you for being my support system and source of happiness.

TABLE OF CONTENTS

INTRODUCTION 1

LITERATURE REVIEW 4

2.1 Digitalization 4

2.1.1 Digitalization of SMEs in Türkiye 5

2.1.2 Digitalization and cyber security 9

2.2 Cyber security and cyber risk for organizations 10

2.2.1 Cyber security 10

2.2.2 Cyber risk management 12

2.2.3 Types of cyber attacks 14

2.2.4 Globally accepted cyber security standards 16

2.2.5 Cyber risk management measurements in Türkiye 17

2.2.6 Cost of cyber security incidents 20

2.3 Cyber insurance 21

2.3.1 Cyber insurance for retail customers 22

2.3.2 Cyber insurance for business customers 23

2.3.3 Cyber insurance coverage for business customers in Türkiye 24

2.3.4 Problem Areas of Cyber Insurance 27

2.4 Measuring insurance acceptance 30

2.5 Frameworks for technology adoption 31

2.5.1 TOE framework 32

2.5.2 Extended TOE frameworks with individual context 33
2.5.3 Adaption of TOE for cyber decisions and cyber insurance studies 34
2.6 Results of literature review 36
FRAMEWORK AND HYPOTHESES 38
3.1 Technology context 40
3.2 Organizational context 42
3.3 Environmental context 43
3.4 Individual context 45
3.5 Post cyber insurance adoption 46
3.6 Final model 47
RESEARCH METHODOLOGY 49
4.1 Survey development 49
4.2 Data collection 51
4.3 Data cleaning 52
DATA ANALYSIS 54
5.1 Demographic profile of respondents 54
5.2 Analysis of the model 60
5.2.1 Measurement model 60
5.2.2 Structural model 63
DISCUSSION AND CONCLUSION 68
6.1 Factors affecting cyber insurance adoption 68
6.2 Effects of cyber insurance adoption on cyber readiness 72

6.4 Limitations and areas for further research 74

APPENDIX A. DEMOGRAPHIC QUESTIONS 75

APPENDIX B. INDICATORS FOR THE MODEL 81

APPENDIX C. ETHIC COMMITTEE APPROVAL OF THE SURVEY 86

APPENDIX D. LOADING AND CROSS-LOADING FOR INDICATOR RELIABILITY 87

APPENDIX E. MODERATING EFFECT OF CYBER READINESS BETWEEN CYBER INSURANCE ADOPTION, ICT ADOPTION 91

APPENDIX F. THE RESEARCH MODEL WITH PATH COEFFICIENTS AND P-VALUES 92

REFERENCES 93

LIST OF TABLES

Table 1. Türkiye Digital Transformation Index 5

Table 2. Total Number of SMEs in Each Category in Türkiye 6

Table 3. Percentage Of Information Technologies (IT) Acquired By Smes And Large Enterprises 7

Table 4. Number of ISO Certificates Given in Türkiye Based on Sector 19

Table 5. Coverages of Cyber Insurance Policies in Türkiye 26

Table 6. Explanations and Examples of Global and Internal Correlations of Cyber Risk 29

Table 7. The Definition of Constructs 39

Table 8. Respondents' Demographics 55

Table 9. IT and Cyber Security Knowledge of the Respondents 56

Table 10. Company Information of the Respondents 57

Table 11. Cyber Security Tools Frequency Table Based on the Number of Security Tools Used 58

Table 12. The Number of Security Measures Used Per Respondent 59

Table 13. Cyber Insurance Adoption Based on Cyber Security Knowledge 59

Table 14. Composite Reliability and Cronbach's Alpha Results for Internal Consistency, AVE for Convergent Validity 61

Table 15. Correlations and Square Roots of Average Variance Extracted (AVE) Values 62

Table 16. Explanatory Values for the Model 63

Table 17. P-values of Path Coefficients with Stable 3, Jackknifing and Bootstrapping Methods 64

Table 18. P-values, Patch Coefficients and Effect Sizes for The Paths in the Model 65

Table 19. R^2 Coefficients and Q^2 Coefficients 65

Table 20. Total Effects of the Constructs..... 66

Table 21. Hypotheses in the Model..... 67

CHAPTER 1

INTRODUCTION

Digitalization has become one of the key metrics for the economy, business and society in Türkiye. It has become a vital and necessary advancement in twenty first century for businesses in order to be competitive as well as efficient. Digitalization, although modernizes a business to bring efficiency and business value, also creates cyber risk for businesses due to increased levels of connectivity and integration of networks. A survey conducted to business managers in Türkiye suggests even though there are significant cyber security investments made, the surveyed managers state that they do not have high levels of cyber security directives in their businesses (KPMG Türkiye, 2021). This can imply that even though cyber security is a major concern for companies, cyber threats are not considered or discussed in an organizational level.

Using information and communication technologies (ICT) in a daily basis, sharing data and integrating with third party software increases vulnerability for businesses. The number of cyber attacks increased by 80% in 2020 reaching 1.6 million in total numbers (Yalçın, 2021). Small– and medium- sized enterprises (SMEs) are one of the main targets of business level cyber attacks, as they are low of awareness when it comes to cyber security thus creating an easier target for cybercrime (BloombergHT, 2021).

Cyber security insurance or cyber insurance has been known as a notable tool for risk mitigation for businesses; the coverage of cyber insurance includes reimbursements of the costs of cybercrime as well as guidelines and tools for advanced cyber security (Lindros & Tittel, 2016). The direct benefits of cyber

insurance rely on its coverage in case of an incident and additional services provided depending on the insurance company. Cyber insurance adoption requires some level of self-protection from companies (Anadolu Sigorta, 2022; Ak Sigorta, 2022; Allianz, 2014; Doğa Sigorta, 2022). These requirements may indirectly mean that cyber adoption insurance increase cyber readiness which in turn increase the organizational security performance (Hasan, Ali, Kurnia, & Thurasamy, 2021). In addition, the adoption of cyber insurance can affect the perceived adoption of information security systems (ISS), which can fuel the intention to invest and adopt other information communication technologies (ICT) tools. To the best our knowledge, there are no researches conducted to directly analyze the effects of cyber insurance adoption on digitalization of a company.

Cyber insurance has created high levels of interest in the academic field; there have been significant research on subjects related to cyber insurance such as pricing, awareness and risk calculation. However, since it is a relatively new insurance type in a dynamic cyber security environment, currently cyber insurance has not reached maturity globally nor in the Turkish market (Biener, Eling, & Wirfs, 2015; Altuntaş, Kara, Soylu & Kırkbeşoğlu, 2018; BloombergHT, 2021). The literature focusing on the factors effecting the adoption of cyber insurance is limited to qualifying questions (Mbatha, 2020). To the best of our knowledge, a quantifying survey in a larger scale was never done to analyze the potential factors for cyber insurance adoption in SMEs.

This study aims to fill in the gap for a quantitative study for adoption of cyber insurance. The literature review for the study starts by understanding digitalization and cyber risk management for SMEs, focusing on current landscape in Türkiye. Then it analyzes cyber insurance as a cyber risk tool, the draw out the benefits and

problematic areas as well as the current cyber insurance market as on 2022. In the final section of literature review, different adoption methodologies and insurance purchase decision making studies are mentioned to validate the choosing of the methodology and the model.

After the literature review, the hypothesis and the model are discussed. In the pre adoption phase, to analyze factors affecting business level cyber insurance adoption as a risk management tool in digitalization for SMEs in Türkiye, the study uses the Technology-Organization-Environment framework extended with individual context considering the behavioral intentions of the managerial position. In the post cyber insurance adoption part of the model, the relationship with cyber insurance and cyber readiness, organizational performance, ISS and finally ICT adoption is measured.

This study aims to answer following research questions:

RQ1: What factors influence businesses to adopt cyber insurance as a cyber risk management tool in digitalization?

RQ2: How does cyber insurance effect cyber readiness in Turkish SMEs?

RQ3. How does cyber insurance effect adoption of information and communication technologies for Turkish SMEs?

CHAPTER 2

LITERATURE REVIEW

The literature research was conducted in order to understand the importance of the researched topic, the elements for the research question and analyze studies related to cyber insurance. We first started by looking at the current perspective of Turkish SMEs towards digitalization and cyber security. Then, the definition of cyber security, types of cyber attacks and cyber security measures were explained in order to capture the essence of cyber risk management. Later, cyber insurance was thoroughly analyzed with its coverages, benefits, problems and position in Turkish insurance market. Lastly, in order to decide on a methodology and a framework for the paper, technology adoption frameworks and previous research papers regarding cyber insurance were analyzed.

2.1 Digitalization

Throughout literature, digitalization, digitization and digital transformation are most commonly used to describe the use of information technologies for personal or business use. Digitization is most commonly referred as “the technical process of data conversion, generation, storage or processing”, digitalization is used to describe `the socio-technical phenomenon, the use of digital technologies and their influence” and finally digital transformation is described as “a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies” (Vial, 2019, p. 3; Frenzel, Muench, Bruckner, & Veit, 2021, p. 7). In this paper, the description for digitalization provided by Eling and Lehmann (2018, p. 359) as it embraces

elements from digitalization, digitization and digital transformation definition in turn allows us to extend the literature research: ‘‘The integration of the analogue and digital worlds with new technologies that enhance customer interaction, data availability and business processes.” (2018).

There are several aspects to measure level of digitalization. As seen on Table 1, Informatics Industry Association (TUBISAD) calculates countrywide digitalization of Türkiye using sixty-four indicators that is under four main categories which are environment, readiness, usage and impact (TUBISAD, 2021). Based on these categories and indicators, Türkiye as a country consistently improves its the digitalization score, moving upwards from 2,94 to 3,24 out of 5,00 in two years. Skills under readiness index and business and innovation environment under environment indexes are two of the lowest indexes (TUBISAD, 2021).

Table 1. Türkiye Digital Transformation Index

	2019	2020	2021
Turkish Digitalization Index	2.94	3,03	3,24
A. Environment	2.87	2.95	3.09
Political and regulatory environment	2.76	2.82	3.01
Business and innovation environment	2.98	3.09	3.17
B. Readiness	3.19	3.21	3.37
Infrastructure	2.34	3.27	3.32
Affordability	4.54	4.54	4.63
Skills	2.69	2.82	3.17
C. Usage	2.88	3.16	3.36
Individual usage	3.20	3.24	3.31
Business usage	2.77	3.32	3.41
Government usage	2.66	2.92	3.37
D. Impact	2.81	2.81	3.14
Economic impacts	2.36	2.05	2.25
Social impacts	3.26	3.58	4.03

[TUBISAD, 2021]

2.1.1 Digitalization of SMEs in Türkiye

SMEs are the hearth of Turkish economy; Table 2 shows that there are 3.6 million SMEs that constitutes %99.83 of all enterprises in Türkiye (Küçük ve Orta Ölçekli

Sanayi Geliştirme ve Destekleme İdaresi Başkanlığı [KOSGEB], 2021). Although SMEs significantly outnumber large enterprises, there is an imbalance of economic power between them. Even though SMEs constitute 99.83% of all businesses in Türkiye with 72.4% of total employment, in 2019 they were accounted for the 50% of the total yearly revenue, 44% of the total production value and 41% of total R&D investment out of all enterprises. The large enterprises on the other hand, responsible for as much as the total revenue of all SMEs combined albeit being only the 0.2% of all enterprises in Türkiye (Turkish Statistical Institute, 2020). The imbalance of economic value can be explained by the number of micro businesses with yearly revenue less than 5 million TL; they are 93,6% of all SMEs combined. In addition, large enterprises increase their business value by combining their extensive and significantly larger resources on acquiring new technologies with the ability to find talented employees to efficiently use them. SMEs fall short in terms of both available resources and talented personnel to create a digital strategy to increase sales and achieve efficiency (Yılmaz, 2021).

Table 2. Total Number of SMEs in Each Category in Türkiye

SME type	# of employees	Yearly revenue	Counted number of SMEs as of 2021	Percentage (in SMEs) as of 2021
Micro	<10	≤5 million TL	3.420.580	93,65 %
Small	<50	≤50 million TL	193.304	5,29 %
Medium	<250	≤250 million TL	32.585	0,89 %

[KOSGEB, 2021; KOSGEB, 2022].

As we use digitalization as an umbrella term to enhance customer interaction, data availability and business processes with digital tools and new technologies, we can categorize the different ways a SME can be called digitalized. According to

Table 3, the most frequent use for digitalization are digital marketing, e-commerce, business process programs and industry 4.0 tools (Turkish Statistical Institute 2021).

Table 3. Percentage Of Information Technologies (IT) Acquired By Smes And Large Enterprises

Category	Small businesses	Medium businesses	Large enterprises
Internet access	94.7%	98.0%	99.9%
Website ownership	45.1%	67.6%	91.4%
Social media account ownership	31.7%	45.6%	72.0%
e-sales through websites or EDI	11.6%	14.8%	27.0%
ERP software usage	23.7%	45.7%	74.9%
CRM software usage	9.3%	14.7%	33.6%
Paid cloud technologies usage	8.5%	19.5%	41.0%
Robot usage	3.7%	8.5%	23.7%

[Turkish Statistical Institute, 2021].

Website and social media ownership is considered as a stepping stone for digitalization. For many businesses the percentage of internet users in Türkiye has reached 82% out of the population in 2021 as it became the first point of contact with customers (We are social, 2022). Digital marketing can be defined as the usage of digital technologies to reach customers from new channels to fulfill customer needs, not limited to internet, mobile and social media marketing but also other household appliances and devices. Digital marketing is highly related to data analysis for deploying customer relationship management (CRM) campaigns, creating personalized experiences, and effectively targeting right customer at the right time (Sawicki, 2016). Thus ethically keeping customer data and ensuring its safety is a crucial aspect of digital marketing, which is ensured by national regulations.

With the increase of internet usage of individual consumers, especially since COVID pandemic, outreach in terms of sales became more crucial than ever; 13.6% of small businesses and 15.2% of medium sized businesses started or increased their e-sales activities in order to stay in market (Turkish Statistical Institute, 2021). The level of digitalization is in a basic level and there are some concerns among SMEs to shift their business models and strategies. However, benefits such as reaching a bigger customer base, having more options for purchasing, shortening transaction processes with secure payment options and creating a corporate image with a website motivates SMEs towards digitalization (Ayaydın, 2021).

Coined in the 1990s, ERP programs have been important for data management and resource planning. Successful ERP implementations can enhance supplier relationships, increase customer satisfaction, reduce inefficient spending, improve forecasts for sales and inventory and enable greater productivity (Rashid, Hossain, and Patrick, 2002). However due to difficulties in implementation and change management process, ERP adaption can be painful for companies, emphasized by the lack of IT employees and unfamiliarity with the product. Thus, it is even more challenging for SMEs to successfully implement ERP programs (Ekren, Erkollar, & Oberer, 2019).

Industry 4.0 is described as the introduction of connectivity among people, machines and products. This connectivity enables greater data generation, automatization and prediction. Digitalization with new technologies such as cloud computing and data storage, robotics and automation systems, Internet of Things (IoT), machine learning and artificial intelligence fall under the umbrella of industry 4.0 (Matt, Modrák & Zsifkovits, 2020). Industry 4.0 is a major direction towards digitalization for SMEs in Türkiye since manufacturing sector which is the third

biggest sector of SMEs in Türkiye (Turkish Statistical Institute, 2020). According to surveys made on the digitalization and industry 4.0, even though currently SMEs in Türkiye are in a foundation level of industry 4.0 readiness, managers understand the necessity of these systems and wish to achieve higher levels (Yiğitol, Güleş, & Sarı, 2020).

2.1.2 Digitalization and cyber security

The tools for digitalization are only the half of the story. To fully capitalize the digitalization potential of a business, it is necessary to support these tools with required ICT/IT talent which SMEs lack (Yiğitol et al., 2020; Yılmaz, 2021). The lack of talented ICT/IT employees are one of the main reasons that SMEs suffer from cyber-attacks. Due to lack of know-how provided by an IT security personnel, the necessary security measures are not taken in the case event of a cyber attack, thus it takes approximately 197 days to identify compromised data (Eş & Serdar, 2021). Even though the need for IT/ICT talent is supported with data, they are not viewed as critical employees for SME owners and managers. It is well documented in the literature that cyber security issues are not unknown for SMEs and their top level management, but they are taken less of a priority due to lack of awareness of the consequences (Alahmari & Duncan, 2020). In addition, SMEs faced economical difficulties during COVID pandemic even though COVID pandemic itself brought up digital requirements to stay in business. Because of these reasons, the percentage of IT/ICT talent SMEs employ among their other employees lowered in the past two years (Yılmaz, 2021). The lack of ICT/IT personnel shows that even though SMEs are aware of the need for digitalization, there is still a big gap between awareness and creating efficiency and staying in competition with digitalization as well as

protecting their information assets. In addition, the lack of quality IT personnel and cyber awareness creates vulnerabilities for digital SMEs; many of the technological improvements that fall under industry 4.0 such as IoT devices and cloud computing are also potential data breach points (Eş & Serdar, 2021). IT security issues and reliability of the systems are concerning for manufacturers that are considering adopting industry 4.0 (Aygün & Sati, 2022).

2.2 Cyber security and cyber risk for organizations

2.2.1 Cyber security

The International Telecommunications Union (ITU) defines cyber security as the of equipment or measures taken in terms of policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that is applied in order to safeguard the cyber environment and organization and user's assets (International Telecommunication Union [ITU], 2021). The assets mentioned include hardware such as computing devices, software such as infrastructure, applications, services, telecommunications systems, and the information about both the company and its users that is kept, used and transmitted in the cyber environment (ITU, 2021).

According to Samonas and Coss (2014) there are three objectives that are traditionally associated with cyber security known as the CIA triad: Confidentiality is compromised when the message in a transaction or data in a computer is read by and taken advantage of by an unauthorized person. This includes incidents when the information is not read but the transaction of the information is observed. Integrity is compromised when unwanted changes are made in a massage or transaction by an

unauthorized person, even if the information is not visible to the intruder. Availability is compromised when an event is prevented by an unwelcomed and unexpected intruder or an information is modified.

Although being the traditional base of cyber security, the CIA triad and the focus on technical and formal aspect of security have been criticized by academics for not being fit to modern organizations due the fact that it only considered the functional aspect of cyber security (Dhillon & Backhouse, 2001). Socio-technical models for cyber security have been introduced to the literature that still considers CIA triad but also adds some human and organizational aspects. Going beyond the CIA triad in terms of socio-technical approach, Technical Formal Informal (TFI) model was introduced by Dhillon (1995) which states that the organizational behavior and intentions of the individual members of the organization are critical systems that is highly effective for maintaining cyber security in an organization. As Berghel and Stundt put it, with the human perspective included, creating a cyber security system in a business started be known as a combination and coordination between technological aspects and managerial methods (as cited in Bozgeyik, 2018, p. 68).

