ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (PhD) THESIS

ESMERALDA KADËNA

A Threat Avoidance Perspective of Users' Security Behaviours in Smartphones: Albania versus Hungary

Supervisors: Dr. András Keszthelyi and Prof. Dr. Katalin Takács-György

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

Budapest, 2022

Complex Exam Committee:

President:

name

Members:

name

name

Public Defence Committee:

President:

name

Secretary:

name

Members:

name

name

name

Reviewers:

name

name

Date of the Public Defence:

……

Statement

I, Esmeralda Kadëna, declare that the content of this dissertation is the product of my original work, and it contains no sources or resources other than the ones mentioned and acknowledged. This work has not been submitted to another institution, neither in Hungary nor outside, nor in the same or similar way.

To my family.

Most especially to my Mother and Father, who supported me through this and everything in my life!

Abstract

The thesis' research was conducted around the idea of giving a better understanding of the factors responsible for the users' security behaviours in smartphones. The study's primary purpose was to assess the influence of smartphone users' cognitive factors and individual differences and determine whether the motivation of using smartphone security technologies leads to better security behaviour in different cultures. The conceptual model was developed based on the contextualization of Technology Threat Avoidance Theory (TTAT) as an extension of the Protection Motivation Theory (PMT). The cognitive factors incorporated the TTAT predictors of behaviour in the form of threat appraisal factors (threat perception and its two antecedents: perceived threat susceptibility and severity) and coping appraisal factors (safeguard effectiveness, safeguard cost, and self-efficacy). In addition, three broad constructs, impulsivity, risk, and distrust propensity of users were included.

This study focused on Albanian and Hungarian smartphones users. A web-based survey was used to gather the data, and in total, 588 responses were kept for analysis. Descriptive statistics and the Partial Least Square Structural Modeling (PLS-SEM) were used to analyze the gathered data. To better explain the threat assessment process in different cultures, an alternative approach was proposed by conducting a Multi-Group Analysis that involved two groups of interest. At first, the model was tested with all the valid data. Then, the multigroup analysis between users in Albania and Hungary was performed, and the results were presented in a systematic and detailed way. Path coefficients, t-statistic values, and p-values were generated by emphasizing significant differences and similarities between the two countries. Also, a separate analysis was performed for each group for a better understanding.

The most finding to emerge from this study is that applying the theoretical model across different countries will lead to different results for each of them. These results improve knowledge and understanding of the effect of cultural differences in the smartphone security context. This suggests that cultural differences should be considered in future studies when investigating individuals of different cultures. This dissertation provides a significant opportunity to advance the knowledge regarding human behaviours in smartphone security. It can be regarded as a first step towards understanding Albanian and Hungarian smartphone users.

Contents

INTRODUCTION

"Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information." – Kevin Mitnick (2000, p. 8)

Nowadays, mobile technology has become an inevitable part of almost every aspect of our lives. Since smartphones enable users to access many services, they have become essential [1]. People are constantly connected with their mobile devices to the Internet. The world is changing rapidly, and the digital revolution is becoming hardly stoppable. Besides the chances of innovation in society, smartphones present significant risks [2]. Their increasing popularity raises many security concerns. Security breaches on these devices can cause damage to individuals as well as organizations. Users can become victims of many security threats. On the other hand, their unsafe behaviours may create opportunities for hackers to attack the companies' applications and systems they access with their devices.

Problem Statement

Since smartphones have been increasing, they have become an easy target for hackers [3]. The valuable information they contain poses risks of breaches to information security at the individual and organizational levels. Besides addressing and mitigating security threats in smartphones, users' risky behaviours remain the most critical challenge in cybersecurity. Along with technological advancements, there is an increasing concern over the factors contributing to users' intentions and behaviours in security. Consequently, technology alone is not enough to ensure security. A vast number of security incidents and data breaches within organizations are associated with users' behaviour on mobile devices for personal and business reasons. Scholars and professionals continuously recommend awareness practices for users that focus on understanding smartphone security. It is still challenging to identify if users understand and apply them correctly. We are in a situation where many cyber incidents can be avoided, but they continue to occur. Naturally, a question arises: Why do people not

protect themselves? The human aspect of security has gained many researchers' interest [4], [5]. The lack or minimal exploration in this area may be attributed to the fact that the human factor is complex to understand and manage within the information security context because human behaviour is unpredictable [6].

Researchers in information security has been focused on measuring the actual behaviours based on behavioural intention [7], [8], [9]. However, many issues are present due to other factors influencing users' intentions. Thus, other researchers have faced difficulties in predicting information security behaviours [10], [11], [12], [13]. Besides, little is known about users' behaviours and their peculiarities from the countries of interest in this research. The lack of literature examining users' (in Albania and Hungary) behaviours in smartphones from the threat avoidance perspective presents an opportunity to add to the body of knowledge on smartphones' security. Thus, this study aims to address a gap and provide more evidence regarding users from Albania and Hungary on the factors that influence users' perceived threats and the factors that affect their intentions to use security technologies, which consequently can behave securely in smartphones.