The cyber security is considered as a serious issue for big corporations with enough economical power to invest in cybersecurity. As the size of the company gets bigger, the data it owns is shared with third parties due to operational and managerial purposes. This causes cyber risk management to be more difficult and as well as critical (Li & Liu, 2021). Being cyber ready increases organizational security performance which in turn influences financial and non-financial performances in a positive manner (Hasan et al, 2021). Organizations who are considered ready for cyber risks are aware of the cyber risks, are prepared for the outcome with a

comprehensive risk management plan and carry out with the plan (Hasan et al., 2021). Meanwhile Sharma, Singh, and Sharma (2009) state that the same attention level is nonexistent in SMEs, thus being connected to internet for external information and carrying out electronic transactions combined with the lack of awareness for cyber security issues make SMEs a target to cyber security attacks.

2.2.2 Cyber risk management

Risk is described as a function of the possibility of a threat to take advantage of potential vulnerability and the resulting impact (Refsdal, Solhaug, & Stolen, 2015; McShane Eling, & Nguyen, 2021). Handling cyber security issues with risk-based mindset have been overly discussed in the literature (McShane et al., 2021). There are three main steps in risk management which are risk assessment, risk mitigation and process evaluation (Stoneburner, Gougen, and Feringa, 2002). The main steps of risk assessment includes risk identification, risk analysis, evaluation of impacts and risk treatment (Stoneburner et al., 2002; Refsdal et al., 2015; McShane et al. 2021).

Identification of risk have primarily been in a reactive manner when an event, a vulnerability or an attack occurs and effects an asset negatively. In the past decade, some conceptual models have been proposed to identify cyber risks proactively (McShane et al., 2021). The key identifiers of a risk are the asset in question, possibility of an event to occur, the impact of the event, the vulnerability that causes the event and the source of the threat (Stoneburner et al., 2002; Refsdal et al., 2015).

Cyber risk are identified by the following nine steps: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendation and result documentation (Stoneburner et al., 2002). Threats for an IT system can be

sourced from external events such as natural disasters or environmental negligence that can harm hardware. On the other hand, cyber-attacks are executed by hackers, terrorists, competitive companies or insiders which makes them human sourced threats. Vulnerabilities are weaknesses in the security procedures, design, implementation or internal controls that threats can exploit. Automated vulnerability scanning tool, security test and evaluation and penetration testing are used to identify vulnerabilities. Controls are implemented to minimize the probability of a threat to occur. They can be technical (e.g. encryption methods, identification and authorization controls) or non-technical (e.g. procedures and policies) as well as preventative or detective. Impact analysis done by calculating the loss of integrity, availability or confidentiality of the information asset in the event of a threat exercised. Both tangible and intangible impact must be measured to correctly evaluate the impact. (Stoneburner et al., 2002). After risk identification, the risk is analyzed by assessing likelihood and consequences of a risk and evaluated whether the risk should be treated (Refsdal et al., 2015). The risk is determined by the function of likelihood of a threat, the impact of the threat and the controls to eliminate the threat (Stoneburner et al., 2002).

In the risk treatment phase, the goal is to treat the risk by prioritizing, evaluating, and implementing adequate controls. Four options for risk treatment are to reduce the risk, retention of the risk, avoid the risk and mitigate the risk. While considering risk treatment, the cost and benefit of the risk must be evaluated thoroughly (Refsdal et al., 2015). Risk is never fully eliminated unless in some cases function causing the risk can be removed such as not integrating third party applications. A cyber risk can be accepted and the IT processes can continue as business as usual. Then the controls can be implemented to lower the impact or

likelihood of threat to exercise a vulnerability. Lastly, the risk that cannot be eliminated or minimized can be transferred (Stoneburner et al., 2002). That is where the topic of cyber insurance comes in (Gordon, Loeb, and Sohail, 2003).

2.2.3 Types of cyber attacks

When an individual or an organization purposefully attempts to breach the information system of another individual or organization to compromise CIA triad or other components of cyber security, it is called cyber-attack (Cisco, 2021a). The threat identification step in cyber risk management aims to find whether the threat in question is one of the following (Refsdal et al., 2015).

Cyber attacks are categorized by the methods the attackers use:

- Malware attacks include malicious software attacks such as ransomware, viruses, spyware and worms. A malware attack can effect each and any component of CIA triad. For example, a virus can block availability of a system whereas spywares are made to compromise confidentiality of the system and deliberately leak information outside (Cisco, 2021b). Viruses need to be run by the administrator to spread whereas worms are autonomous systems. (Li & Liu, 2021). Trojan viruses were one of the most common cyber attacks in Türkiye in 2020 (Yalçın, 2021). In case of trojan horses and trojan viruses, malware attacks can be disguised as useful software until run by the administrator (Li & Liu, 2021).
- Social engineering is one of the most frequently used method for cyber attacks. In this method, attackers get sensitive information from their victims by using any information about their targets to form a relationship, exploit the

information and exit without leaving a trace to follow (Salahdine & Kaabouch, 2019). Phishing is another commonly known cyber attack in which the attacker sends fraudulent communications that appear authentic to gain sensitive information about an individual such as credit card information and social security number (Cisco, 2021c).

- Man-in-the-middle attacks also break CIA triad as in an attacker can insert themselves in a transaction without the knowledge of the two main parties of the same transaction. The attacker can receive the information passing through and/or interfere with the information (Cisco, 2021a).
- Distributed-denial-of-service (DDoS) attack exhausts the bandwidth of a system resulting in inability to fulfill legitimate requests such as replying to a customer request or connecting with a supplier (Cisco, 2021a). More than one third of the DDoS attacks last an hour, where as two thirds of the attacks lasts less than a full day. Fifteen percent of the attacks can last for a month (Cisco, 2021d).
- An SQL statement is used for retrieving information, administering database systems and operating functions. SQL injections can share information that would not have been shared if not for the malicious code or operate a function that was not intentional (Cisco, 2021a).
- DNS protocols are widely used in systems such as hotspot security controls. Attackers abuse DNS protocol to create non-DNS traffic over port 53. There are several methods of abuse DNS protocol, included but not limited to exploiting data using outbound DNS requests and bypassing network and authorization controls (Cisco, 2021e).

- Attackers find a system's vulnerability with exploit attacks to later abuse these exploits (Cisco, 2021f).

The most commonly faced cyber threats for SMEs are theft and fraud, copyright infringement, phishing and denial of service (Wekundah, 2015). In Türkiye, over 1.6 million attacks occurred in 2020, almost one third of those attacks are exploits and trojan horses which is a type of malware (Yalçın, 2021). The increasing number of cyber attacks on SMEs is a global phenomenon and is a result of lack of importance put on cyber security by SMEs (Alahmari & Duncan, 2020). There are many ways cyber security can be handled. Businesses can apply individual cyber security tools for their needs such as anti-virus tools and vulnerability testing to proactively identify systems vulnerability (Yalçın, 2021). There are also globally accepted methodologies for cyber security for general use or industry specific guidelines for specialized needs.

2.2.4 Globally accepted cyber security standards

Increasing number of breaches is recognized by many international, national, federal and industrial authorities. There are several standards for cyber security, either covering all industries or specified to an explicit industry. ISO/IEC 27000 family is the most common global standards for IS security management. ISO 27000 standards family identifies in detail methods and steps needed to be taken in order to provide information security (Bozgeyik, 2018). ISO 27001 classifies information security controls under fourteen titles each regarding people, process and technology (Irwin, 2020). In 2020, total number of ISO/IEC27001 certificates given was 180.491 , Türkiye ranked as thirteenth in number of ISO27001 certificates given with 881 certificates (ISO, 2020a).

Industries tend to have specific needs and security concerns, thus there are industry specific standards to abide. For example, fifteen technical security standards and programs prepared by Payment Card Industry Security Standards Council (PCI-SSC) are critical to any stakeholder in the payment process that provides transactions and withholds credit card information in their systems such as banks, merchants, vendors and solution providers (PCI Security Standards Council LLC ,2021). The PCI Data Security Standards (PCI-DSS) that merchants can follow to be safe and to be certified change based on the amount of transactions they have each year (Iyzico, 2016).

UL 2900 is another standard about cybersecurity, specialized in IoT technologies. FDA has recognized UL 2900 for medical devices which have been targeted for data breach for the last few years (UL, 2018). Even though external standards provide a guideline for cyber security, they cannot keep up with the technological advancements of the sector. Thus each business should protect themselves with the standards of their own country, industry and create internal standards (CGI Inc, 2019).

Lastly, even though businesses are getting more protective towards their ICT assets, attackers also evolve into new methodologies for breach. A common method observed is to aim for indirect contact such as vendors (Accenture, 2019). Therefore, businesses need to consider not only themselves but also the digital connections they make with their vendors and suppliers.

2.2.5 Cyber risk management measurements in Türkiye

Cyber risk has been a big concern for Türkiye especially in a military level since early 90's. In recent years, with the foundation of Turkish Data Protection Authority

and National Computer Emergency Response Center, private and public businesses are also required to follow a government regulated guideline to protect their cyber assets, focusing on personal data (Turkish Data Protection Authority, 2021).

Protection of personal data is regulated under the Law on Protection of Personal Data which was published in 2016. In order to protect the personalized data, educate the public on the importance of data security and execute necessary measurements to protect the personal data, Turkish Data Protection Authority was established under the same law. All public and private organizations are subjected to the principles of data processing stated in the Law on Protection of Personal Data: Processed personalized data must be accurate, data processing must be done lawfully, truthfully with legitimate and relevant purposes (Turkish Data Protection Authority, 2021). Failing to comply the law can result in monetary consequences. In 2021, the total number of monetary sanctions the Authority collected amounted to more than 31.7 million TL, 15.4 million TL coming from sanctions caused by misprocessing of personal data and 16.3 million TL coming from sanctions caused by notices made to the Authority (Turkish Data Protection Authority, 2022).

ISO 27001 is a legally required security standard for some sectors such as energy and communications. Energy production companies who attend in bidding processes, e-billing service providers, communications including landline, mobile and internet providers (Resmi Gazete, 2010; T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi, 2013). This requirement reflects on the total number of ISO27001 certifications in Türkiye; Table 4 shows that information technology firms have the more than 40% of all the ISO27001 certificates (International Standards Office [ISO], 2020b). Banking Regulation and Supervision Agency states that merchants and third party organizations that are involved with card transactions including

holding card information are required to comply with PCI-DSS standards (T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi, 2007).

Table 4. Number of ISO Certificates Given in Türkiye Based on Sector

Land/Sector	Number of certifications
Information technology	376
Sector unknown	104
Basic metal & fabricated metal products	63
Transport, storage and communication	60
Wholesale & retail trade, repairs of motor vehicles, motorcycles & personal & household goods	33
Electrical and optical equipment	31
Engineering services	27
Machinery and equipment	25
Rubber and plastic products	22
Electricity supply	21
Other Services	21
Textiles and textile products	14
Chemicals, chemical products & fibres	13
Food products, beverage and tobacco	9
Health and social work	9
Other transport equipment	8
Construction	8
Gas supply	7
Other social services	7
Recycling	6
Education	6
Non-metallic mineral products	4
Pulp, paper and paper products	2
Pharmaceuticals	2
Shipbuilding	2
Financial intermediation, real estate, renting	2
Manuf. of coke & refined petroleum products	1
Hotels and restaurants	1

[ISO, 2020b]

In 2013, National Computer Emergency Response Center (USOM) was founded within Information and Communication Technologies Authority with purpose to protect Türkiye's cyber security for critical public and private sectors. USOM accomplishes its purpose by specifying possible threats, taking necessary measures for reducing or eliminating the effect of possible attacks, informing individuals and organizations about the attacks, and urging practices of national and

international cyber security exercises to increase awareness (Ulusal Siber Olaylara Mudahale Merkezi [USOM], n.d.) One of the main functions of USOM is to coordinate back and forth communication between public organizations and sectoral Cyber Security Response Teams. These teams report information related to before, during and after cyber incidents to USOM and receive alerts and information before and during a cyber attack.

2.2.6 Cost of cyber security incidents

According to the global study conducted by IBM Security (2021), in 2021 total cost of data breach for a company was in average 4.24 million dollars, 1.07 million dollars higher for companies who adapted remote working due to COVID-19 pandemic. This number includes direct financial losses, disruption of business, the legal actions, the ransom asked for the data and the fines charged by authorities due to the leakage of customers' personal data, which is reportedly 80% of the data that is breached. According to the report, costliest attacks were business email compromise, phishing, and social engineering. In Türkiye, average cost of data breach rose from 1.91 million dollars from 1.77 in the previous year (IBM Security, 2021).

There are many exemplary cases showing even the most secure systems can face these attacks. In 2018, Marriott Hotel was attacked resulting in the exposure of personal data belonging to more than 500 million guests and in 2014, eBay had 145 million of its customers to change their login information, due to being hacked (Holmes, 2019). An attack in one of the most famous Turkish e-commerce sites, Yemeksepeti.com, effected more than 21 million users, resulting in fine of 3 million TL to Turkish Data Protection Authority (Kartal, 2021). As the study conducted by

IBM and examples of eBay and Yemeksepeti show, the biggest cost of cybercrime is the consequences that come from not protecting customer data (Holmes, 2019; IBM Security, 2021).

Cyber incidents that do not involve breach of information are also great risk for all size of businesses; the average cost of a DDoS attack is 120 thousand dollars for a small business whereas for a large corporation this can be as high as over two million dollars (Kapersky, 2018). Although the costliest attacks occur to large enterprises, 43% of business level cyber attacks happen to SMEs. They are easier targets for cyber criminals due to low protection on their intangible assets and the damage is more critical when an attack occurs considering that 75% of SMEs do not have cyber insurance. In average, if a SME was cyber attacked, they tend to be out of business in the next six months (Eş & Serdar, 2021). This is due to the fact that cyber incidents such as data breaches can take up to 200 days to identify and 75 days to contain (IBM Security, 2021).

2.3 Cyber insurance

By definition cyber insurance aims to cover the cost of recovery after a cyber-related security breach (Lindros & Tittel, 2016). It is used as a risk mitigation tool in the case of an unreduced remaining cyber risk (Gordon et al., 2003). There are two main categories of cyber insurance, targeting individual or business customer. These insurance types are different in terms of customers they serve, threats covered and costs claimed, retail cyber insurance and business cyber insurances need to be studied separately. Policies for retail customers and the main coverages offered in the Turkish insurance market will be identified briefly. The main focus of the literature

research is kept on the cyber insurance for business customers and their adoption in the market.

2.3.1 Cyber insurance for retail customers

Retail cyber insurance covers the results of cyber incidents happened to each individual customer. The biggest items of this type of insurance are financial compensation in the event of stolen data, access of the credit card information and false transactions. Insurance companies also offer legal consultancy in the event of stolen data or credit card information and cover the charges of the legal process (Woods, Agrafiotis, Nurse, & Creese, 2017).

Cyber insurance for retail customers is focused direct and indirect cost of cyber crimes, such as identity theft and fraud. Third party involvement involves the fees of legal consultants which are compensated directly to the victim. As these threats are identifiable in each customer and does not change for each individual, insurance policies for individual customers are more structured. Unless extra coverages are requested, insurers provide fixed price and claim to every customer. Detailed list of coverages offered in Turkish insurance market for cyber insurance for retail customers are:

- After incident - direct financial cost coverage
    - Losses related to identity theft
    - Losses related to payment systems fraud
    - Losses related to password theft
- After incident - indirect financial cost coverage
    - Harm done to online dignity
    - Online shopping fraud

    - Physical attack (for credit card theft)
    - Legal support
    - Solution consultancy
- Preventative measures:
    - Antivirus programs
    - Identity monitoring (Woods et al.,2017).

2.3.2 Cyber insurance for business customers

Cyber insurance for businesses covers losses effecting intangible and digital assets of a firm such as information assets (Herath & Herath, 2011). Cyber insurance for the business customers covers higher level of cyber security risks with higher and more complex financial outcomes. Unlike the case of retail customers, the policies require more detailed approach to each business. Thus, pricing and the coverages are most likely change for each business customer. The business type of cyber insurance covers first party and third party losses (Lindros & Tittel, 2016).

The first party costs include but not limited to the following:

- Recovery cost from a cyber attack
- Investigation of the cybercrime,
- Data recovery,
- Loss of income due to unavailability,
- Cost of dealing with hackers,
- Loss of trust towards the company (Lindros & Tittel, 2016)

Third party costs mean the fees the insured company is required to pay due to a fine, such as charges they may face by not abiding to the legal requirements (Lindros & Tittel, 2016).

2.3.3 Cyber insurance coverage for business customers in Türkiye

At the time this research was conducted, there were four companies that offer cyber insurance for businesses in Türkiye; Anadolu Sigorta, Ak Sigorta, Allianz, Doğa Sigorta. Amongst the most popular insurance companies in Türkiye, Table 5 puts the benefits in perspective (Anadolu Sigorta, 2022; Ak Sigorta, 2022; Allianz, 2014; Doğa Sigorta, 2022). According to the information provided by the company guidelines, cyber insurance policy come with prerequisite for customers to follow (Anadolu Sigorta, 2022; Ak Sigorta, 2018; Allianz, 2014; Doğa Sigorta, 2022). An example of Doga Sigorta (2021) can be given as to what these requirements are;

- The insured company must back-up its critical data once a week
- Necessary anti-virus software must be installed and updated regularly
- The safety of computing systems should be protected with regularly changing passwords, software patches, firewalls and system upgrades.
- Computing systems must be accessible to only authorized personnel
- Cloud computing must be accessible through a secure VPN
- Security logins must be in place for critical IT systems
- If applicable the insured company must follow necessary regulations
- The insured company must educate their employees about cyber security
- The insured company must have a documented incident response plan the includes IT recovery and business continuity

Cyber incidents create regulatory consequences for companies. One of the biggest examples of that is the Law Under Protection of Personal Data; there are rules and guidelines which each company must comply with under the Turkish Data Protection Authority and renege to these rules and guidelines are fined by the company accordingly (Turkish Data Protection Authority, 2021). As seen in Table 5, cyber insurance companies in Türkiye include anti-virus protection and consultancy against cyber risk in their policies as well as cover a portion of the legal fines issued by Turkish Data Protection Authority (Anadolu Sigorta, 2022; Ak Sigorta, 2022; Allianz, 2014, Doğa Sigorta, 2022).

As a company gravitate towards being fully digital, the dependence on the technology increases and the availability of technology becomes critical to conduct daily processes. If a cyber attack that prevents availability of services and processes that connect customers to businesses or supplier and third parties, companies would not be able to serve their customer unless they still have offline options, which are most likely to be more costly than online processes (Bandyopadhyay, 2012). Many cyber insurance policies cover the downtime cost in the event of a cyber attack (Anadolu Sigorta, 2022; Ak Sigorta, 2022; Allianz, 2014, Doğa Sigorta, 2022).

The role of cyber insurance is not limited to financial claims and covering losses. Cyber insurance is also beneficial for reducing the risk of the cybersecurity breach. Lloyd (2018) explains this in his research; as a business model, insurance companies take calculated risks, they would create better policies for the firms with better security measures. They prioritize a customer that is already aware of the risk factors and up to date with necessary measures. If a potential customer does not have the necessary measure taken, the insurance companies either impose these measures, change the coverage of the policy or do not insure the said customer. Therefore,

cyber insurance works best for companies that is aware of the risks and protects their infrastructure accordingly. This creates a win-win situation for both sides. For the insurance company side, the probability of an attack decreases if the customer is already protected. For customer side, since they got better protection the probability of loss is reduced. Even if an event occurs, they are covered by their cyber insurance.

Table 5. Coverages of Cyber Insurance Policies in Türkiye

Companies/ Coverages	Anadolu Sigorta	Ak Sigorta	Allianz Sigorta	Doga Sigorta
Data damage coverage	✓	✓ (additional)	✓	✓
Business downtime cost	✓	✓ (additional)		✓
Legal charges (KVKK)	✓	✓	✓	✓
Ransom demanded from the hackers	✓	✓		✓
Blackmail cost				✓
Customers demands from the insurer due to data security negligence costs	✓	✓	✓	✓
Investigation of the cybercrime		✓		✓
PR support		✓		✓
Identity theft		✓		✓
Reconstruction cost		✓		
Network and hardware defection costs		✓		
PCI-DSS neglegtion cost and recertification		✓ (additional)		
Online media responsibility costs		✓ (additional)		✓
Legal support charges	✓	✓	✓	✓

[Anadolu Sigorta, 2022; Ak Sigorta, 2022; Allianz, 2014; Doğa Sigorta, 2022].

From data storage to transactions, every single operation that is controlled by elements of information systems are vulnerable to breach. This can mean a great loss, as mentioned earlier. In 2017, 10 % of organizations in UK had to change their entire operations due to security events (Low, 2017). Many academics and industry specialists view cyber insurance a risk management tool in a financial level, as in to decrease the monetary losses to a minimum while supporting the existing cyber

security measures. (Gordon et al., 2003; Öğüt, Menon, & Raghunathan, 2005). Even if companies have already advanced cyber security measures, cyber security environment is ever evolving and vulnerable to new type of cyber risks. Thus it would be less cost effective to implement more technical cyber security such as additional firewalls or software, then to diverse the cyber risk into a financial instrument such as cyber insurance (Bandyopadhyay, 2012).

2.3.4 Problem Areas of Cyber Insurance

As with all services, there are several issues regarding cyber insurance that prevents it from reaching its full potential as a common cyber security risk management tool and a common insurance product for insurers. Biener et al. (2015) looked at cyber insurance through Berliner framework of insurability and deducted that although cyber risks are insurable, cyber insurance remains problematic. There are many researches done, including Biener et al. (2015), that exemplifies the problems with cyber insurance. These problems, although related to each other, can be identified as the immaturity of insurance market, the correlation of cyber security risks, and the moral hazard of cyber insurance.

In the center of the problems cyber insurance face, the lack data due to immaturity of cyber insurance market and lack of know-how for insurers come first (Anderson & Moore, 2006, Biener et al, 2018). Low number of insurers and low awareness of businesses for cyber insurance limits the availability of the product to expand the market. Since the product is not expanded to the market, the volume of the data necessary to correctly identify risk has not been reached. Maturity of cyber insurance means there will be more data to correctly calculate the core aspects of cyber insurance such as premium pricing and risk management, resulting in

increased coverage and market expansion (Biener et al., 2015). Until then, low volume and liquidity for insurers enforces them to high premiums that in return lowers the demand for cyber insurance (Anderson & Moore, 2006). There are several researches done and methods suggested in an academic level that hackles the issue of pricing of premiums for cyber insurance (Herath & Herath, 2011; Xu & Hua, 2019; Wang, 2019)

The immaturity of cyber insurance market and the lack of data for cyber insurance has caused the researches for the subject to be more in line with qualitative attributes. According to the research done by Dambra, Bilge and Balzarotti (2020), unlike other insurance policies, the risk assessment of cyber insurance and the applicability to the real-world cases is mostly done following a qualitative approach based on expert opinions. Even though cyber insurance has been around for more than a decade, quantitative approaches such as cyber risk measurement of potential cyber insurance buyers and investment calculation based on risk averseness of said buyers is relatively new (Dambra et al., 2020; Uuganbayar, Yautsiukhin, Martinelli, & Massacci, 2021).

Study done by Baer and Parkinson (2007) related to cyber insurance is often cited in many researches about the subject. The remark they made about the nature of cyber security risks to be correlated and interdependent is still valid today. In the literature, the correlation of risks is divided into two sections. First off, a vulnerability in a system can affect multiple firms that are using the same system, which is called global risk correlation. The second section for correlation comes is internal correlation, which is when a vulnerability in a system can effect another system a business uses (Böhme & Kataria, 2006). An example to the global and internal correlation can be given as in Table 6.

Concurrent attacks are particularly tricky for cyber insurers to include in the policy conditions, which is why it can be excluded in cyber insurance policies. According to Baer and Parkinson (2007), this nature of cyber insurance differentiates it from traditional policy types and makes it difficult to standardize a formulation for pricing. Böhme and Kataria (2006) concluded that cyber insurance market can exist when cyber risk is subjected to high internal correlation among firms and there is low global correlation of cyber risk between different firms. If there is low internal correlation of cyber risk in a company, then that said company will not need insurance since they already managed their risk, unless they show extreme levels of risk-averseness. On the other hand, the existence of high global correlation in cyber risks will lead lower supply for cyber insurance.

Table 6. Explanations and Examples of Global and Internal Correlations of Cyber Risk

		Global Correlation	
		Low	High
Internal correlation	Low	Does not affect all internal systems or other businesses. For example: Hardware failure	Does not affect all internal systems but can be seen in other businesses. For external: Phishing
	High	Effects internal systems in the business but not the other businesses Example: Insider attack	Effects both the internal system in the business and other businesses. For example: Viruses

[Böhme & Kataria, 2006]

Need for cyber insurance and awareness of cyber security has an intriguing relationship best identified by Baer and Parkinson (2007); customers with higher risk of a loss will find cyber insurance more appealing than customers with lower chance of a loss. If a customer is aware of the risk, repeatedly assesses the vulnerability of their systems and effectively protect their intangible assets, they will have lower premiums (Wang, 2019). However, this creates a paradox; lower premiums that

come from lower cyber risk may discourage a company with strong protection on its cyber assets to purchase cyber insurance. Öğüt et al. (2005). points out that once the availability of cyber insurance occurs, it is more likely that the business will choose cyber insurance and lower the self-protective investments. The fact that cyber insurance creates a moral hazard led to many academic researches defining incentive based cyber insurance models aiming to find companies who invest in self-protection to also invest in cyber insurance (Dou, Tang, Wu, Qi, Xu, Zhang, & Hu, 2020).

Biener et al. (2015) states that cyber insurance and self-protection can be complementary to one another; in order to reduce the risk, they are taking with the unpredictability of cyber insurance, insurance firms asses the cyber risk of a business before constructing the condition of a cyber insurance policy. Therefore, even though the paradox of moral hazard seems to create an illusion that cyber insurance and self-protection from cyber risks are interchangeable, they actually feed and aid each other in terms of risk elimination and risk diversification.

2.4 Measuring insurance acceptance

The researches aimed to evaluate the demand and acceptance of insurance tends to focus on the purchasing decision. There are several points of view for analyzing decision to purchase an insurance policy; individual's risk perception and the amount of loss is the base point of the literature in this area (Slovic, Fischhoff, Lichtenstein, Corrigan, & Combs, 1977; Laury, McInnes, & Swarthout, 2008). However, distortions in risk perception may result in irrational decision making in purchase decision; such as paying premiums that are more than necessary for flight insurance (Johnson, Hershey, Meszaros, & Kunreuther, 1993). Purchasing decision can also be formulated using willingness to pay and utility functions (Wang et al, 2012; Showers

& Shotick,1994). These studies indicate that the purchasing decision depends on the consumer's behavior, risk averseness and the monetary costs.

There are three points to consider when we evaluate these types of studies. These studies focus on initial purchasing decision, as in whether a consumer is willing to take the risk of a financial loss considering the probability of the risk. However, cyber insurance does not only cover losses in the case of an event, but also provides protective services to the insured, conducts due diligence to the insured company's current systems which points out potential vulnerability spots and creates prerequisite that the insured must oblige before purchasing or renewing the policy (Gordon et al., 2003; Öğüt et al., 2005). Thus, even though the purchasing decision can be dependent on the risk perception of the consumer, insurance can also function as a risk management tool and a technological innovation.

Second point to consider is that to our knowledge, these studies are aimed at individual level of insurance such as flight of disaster insurance. The decision to accept cyber insurance is dependent on an individual, but the cost of the purchasing decision and the decision itself affects a business. The last point of consideration is that to our knowledge, these studies does not include cyber insurance, which is relatively new to the insurance market and not matured yet.

2.5 Frameworks for technology adoption

There have been a variety of frameworks in the literature to study technology adoption, including but not limited to Diffusion of Innovation Theory (DOI), Perceived Characteristics of Innovation (PCI), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Technology Acceptance Model (TAM), Technology – Organization- Environment (TOE) Model and the Unified Theory of

Acceptance and Use of Technology (UTAUT) model (Awa, Ukoha, & Igwe, 2017; Hameed & Arachchilage, 2017). DOI and TAM focuses on the perceived characteristics of an innovation whereas TPB and UTAUT emphasizes behavior; either way these frameworks have been used widely in the literature mainly focusing on individual adoption of technologies rather than business adoption (Hameed & Arachchilage, 2017). TOE on the other hand, have been used heavily for organizational approach to technology adoption (Wen and Chen, 2010; Lane and Marie,2010; Awa et al. 2017). One drawback of TOE framework is the lack of individual context of the decision maker, thus there are many studies that extends the TOE framework with factors from TAM, TBP, DOI and UTAUT frameworks (Thong, 1999; Rosli, Yeow, & Siew, 2012; Hameed & Arachchilage, 2017; Awa et al. 2017; AlBar & Hoque, 2019)

2.5.1 TOE framework

TOE framework looks at technology adoption from an organizational point of view and bases technology adoption above three main contexts which are technology, organizational and environmental (Baker, 2012). In the broadest definition, technological context includes existing technology in a firm, available technologies outside of the firm and the characteristics of technological innovation to be adopted (Tornatzky & Fleischer, 1990). Firms need to evaluate both its existing technology and the new technology to be adopted, as the size of the change to be made depends on both (Baker, 2012). Organizational context includes the innerworkings of a firm such as decision making structure, organizational strategy, size of the organization, communication process, and employee relations (Baker, 2012). Environmental context considers external elements to technology adoption. This definition includes

industrial aspects such as state of technological advancements in the industry and competition, as well as regulatory inputs such as governmental safety measures (Baker,2012).

2.5.2 Extended TOE frameworks with individual context

In recent studies, the TOE framework is found to be limited to firm level contexts. For technology context, the characteristics of the existing IT structure of the firm and the new technology to be adopted are considered whereas for the organizational structure and size and macro environmental influences such as governmental regulations are explained. The decision maker's perspective and concerns when deciding to adopt and use the technology is disregarded in TOE framework; thus the TOE framework is often extended by adding individual context with factors coming from TAM, TBP, DOI and UTAUT frameworks (Thong, 1999; Venkatesh, Moris, Davis, & Davis., 2003; Rosli et al., 2012; Hameed and Arachchilage, 2017; Awa et al. 2017; AlBar & Hoque, 2019).

Models extend TOE with individual context state that subjective factors such as technology, organization and environmental influence are not the only features that influence a firm's acceptance of technology, but also the decision maker's intention to use the technology affects the firm's intention to use the technology, thus merging individual intention and firm's intention with TOE framework (Rosli et al., 2012; Awa et al. 2017). According to TAM, TBP and UTAUT frameworks, individual's intention to accept the technology are dependent to performance expectancy, effort expectancy, social influence and facilitating surroundings (Venkatesh et al., 2003).

Another perspective of individual context focuses on the affiliation of the CEO with technology and defined the CEO characteristics context with CEO's innovativeness and CEO's IS knowledge; Innovative, risk taker and IS savvy CEOs of small businesses are more likely to adopt IS as there is a financial investment required. (Thong,1999). CEO's support in innovation adoption and the general knowledge of ICT positively effects technological innovation adoption (AlBar & Hoque, 2019).

2.5.3 Adaption of TOE for cyber decisions and cyber insurance studies

The dynamic nature of cyber security makes relative advantage, compatibility, and trialability difficult to assess for regular cyber security tools (Avina, Bogner, Carter, Friedman, Gordon, Haney, & Wolf , 2017). Wallace et al. (2020) covered the constructs under TOE framework under higher focus on cyber security. For example, IT standards are added to environmental context in addition to governmental regulations. Wallace et al. (2020) also tailored the TOE framework to fit cyber security by adding cyber catalysts, practice standards- two dimensions specific to cyber security issues that are not covered by any of the technology, organization or environment contexts.

Hearth et al. (2020), created an integrative model from DOI and TOE frameworks to study the constructs effecting information security system adoption. Complexity, compatibility and perceived gain are three of the five main characteristics according to the DOI framework which are included in the technology context of Hearth et al. (2020)' s integrative model.

At the time being, to the knowledge of the author of this research paper, there are only two studies focused on cyber insurance from TOE framework.

Bandyopadhyay (2012) specialized the contexts of TOE for cyber insurance; in the study the technology context was labeled as organization's technology, the organizational context was labeled as organization's risk management and environment context was labeled as organization's environment. Under these labels, Bandyopadhyay (2012) created total of nine hypotheses for adoption of cyber insurance for businesses. Technology influences included firm's existing technological structure in the means of technology competence, control intensity and technology dependence. Organization perspective was narrowed down to risk management context, stating that risk management, organizational risk profile and communication between departments about risk management influences firm's decision to utilize cyber insurance. Finally, the regulatory needs for information protection, the level of competition and value of corporate data and the information security communities create the environmental context.

Mbatha (2020) referenced Bandyopadhyay's work to create three propositions, one for each context of the TOE framework. The research was aimed to adopt the TOE framework for cyber insurance adoption in South African market. From the technology context Mbatha (2020) proposed that if in South Africa enterprises are aware of effective cybersecurity technology controls as well as having cyber insurance, the impact of cyber-attacks would be reduced. From the organizational context Mbatha (2020) proposed that cyber risk management is supported if cyber risk is discussed in an organizational level. Finally, from the environmental context Mbatha (2020) proposed that governmental and industrial obligations to follow certain cyber security tools pushed organizations to adopt cyber insurance.

2.6 Results of literature review

In order to understand if cyber insurance can be a risk management tool for SMEs in digitalization, we looked at the gap for digitalization in Türkiye for SMEs. The number one gap for SMEs in the road for digitalization is the lack of human resources for the ICT tools they adopt. The lack of qualified IT personnel and the increased amount of integration and data exchange lead to cyber risk. This is evident by the targeting of SMEs for cyber crime in Türkiye.

In terms of risk management, cyber security tools and measures are used to decrease the risk of a cyber incident. However, cyber attack tools develop overtime and existing cyber security tools may not be as effective in the future. The undealt remaining risk needs to be delegated using financial tools, thus the necessity for cyber insurance arises.

We looked at how cyber insurance can help companies to mitigate the cyber risks they take by looking at the benefits and problems of cyber insurance. We found out that all cyber insurance options cover downtime in case of cyber breach, regulatory fines and legal fees as well as offer some level of cyber security protection to their customers. Some options also cover ransomware and industry specified regulation fines. We also found that cyber insurance has several key problems that keeps the cyber insurance market from maturing. Nevertheless, the market is growing and the literature about the subject is expanding.

Finally, we looked at existing studies that measured decision making of insurance and technology adoption. Decision to adopt insurance is typically measured with willingness to pay and utility functions. These measurements centers around price of insurance and it’s utility for a company. It does not provide an explanation for the effects of external and internal factors for adopting cyber

insurance for cyber risk mitigation. However, these researches showed us that individual perspective is effective when purchasing insurance, even when it is for an organization. We looked in studies that focused on cyber insurance adoption. The studies we found both studied cyber insurance adoption with TOE framework. The aforementioned sections of our literature research, the technological, organizational and environmental contexts, also led us to believe that TOE framework would fit to look at business levels of influences.

TOE framework is widely used in studies because it can be interpreted to fit multiple sectors and technologies by changing the constructs in each context. For cyber decisions and cyber insurance studies the TOE is the primary framework. Studies conducted for other industries and technological innovations added individual context based on behavioral components from DOI and UTAUT frameworks. However to our knowledge, cyber insurance is a field that has not been researched yet using extended TOE frameworks nor to a quantitative survey was conducted to research cyber insurance adoption in a mass scale.

CHAPTER 3

FRAMEWORK AND HYPOTHESES

As seen in the literature review, the topics of ISS and cyber security technology adoption have been studied under the technology-organization-environment context (Herath, Herath & D'arcy, 2020; Hasan et al., 2021). Individual perspective is added to these studies based on the literature focused on SMEs due to the fact that the main decision maker is often the CEO or the owner (Thong, 1999). The combination of requirements and policy coverage makes cyber insurance a cyber risk management tool: The prerequisites to be fulfilled such as surveillance tools are used for risk identification, secure password policies and anti-virus tools are useful for risk elimination and finally in case of an event the policy coverage provides risk mitigation. The effects of adoption of cyber security technology to the business is also often studied following post adoption. Cyber insurance policies offer lower premiums to the businesses that follow effective cyber security policies, therefore the effects of adoption of cyber insurance is relevant after the purchase. Thus our conceptualization for pre and post cyber insurance adoption is in the likeness of other ISS and cyber security technologies.