This dissertation is presented along with the rise in cybercrime moving towards smartphones by emphasizing users' differences and their behaviours in security.

Research Objectives

This dissertation's key objective was to determine, with empirical data, the factors that influence users' security behaviours in smartphones. The research was classified from the perspectives of inquiry and objectives mode. From the viewpoint of inquiry, the study is conducted based on qualitative and quantitative data. From the objectives point of view, the research methods used were descriptive and explanatory. At first, preliminary research was conducted to accomplish the following objectives:

- O1: To introduce security and threats regarding smartphones.
- O2: To gain insight into user behaviour of smartphone security and their using habits based on related research findings.
- O3: To explore the research methods and theories for users' cyber-security motivations, threat perception, coping ability, and cybernetics.

- O4: To explain the samples used in the research model and define each users' group's cultural characteristics.

After content analysis, the following objectives were specified:

- O5: To examine the Albanian and Hungarian users' perceived threat regarding smartphones.
- O6: To examine the effects of safeguard measures (cost, effectiveness, and self-efficacy) in the Albanian and Hungarian users' motivation to use security technologies.
- O7: To investigate the influence of individual differences (Albania and Hungary) in motivation of using security technologies, and security behaviours in smartphones.
- O8: To investigate the Albanian and Hungarian users' security motivation and behaviour of using smartphones' security technologies.
- O9: To compare research results and highlight differences between Albanian and Hungarian users.

Thesis Structure

Following the introduction part, the thesis is categorized into the following chapters:

Chapter 1 (Security and Smartphones) presents a literature review, related work, and relevant information about the security concept and its dimension. The chapter continues by outlining the main security threats and challenges in smartphones.

Chapter 2 (Theoretical Framework: Threat Avoidance) begins with a particular focus on the human factors in Information Security. It extends to the cultural theories by highlighting the main differences between Albania and Hungary. The last part elaborates theoretical approaches related to the influence of cognitive factors and individual differences on threat perceptions, motivations, and behaviours of users in IT systems. The hypotheses and research model used in this dissertation are represented in the end.

Chapter 3 (Methodology and Data) presents the research methodology that comprises three phases. In the first phase, a pilot survey was conducted to pre-test the instrument that included items from prior research, but they were put in smartphones' context. In

the second phase, several changes were made to the existing survey, and after finalizing it, data collection was performed using a web-based survey in three languages (Albanian, English, and Hungarian). Data analysis was conducted and presented in the third phase. Data were checked for missing values and possible outliers in the preliminary analysis. Then, assumptions before conducting factor and path analysis were evaluated. To examine the linearity, the scatterplots of the standardized residuals versus predicted values were accessed for the three dependent variables in SPSS. Later, the Durbin-Watson statistic test was performed to assess the independence of residuals of errors. Measures of kurtosis and skew were generated to check if the indicators used in the study met the normality assumption. As the independent variables should not be highly correlated, multicollinearity was examined with the help of the variance inflation factor (VIF). The results highlighted that assumptions for conducting Factor and Path Analysis were not violated. Since several changes were made to the instrument after the pilot phase, Cronbach's Alpha, Average Variance Extracted (AVE), Composite Reliability, and rho_A were examined to measure the internal reliability consistency and convergent validity of the constructs. Moreover, discriminant validity was examined by accessing HTMT values.

Chapter 4 (Main Research Results: Questions and Hypotheses) is the essential part of this study. Firstly, this chapter presents the demographics of the respondents, insights regarding smartphones' selection, usage purposes, users' accounts of importance, and their habits and practices in smartphones.

PLS-SEM addressed the five research questions as well as seven hypotheses. At first, the model was tested with all the valid data, and then multigroup analysis between users in Albania and Hungary was performed. The results and study findings are presented systematically and detailed in the last part of the chapter.

Chapter 5 (Conclusions) presents the main research findings and the overall thesis contributions. In addition, this section includes limitations of the study and directions and recommendations for future work.

1 SECURITY AND SMARTPHONES

"The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself."

– Sun Tzu (1910, p. 12).

A considerable number of studies have attempted to define the security concept. By its meaning, security can be regarded as the state of being free from poverty or want, protective measures taken against a threat, espionage, or a person/thing [14]. From the viewpoint of its nature, security is multidimensional, and from practice, it is diverse. Therefore, it can be considered challenging to provide a single definition for different security domains.

"Security" is not an old term from the political point of view. After World War I, the most prominent term in academic and political discussions has been "national security" – the safety of individuals and states from danger and threats to maintain a certain standard of living [14]. Post, Kingsbury, and Schachtsiek state that private and commercial sectors' security can be achieved by paying services that prevent undesirable, unauthorized, or harmful losses to an organization's assets [15]. After the Cold War and since the Human Development Report in 1994, researchers in Political Sciences and International Relations have attempted to redefine security [16]. The concept evolved and extended in line with the political security landscape during this period, focusing on peace, human rights, and society booming. Other authors highlighted the new security approaches such as social security, human security, and international and national security [17], [18]. Fischer et al. defined security as a stable and predictable environment where individuals or different groups may seek its ends without disruption, harm, fear, and injury [19].