Table 7. The Definition of Constructs

Context	Construct	Definition	Field of referenced study	Referenced Study
Technology	Perceived gain	The expected financial and non financial gain from adopting the cyber insurance	ISS	Herath et al. (2020)
	Complexity	The difficulty of adopting cyber insurance due to the prerequisites of the policy	ICT	AlBar & Hoque (2019)
	Perceived observability	The ability to realize the benefits of adopting cyber insurance from others	Smart contracts	Badi, Ochieng, Nasaj, & Papadaki (2021).
Organizational	Top management support	The emphasis and support of top management to adopt cyber insurance and the prerequisites that comes with	Cyber insurance, ICT, Cyber security	Bandyopadhyay (2012), AlBar & Hoque (2019), Hasan et al. (2021)
	Organizational culture	The collaboration, communication and centralization of risk management in the organization		
Environmental	Competitive environment	The nature of the industry the company is in	Cyber insurance, ICT	Bandyopadhyay (2012), AlBar & Hoque (2019)
	External pressures	The regulatory obligations, supplier requirements and customer demands that the company must follow	ISS, Cyber insurance Cyber security	Herath et al. (2020), Mbatha (2020), Hasan et al. (2021)
Individual	Owner/manager innovativeness	The characteristic of owner/manager to innovative technologies	ICT	Thong (1999), AlBar & Hoque (2019)
	Owner/manager knowledge	The level of knowledge of the owner/manager on cyber insurance and cyber security		
Adoption	Behavioral intention	The mindful and aware behavior of a person in future events.	NFC technology	Khalilzadeh, Öztürk, & Bilgihan, 2017
Post adoption	Cyber readiness	Organization's awareness and preparedness of possible cyber attacks	Cyber security	Hasan et al. (2021)
	Organizational security performance	Benefits of keeping a secure system against a cyber attack	Cyber security	Hasan et al. (2021)
	ICT Adoption intention	The willingness to adopt ICT tools	ICT	AlBar & Hoque (2019)

3.1 Technology context

Relative advantage has long been considered one of the influences on technology adoption, as it had been part of one of the most referenced frameworks in the literature, diffusion of innovation (DOI) framework by Rogers (1995). Herath et al. (2020) stated that unlike in traditional innovation characteristics of DOI, relative advantage for security innovation does not translate into cost reduction or revenue increase. Instead, it reflects as increase in security that results in lower chance of cyber incidents and thus higher market share and profitability due to decreased cyber costs. With this insight they argued that the perceived gain coming from adopting information security technologies positively affects adoption of said technologies. Even though cyber security measures cover the risk elimination and risk minimization phases of risk management, there is still a leftover risk that is either disregarded of insured. Cyber insurance is considered as a cyber risk mitigation tool, thus the adoption of it is considered a technological innovation.

In order to have a cyber insurance policy, companies need to adopt other IS security technologies. First the company needs to successfully implement the prerequisites required by the insurance firms, i.e. the potential weaknesses are sorted, necessary tools are implemented and policies are adopted throughout a company. Once the company implements the prerequisites, cyber insurance policies cover basic leftover risks that cannot be eliminated by the necessary security measures such as cost of fraudulent events. In summation, adopting cyber insurance first requires eliminating and minimizing cyber risk with cyber security tools, then the cyber insurance itself covers direct and third party costs. If adopted, cyber insurance adds to the already existing IS security gains.

In addition to cyber gains, businesses are obligated to protect their customers' data by Turkish Data Protection Authority and inform their customers' about their data usage and protection policies. In case of a dispute against Turkish Data Protection Authority or an attack aimed to disrupt confidentiality of IT systems and transfer customer data outside of the company, the reputation of the business is expected to be affected, worse if the company cannot pay the fine in case of legal requisites occur. Cyber insurance resolves any dispute and covers charges so the insured business is not financially harmed. Therefore we can hypothesize that perceived gains from cyber insurance will have a direct positive effect with cyber insurance adoption within Turkish SMEs (H1).

Combination of ease in adopting a technology, understanding the technology and using the technology turns into complexity, a key construct in technology adoption (Venkatesh et al, 2003). Easy to understand and easy to implement technologies are more likely to be adopted by SMEs (AlBar & Hoque, 2019). Cyber insurance on the other hand is known to be a complex policy type; especially the pricing policies and the coverage of the policies can be misunderstood by the customers (Dambra et al., 2020; Uuganbayar et al., 2021). In addition, insurance companies add prerequisites to their policies in order to reduce their own risk. These prerequisites vary from adopting cyber security tools to implementing companywide policies and regularly training staff to increase awareness (Anadolu Sigorta, 2022; Ak Sigorta, 2018; Allianz, 2014, Doğa Sigorta, 2022). Adopting cyber insurance does not only mean to purchase an insurance, but it also requires IT talent to understand necessary cyber security tools and cultural awareness on security. SMEs in Türkiye generally lack both the IT talent and cyber awareness (Eş & Serdar,

2021). It can be hypothesized that complexity will have a direct and negative effect on the adoption of cyber insurance within Turkish SMEs (H2).

It is often suggested that if people have positive reaction to a new technology, it will increase the chances of being adopted by others (Badi et al., 2021). Rogers (1995) called this observability claimed that due to the fact that preventative innovations are less observant, their adoption is slower. Insurance sector also suffers from observability problem. The whole basis of the sector, as can be seen from the cyber insurance example, is to insure against the risk of a rare and negative event. If a customer protects themselves against that said risk, they may prefer not to insure themselves against any leftover risk even though they have a higher chance of getting lower premiums (Baer & Parkinson, 2007; Wang, 2019). On the other hand, customers still may not choose to adopt insurance even without existing self protection because simply they do not observe the risk or take the risk seriously. The disaster policies are a good example of the effects of observability of insurance in adoption; people purchase more policies after the disaster occur and likewise, they give up the insurance after years of not experiencing a disaster (Buzatu, 2013). Keeping in mind that cyber insurance is not yet a mature market, it can be said that cyber insurance adoption will benefit from observability. It can be suggested that perceived observability will have a direct and positive effect cyber insurance adoption within Turkish SMEs (H3).

3.2 Organizational context

Support of top management has been considered to have strong and positive influence on ICT and new technology adoption by numerous studies, especially when in the case of SMEs, the decision maker of a technology adoption would be

very likely to be in top management (AlBar & Hoque, 2019). According to Hasan et al. (2021), the top management support for adopting cyber security tools emphasizes the importance of cyber security for the company which reflects upon the employees' behavior. This results in successful adoption of cyber security policies and tools and thus makes organization ready for cyber attacks. Thus, it can be hypothesized that top management support will have a direct and positive effect on the adoption of cyber insurance within Turkish SMEs (H4).

Open communication and organizational culture have been considered to have a positive impact on technology adoption (AlBar & Hoque, 2019). Cyber insurance is as much as a cyber risk management tool as it is a financial tool, since it is multidisciplinary, it is important to keep the communication open between all related parties (Hasan et al., 2021). According to Bandyopadhyay (2012), businesses that have a central risk management system with multiple managers decide on the risk related issues, such as whether cyber insurance is an adequate risk mitigation tool, are more likely to adopt cyber insurance. It can be suggested that the organizational culture will have a direct and positive effect on the adoption of cyber insurance within Turkish SMEs (H5).

3.3 Environmental context

Competitive advantage has long been considered as an important factor affecting technology adoption in businesses (AlBar & Hoque, 2019). As the business strategies become heavily dependent on digitalization, the assets of the companies and their business processes shift towards intangible assets and electronic processes. The technology dependence that are caused by these intangible assets and digital processes can give different results for companies in different industries and markets.

Breach of customer data may have more impact if the market has two big players or cyber-attacks that interjects availability of a company may cause more harm to a company that serve end user directly if the customer reviews are critical in the industry (Bandyopadhyay, 2012). It can be hypothesized that a competitive environment will have a direct and positive effect on the adoption of cyber insurance within Turkish SMEs (H6).

Herath and Herath (2011) state that both horizontal and vertical business partners consider the safety measures taken by a business to work in alliance. Cyber attacks such as viruses are both globally and internally correlated in high levels which means not only they affect internal systems of a company, they also very likely to make an impact to third parties and business partners (Böhme & Kataria, 2006). Therefore, it can be considered that in an environment where the businesses are connected through digital systems and software, when choosing a business partner, companies may be influenced by the information security strategy of their potential partners among other candidates.

In addition to the business partners, there are obligatory requirements to follow when implementing information systems. One of the biggest examples of that is the Law Under Protection of Personal Data; any breach of data must be reported to Turkish Data Protection Authority which in turn may fine the company accordingly (Turkish Data Protection Authority, 2022). According to study conducted by Hasan et al. (2021), the regulatory environment plays a significant role in the organizational readiness for a cyber incident due to monetary fines in case of violation or regulation. These regulations are in place for protecting customer data. Customers have a right to address to the necessary authorities if a company is unable to comply with these regulations.

Cyber insurance companies in Türkiye include anti-virus protection and consultancy against cyber risk in their policies as well as cover a portion of the legal fines issued by Turkish Data Protection Authority (Anadolu Sigorta, 2022; Ak Sigorta, 2018; Allianz, 2014, Doğa Sigorta, 2022). In addition, as a part of the cyber insurance eligibility, insurance companies issue due diligence on their customers to see if they took the necessary measurements themselves (Biener et al., 2015). Through these measures the cyber insurance takes role as a risk identification and risk elimination. Mbatha (2020) states that the benefits of cyber insurance against the external pressures of regulatory obligations is positively related to the adoption of cyber insurance. It can be suggested that external pressures will have a direct and positive effect on cyber insurance adoption in Turkish SMEs (H7).

3.4 Individual context

The decision-making mechanism for SMEs for any subject is affected by the owner's own beliefs, knowledge and behavior which typically is the main decision-maker (Thong, 1999). Insurance purchase and adoption decision is also heavily influenced by the decision-maker's approach to risk (Slovic et al., 1977; Laury et al. 2008). Thus, when looking at the adoption of cyber insurance for SMEs, firm level context is not sufficient, and the individual context is required. The workforce consisting of ICT/IT talent is less than 10% for small businesses and less than 27 % for medium size businesses, thus it is safe to assume that the innovative decision making is heavily done by the central decision maker (Yılmaz, 2021). For SMEs, the proposal for a purchase comes from relative department, such as purchasing or finance, although the decision maker is often the owner-manager or CEO (Thong, 1999; AlBar & Hoque 2019). This is also true for the information and cyber security

decision making (Alahmari & Duncan, 2020). It can be said that the characteristics of SMEs and the knowledge upon the subject of innovation positively effects the adoption of innovation (Thong, 1999; AlBar & Hoque 2019). Therefore it can be hypothesized that owner/manager innovativeness (H8) and cyber insurance knowledge (H9) will have a direct and positive effect on the adoption of cyber insurance within Turkish SMEs.

3.5 Post cyber insurance adoption

For a company to acquire cyber security insurance, having an existing IT and cyber security infrastructure is required. In addition, variety of cyber security tools can be provided by the insurance company based on the policy coverage. If they already have cyber insurance and intend to renew their policy, this means that they are ready to protect themselves in case of a cyber event. If they have not adopted cyber insurance but have intentions of adopting or have adopted cyber insurance, they must be committed to have necessary IT infrastructure to protect themselves (Lloyd, 2018). It can be said that adoption of cyber insurance would effect the cyber readiness of an organization in a positive way for Turkish SMEs (H10).

Organizational security performance consists of system protection and combat capabilities as well as database availability (Hasan et al. 2021). According to Hasan et al. (2021), even if IT infrastructure and cyber security tools cannot prevent cyber attacks %100 of a time, they still lower the impact of an attack on the company's systems and databases. They claim that cyber security readiness positively effects organizational security performance. Therefore, it can be hypothesized that cyber readiness of an organization would affect the organizational security performance in a positive way for Turkish SMEs (H11).

Digitalization comes with cyber vulnerabilities which can be considered a barrier for digital transformation. Studies suggest that although not as critical as lack of resources, the concern for cyber security is amongst barriers against industry 4.0 transformation for SMEs (Gergin et al., 2018; Aygün and Sati, 2022). Since digitalization is a data-based management model, privacy of business and customer data must be top priority to prevent customer dissatisfaction and legal fees which can be a concern for SMEs upon adopting new technologies (Ulaş, 2019). Thus it can be said that cyber readiness of an organization would affect the ICT adoption intention in a positive way for Turkish SMEs (H12).

If a SME has higher cyber readiness, it can be suggested that they would be less concern with security and privacy and more willing to digitalization through adoption of ICT. Adoption of cyber insurance would affect the ICT adoption in a positive way for Turkish SMEs (H13).

3.6 Final model

The constructs and indicators for the model that is shown in Figure 1 was sourced on different studies based on other technological innovations. As explained thoroughly in the developments of our hypothesizes, we propose that cyber insurance adoption is affected by nine constructs based on commonly used constructs of TOE framework for ISS and ICT adoption extended with individual context. We suggest that the cyber insurance adoption positively affects cyber readiness of an SME. In continuum, as suggested by Hasan et al. (2021), cyber readiness positively affects organizational security performance. We complete our model by suggesting that for SMEs, cyber readiness also creates a sensation of trust that positively influences intention to adopt ICT tools.

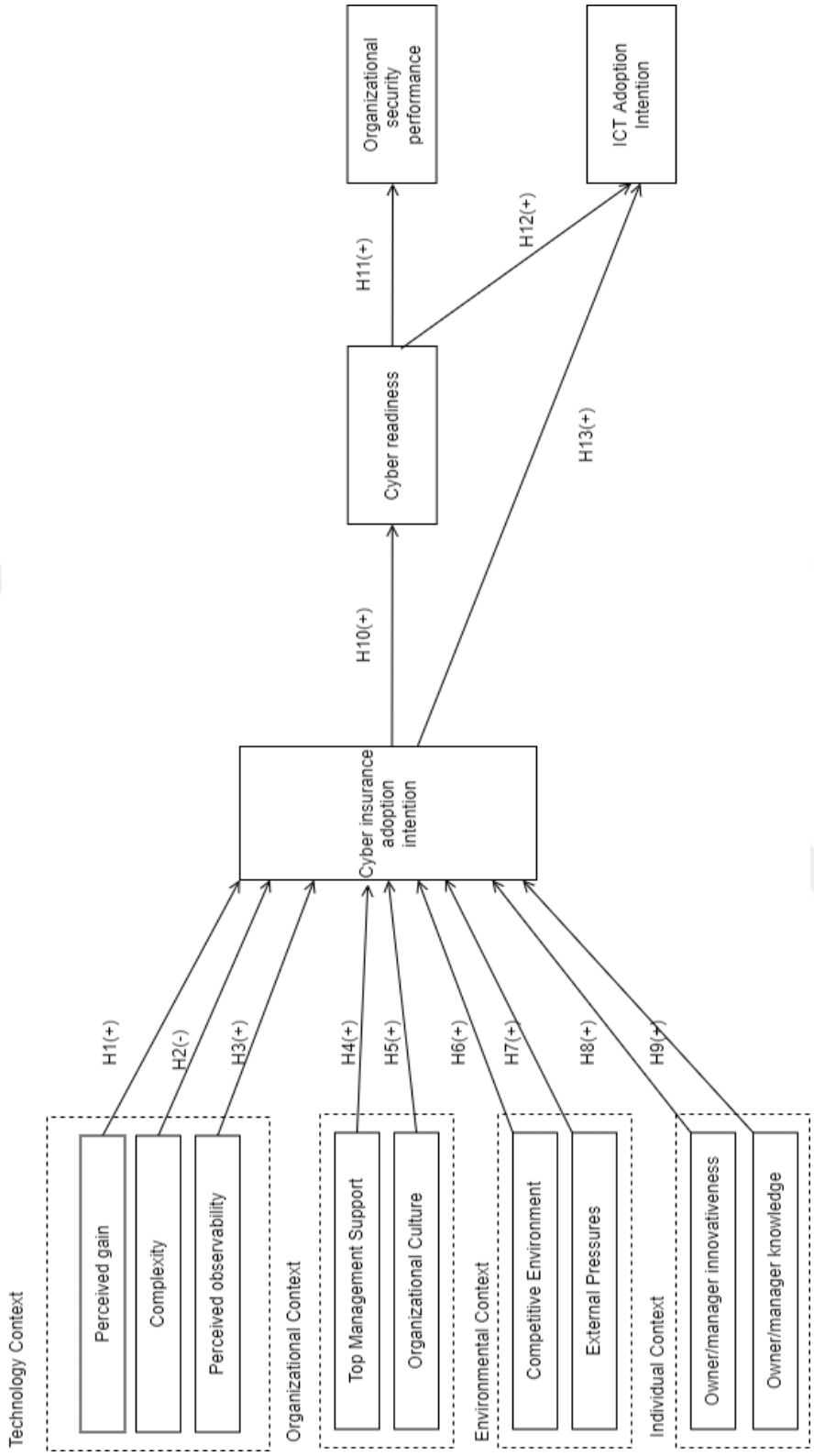


Figure 1. Cyber Insurance Adoption Intention Model for SMEs

CHAPTER 4

RESEARCH METHODOLOGY

This chapter provides information about the methodology of the study regarding preparation of the questionnaire, survey questions, conducting of the survey and sample of respondents.

4.1 Survey development

For the study, a quantitative survey was prepared based on the literature review. First, the demographic questions were asked to the respondents. In the first section of the survey was profile questions that were aimed to gain insight on the respondents' knowledge and experience on ICT and IS tools, cyber security and cyber security insurance. Profile questions were taken from AlBar and Hoque (2019). In this section of the survey respondents were also asked about their current level of knowledge of cyber security and the cyber security measures that are taken in their firm. These questions were not used directly in the testing of the model or hypotheses, but they were instrumental for data cleaning and discussing parts.

The second part of the survey aimed to test the model. The survey was a combination of the questionnaires that the latent variables of the models were based on. The questions were selected based their adaptability for cyber insurance context. Since the survey is aimed towards owners or managers of a firm, phrases that indicate the object of the questions were change i.e "ICT", "security practices", "security program", "NFC", and "smart contracts" (Khalilzadeh et al., 2017; AlBar & Hoque, 2019; Herath et al., 2020; Badi et al., 2021; Hasan et al. 2021). All the

questions asked are included in the Appendix A and Appendix B along with the Ethics Committee approval in Appendix C.

Since the questions were collected from English resources and the survey was targeted for Turkish respondents, the questions were translated to Turkish. The questions were then back translated into English for confirming correct translation (Brislin, 1970). The questionnaire was shared with cyber security and insurance sales experts for pre-testing the clarity on the questions and content validity (Forsyth, Kudela, Levin, Lawrence, & Willis, 2007; Urbach & Ahlemann, 2010). All the scales were kept same as the sourced surveys.

Technology context indicators measure the respondents' opinions of cyber insurance adoption in terms of perceived gain (PG), complexity (COM) and perceived observability (PO). The questions are adapted from surveys that measure the same values for different IT sectors such as ICT or IS adoption. Organizational context questions measure the readiness of the organization for cyber insurance adoption through top management support (TM) and willingness for organizational change through organizational culture (OC). Environmental context analyzes the external factors that affect the adoption of the cyber insurance. Competitive environment (CE) questions aim to measure the perceived criticality of a cyber incident depending on the competitive environment based on the financial and reputational damage a firm would take. External pressure (EP) questions measure the effect of non-regulatory external forces such as the importance of cyber security and data protection for business partners and consumers. The questions measuring the owner/manager innovativeness (OMI) were kept the same as to the original questionnaire to measure broader innovative perspective. Owner/manager knowledge (OMK) questions were adapted to cyber insurance. Cyber insurance adoption

indicators were adapted from UTAUT's behavioral intention (BI). Cyber readiness (CR) was measured by the capabilities of the firm in terms of vulnerability identification, protection of assets, detection of cyber incidents, ability to respond and recover. Organizational security performance (OSP) questions aimed to measure the advancements of security performance after upon increasing the level of cyber readiness. Finally, ICT adoption intention (ICT) questions measure the firm's willingness and intention to adopt ICT. The indicators of the model were shared in Appendix B.

4.2 Data collection

Initial pilot study was conducted with twenty respondents. Grammatical errors were corrected and questions that were less understandable were re-translated. For measuring the reliability and internal consistency of the initial study, Cronbach's alpha was calculated above 0.7 for each group of items that will be used to measure each construct (Gliner, Morgan, & Leech, 2000).

In many cases when the purpose of a research is not generalization but is theory development or theory testing, non-probabilistic sampling is often found suffice. (Hulland, Baumgartner, & Smith, 2018; Memon, Ting, Ramayah, Chuah, & Cheah, 2017). Thus, data for the survey was collected through link sharing in social media platforms such as Facebook, LinkedIn and Twitter. The target audience of our survey was owners or managers of SMEs that were qualified to participate in the cyber insurance adoption decision making, i.e. owner/CEO of the company or managers for finance and purchasing departments.

Social media platforms have been accepted as means of data collection in the literature for some time. For example, Barzilay and Urquhart (2014) used LinkedIn

to reach respondents for their study of code reuse in software development. Dusek, Yurova and Ruppel (2015) presented a case study that LinkedIn is an effective tool to reach a difficult to reach audience.

For determining the minimum sample size, three different methodologies were followed. First methodology is the rule of thumb used for PLS-SEM models, which is at least ten times the number of hypotheses (Hair, Ringle and Sarstdet, 2011). Following the rule of thumb, the sample size would be 130S. The second and third methodologies were developed by Kock and Hadaya (2018). Gamma-exponential and inverse square root methods consider the minimum absolute path coefficients, significance levels and statistical power required. The rule of thumb for these methodologies is to take minimum absolute path coefficient as 0.197, which is the value that solves Cohen's f^2 for 0.04 which is twice the minimum. We took the significance level desired as 0.95 and statistical power required as 0.80. Thus, minimum sample size calculated for gamma-exponential method was 146 and for inverse square root method the minimum sample size was calculated as 160.

For online questionnaires, non-response bias is accepted as a concern that should be addressed. In order to emulate non-response characteristics, the data was chronologically divided into two set. The demographic values of the two sets of data were compared by using t test with two samples. The significance levels for two tail testing were above 0.05, thus the differences between two datasets were found non-significant.

4.3 Data cleaning

From online link sharing through social media posts the collected response reached to 486. Data cleaning was conducted to eliminate non-SME respondents. Responses

with missing data were disregarded as they were missing completely and the remaining responses were enough for the minimum sample size requirement (Acock, 2005). Respondents who give repetitive answers to every question, i.e. giving the same answer for all multiple choice questions were eliminated. The respondents who were not qualified to participate in the decision-making process for cyber insurance adoption were identified by their position in the company and their knowledge for the current cyber insurance adoption status. The remaining answers to the survey accumulated to 168, which is higher than three methods of minimum sample size.

CHAPTER 5

DATA ANALYSIS

This chapter analyzes the results collected through the questionnaire. The demographic information about the respondents and cyber security measures of the companies are shared to give perspective. Partial least squares structural equation modeling (PLS- SEM) was used to analyze the theorized model.

5.1 Demographic profile of respondents

Demographics of respondents individually is shown in Table 8. Out of 168 respondents that the data analysis was made, 91 were men and 77 were women. Many of the respondents were between the age of 21-40. Undergraduate degree or higher were most common educational level amongst respondents. 63 respondents were the owners of the company and 29 respondents were the CEOs, thus fully authorized to make the cyber insurance adoption decision. Rest of the respondents were in managerial positions with authority and relevance to consider cyber insurance as a risk management tool and suggest to the owner or CEO. The respondents who were not the owners or the general managers were separated diversely, 27 respondents were IT managers and 31 respondents were procurement managers, 10 respondents were accounting managers and 3 respondents were finance managers. Rest of the respondents were either project or product managers depending on the industry they work in.

Table 8. Respondents' Demographics

Description – Respondent demographics	Frequency
Gender	
Female	77
Male	91
Age	
Between 21-30	66
Between 31-40	55
Between 41-50	28
Above 50	19
Education level	
Middleschool	2
Highschool	22
Preliminary	30
Undergraduate	90
Graduate	22
Doctorate	2
Role in the company	
Owner of the company	63
Procurement manager	31
CEO	29
IT manager	27
Accounting manager	10
Project/production manager	5
Finance manager	3

The respondents were asked about their knowledge and experience with using IT tools such as ERP and cyber security. Table 9 shows that 110 respondents stated that they have been using IT tools for between one and ten years, 27 respondents have been using IT tools for more than ten years. 54 of the respondents stated that they have been victims of a cyber security incident in their career. Amongst the respondents that claimed to be a victim of cyber incident in their work, 24 of them stated that cyber incident caused disruption of work, 18 of them stated that internal data was loss and 16 of them claimed that they received customer complaints. Respondents were allowed to choose multiple answers, so there were overlapping responses.

Table 9. IT and Cyber Security Knowledge of the Respondents

Description – IT and cyber security knowledge	Frequency
Use of IT in their career	
Did not specify	6
Less than a year	25
Between 1-10 years	110
More than 10 years	27
Cyber security knowledge (out of 10)	
1	10
2	4
3	8
4	10
5	26
6	34
7	23
8	23
9	13
10	17
Experienced a cyber security incident in their career	
I prefer not to specify	10
I do not know	7
Yes	54
No	97
Result of cyber security incident	
Disruption of work due to incident	24
Loss of internal data	18
Customer complaints	16
Legal process fees	13
Compliance penalty	9
Ransom payment to cyber criminals	6
Stolen customer data	6
Stolen trade secrets	5

2. Company information

As part of the demographic questions, the respondents were asked to answer questions about their company and their cyber security measures. Out of 168 respondents, 70 of their businesses belonged in the micro segment, 58 respondents owned or were managers of small enterprises and 40 respondents worked or managed medium segment businesses. The majority of the company profile divided

between three major industries; service with 51, production with 30 and wholesale/retail commerce with 25.

Table 10. Company Information of the Respondents

Description – Company information	Frequency
Size of the company	
Micro segment or self employed	70
Small enterprises	58
Medium enterprises	40
Industry	
Service	51
Production	30
Wholesale or retail commerce	25
Accommodation	14
e-Commerce	12
Construction	9
Managerial services	6
Content creator (blog, digital media etc.)	5
Health	5
Education	2
Information technologies	2
Insurance	2
Logistics and storage	2
Biotechnology	1
Other	1

The respondents were asked the cyber security tools they use to protect their systems. Table 11 reports that only 16 respondents claimed that they are not using cyber security tools while 133 respondents stated that they use more than one cyber security tool. Among other tools, anti-virus software was the most commonly used cyber security tool with 125 respondents' preference. Anti-virus software is also the number one choice among respondents who use one cyber security tool, followed by digital identity. Firewalls and user authorization followed anti-virus software for the most frequently used cyber security tool albeit they were more common among respondents who use more than three or four cyber security tools.

Table 11. Cyber Security Tools Frequency Table Based on the Number of Security Tools Used

	Number of cyber security tools used per respondent	0	1	2	3	4	5	6	7	8	9	10	#of respondents
	Total # of respondents per # of cyber security tools used	16	19	17	22	35	13	16	13	4	3	10	168
Cyber security tools used by respondents	Anti-virus software	0	9	11	20	32	9	15	12	4	3	10	125
	Firewalls	0	1	3	8	23	9	11	11	4	3	10	83
	User authorization	0	1	5	13	16	9	12	10	3	3	10	82
	File encryption	0	1	2	8	18	7	10	11	3	3	10	73
	Content filtering	0	2	3	3	10	6	9	11	4	3	10	61
	Strong password requirement	0	1	3	4	8	3	10	11	3	3	10	56
	Anti-spam software	0	0	1	4	12	4	10	8	3	2	10	54
	Digital identity	0	3	1	3	5	7	7	8	2	3	10	49
	One time password	0	1	5	1	12	4	2	6	3	2	10	46
	VPN access	0	0	0	2	4	7	10	3	3	2	10	41
	I do not know	11	0	0	0	0	0	0	0	0	0	0	11
	None	5	0	0	0	0	0	0	0	0	0	0	5

In addition to using cyber security tools, 145 respondents also claimed that they practice cyber security measures such as data backups, compliance controls and employee trainings. Among their cyber security preferences, critical data backup and the Law Under Protection Of Personal Data compliance controls were the most frequent measure among the respondents. Table 12 shows that more complex measures such as vulnerability testing and system logs were seen among respondents that already take other measures as well. Employee training, recovery plan and getting certified were more common among respondents that take more than five cyber security measures. There were seven respondents who take all the security measures.

In Table 13, cyber insurance adoption of the respondents are shared. Out of 168 respondents, 39 claimed to have adopted cyber insurance while 95 claimed they have not adopted cyber insurance and 34 stating that they do not know whether they

have adopted or not. Out of 39 respondents that do have cyber insurance, 37 of them claimed to have level 4 of cyber security knowledge out of 10. In the highest levels of cyber security knowledge such as 9 or 10, the number of respondents that adopt cyber insurance adoption is closer to the number of non-adopters.

Table 12. The Number of Security Measures Used Per Respondent

	Number of cyber security measures taken per respondent	0	1	2	3	4	5	6	7	# of respondents
	Total # of respondents per total # of measures taken	23	50	39	26	12	9	2	7	168
Cyber security measures	Backups of critical and personal data (at least once a week)	0	24	26	20	11	7	2	7	97
	Regular controls for compliance with Law Under Protection Of Personal Data	0	14	29	16	9	8	2	7	85
	Regular cyber security test (vulnerability testing, IT auditing etc.)	0	4	4	12	12	6	2	7	47
	Conducting employee trainings on cyber security	0	5	5	11	5	7	2	7	42
	System logs	0	1	4	11	4	6	0	7	33
	Recovery plan in case of an incident	0	1	6	4	4	8	2	7	32
	Getting internationally recognised certifications such as PCI-DSS , ISO27001	0	0	3	4	3	3	2	7	22
	Others	0	1	1	0	0	0	0	0	2

Table 13. Cyber Insurance Adoption Based on Cyber Security Knowledge

		Cyber insurance adoption			
		I do not know	Yes	No	Total
Cyber security knowledge	1	5		5	10
	2	1	1	2	4
	3	1		7	8
	4	2	1	7	10
	5	4	4	18	26
	6	7	8	19	34
	7	3	5	15	23
	8	8	5	10	23
	9	1	7	5	13
	10	2	8	7	17
	Total	34	39	95	168

5.2 Analysis of the model

For the analysis of the survey, partial least squares structural equation modeling (PLS- SEM) was used. PLS-SEM is suitable for theory development with complex models as well as smaller sample sizes and non-normalized data (Hair et al, 2011). In the literature, it is used when the researcher generates their theory based on the literature survey and expertise but their theory is less developed (Hair et al., 2011; Memon et al., 2017). The high statistical power the PLS-SEM method has makes this method suitable in research where the theory is still in the development phase (Sarstedt, Ringle, and Hair, 2017). For this study WarpPLS 8.0 was used for reflective measurement model and structural model analysis. In the analysis, behavioral intention indicators were used to measure cyber insurance adoption intention and symbolized as BI in the model (Khalilzadeh et al., 2017).

5.2.1 Measurement model

As the constructs that created the model were adapted from previous literature, their features were also kept the same and added as reflective constructs. The questions also support this decision as they are interchangeable and have common theme which qualifies them to be defined as reflective (Herath et al., 2020). In the reflective measurement model, indicator reliability, internal consistency reliability, convergent validity and discriminant validity values are measured for evaluation (Sarstedt et al., 2017). Indicator reliability for the model was measured with indicator loadings, each of the indicator loadings where above the threshold of 0.7 (Urbach & Ahlemann, 2010; Sarstedt et al., 2017). The indicator loadings are shared in Appendix D. P-values of the indicators were below 0.001 thus prove reliability (Kock, 2014). For internal consistency both composite reliability and Cronbach's alpha were above the

threshold values of 0.80, for all indicators and constructs as can be seen from Table 14 (Urbach & Ahlemann, 2010; Sarstedt et al., 2017).

Table 14. Composite Reliability and Cronbach's Alpha Results for Internal Consistency, AVE for Convergent Validity

	Composite reliability coefficients	Cronbach's alpha coefficients	Average variances extracted (AVE)
BI	0.967	0.948	0.906
PG	0.921	0.892	0.701
COM	0.852	0.739	0.657
PO	0.901	0.835	0.752
OC	0.911	0.854	0.774
TM	0.921	0.87	0.796
CE	0.901	0.835	0.753
EP	0.928	0.883	0.812
OMI	0.879	0.792	0.707
OMK	0.934	0.894	0.826
CR	0.967	0.963	0.73
OSP	0.899	0.859	0.644
ICT	0.96	0.937	0.889

Convergent validity was confirmed with average variances extracted (AVE) calculations which if AVE values are above 0.5 then convergent validity is satisfied (Urbach & Ahlemann, 2010). In addition loadings and cross loadings were used to confirm convergent validity; for all indicators the loadings were higher than the threshold for their constructs and lower for other constructs with p-value of below 0.001 (Amora, 2021). In order to confirm discriminant validity, we confirmed that the square root of AVE values for each construct were higher than other latent variables as seen on Table 15 (Kock & Lynn, 2012).

As the data was collected through an online questionnaire, common method bias (CMB) was measured using Harman's single factor test and full collinearity variance inflation factors (FVIF) (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Kock, 2015a). According to Kock (2021), Harman's single factor test can be done using WarpPLS 8.0 by adding all indicators to single latent variable and calculating

the AVE; if the AVE value is lower than 0.5 for the single latent variable, the common method bias is avoided. For our indicators the calculated factor-based Harman's single factor test AVE was 0.434 and composite-based AVE was 0.443. For measuring common method bias using FVIF values, threshold of 5 and lower is accepted to dismiss the bias (Kock, 2015a). In our model, full collinearity VIFs were below 5. Thus, by using both Harman's single factor test and full collinearity VIFs, common method bias was not considered an issue for our model.

Table 15. Correlations and Square Roots of Average Variance Extracted (AVE) Values

	BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR	ICT	OSP
BI	0.952												
PG	0.359	0.837											
COM	-0.084	0.171	0.811										
PO	0.558	0.57	0.12	0.867									
OC	0.349	0.317	-0.054	0.297	0.88								
TM	0.735	0.403	-0.065	0.628	0.458	0.892							
CE	0.449	0.497	0.12	0.572	0.139	0.48	0.868						
EP	0.697	0.39	-0.061	0.635	0.269	0.718	0.52	0.901					
OMI	0.636	0.314	-0.009	0.535	0.298	0.617	0.507	0.63	0.841				
OMK	0.676	0.389	0.036	0.667	0.32	0.764	0.528	0.716	0.622	0.909			
CR	0.739	0.415	-0.183	0.638	0.398	0.727	0.488	0.73	0.65	0.639	0.854		
ICT	0.687	0.275	-0.195	0.462	0.397	0.632	0.288	0.495	0.449	0.524	0.701	0.943	
OSP	0.658	0.499	-0.066	0.618	0.38	0.665	0.511	0.612	0.536	0.624	0.724	0.705	0.802

5.2.2 Structural model

For the evaluation of the structural model, collinearity, significance of path coefficients, the magnitude and explanatory power of path coefficients and predictive power are calculated (Sarstedt et al., 2017). Several models were studied with the given indicators and the model with highest scoring R^2 value was accepted for the accepted model. Average path coefficient, average R^2 value, and average full collinearity VIF values are in the satisfactory region for the model as seen in Table 16. The model does not have a problem of collinearity as the average VIF values are below the threshold of 3.3 (Kock & Lynn, 2012).

Table 16. Explanatory Values for the Model

Average path coefficient (APC)	0.258, P<0.001
Average R-squared (ARS)	0.571, P<0.001
Average adjusted R-squared (AARS)	0.563, P<0.001
Average block VIF (AVIF)	2.214, acceptable if <= 5, ideally <= 3.3
Average full collinearity VIF (AFVIF)	2.705, acceptable if <= 5, ideally <= 3.3

P-value calculation was done using Stable3, jackknifing and bootstrapping techniques with one-tailed test which is the default and recommended setting in WarpPLS (Urbach & Ahlemann, 2010; Kock, 2015b). Stable3 method is the default setting in WarpPLS that returns precise standard error prediction, jackknifing is recommended for smaller sample sizes with outliers and bootstrapping is typically used for larger sample sizes with evenly distributed data (Kock, 2018). The results of three methods are shared in Table 17. Stable3 is the preferred method for WarpPLS as it returns closer estimates to actual standard errors (Kock, 2018). In addition, Table 18 shows that this method brought the highest number of constructs with p-values below 0.05. Thus it was used as the main sampling method for this study.

Path coefficients with their p-values are shared in the Table 18. Path coefficients of PG, PO, OC and CE constructs were under the threshold of 0.1 and statistically non-significant due to their p-value being higher than 0.05. COM, TM, EP, OMI and OMK constructs are statistically significant according to p-value of 0.05. Their path coefficients satisfy the threshold of 0.1 in magnitude. COM has negative sign that leads to a negative relationship between COM and BI constructs. TM, EP, OMI and OMK constructs have positive effect on BI. BI also have positive and significant relationship with CR, OSP and ICT constructs supported with high magnitudes and p-values lower than 0.05.

Table 17. P-values of Path Coefficients with Stable 3, Jackknifing and Bootstrapping Methods

Stable3											
	PG	COM	PO	TM	OC	CE	EP	OMI	OMK	BI	CR
BI	0.379	0.019	0.409	<0.001	0.307	0.411	0.002	0.006	0.039		
CR										<0.001	
OSP											<0.001
ICT										<0.001	<0.001
Jackknifing											
	PG	COM	PO	TM	OC	CE	EP	OMI	OMK	BI	CR
BI	0.378	<0.001	0.433	0.003	0.257	0.457	0.02	0.008	0.07		
CR										<0.001	
OSP											<0.001
ICT										<0.001	<0.001
Bootstrapping											
	PG	COM	PO	TM	OC	CE	EP	OMI	OMK	BI	CR
BI	0.334	0.077	0.4	<0.001	0.236	0.416	0.006	0.006	0.042		
CR										<0.001	
OSP											<0.001
ICT										<0.001	<0.001

Coefficient of determination (R^2) of the exogenous latent variables were measured to ensure model validity. As seen from Table 19, R^2 of BI was 0.641 which is considered close to substantial, 0.549 for CR, 0.538 for OP and 0.555 for ICT which are all above 0.333 average threshold (Urbach & Ahlemann, 2010). Effect

size is considered a step for model validation, as it explains the effect of an independent latent variable on a dependent variable, thus measured for this model (Urbach & Ahlemann, 2010). Paths from COM, EP, OMI and OMK to BI are considered to have small effect size whereas TM has a medium effect size for BI. On the other hand, paths that are from BI to CR and CR to OSP have large effect sizes. Finally, paths lead to ICT from BI and CR have medium effects. Predictive relevance was measured using Q-squared coefficients for all paths leading to exogenous variables. Above zero as a threshold value for most naïve benchmark was achieved for all exogenous latent variables (Urbach & Ahlemann, 2010; Sarstedt et al., 2017).