Security may be defined as all of these, but the consequence is a society without a clear understanding of it. Hence, Manunta points out the need for and the possibility of a shared conceptual definition [20]. Brooks found that an applied security explanation can be given through knowledge categorization [21]. The meaning of the security concept has become broader and recently covers more fields than before. Thus, a shared conceptual definition is

difficult or almost impossible to be achieved. Security can have several meanings, but what does it mean now in cyberspace in our era?

1.1 Cybersecurity

In this era, and especially now, the concept of security has taken another dimension. Nowadays, the "Internet of Things" (IoT) affects the world culture, and people live in a new cyber environment and depend on digitalization. Cyberspace is a domain within the information environment comprising IT interdependent networks and data such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers [22]. Besides the advantages that cyberspace brings, it also poses security risks. Now we are in the middle of a paradigm shift where Information Technology and its tools affect national security [23]. Therefore, in this dissertation, security is explained under the technological advancements and new issues that rely on technical challenges and human factors.

At the end of World War I, one of the most significant inventions was the Enigma machine, designed to protect confidential communication [24]. Before and during World War II, many countries adopted and used it for military and government services. A young man called Alan Turing specified and developed an electromechanical machine called the "Colossus" to break the enigma - believed to be the first mechanical computer [25]. The first cybersecurity concept dates back to 1970 with the invention of the ARPANET network [26]. Bob Thomas created "Creeper" — a computer program and self-replicating one to move across this network. When organizations started using the telephone to develop remote networks, challenges and risks in these new technologies became more critical. Since then, each piece of connected hardware presented a "hole" and entry point that needed protection. Governments and organizations started to be cautious that security was essential. From 1972 to 1974, there was an increase in discussions around security by researchers and IT professionals.

In 1979, ESD and ARPA, with the U.S Air Force and other organizations, were the first to create early computer security [27]. The computer technology security plan explored system security by identifying possible and automatable techniques for detecting risks in software. The distinguished computer security consultant, author, and hacker started to hack the

computer at the Digital Equipment Corporation used for operating systems development in the same year. Several cyberattacks followed this, and thus, he was arrested and jailed. The year 1980 marks the shift from ARPANET to the Internet, followed by an increase in high-profile attacks, and for the first time, the Trojan Horse and Virus were found [28]. During the Cold War, the risks of cyber espionage evolved. Hence, in 1985 the US Department of Defence published the "Orange Book," containing guidance on the risks that can be placed in software that processes classified or other sensitive information [29].

In 1987, several security technologies and product events marked cybersecurity's birth [30]. Bernd Fix performed one of the first documented antiviruses when he neutralized the Vienna virus – malware intended to corrupt files with computers. Andreas Lüning and Kai Figge, who founded G Data Software, released their first commercial antivirus (Ultimate Virus Killer-UVK) for the Atari ST platform. Then, the first NOD antivirus version was created by three Czechoslovakians, and in the U.S., McAfee was founded that released VirusScan. In the following year, many antivirus companies around the world were established. The working principle of the early antiviruses was simple. They could perform only context searches to detect unique virus code sequences. As the world started to notice the risks and drawbacks of viruses, more inventions were added to the cybersecurity market.

Since 2000, with the Internet available globally, and because data started to be kept digitally, attackers had more devices and software vulnerabilities to exploit [31]. New infection techniques appeared. The viruses could be present when users download infected files and visit infected websites. Because the antiviruses were slowing computer performance, companies started to design their products with the idea of moving the computer software into the cloud. They began to combine cloud technology with threat intelligence in their antivirus products. The Anti-Malware Testing Standards Organization (AMTSO) was established and started to work on cloud products.

Moreover, another innovation was the Operating System Security, where the cybersecurity was built in OSs, providing an additional layer of protection. In other words, OSs were able to perform patch updates and keep up to date the antiviruses engines and software, firewalls, and secure accounts with user management. Then with the rapid increase of smartphones, antiviruses were also developed for mobile systems.

The next generation is considered to date in the 2010s. Many high-profile breaches and attacks started to occur, consequently impacting countries' national security and costing businesses financial losses. In 2013, a former CIA employee and former contractor for the U.S. government copied and leaked classified information from the National Security Agency (NSA). It became the most significant threat in history that had the most societal impact and controversy. Snowden made public that the smartphone could be used as a spying tool by governments by causing threats to individuals' privacy and fundamental human rights [32]. The most extensive data breach occurred during 2013-2014; a group of hackers broke into Yahoo and compromised the accounts and personal information, from names to passwords and security questions of 3 billion users. In 2017, a ransomware crypto worm called "WannaCry" affected 230.000 Windows computers in 150 countries and demanded crypto payments in Bitcoins.