Table 18. P-values, Patch Coefficients and Effect Sizes for The Paths in the Model

Path	p-value	Path coefficient	Effect size
PG → BI	0.379	0.024	0.011
COM → BI	0.019	-0.156	0.054
PO → BI	0.409	0.018	0.075
TM → BI	<0.001	0.286	0.218
OC → BI	0.307	0.039	0.009
CE → BI	0.411	-0.017	0.00
EP → BI	0.002	0.218	0.155
OMI → BI	0.006	0.187	0.098
OMK → BI	0.039	0.133	0.091
BI → CR	<0.001	0.741	0.593
CR → OSP	<0.001	0.734	0.549
CR → ICT	<0.001	0.430	0.303
BI → ICT	<0.001	0.366	0.252

Table 19. R^2 Coefficients and Q^2 Coefficients

R^2 coefficients												
BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR	OSP	ICT
0.641										0.549	0.538	0.556
Q^2 coefficients												
BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR	OSP	ICT
0.662										0.551	0.539	0.56

On Table 20 the total effects of COM, TM, OMI, OMK on CR and ICT are shown and significant with p-values lower than 0.05 and effect sizes over than 0.02. TM, OMI and OMK has also positive and significant relation with OSP. COM's negative relation with OSP is significant but the effect size is lower than the threshold of 0.02, thus not supported in our model. BI's direct effect to ICT adoption was shown by path coefficients. The indirect effect over OSP is also positive and significant with p-value lower than 0.05 and effect size over than 0.02. We tested the indirect relationship between BI and ICT through moderation by cyber readiness, the moderating relationship was non-significant with low path coefficient and effect size as can be seen in Appendix E.

Table 20. Total Effects of the Constructs

Total effects of latent variables											
	BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR
BI		0.024	-0.156	0.018	0.039	0.286	-0.017	0.218	0.187	0.133	
CR	0.741	0.018	-0.116	0.013	0.029	0.212	-0.013	0.162	0.139	0.099	
OSP	0.544	0.013	-0.085	0.01	0.021	0.155	-0.009	0.119	0.102	0.072	0.734
ICT	0.685	0.016	-0.107	0.012	0.026	0.196	-0.012	0.15	0.128	0.091	0.43
p-values of total effects											
	BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR
BI		0.379	0.019	0.409	0.307	<0.001	0.411	0.002	0.006	0.039	
CR	<0.001	0.374	0.016	0.405	0.299	<0.001	0.407	0.001	0.005	0.033	
OSP	<0.001	0.386	0.027	0.414	0.318	<0.001	0.416	0.003	0.01	0.05	<0.001
ICT	<0.001	0.383	0.023	0.412	0.313	<0.001	0.414	0.003	0.008	0.045	<0.001
Effect size of total effects											
	BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR
BI		0.009	0.041	0.01	0.014	0.21	0.008	0.155	0.119	0.09	
CR	0.549	0.007	0.021	0.008	0.011	0.154	0.006	0.118	0.09	0.063	
OSP	0.358	0.006	0.006	0.006	0.008	0.103	0.005	0.073	0.055	0.045	0.538
ICT	0.471	0.004	0.021	0.006	0.011	0.124	0.003	0.074	0.058	0.048	0.303

The final results of the questionnaire on the structural model is shown in Table 21. Nine out of thirteen hypothesis in our model are supported based on their p-values, magnitude, effect size and total effects show significant relationships between constructs. The model itself can be seen in Appendix F with the aforementioned path coefficients and p-values.

Table 21. Hypotheses in the Model

Hypothesis	Supported/Not Supported
H1: Perceived gains from cyber insurance will have a direct positive effect with cyber insurance adoption within Turkish SMEs	Not supported
H2: Complexity will have a direct and negative effect on the adoption intention of cyber insurance within Turkish SMEs.	Supported
H3: Perceived observability will have a direct and positive effect cyber insurance intention within Turkish SMEs	Not supported
H4: Top management support will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.	Supported
H5: The organizational culture will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.	Not supported
H6: A competitive environment will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.	Not supported
H7: External pressures will have a direct and positive effect on cyber insurance adoption in Turkish SMEs.	Supported
H8: Owner/manager innovativeness will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.	Supported
H9: Owner/manager cyber insurance knowledge will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.	Supported
H10: Adoption of cyber insurance would effect the cyber readiness of an organization in a positive way for Turkish SMEs.	Supported
H11: Cyber readiness of an organization would effect the organizational security performance in a positive way for Turkish SMEs.	Supported
H12: Cyber readiness of an organization would affect the ICT adoption intention in a positive way for Turkish SMEs.	Supported
H13: Adoption of cyber insurance would affect the ICT adoption in a positive way for Turkish SMEs.	Supported

CHAPTER 6

DISCUSSION AND CONCLUSION

This section talks about the hypothesis of the study combined with the findings of demographics and relevant literature.

6.1 Factors affecting cyber insurance adoption

Based on our model, complexity, top management support, external pressures, owner/management innovativeness and cyber insurance knowledge have direct effects on cyber insurance adoption. Complexity is one of the well known factors that discourages technology adoption, which our model supported as true for cyber insurance adoption. Lack of IT employees in SMEs might be a factor in perceiving cyber insurance difficult to integrate to current IT infrastructure and manage the requirements that come with the policy. The prerequisites such as log controls, database management, and creating a recovery plan is not a simple task to achieve without qualified IT employees. If a business does not already have these systems at hand, implementing or even understanding the necessary actions before cyber insurance adoption can be challenging.

In addition, even if cyber insurance providers offer anti-virus software as part of the package, integrating a new software to already existing systems can be challenging with or without an IT team present. Since the most digitalized era of our times also coincided with an economical crisis, IT resources became the most expandable item to save cost. How can we expect SMEs to understand cyber risk when the number of IT employees among SMEs are decreasing? There is no indication that Turkish SMEs are knowledgeable enough to be aware of cyber risk let alone how to manage

the risk. Proposing a product such as cyber insurance requires understanding of topics such as cyber attacks and risk delegation.

In the existing literature, while complexity negatively effects technology adoption, the gain from technology to be adapted supports it. Interestingly, this has not been the case in our model. Perceived gain and perceived observability under the technology context were not shown to have positive effect on cyber insurance adoption behavior. This may be the result of the immature cyber insurance market, as the product is not well known and the benefits of it are not well observed. In addition, there are only handful of insurance companies are in the market that offer cyber insurance. The immature market leads to unstandardized policies, coverages and pricing. Anderson and Moore (2006) as well as Biener et al. (2015) previously claimed that changing pricing policies, non-standardized calculation methods and non-sufficient coverages have been claimed to negatively affect the perceived gain from adopting insurance. Another point to consider is that the lack of awareness for the results of cyber security may lead to underestimation of the financial risk from undelegated cyber security risks. Combined with the problem areas of cyber insurance, SMEs are most likely not yet trusting in cyber insurance nor perceive it as necessary, even though cyber insurance not only delegates cyber risks but also ensures cyber security by providing necessary tools and services as well as regularly renewing due diligence.

In summation for the technology context, our model shows that cyber insurance as a new insurance product is seen so complex that it surpasses the benefits in the eyes of SMEs. Neither perceived gain nor the visibility of the cyber insurance benefits overcome the discouragement that comes from the complexity. It can be said that in order to expand the cyber insurance adoption for SMEs in Türkiye, easing the

adoption process would most likely to be more effective than deliberating why cyber insurance would benefit a business. If insurance companies can be more open and clearer about the requirements and the adoption process, it might lead to a higher chance of cyber insurance adoption.

One of the common coverages of cyber insurance is support in legal fees caused by Law Under Protection of Personal Data. Even though as previously mentioned, perceived gain does not have a positive relationship with adoption, external pressure that comes from the mandatory rules regarding the Law Under Protection of Personal Data compliance does. Law Under Protection of Personal Data is regarded as a highly important legal practice for customer data protection with high financial consequences unless compliance is achieved. The risk of a financial burden of non-compliance pushes businesses to adopt cyber insurance. The significant effect of environmental pressure on cyber insurance adoption emphasizes the success of the regulatory controls of cyber protection for businesses. Obligatory measures push companies to be more careful, proactively protect themselves and adapt a risk management perspective. If these rules and regulations were to increase to cover cyber insurance, collective cyber readiness of Turkish SMEs would also increase. For instance, insurance companies conduct due diligence process upon insuring a business. Not only cyber insurance would mitigate the financial risk of a cyber attack, a more mature market might also relax the prerequisites of insurance companies. In addition, mitigating the financial aspect of the cyber risk can reduce the risk of bankruptcy in case of cyber events which would be beneficial macro-economically. Even though cyber insurance is not mandatory for businesses yet, the effect of protecting customer data with regulations can be seen as a positive step towards safe digitalization for SMEs.

Insurance adoption is highly receptive of the willingness of the insured individual to take risk. In the case of commercial insurance such as cyber insurance, the risk assessment of the insured would be based on either the top management for the SMEs or the central risk management if the organization has one. While the top management support affects cyber insurance adoption in a positive way, organizational culture does not have a positive impact. We can interpret this result in a combination with the individual context in our model. Owner/manager innovativeness and cyber security knowledge affects the adoption of cyber insurance for SMEs. This means that the owners/managers in SMEs that are innovative, look for new ways to be digital and aware of cyber risks also influence top management to push for using the coverages and benefits that comes with cyber insurance adoption. It can be said that if top management including the owner/manager is knowledgeable on the cyber insurance or cyber security topics in general, hesitation due to complexity may not be problem. In order to reach more customers, insurance companies can create awareness over cyber security topics, educate their customers on cyber security and then offer cyber insurance as a complementary risk mitigation tool for SMEs that have become knowledgeable about security topics.

Unlike Bandyopadhyay's (2012) theory that highly competitive environment is effective to cyber insurance adoption, this relationship is not supported in our model. Even though in order to have competitive advantage digitalization is becoming more common among SMEs, the cyber security side of the integrations and data sharing seems to be unacknowledged. Awareness of the vulnerabilities that come with the digitalization is necessary for both safety of SMEs and the growth of cyber insurance market. In terms of competitive environment, the reputational damage that companies may face in case of cyber incident was also regarded as a

part of the competitive environment effect. While this concern was not shown in our model for SMEs, it might be a valid concern for large enterprises. The financial consequences and the reputational damage can be more severe, as can be seen by the recent data leakage examples in Türkiye. Thus, competitive environment may show positive and significant effect in a model fit for large enterprises.

6.2 Effects of cyber insurance adoption on cyber readiness

Results of our model indicated a positive relationship between cyber readiness and intention to adopt cyber insurance. This is parallel with the prerequisites of cyber insurance; in order to be qualified to be insured, businesses must already have implemented cyber security tools such as anti-virus tools, password protection and user authorized access. Insurance companies also evaluate companies based on their cyber security measures such as having a recovery plan, educating employees and backing up databases. Not only these tools and measures would reduce the chance of being affected by a cyber attack, the increased self protection would ensure lower premiums from insurance companies. Our model states that unlike Öğüt et al. (2005)'s suggestion, cyber insurance adoption will not encourage companies to forgo cyber readiness and self-protection. According to our model, businesses do not see cyber insurance as a replacement for cyber readiness and relax their cyber security systems once the cyber insurance policy is in effect.

Being cyber ready by using appropriate tools such as firewalls and anti-virus software supported by regular compliance controls strengthens cyber security and reduces a chance of an attack. Since SMEs are often targeted by hackers and cyber attackers, the likelihood of becoming a victim is increasing each year. Thus being prepared by protection and monitoring in case of an event further reduces the direct

and indirect costs, thus increasing organizational security performance. As shown by the indirect effect supported in our model, cyber insurance adoption has a positive relationship with organizational security performance. Adoption of cyber insurance requires self protection, regular monitoring and a recovery plan, thus enabling cyber readiness and increasing organizational security performance.

6.3 Effects of cyber insurance adoption on ICT adoption

The positive relationship between cyber insurance adoption and ICT adoption can be caused by multiple reasons. For starters as cyber insurance is a risk mitigating tool for remaining cyber risks, the coverages of cyber insurance can lead to a sense of security for the business which may result in more adoption of ICT tools. There are various risks waiting an SMEs in the road for digitalization; each year number and financial impact of cyber attacks targeting SMEs are increasing, failing to be compliant with Law Under Protection of Personal Data can lead to high financial fees, and cyber tools may be complicated and costly. Because of these worries SMEs can be absent from digitalization. Thus adopting cyber insurance can create sense of security and lead to digitalization through ICT tool adoption. In addition, cyber insurance adoption is positively related to owner/manager's innovativeness. According to the total effects of the constructs of our model, owners/manager's innovativeness has a significant and positive relation to ICT adoption. It can be said that the innovative nature of the owner/manager leads to both cyber insurance and ICT adoption. The extension of TEO framework with individual context has been previously supported for researches that focus on SMEs. Our model also supports that ICT adoption as well as cyber insurance adoption has a relationship with owner/manager's behavior.

Finally, the positive and direct effect of cyber insurance adoption over ICT adoption showcases the opportunity for digitalization for Turkish SMEs with cyber insurance. Cyber security investments may come to an upper limit in terms of effectiveness. In a certain level, it would not be beneficial to invest in cyber security for risks that may never be eliminated. Therefore investing in cyber insurance and other ICT tools can overall be more effective. In case of a cyber attack, the direct financial effects such as ransom or unwanted financial transaction can be too difficult to recover from. As cyber insurance adoption mitigates the financial risk, companies can use their financial resources on investing in other digitalization tools and technologies.

6.4 Limitations and areas for further research

As this research aimed at theory creation and testing, sampling was not aimed to be used for statistical conclusions. The model can be tested with a more specialized sample such as size or industry for obtaining statistical results that can be generalized.

Further improvement on this study might be to adapt other constructs from literature such as compatibility and cost (AlBar & Hoque, 2019, Herath et al. 2020). The best approach to enhance our model would be to create original constructs tailored to cyber insurance adoption. A quantitative survey about cyber insurance adoption that used a variation of TOE was not available at the time of our research. In addition, a deep dive qualitative research with personal interviews can improve the model and bring an understanding on the factors that affect cyber insurance adoption.

APPENDIX A

DEMOGRAPHIC QUESTIONS

- Gender:
    - Female,
    - Male,
    - Do not wish to share
    - (open text)
- Age:
    - 20 or younger
    - 21-30
    - 31-40
    - 41-50
    - 50 or above
- Level of education:
    - Middleschool
    - Highschool
    - Preliminary
    - Undergraduate
    - Graduate
    - Doctorate
- The size of your company:
    - Micro segment or self employed
    - Small enterprises (number of employees are between 10-50 and annual income is between 3-25 million TL)

    - Medium enterprises (number of employees are between 50-250 and annual income is more than 125 million TL)
- Number of employees:
    - 1-10
    - 10-50
    - 50-250
    - Over 250
- Annual income
    - Less than 3 million TL
    - Between 3-25 million TL
    - Between 25-125 million TL
    - Over 125 milyon TL
- Industry
    - Service
    - Production
    - Wholesail or retail trade
    - Accomadation
    - e-Commerce
    - Construction
    - Managerial services
    - Content creator (blog, digital media etc.)
    - Health
    - Education
    - Information technologies
    - Insurance

    - Logistics and storage
    - Biotechnology
    - Other (please state)
- Role in the company
    - Owner of the company
    - CEO
    - IT manager
    - Procurement manager
    - Accounting manager
    - Finance manager
    - Project/production manager
    - Other (please state)
- How long have you been using information technologies in your career? (Information technologies are used to create and access data. For example accounting, inventory and ERP programs are considered information technology)
    - Did not specify
    - Less than a year
    - Between 1-10 years
    - More than 10 years
- Number of years your company have been active
    - Did not specify
    - Less than a year
    - Between 1-10 years
    - More than 10 years

- Number of years you have been actively working
    - Did not specify
    - Less than a year
    - Between 1-10 years
    - More than 10 years
- Number of years you have been actively working for your current company
    - Did not specify
    - Less than a year
    - Between 1-10 years
    - More than 10 years
- Your level of cyber security knowledge (choose between 1-10, 1 being I have no knowledge and 10 being I have expert level of knowledge)
- Which of these following cyber security tools are been utilized in your company?
    - Anti-virus program
    - Firewalls
    - User authorization
    - File encryption
    - Content filtering
    - Strong password requirement
    - Anti-spam software
    - Digital identity
    - One time password
    - VPN access
    - Others (please state)

- I do not know

- Which of these cyber security measures are been taken in your company?
  - Backups of critical and personal data (at least once a week)
  - Regular controls for compliance with KVKK
  - Regular cyber security test (vulnerability testing, IT auiditing etc.)
  - Conducting employee trainings on cyber security
  - System logs
  - Recovery plan in case of an incident
  - Getting internationally recognised certifications such as PCI-DSS , ISO27001
  - Others (please state)
  - I do not know
- Have you ever been a victim of a cyber attack?
  - Yes
  - No
  - Do not wish to share
- If you have ever been a victim of a cyber crime, what were the consequences you have faced?
  - Disruption of work due to incident
  - Loss of internal data
  - Customer complaints
  - Legal process fees
  - Compliance penalty
  - Ransom payment to cyber criminals
  - Stolen customer data

    - Stolen trade secrets
- What non-mandatory insurance policies you have?
    - Office policies (Policies specialized for SMEs and industries that cover unexpected incidents)
    - Others (please specify)
- Do you have cyber insurance?
    - Yes
    - No

APPENDIX B

INDICATORS FOR THE MODEL

Construct	Adapted questions	Source	Scale
Perceived gain (PG)	PG1: Cyber insurance decreases potential losses due to security incidents	Herath et al. (2020)	7-point Likert scale (form strongly disagree to strongly agree)
	PG2: Cyber insurance keeps risks related to security incidents to a minimum		
	PG3: Cyber insurance has contributed to the value of our business.		
	PG4: Cyber insurance has increased our market share (profitability) due to secure transaction practices.		
	PG5: Cyber insurance has increased the competitive advantage for our company		
Complexity (COM)	COM1: We believe that cyber insurance is very difficult to use	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	COM2: The skills required to use cyber insurance are too complex for our employees		
	COM3: Integrating cyber insurance into our work practices will be very difficult		
Perceived Observability (PO)	PO1: There is good publicity about the positive effects of cyber insurance	Badi et al. (2021).	5-point Likert scale (form strongly disagree to strongly agree)
	PO2: Other organizations using cyber insurance liked using them.		