With the proliferation of the IoT, more interconnected devices, and the ongoing digitalization of many aspects of life, especially during the pandemic, cybercriminals have more opportunities to exploit [33]. Therefore, the security of data and information is becoming a critical issue for individuals and organizations [34]. In the literature exist several definitions regarding information security. The most dominating definition relies on the triad CIA security model mentioned first in a NIST publication [35], [36]. The triad model is comprised of three elements [37]:

- Confidentiality: information should not be available or disclosed to individuals, entities, or processes without authorization. It can be considered equal to privacy.
- Integrity: maintaining the accuracy, completeness, and trustworthiness of data.
- Availability: information and data should be accessible and usable from the authorized entities.

An attack that is successfully realized can compromise this triad. Theft and espionage from the attackers' groups can result in financial, proprietary, and personal information loss without the victims' knowledge. Attacks like denial-of-service can cause the slowness of systems or prevent legitimate users from accessing a system. Other security risks such as botnet malware can allow attackers to command a system for cyberattacks in other systems.

Additionally, attacks against control systems can cause damage or interruption of devices they control like centrifuges, generators, pumps, etc. In some cases, cyberattacks have no vast impacts, but if they are done against critical infrastructure could have sufficiently significant security effects on the national level, economy and life, and safety of people. Therefore, an infrequent successful attack with considerable impact can present a more significant risk than an ordinary attack with low influence.

Cybersecurity is developing to tackle the range of attack types while the attackers respond with their innovative hacking methods. Nowadays, cybersecurity uses different approaches to increase detection of the threats, such as multi-factor authentication (MFA), Network Behavioural Analysis (NBA), Threat Intelligence and automatic update, real-time protection, sandboxing, forensics, backup, and mirroring, and Web app firewalls [38].

1.2 Security Threats in Smartphones

Smartphones have rapidly become more popular than personal computers/laptops at home and the workplace. However, smartphone ownership varies across different economies [39]. Smartphone users are significantly higher across developed countries in Europe, the US, Australia, South Korea, and Japan. The low usage in emerging economies is attributed to their high poverty rates, making them unaffordable.

Smartphones make up more than 75% of all the mobile handsets used today [39]. In 2020, smartphone users surpassed three billion, marking an approximately 6% annual increase [40]. Figure 1 shows the increasing number of smartphone users from 2013 and its trend until 2023.

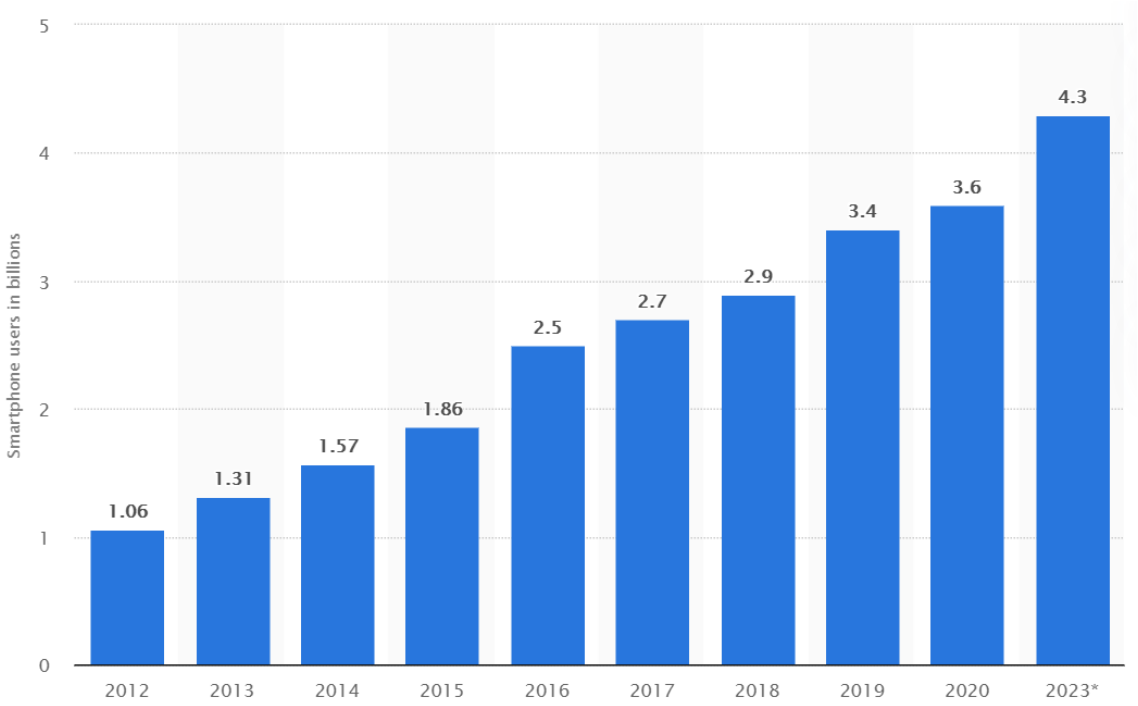

Figure 1: Number of smartphone users worldwide from 2016 to 2023 [40]

From 2013 to 2020, smartphone users grew by 17% annually, with the most significant growth in 2016 (around 35%). By 2023 this number is estimated to increase and hit 4.3 billion users. Given the expected global population by then, the smartphone penetration rate is forecasted to be more than 50%.

With the increased use of mobile applications, virtual private networks (VPSs), and hotspots, especially during the COVID-19 pandemic, the risks within these smart devices are more pervasive than ever. On the other hand, these devices communicate and transmit data via a network and are prone to several threats in network traffic [41]. More details regarding the most critical threats and conditions in smartphones are listed in the following part of this section.

1.2.1 Man-in-the-middle (MITM)

The MITM refers to the attacks that occur during the communication between a user and a legitimate organization. The most threatening part of a MITM attack is its ability to perform packet sniffing through encrypted communications [41], [42]. This kind of attack requires three actors: two communicators that want to send and receive information between them and the "man-in-the-middle" who intercepts the victim's communication. None of the

communicators is aware of the MITM, one of the most exploited ways hackers steal information and money in online communication. Here is a list of the most common types of MITM attacks.

- *IP Spoofing:* The Internet protocol address on a network identifies a device. This address is similar to a location address used to locate a place. An attacker can spoof an IP address by masking himself as an application and altering packet headers in an IP address [43]. The users trying to access a URL connected to such applications are sent to the hacker's website. Consequently, their information and data end up being available to the hacker. Considering that thousands of packets at a time should be modified, this method is not easy on a remote system.

  Nonetheless, it is effective when trust exists between endpoints, such as insecure networks. There are specific tools that can send a spoofed datagram to any target. Using such spoofing IP datagrams, a MITM attacker hijacks the communication to get exchanged public keys between communicators so that he can modify those keys. He can also hijack the encrypted messages and responses and then use the correct public keys to decrypt and encrypt them again for all the communication segments to avoid any possible suspicion.
- *Domain Name Server (DNS) Spoofing:* The primary purpose of DNS is to resolve domain names to IP addresses [44]. In this type of attack, the ID of any DNS request is sniffed, and the attacker replies to the target request with the incorrect ID before the actual DNS server. DNS spoofing technique makes the user navigate to a duplicated website created by the hacker and not to the real one intended by the user to visit [45]. The users are unaware that they are not visiting a safe and trusted website but interacting with the hacker to capture the user's login and other important information.
- *Address Resolution Protocol (ARP) Spoofing:* Unauthorized ARP messages are sent by an attacker to both sides of communication (to the user and the legitimate side) [46], [47]. These messages are used to link an attacker's MAC address with the IP of the legitimate user on a local area network. As a result, the user sends the data to the attacker instead of the host IP.
- *Hypertext Transfer Protocol Secure (HTTPS) Spoofing:* HTTPS is widely used on the Internet to secure communication over a computer network [48]. An attacker can deceive

a browser and make users think it is a trusted website [41]. The browser redirects to this insecure website, and the attacker can monitor the user interactions and steal personal and sensitive information.

- *Secure Socket Layer (SSL) hijacking:* SSL protocol establishes links between the browser and web server. The hacker does not attack SSL itself but the transition from non-encrypted communication to encrypted one [49]. The attacker passes false authentication keys to both the user and application sides. The connection appears secure when the MITM controls the entire session.
- *Wi-Fi Eavesdropping:* This type of MITM, also known as an "evil twin" attack, tricks random victims into connecting to a malicious Wi-Fi network [50]. Imagine you are at an airport/coffee bar/hotel and want to find free Wi-Fi. By scanning, your smartphone is going to show the Wi-Fi access points. That is an accessible channel for hackers to inject malicious codes into your smartphone. Once the user connects to such Wi-Fi hotspots with no security, the attacker will steal anything unencrypted from login credentials to file financial information [51].
- *Stealing browser cookies:* Browser cookies are small pieces of information that a website stores on devices. During browsing sessions, the user creates cookies that make his browsing easier next time. Cookies store information from the browsing sessions, and if a cybercriminal has access to them, he can gain access to users' passwords and other sensitive information. A hacker can impersonate websites or applications users want to use and access those cookies [53].

1.2.2 Malware

Malicious Software (Malware) tends to disturb users by entering private specific information; they may cause a breakdown of the device and lead to stolen or to become unusable information/documents of the users [52]. Such illegal software, not installed by the user, takes advantage of the vulnerabilities in the device/system. Apple is more protected against OS malware software thanks to its closed system. In contrast, Android OS has become the most target of Malware attacks. That is because the applications can be taken from many secure-insecure sources. The current platforms ask users to decide on access. For example,

iOS asks users to determine if an application may access a feature such as location. Android asks them to agree to an install-time manifest of permissions requested by an application.

Unfortunately, these permission-granting approaches place too many obstacles on users. Most of them are often ignored or not understood by users, and permission prompts are disruptive to the user's experience [53], [54]. Consequently, users unintentionally grant applications too many permissions and become vulnerable to applications that use the approvals in malicious or questionable ways (i.e., secretly sending SMS messages or leaking location information).

Malware in smartphones can be classified into four main categories: Virus, Trojan, Spyware, and Worm [55], [56].