	PO3: I have a clear understanding of the positive effects of a cyber insurance		
Top management support (TM)	TM1: Top management enthusiastically supports the adoption of cyber insurance	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	TM2: Top management has allocated adequate resources to the adoption of cyber insurance		
	TM3: Top management actively encourages employees to use cyber insurance		
Organizational culture (OC)	OC1: Our organization is very responsive and changes easily	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	OC2: There is a high level of agreement about how we do things in this company		
	OC3: There is a shared vision of what this organization will be similar to in the future		
Competitive Environment (CE)	CE1: We believe we will lose our customers to our competitors if we do not adopt cyber insurance	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	CE2: We feel it is a strategic necessity to use cyber insurance to compete in the marketplace		
	CE3: We believe we will lose our market share if we do not adopt cyber insurance		
External Pressure (EP)	EP1: Our business partners require that we have strong security program.	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	EP2: Our suppliers/business		

	partners require use of specific security technologies and practices from us.		
	EP3: Our consumers are demanding about privacy and security		
Owner/manager innovativeness (OMI)	OMI1: If we heard about a new information technology, we would look for ways to experiment with it	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	OMI2: Among our peers, we are usually the first to try out new information technology		
	OMI3: We do not hesitate to try new information technology		
Owner/manager knowledge (OMK)	OMK1: We have the necessary skills and knowledge to use cyber insurance	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	OMK2: We are familiar with cyber insurance		
	OMK3: We have the experience to use cyber insurance		
Cyber insurance adoption intention (BI)	BI1: Given the chance I intend to use cyber insurance	Khalilzadeh et al. (2017)	7-point Likert scale (form strongly disagree to strongly agree)
	BI2: Given the chance I predict I should use cyber insurance		
	BI3: Given the chance I plan to use cyber insurance		
Cyber Readiness (CR)	CR1: Our organization is aware of and committed to using advanced methods for vulnerability assessment.	Hasan et al. (2021)	5-point Likert scale (form strongly disagree to strongly agree)
	CI2: Our organization is committed to controlling computer ports that could be used for attacks.		

	CR3: Our organization is committed to ensuring that system vulnerabilities are within accepted risks.		
	CR4: Our organization is aware of and committed to using data encryption at the end-point.		
	CR5: Our organization is aware of and committed to using virus protection software.		
	CR6: Our organization is aware of and committed to enforcing a strong password policy.		
	CR7: Our organization is aware of and committed to enabling proactive management of emerging threats before they occur (e.g., threat intelligence).		
	CR8: Our organization is aware of and committed to performing operational and strategic analyses of published security incidents.		
	CR9: Our organization is aware of and committed to continuously monitoring security alerts to detect cyber-attacks.		
	CR10: Our organization is aware of and committed to having procedures for recovery plan implementation.		
	CR11: Our organization is committed to		

	recovering from failure through keeping and updating backup databases.		
Organizational security performance (OSP)	OSP1: The number of data breaches in our organization is decreasing over time.	Hasan et al. (2021)	5-point Likert scale (form strongly disagree to strongly agree)
	OSP2: Our organization has a legitimate security reputation.		
	OSP3: The internal processes of our organization are becoming more secure.		
	OSP4: Our organization's databases are available whenever needed.		
	OSP5: Our organization has a reliable system with adequate capabilities and capacities for information processing.		
ICT Adoption Intention (ICT)	ICT1: We have a high intention to use cyber insurance in our organization	AlBar & Hoque (2019)	5-point Likert scale (form strongly disagree to strongly agree)
	ICT2: We intend to learn about using cyber insurance		
	ICT3: We plan to use cyber insurance to manage our business		

APPENDIX C

ETHIC COMMITTEE APPROVAL OF THE SURVEY

Evrak Tarih ve Sayısı: 07.01.2022-46713

T.C.
BOĞAZİÇİ ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER YÜKSEK LİSANS VE DOKTORA TEZLERİ ETİK İNCELEME KOMİSYONU
TOPLANTI KARAR TUTANAĞI

Toplantı Sayısı	:	26
Toplantı Tarihi	:	05.01.2022
Toplantı Saati	:	14:00
Toplantı Yeri	:	Zoom Sanal Toplantı
Bulunanlar	:	Prof. Dr. Ebru Kaya, Prof. Dr. Fatma Nevra Seggie, Dr. Öğr. Üyesi Yasemin Sohtorik İlkmen
Bulunmayanlar	:	

Aslı Özkeleş
İşletme Bilişim Sistemleri

Sayın Araştırmacı,

"Dijitalleşmede Risk Yönetimi İçin Sibergüvenlik Sigortasının Tercih Edilmesinin Etkenleri" başlıklı projeniz ile ilgili olarak yaptığınız SBB-EAK 2021/80 sayılı başvuru komisyonumuz tarafından 5 Ocak 2022 tarihli toplantıda incelenmiş ve uygun bulunmuştur.

Bu karar tüm üyelerin toplantıya çevrimiçi olarak katılımı ve oybirliği ile alınmıştır. COVID-19 önlemleri kapsamında kurul üyelerinden ıslak imza alınamadığı için bu onay mektubu üye ve raportör olarak Fatma Nevra Seggie tarafından bütün üyeler adına e-imzalanmıştır.

Saygılarımızla, bilgilerinizi rica ederiz.

Prof. Dr. Fatma Nevra SEGGIE
ÜYE

e-imzalıdır
Prof. Dr.Fatma Nevra SEGGIE
Raportör

SOBETİK 26 05.01.2022

Bu belge 5070 sayılı Elektronik İmza Kanununun 5. Maddesi gereğince güvenli elektronik imza ile imzalanmıştır.

APPENDIX D

LOADING AND CROSS-LOADING FOR INDICATOR RELIABILITY

	BI	PG	COM	PO	OC	TM	CE	EP	OMI	OMK	CR	OSP	ICT
BI1	0.95	-0.03	0.01	-0.01	-0.02	0.02	0.00	0.01	-0.05	-0.01	0.06	0.05	-0.06
BI2	0.95	0.00	0.00	-0.05	0.04	0.13	0.02	0.06	0.01	-0.03	-0.06	0.00	-0.02
BI3	0.95	0.03	-0.01	0.06	-0.03	-0.14	-0.02	-0.07	0.04	0.04	0.00	-0.05	0.08
PG1	-0.26	0.80	0.03	0.08	0.11	0.06	-0.12	-0.03	0.21	-0.20	0.20	-0.11	0.13
PG2	-0.24	0.79	0.04	0.01	0.03	0.14	-0.14	0.07	0.09	0.05	0.03	0.21	-0.07
PG3	0.07	0.91	0.02	-0.10	-0.11	0.16	-0.07	-0.11	-0.01	-0.06	0.00	-0.03	0.08
PG4	0.13	0.82	-0.06	0.01	0.01	-0.16	0.15	0.13	-0.18	0.11	-0.07	-0.01	-0.18
PG5	0.27	0.86	-0.03	0.02	-0.03	-0.20	0.16	-0.05	-0.09	0.11	-0.14	-0.05	0.04
COM1	0.05	0.09	0.79	-0.09	-0.08	0.06	0.02	0.08	-0.06	0.16	0.10	-0.11	-0.04
COM2	-0.07	-0.03	0.81	0.21	0.03	0.09	0.06	-0.16	-0.11	-0.20	-0.14	0.06	0.12
COM3	0.03	-0.06	0.83	-0.12	0.04	-0.14	-0.08	0.08	0.17	0.05	0.04	0.05	-0.08
PO1	-0.06	0.01	0.07	0.84	0.03	0.08	-0.09	0.18	-0.21	-0.18	-0.14	-0.02	0.07
PO2	0.01	-0.03	0.02	0.90	0.03	0.06	0.12	-0.06	0.06	-0.15	0.16	0.02	-0.09

PO3	0.05	0.02	-0.09	0.86	-0.06	-0.14	-0.04	-0.11	0.15	0.34	-0.03	0.00	0.03
OC1	-0.03	0.00	-0.02	0.00	0.90	-0.02	-0.04	-0.05	0.11	0.04	0.04	0.03	-0.06
OC2	-0.07	0.01	-0.01	0.07	0.88	0.13	-0.12	0.05	0.05	-0.10	-0.08	0.02	-0.01
OC3	0.11	-0.01	0.03	-0.06	0.86	-0.12	0.17	0.01	-0.17	0.06	0.04	-0.05	0.07
TM1	0.18	0.03	-0.06	0.01	-0.01	0.92	0.01	0.03	0.04	0.17	-0.20	0.02	0.01
TM2	-0.22	0.04	0.06	-0.06	-0.06	0.82	-0.02	-0.26	-0.01	-0.08	0.23	-0.04	-0.13
TM3	0.02	-0.07	0.00	0.05	0.06	0.93	0.00	0.19	-0.03	-0.10	-0.01	0.02	0.11
CE1	-0.03	-0.09	0.02	-0.16	0.02	0.12	0.90	0.03	-0.07	-0.06	-0.07	-0.04	0.05
CE2	0.02	0.16	-0.03	0.24	-0.03	-0.13	0.81	-0.10	0.15	0.07	0.14	-0.05	-0.07
CE3	0.01	-0.05	0.01	-0.06	0.01	0.00	0.90	0.05	-0.07	0.01	-0.06	0.09	0.01
EP1	-0.01	-0.06	-0.09	0.08	0.01	0.02	0.04	0.93	0.05	0.14	-0.07	0.02	-0.11
EP2	-0.03	-0.01	-0.05	-0.04	-0.06	0.16	0.04	0.93	-0.08	0.08	0.08	-0.09	-0.11
EP3	0.04	0.07	0.16	-0.04	0.05	-0.20	-0.10	0.84	0.04	-0.24	-0.01	0.07	0.24
OMI1	0.12	0.10	-0.02	0.18	-0.05	0.15	-0.06	-0.12	0.87	-0.18	-0.03	-0.06	0.02
OMI2	0.01	-0.11	0.08	-0.26	0.02	-0.21	0.10	0.01	0.79	0.39	0.09	0.10	-0.21
OMI3	-0.13	0.00	-0.05	0.05	0.03	0.04	-0.03	0.12	0.86	-0.17	-0.05	-0.03	0.18

OK1	0.09	0.01	0.04	0.02	0.02	-0.13	-0.06	-0.11	0.12	0.93	0.09	-0.04	0.01
OK2	-0.02	0.01	0.04	0.01	0.00	-0.07	-0.01	-0.07	0.02	0.93	0.15	0.03	0.02
OK3	-0.08	-0.01	-0.09	-0.03	-0.02	0.21	0.08	0.20	-0.15	0.86	-0.26	0.02	-0.04
CR1	0.04	-0.03	-0.02	-0.03	0.13	-0.06	0.06	0.18	-0.11	0.04	0.83	0.13	-0.06
CR2	0.08	-0.15	-0.04	0.11	-0.10	0.05	0.07	0.06	-0.06	0.09	0.83	0.16	-0.28
CR3	0.07	-0.08	-0.03	-0.05	0.08	-0.19	0.09	0.08	-0.03	0.16	0.89	0.02	-0.11
CR4	0.10	-0.07	-0.05	-0.05	0.11	-0.21	0.09	0.08	-0.21	0.23	0.87	-0.10	0.15
CR5	-0.24	0.01	0.17	-0.22	0.00	0.09	0.02	-0.03	-0.02	0.05	0.81	-0.06	0.31
CR6	-0.05	0.10	0.05	0.06	0.07	0.30	-0.06	-0.02	-0.10	-0.33	0.77	0.03	0.18
CR7	0.00	0.03	-0.06	-0.04	-0.04	0.04	0.05	-0.06	0.09	-0.01	0.91	-0.14	0.02
CR8	0.03	0.00	-0.02	0.12	-0.02	-0.04	0.01	-0.01	0.06	0.02	0.88	-0.15	-0.11
CR9	0.15	0.03	0.00	0.14	-0.05	-0.17	-0.04	-0.08	-0.01	0.13	0.90	-0.12	-0.06
CR10	-0.05	0.10	-0.11	0.04	-0.11	0.16	-0.12	-0.10	0.14	-0.20	0.88	0.07	-0.12
CR11	-0.17	0.07	0.12	-0.09	-0.07	0.07	-0.17	-0.11	0.22	-0.23	0.83	0.18	0.12
OSP1	-0.18	-0.19	-0.03	-0.04	-0.10	-0.04	0.11	0.20	-0.02	-0.09	-0.18	0.77	0.02
OSP2	-0.01	0.07	-0.05	0.04	0.09	-0.29	0.01	-0.02	0.07	0.28	-0.08	0.85	0.02

OSP 3	-0.10	0.00	0.01	0.00	0.10	-0.17	-0.18	0.02	0.07	0.14	0.10	0.88	0.15
OSP 4	0.14	0.00	0.10	0.09	-0.15	0.40	0.17	-0.20	-0.11	-0.33	-0.06	0.66	-0.11
OSP 5	0.17	0.10	-0.01	-0.08	0.02	0.20	-0.07	-0.03	-0.04	-0.08	0.18	0.84	-0.12
ICT 1	0.01	-0.08	0.01	0.08	0.10	0.00	0.03	0.03	0.01	-0.18	-0.01	-0.04	0.96
ICT 2	-0.04	0.09	0.06	-0.13	-0.05	0.03	0.02	0.01	0.03	0.05	-0.01	0.04	0.94
ICT 3	0.02	-0.01	-0.07	0.05	-0.05	-0.03	-0.05	-0.04	-0.04	0.14	0.02	0.00	0.93

APPENDIX E

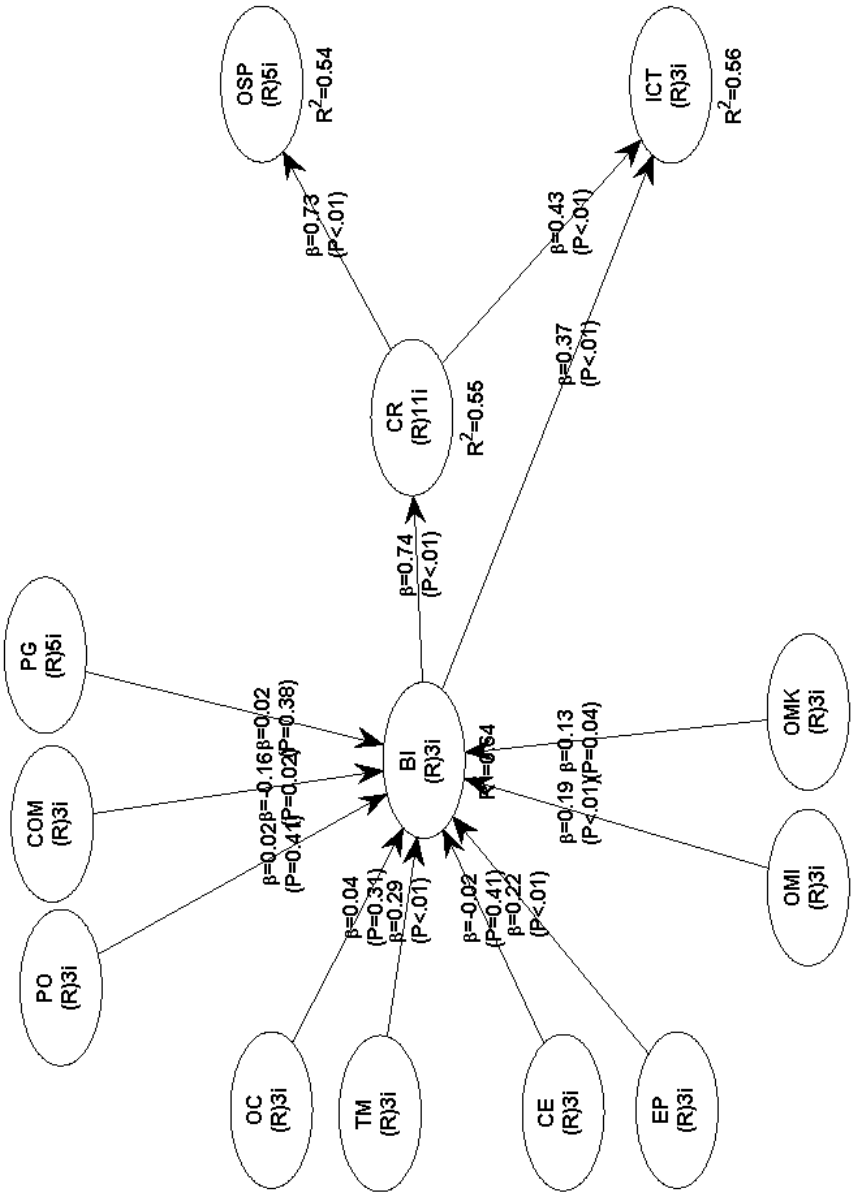
MODERATING EFFECT OF CYBER READINESS BETWEEN CYBER INSURANCE ADOPTION, ICT ADOPTION

In the model we also controlled if the link between cyber insurance and ICT adoption was moderated by the cyber readiness of the business as they would feel more confident to acquire more tools for digitalization. The moderating effect of CR over BI and ICT's relationship is not supported by our model due to P-value higher than 0.05.

Path	p-value	Path coefficient	Effect size
BI→ CR → CT	0.312	-0.038	0.016

APPENDIX F

THE RESEARCH MODEL WITH PATH COEFFICIENTS AND P-VALUES



REFERENCES

Accenture (2019). *The cost of cybercrime.* Retrieved from: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Acock, A. C. (2005). Working with missing values. *Journal of Marriage and Family*, *67*(4), 1012-1028.

Ak Sigorta (2022). *Siber koruma sigortası* Retrieved June 13, 2022, from https://www.aksigorta.com.tr/urunler/kurumsal-urunler/diger-sigortalar/siber-koruma-sigortasi

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-5). IEEE.

AlBar, A. M., & Hoque, M. R. (2019). Factors affecting the adoption of information and communication technology in small and medium enterprises: A perspective from rural Saudi Arabia. *Information Technology for Development*, *25*(4), 715-738.

Allianz Sigorta (2014). *Finansal Sigortalar* Retrieved 13 Juna 2011, from https://www.allianz.com.tr/tr_TR/urunler/diger-urunler/sorumluluk-sigortalari/finansal-sigortalar.html

Altuntaş, E., Kara, E., Soylu, A. B., & Kırkbeşoğlu, E. (2018). Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar. *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, (12), 8-22.

Amora, J. T. (2021). Convergent validity assessment in PLS-SEM: A loadings-driven approach. *Data Analysis Perspectives Journal*, *2*(3), 1-6.