- *Virus:* It was first found on mobile devices in 2004. Malicious software that can penetrate documents and send them elsewhere distorts their contents or makes them unusable and slows down the hardware elements [57]. Infected programs can also be installed in other devices. In 2010 in China, a virus named "Zombie" infected more than 1 million smartphones causing a loss amounting to $300,000 per day. This was also followed by data loss, data leakage, and disruption of the conversations [58]. Usually, these kinds of malware are camouflaged as a game, a security patch, or other attractive applications that are then downloaded to a mobile device. They can be spread through internet downloads, memory cards, and Bluetooth. The most common ones spread through Bluetooth are Bluejacking and Bluesnarfing. The first send spontaneous messages over Bluetooth to Bluetooth, whereas Bluesnarfing's ability extends to accessing unauthorized information in mobile devices via Bluetooth connection.
- *Trojan:* Trojan's activities in smartphones are related to recording calls, online chats that offer real-time text transmission via the Internet, locating via GPS, sending to other parties call logs and other essential data of the user. Trojan software aims not to spread itself but to seize the device's management and information [57]. Here they differ from worms and viruses. The most common form of Trojans is keyloggers transmitted via SMSs transmitted under the cover of a file, and the user can unintendedly activate it. An SMS runs in the background of an application and sends messages to a premium rate

number that belongs to the attacker. At that moment, it has the entire device in the background under control and not noticed by the user.

An example is the HippoSMS which increases the billing charges of users by sending SMS to premium account numbers. Also, it blocks messages from service providers to users and makes them pay additional charges. For this reason, while downloading an application necessary for smart devices, it is essential to search before it and check if it is reliable software.

- *Spyware:* They collect information and data regarding a target subject. They specify that their usage is for advertising and promotional purposes (adware) or to offer better service to users (cookies), while what they do is collect information about a person/organization and send it to someone else without their permission (here works like a Trojan) [57]. It can be caused by malicious people and aimed at controlling the infected devices. According to McAfee mobile threat report, for iOS, the biggest threat can come from applications with very aggressive adware, while Google Play saw several applications infected with malware [59]. In considerable studies by security firms, it is seen that malware software is not only used by hackers but also created by some profit-oriented "teams," i.e., in an incident in the year 2013, the Trojan "botnet Trojan-SMS.AndroidOS.Opfake.a" enabled the spread of the malware software "Backdoor.AndroidOS.Obad.a". It sent spam containing the malware to its victim list [60].

  Spyware activities invade users' privacy by collecting their information without their knowledge. This type of malware is one of the most dominant, especially in Android smartphones [61]. They can be dangerous and intrusive for the users. With the newly added features and social media applications, smartphones are becoming more and more posed to spyware attacks. They can monitor users' activities on their devices, including photos, videos they take, websites they visit, receive and sent messages, call history, and location.
- *Worm:* A worm is a virus that does not require user interaction to reproduce itself. So, users tend to be careless and not pay attention. Worms are designed to spread through the network [59]. Transmitting forms: SMS, MMS, and activated by clicking on a file or opening a plug-in sent by e-mail, i.e., social engineering. Worm penetrates using this

vulnerability and integrates itself into a service running in the OS. It can then act as a spy inside the device, send the required information to the managed center, and create an unnecessary data flow that can cause clogging and slowing down in the Internet bandwidth and reduce the device's performance.

1.2.3 Bring-your-own-device (BYOD)

Because of the smartphone's benefits in terms of cost and ease of use, individuals and organizations have embraced the BYOD concept. BYOD implemented in different organizations can bring many advantages such as increased efficiency and convenience. As it was shown until now, what is convenient for users can also be suitable for attackers. Consequently, BYOD adoption can lead to several security risks for IT infrastructure, enterprise data, and users [62].

Certain factors increase the risks posed by BYOD [63], [64]. When the business and personal data are allowed to coexist in the same device that is not a corporate asset, it is very problematic and challenging to balance the security control of the organization and personal data privacy. It might not be easy for IT departments to support different devices, operating systems, and carrier combinations that are changing and getting outdated quickly along with technological advancements. Furthermore, the increased processing power, memory, data transmission capabilities of networks, and open and third-party extensible operating systems make smartphones an interesting target for hackers. Experts and researchers in this field believe that if nothing is done against cyber-threats, organizations worldwide will continuously face cybersecurity breaches.

The costs of incidents can vary from loss of revenues to brand and reputation damage. Yeboah-Boateng stressed that most SMEs in developing countries pretend that their data are not attractive to hackers and do not face any attacks [65]. Since companies have more data on employees, clients, suppliers, partners, or other related entities, attackers are more interested in having considerable information on their hands. But the reality is different, there are no limits for the attackers, and everything and everyone is posed to such risks. The most critical risks associated with BYOD are listed as follows.

- *Data leakage:* There are many reasons why and when data leakages can occur. An attacker can access the data on a lost or stolen device with unprotected memory [66]. If the data on the BYOD is not correctly secured and encrypted, it is effortless for the attacker to gain access. Another scenario can be when the enterprise information and sensitive data are sent by mistake to personal contacts. Usually, users store important and valuable personal information on their devices, such as credit card data, bank account numbers, and passwords/PINs. So, because of their portable nature, they are the main store for the users. Simultaneously, if they bring and use the same device for work, they can store sensitive corporate data.
- There are also chances that some employees may share confidential business data they have stored on their mobile devices with competitors, leading to a competitive disadvantage for the organization. Another cause can be improper decommissioning and transferring a smartphone to another without removing sensitive stored data. The hacker can benefit from gaining access to the data on it quickly. Considering that personal devices are not part of the business IT infrastructure, they are not protected by companies' firewalls and systems (unless they have taken countermeasures). Hence, data leakage from BYOD can cause problems to users and the organizations' systems by making them vulnerable to data breaches.
- *Phishing and SMiShing*: An attacker can use Social Engineering forms, phone applications, SMS, or emails that appear unpretentious to collect user credentials like passwords, PINs, bank account information, and other sensitive data [67]. Phishing attacks are very well-known for traditional computers and are increasingly becoming a concern for smartphone platforms. The reduced screen sizes of these devices make it more convenient for attackers to mask helpful hints like whether the website uses SSL and users fail to check and submit the credentials. Also, app stores provide a way of phishing by allowing attackers to place counterfeit apps in the app stores that look like authentic apps.
- *Network Congestion:* Many mobile devices can be connected to an organization's network. Thus, the network resource can be overloaded and then exhausted and unavailable to legitimate users [68]. In addition, the uptake of smartphone usage and

mobile Internet has increased network congestion risk through either signaling or data capacity overload.

- *Vulnerabilities:* Other vulnerabilities, such as several types of Malware, are also a crucial concern for BYOD [69]. Spyware, Viruses, Financial, Surveillance Malware, Trojans, etc., can enter the private information of the target and gain access to what was previously aimed by the hacker. Other "Jailbreaking" or "Rooting" methods can also contribute. Besides different terms, in essence, they mean the same. "Jailbreaking" is applied to iOS devices, and "Rooting" is used for Android smartphones. It is a process that removes the restrictions on smartphones imposed by manufacturers or carriers [61], [70]. Users can sideload unauthorized apps, legal or illegal, from platforms other than official apps (i.e., App Store, Google Play).

  Consequently, they allow third-party apps to perform operations not available to them before, such as controlling CPU clock speed or overwriting files of the system. When a user Jailbreaks/Roots his smartphone, he has more freedom on the device without any restrictions from the manufacturer. The users also can choose the device that they want to work with. Thus, keeping track of vulnerabilities and updates is considerably more complex.

Several organizations are applying and improving their strategies to protect their assets. Others are coming to the need for a BYOD strategy to authenticate and authorize employees to use their own devices on enterprise networks [71].

1.2.4 Cyber threats in the era of COVID-19

The acute severe respiratory syndrome, SARS-COV2 (COVID-19), that appeared at the end of the year 2019 has brought significant changes to the everyday life of everyone. Technological solutions in the mobile and digital era are becoming more helpful in informing the population educational systems, monitoring, tracking the individuals, working, and spending time from home. On the other hand, cyberthreats are continually evolving to take advantage of online behaviour and trends. Smartphone usage is experiencing higher levels than usual. Businesses rely on instant messages, and individuals can spend more time on social media and other apps. Hence, individuals' privacy and security face more challenges regarding the risks to which they are now exposed.

Interpol warned in the Global Landscape on COVID-19 threats report that cybercriminals are using different hacking methods to attack computer networks and systems of individuals and organizations at the national and international levels. Simultaneously, the defense measures might be lowered because of the focus shift to the pandemic crisis. Accordingly, the most critical threats can be listed as follows:

- *Malicious Domains:* Due to people's interest in searching for COVID-19 information on the Internet, more domains registered with the keywords "Corona" or "Covid" are shown. A study report argues that many of them are developed with malicious intent. At the end of April 2020, more than 86.600 newly registered and fully qualified domain names classified as malicious or high-risk were discovered [72]. The United States of America had the highest number of such domains (29.007), followed by Italy (2877), Germany (2564), and Russia (2456).
- *Social Engineering:* The term stands for the art of exploiting human psychology rather than using technical methods of hacking for gaining unauthorized access to systems or data [73], [74], [75]. During the pandemic, these tactics are becoming more attractive for the attackers. According to Zimperium, from the beginning of the pandemic until April 2020, with connected schemes on the rise, phishing attacks have increased six times in mobile devices [76]. Attackers rely on tactics like impersonation to trick users into clicking harmful links or providing sensitive information. IBM found that users are three times more likely to respond to a smartphone's phishing attack than a desktop computer [77].

  Since mobile users have their small devices with them, they are most likely to read emails and messages as soon as they receive them. In addition, the limited display of detailed information (i.e., notifications and one-tap click/send option) can also increase the likelihood of successful phishing. Another issue is related to the continued growth of BYOD work environments. In May 2020, Deloitte CTI observed a threat named "Vendeta" that was based in Europe [78]. This threat aimed to steal business secrets by sending phishing emails that leveraged COVID-19 theme police investigation and detection notices. Workers can now view multiple inboxes connected to job and personal accounts. Thus, the notifications that appear from personal and work-related account does not seem unusual on the screen, and consequently, the user can be confused and tricked.