Anadolu Sigorta. (2018). *Neden Anadolu Sigorta Ticari Siber Güvenlik Paket Poliçesi Almalıyım.* Retrieved June 13, 2022, from https://www.anadolusigorta.com.tr/Files/UrunDetayBilgi/ticari-siber-guvenlik-paket-policesi.pdf

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610-613.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, *14*(3), 396-402.

Avina, G. E., Bogner, K., Carter, J., Friedman, A., Gordon, S. P., Haney, J., & Wolf, D. (2017). *Tailoring of cyber security technology adoption practices for operational adoption in complex organizations.* United States.

Awa, H. O., Ukoha, O., & Igwe, S. R. (2017). Revisiting technology-organization-environment (TOE) theory for enriched applicability. *The Bottom Line*. *30* (1), 2-22.

Ayaydın, H. (2021). Dijitalleşme Kobi'lere Firsat Penceresi Açar Mı? *V. International Kaoru Ishikawa Business Administration and Economy Congress* (pp.11-20). Ankara, Türkiye: Proceedings Book.

Aygün, D., & Sati, Z. E.(2022) Evaluation of Industry 4.0 Transformation Barriers for SMEs in Turkey. *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *17*(1), 239-255.

Badi, S., Ochieng, E., Nasaj, M., & Papadaki, M. (2021). Technological, organisational and environmental determinants of smart contracts adoption: UK construction sector viewpoint. *Construction Management and Economics*, *39*(1), 36-54.

Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in IT security management. *IEEE Security & Privacy*, *5*(3), 50-56.

Baker, J. (2012). The technology–organization–environment framework. *Information Systems Theory*, 231-245.

Bandyopadhyay, T. (2012). Organizational adoption of cyber insurance instruments in IT security risk management: a modeling approach. *Proceedings. Paper*, *5*, 20.

Barzilay, O., & Urquhart, C. (2014). Understanding reuse of software examples: A case study of prejudice in a community of practice. *Information and Software Technology*, *56*(12), 1613-1628.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Pap Risk Insur Issues Pract* 40, 131–158

BloombergHT (2021) *Siber saldırıların yüzde 43'ü KOBİ'lere yapılıyor*. Retrieved from https://www.bloomberght.com/siber-saldirilarin-yuzde-43u-kobilere-yapiliyor-2277647.

Böhme, R., & Kataria, G. (2006). On the limits of cyber-insurance. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 31-40). Berlin, Germany: Springer

Bozgeyik, A. (2018). *Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetim yaklaşımlarının analizi*. (PhD thesis) Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep, Türkiye.

Brislin, R. W. (1970). Back-translation for cross-cultural research. *Journal of Cross-Cultural Psychology*, *1*(3), 185-216.

Buzatu, C. (2013). The influence of behavioral factors on insurance decision–A Romanian approach. *Procedia Economics and Finance*, *6*, 31-40.

CGI Inc. (2019). *Understanding Cybersecurity Standards*. Retrieved from https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf

Cisco. (2021a). *What Is a Cyberattack? - Most Common Types*. Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks.

Cisco. (2021b). *What is Malware? - Definition and Examples*. Retrieved from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html.

Cisco. (2021c). *What Is Phishing? Examples and Phishing Quiz,* Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html.

Cisco. (2021d). *What Is a DDoS Attack? Distributed Denial of Service*. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html.

Cisco. (2021e). *DNSns Tunneling*. Retrieved from https://learn-umbrella.cisco.com/solution-briefs/dns-tunneling

Cisco. (2021f). *What Is a Exploit*. Retrieved from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html

Dambra, S., Bilge, L., & Balzarotti, D. (2020). SoK: Cyber insurance–technical challenges and a system security roadmap. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1367-1383). San Francisco, CA, United States: IEEE.

Dhillon, G. (1995). *Interpreting the management of information systems security* (Doctoral dissertation). The London School of Economics and Political Science, London, United Kingdom.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153.

Doğa Sigorta (2022). *Ticari siber güvenlik sigortası* Retrieved 13 Juna, 2022, from https://www.dogasigorta.com/urunler/ticari-siber-guvenlik-sigortasi

Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, *527*, 576-589.

Dusek, G., Yurova, Y., & Ruppel, C. P. (2015). Using social media and targeted snowball sampling to survey a hard-to-reach population: A case study. *International Journal of Doctoral Studies*, *10*, 279.

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873-2882). Seoul Republic of Korea: Association for Computing Machinery, New York, NY, United States.

Ekren, G., Erkollar, A., & Oberer, B. (2019). ERP-related issues and challenges in Turkey: An overview from ERP experts. *IMISC*. Journal contribution.

Eling, M., & Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. *Geneva Pap Risk Insur Issues Pract*, 43(3), 359-396.

Elradi, M. & Altigani, A. & Abaker, O. (2020). Cybersecurity awareness among students and faculty members in a Sudanese college. In *Electrical Science & Engineering, 2(2), 24-28*

Eş, A. & Serdar, N. Siber Saldirilara Karşi Kobilerin Farkindalik Düzeylerinin İncelenmesi: Ankara İli Örneği. *Düzce Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(1), 133-151.

Forsyth, B. H., Kudela, M. S., Levin, K., Lawrence, D., & Willis, G. B. (2007). Methods for translating an English-language survey questionnaire on tobacco use into Mandarin, Cantonese, Korean, and Vietnamese. *Field Methods*, *19*(3), 264-283.

Frenzel, A., Muench, J. C., Bruckner, M. T., & Veit, D. (2021). Digitization or digitalization?–Toward an understanding of definitions, use and application in IS research". In *Proceeding: 27th Americas Conference on Information Systems (18)*, Montreal, Canada: AMCIS.

Gergin, Z., Üney-Yuüksektepe, F., Güneş Gençyılmaz, M., Tülin Aktin, A., Gülen, K. G., İlhan, D. A., ... & Çavdarlı, A. İ. (2018). Industry 4.0 scorecard of Turkish SMEs. In *The International Symposium for Production Research* (pp. 426-437). Springer, Cham.

Gliner, J. A., Morgan, G. A., & Leech, N. (2000). *Research Methods in Applied Settings: An Integrated Approach to Design and Analysis.* Lawrence Erlbaum Associates Publishers.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85.

Güleç Yalçın, F. (2021). *Türkiye'de bir yılda 1,6 milyon kötü amaçlı yazılım saldırısı düzenlendi.* Fintechtime. Retrieved from: https://fintechtime.com/tr/2021/01/turkiyede-bir-yilda-16-milyon-kotu-amacli-yazilim-saldirisi-duzenlendi/.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139-152.

Hameed, M. A., & Arachchilage, N. A. G. (2020). A conceptual model for the organizational adoption of information system security innovations. In *Security, Privacy, and Forensics Issues in Big Data* (pp. 317-339). IGI Global.

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*, 102726.

Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, *2*(1), 7-20.

Herath, T. C., Herath, H. S., & D'Arcy, J. (2020). Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 51(2),* 12-35.

Holmes, A. (2019). Hackers have become so sophisticated that nearly 4 billion records have been stolen from people in the last decade alone. Here are the 10 biggest data breaches of the 2010s. *Business Insider*. Retrieved from: <https://www.businessinsider.com/biggest-hacks-2010s-facebook-equifax-adobe-marriott-2019-10>

Hulland, J., Baumgartner, H., & Smith, K. M. (2018). Marketing survey research best practices: evidence and recommendations from a review of JAMS articles. *Journal of the Academy of Marketing Science*, *46*(1), 92-108.

IBM Security. (2021). *Cost of a Data Breach Report 2021*. Retrieved from: https://www.ibm.com/downloads/cas/OJDVQGRY

International Standards Office [ISO] (2020a). *1. ISO Survey 2020 results - Number of certificates and sites per country and the number of sector overall.* Retrieved from: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

International Standards Office [ISO] ISO (2020b) *2. ISO Survey 2020 results - Number of sectors by country for each standard functions.* Retrieved from: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

International Telecommunication Union (ITU)ITU. (2021). *Cybersecurity*. Retrieved from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

Irwin, L. (2020). ISO 27001 Annex A Controls Explained. Retrieved from: https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

Iyzico (2016) *PCI DSS Hakkında 4 Soru 4 Cevap.* (2016). [Web log post]. Retrieved from https://www.iyzico.com/blog/pci-dss-hakkinda-4-soru-4-cevap/

Johnson, E.J., Hershey, J., Meszaros, J. & Kunreuther, H. (1993). Framing, probability distortions, and insurance decisions. *Journal of Risk Uncertainty 7*, 35–51.

Kapersky (2018) *DDoS Breach Costs Rise to over $2M for Enterprises finds Kaspersky Lab Report.* Retrieved from: https://usa.kaspersky.com/about/press-

releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report

Kartal, B. (2021). BTK ve KVKK, Yemeksepeti'ne en üst sınırdan ceza kesecek. *Webtekno.com* Retrieved from: https://www.webtekno.com/btk-kvkk-yemeksepeti-en-ust-sinir-ceza-h108622.html

Khalilzadeh, J., Öztürk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, *70*, 460-474.

Kock, N. (2014). Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM. *International Journal of e-Collaboration*, 10(1), 1-13.

Kock, N. (2015a). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, *11*(4), 1-10.

Kock, N. (2015b). One-tailed or two-tailed P values in PLS-SEM?. *International Journal of e-Collaboration*, *11*(2), 1-7.

Kock, N. (2018). Should bootstrapping be used in pls-sem? Toward stable p-value calculation methods. *Journal of Applied Structural Equation Modeling*, *2*(1), 1-312.

Kock, N. (2021). Harman's single factor test in PLS-SEM: Checking for common method bias. *Data Analysis Perspectives Journal*, *2*(2), 1-6.

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227-261.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for information Systems*, *13*(7).

Küçük ve Orta Ölçekli Sanayi Geliştirme ve Destekleme İdaresi Başkanlığı [KOSGEB] (2021). *Definitions and Regulations.* Retrieved from: https://en.kosgeb.gov.tr/site/tr/genel/detay/5667/definitions-and-regulations

Küçük ve Orta Ölçekli Sanayi Geliştirme ve Destekleme İdaresi Başkanlığı [KOSGEB] (2022). *KOBİ tanımı güncellendi!* Retrieved from: https://www.kosgeb.gov.tr/site/tr/genel/detay/8173/kobi-tanimi-guncellendi#:~:text=Y%C3%B6netmelik%20ile%20KOB%C4%B0%20tan%C4%B1m%C4%B1nda%20kullan%C4%B1lan%20kriterler%20g%C3%BCncellendi.&text=Buna%20g%C3%B6re%3B%20250%20ki%C5%9Fiden%20az,a%C5%9Fmayan%20i%C5%9Fletmeler%20KOB%C4%B0%20olarak%20tan%C4%B1mlanacak.

KPMG Türkiye, 2021. *Dijitalleşme Yolunda Türkiye 2021 Trendler ve Rehber Hedefler*. Retrieved from: https://www.tubisad.org.tr/tr/images/pdf/dijitallesme-yolunda-turkiye-raporu-v9.pdf

Lane, M., & Marie, M. (2010). The adoption of single sign-on and multifactor authentication in organisations–A critical evaluation using TOE framework. *Information in Motion: The Journal Issues in Informing Science and Information Technology (Volume 7)*, *7*, 161.

Laury, S., McInnes, M. M., & Swarthout, J. T. (2008). Insurance purchase for low-probability losses. *Andrew Young School of Policy Studies Research Paper*, (08-05).

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Lindros, K., & Tittel, E. (2016). What is cyber insurance and why you need it. *CIO*.

Lloyd, M. (2018). Using cyber insurance to run virtuous circles around cyber risk. *Computer Fraud & Security*, *2018*(10), 6-8.

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*, *2017*(4), 18-20.

Matt, D. T., Modrák, V., & Zsifkovits, H. (2020). *Industry 4.0 for SMEs: Challenges, opportunities and requirements* (p. 412). Springer Nature. (41-43)

Mbatha, N.S. (2020). *Factors influencing cyber insurance adoption in South Africa industry* (Doctoral dissertation). University of the Witwatersrand, Johannesburg, South Africa.

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125.

Memon, M. A., Ting, H., Ramayah, T., Chuah, F., & Cheah, J. H. (2017). Editorial,'A review of the methodological misconceptions and guidelines related to the application of structural equation modelling: a Malaysian scenario'. *Journal of Applied Structural Equation Modeling*, *1*(1), 1-13.

Oellrich, H. (2003). Cyber-insurance update. *CIP Report 2*, pp. 9-10.

Öğüt, H., Menon, N. M., & Raghunathan, S. (2005). Cyber insurance and IT security investment: Impact of interdependence risk. In *WEIS*.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.

PCI Security Standards Council LLC (2021). *PCI Security Standards Council At-a-Glance* Retrieved from: https://www.pcisecuritystandards.org/documents/At_a_Glance_Role_of_the_PCI_SSC.pdf

Podsakoff, P. M., MacKenzie, S. B., Lee,J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, 88(5), 879–903.

Rashid, M. A., Hossain, L., & Patrick, J. D. (2002). The evolution of ERP systems: A historical perspective. In *Enterprise resource planning: Solutions and management* (pp. 35-50). IGI global. (1-8)

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *Cyber-risk management* (pp. 33-47). Springer, Cham.

Resmi Gazete. (2010). *Elektronik Haberleşme Güvenliği Kapsaminda Ts Iso/Iec 27001 Standardi Uygulamasina İlişkin Tebliğ*. Ankara. Retrieved from: https://www.resmigazete.gov.tr/eskiler/2010/10/20101015-9.htm

Rivers, I., & Noret, N. (2010). 'I h8 u': Findings from a five-year study of text and email bullying. *British Educational Research Journal*, *36*(4), 643-671.

Rogers, E. M. (1995). Diffusion of innovations. *New York: Free Press*, 12.

Rosli, K., Yeow, P. H., & Siew, E. G. (2012). Factors influencing audit technology acceptance by audit firms: A new I-TOE adoption framework. *Journal of Accounting and Auditing*, *2012*, 1.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.

Samonas, S., & Coss, D. (2014). The Cia Strikes Back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2017). Partial least squares structural equation modeling. *Handbook of Market Research*, *26*(1), 1-40.

Sawicki, A. (2016). Digital marketing. *World Scientific News*, (48), 82-88.

Sharma, K., Singh, A., & Sharma, V. P. (2009). SMEs and cybersecurity threats in e-commerce. *EDPACS The EDP Audit, Control, and Security Newsletter*, *39*(5-6), 1-49.

Showers, V., & Shotick, J. (1994). The effects of household characteristics on demand for insurance: a tobit analysis. *The Journal of Risk and Insurance*, *61*(3), 492-502. doi:10.2307/253572

Slovic, P., Fischhoff, B., Lichtenstein, S., Corrigan, B., & Combs, B. (1977). Preference for insuring against probable small losses: Insurance implications. *Journal of Risk and Insurance*, 237-258.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *NIST special publication*, *800*(30), 800-30.

T.C. Cumhurbaşkanlığı Cumhurbaşkanlığı Mevzuat Bilgi Sistemi. (2013). *Elektrik piyasasi lisans yönetmeliği* Ankara. Retrieved from: https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=18985&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5

T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi. (2007). *Banka kartlari ve kredi kartlari hakkinda yönetmelik.* Ankara. Retrieved from: https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=11180&MevzuatTertip=5

Thong, J. Y. (1999). An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems, 15*(4), 187-214.

Tornatzky, L. G., & Fleischer, M. (1990). *The process of technology innovation* . Lexington, MA: Lexington Books.

Bilişim Sanayicileri Derneği [TUBISAD] (2021). *Türkiye'nin Dijital Dönüşüm Endeksi 2021* Retrieved from: https://www.tubisad.org.tr/tr/images/pdf/tubisad-2021-dde-raporu.pdf

Turkish Data Protection Authority. (2021). *Data Protection In Turkey.* Ankara: Turkish Data Protection Authority. Retrieved from: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/5c02cb3c-7cc0-4fb0-b0a7-85cb90899df8.pdf

Turkish Data Protection Authority. (20220). *2021 19 Faaliyet Raporu.* Ankara: Turkish Data Protection Authority. Retrieved from: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/eaf2f71e-efa5-48e2-9326-9b7fa2813193.pdf

Turkish Statistical Institute (2020). *Küçük ve Orta Büyüklükteki Girişim İstatistikleri, 2019.* Ankara: Turkish Statistical Institute

Turkish Statistical Institute (2021). *Girişimlerde Bilişim Teknolojileri Kullanım Araştırması, 2021.* Ankara: Turkish Statistical Institute

UL. (2018). *The US FDA has officially recognized the UL 2900 Cybersecurity standard for medical devices*. Retrieved from https://www.ul.com/news/us-fda-has-officially-recognized-ul-2900-cybersecurity-standard-medical-devices

Ulaş, D. (2019). Digital transformation process and SMEs. *Procedia Computer Science, 158,* 662-671.

Ulusal Siber Olaylara Müdahale Merkezi - USOM, (n.d.) *USOM Hakkında.* Retrieved 20 November 2021, from https://www.usom.gov.tr/hakkimizdafrom https://www.usom.gov.tr/hakkimizda

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology theory and Application, 11*(2), 5-40.

Uuganbayar, G., Yautsiukhin, A., Martinelli, F., Massacci, F. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security*, *101*, 102121.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118-144.

Wallace, S., Green, K., Johnson, C., Cooper, J., & Gilstrap, C. (2021). An Extended TOE Framework for Cybersecurity Adoption Decisions. *Communications of the Association for Information Systems*, *47*(2020), 51.

Wang, M., Liao, C., Yang, S., Zhao, W., Liu, M., & Shi, P. (2012). Are people willing to buy natural disaster insurance in China? Risk awareness, insurance acceptance, and willingness to pay. *Risk Analysis: An International Journal*, *32*(10), 1717-1740.

Wang, P., & Park, S. A. (2017). *Issues in Information Systems*, *18*(2).

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173.

We are social. (2022). *Digital 2022: Another Year Of Bumper Growth* [Web log post] Retrieved from: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/

Wekundah, R. N. (2015). *The effects of cyber-crime on e-commerce; a model for SMEs in Kenya* (Doctoral dissertation, University of Nairobi).

Wen, K. W., & Chen, Y. (2010). E-business value creation in Small and Medium Enterprises: a US study using the TOE framework. *International Journal of Electronic Business*, *8*(1), 80-100.

Woods, D., Agrafiotis, I., Nurse, J. R., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, *8*(1), 1-13.

Xu, M., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, *23*(2), 220-249.

Yiğitol, B., Güleş, H. K., & Sarı, T. (2020). Endüstri 4.0 dönüşüm sürecinde, kobi'lerin teknoloji seviyelerinin belirlenmesi: Konya imalat sanayi örneği. *International Journal of Advances in Engineering and Pure Sciences*, 32(3), 320-332.

Yılmaz, Y. (2021). Transition to the Digital Economy, Its Measurement and the Relationship between Digitalization and Productivity. *Istanbul Journal of Economics*. 71, 2021/1, s. 283-316.