Individuals are encouraged to verify the sender with other communication methods via secure channels and not use the contact information found in a message.

- *Data-harvesting malware:* Remote Access Trojan, Spywares, information stealers, banking Trojans can infiltrate the systems by using COVID-19 information as an attempt to compromise networks, deliver money, steal credentials and data, and build botnets [79].
- *Wi-Fi interference:* Users can connect to networks that might not be optimally secured, such as home networks that might be improperly configured for remote workers or public Wi-Fi hotspots. According to Wandera's research in traffic analysis, corporate mobile devices use open Wi-Fi three times as much as they use mobile data [80]. During the first months of the pandemic, nearly a quarter of devices connected to open and possibly insecure networks, and 4% of devices experienced a MITM attack. Even though the numbers are not high because people are not traveling and are working from home, users still need to be cautious.
- *Password hygiene:* Users continue not adequately securing their important accounts. When they carry smartphones that contain work and personal accounts, that can be problematic. Prior studies indicate that users reuse passwords across multiple accounts [81], [82]. Rarely do people use a password manager, which suggests that many individuals do not use a strong password in most cases. Considering the cultures, users can also share their passwords with people they “trust” [83]. Nowadays, smartphones offer biometric authentication, which has become more convenient for users. Nonetheless, as with every system, they are prone to hacking and attacks, and the most important thing is to use them in conjunction with a password or pin code in a multifactor system [84].

It must be noted that individuals should increase their level of awareness, and organizations should strengthen their cyber maturity to protect, detect, address, and mitigate threats.

2 THEORETICAL FRAMEWORK: THREAT AVOIDANCE

This chapter provides insights related to the theoretical approach of this study. It defines the key concepts, evaluates the relevant theories, and explains the assumptions that have guided this research.

2.1 The weakest link: Understanding the Role of Human Factors

In the information security field, human factors play a significant role. The technical and innovative developments in information sciences do not always provide more secure environments. Hence, cyberspace and cybersecurity cannot be understood or defined only by technical problems. Individuals operate computers and other (inter)-connected devices; this means that the security of such devices and environments is a matter of human factors [85]. In many cases, the adoption of security technologies has failed to protect organizations from cyberattacks [12]. People may deny using security technologies, fail to follow the security protocols, engage in harmful activities that cause significant threats to them and organizations, and underestimate the chances of being victims of a cybersecurity breach [86], [87]. Because of these challenges, exploring and studying the role of human factors in information security has been in researchers' attention [88], [89]. Human factors significantly influence people's interaction with information security, and therefore, they can pose many risks to security [90]. Also, other authors highlight the importance of human factors in computer security [91], [92]. Their study explained how human weaknesses could lead to the unintentional detriment to the organization and showed an increase in awareness level could help reduce these weaknesses.

Since smartphones are considered essential devices people own and use [33], they are becoming more threatened by security risks. Several research studies have indicated that security solutions that only go around hardware and software are regarded as unsuccessful [10], [93], [94]. The authors argued that an effective and flexible human factors methodology must be integrated into mobile devices' development process [93]. As technology cannot do it alone, the human factor must also be considered. It is of great interest to investigate the users' behaviours that lead to security risks when studying the human factor. Accordingly, other authors highlighted that mobile devices' security solutions should focus more on the users' behaviour than technical problems [95].

A study comparing college students' and IT professionals' security behaviours showed that almost all the groups put themselves at risk by failing to secure their smartphones properly [39]. Additionally, the authors stated that if smartphone usage and behaviour are in line with security and protection, security issues will not appear. Other researchers studied the factors that influence users' behaviour in mobile devices. They indicated that they make "quid pro quo" when weighing different security behaviours and do not always choose the optimal security-related option [96]. Among the best practices against the threats posed by device proliferation, Romer suggests that if users monitor what applications install in their devices, the data security breaches will not be an issue [97]. Likewise, authentication tokens have been suggested as helpful data security solutions [98].

The human side is complex, and studies have shown that sometimes it is overlooked [99]. Thaler, the Nobel Prize Winner in Behavioural Economics, suggested that the behaviour side be viewed seriously [100]. Besides the relevant literature and recommended practices, there is a lack of research to study users' security behaviours and apply them to mobile devices correctly.

> *"The first lesson of economics is that all costs are (in some sense) opportunity costs. Therefore, opportunity costs should be treated as equivalent to out-of-pocket costs."*
>
> – R. Thaler (1994, p. 8)

Hoskin states that decision-makers can be more concerned about out-of-pocket losses than whether they have made the right decision from all the opportunities. From the viewpoint of IT devices security, choosing security leads to giving up on other options. And the questions that logically follow are "Was it better?, Did I/we make the right decision?". Therefore, all costs in the IT Security field should be considered as opportunity ones too. Organizations take measures, and still, the accidents continue to occur. Studies have shown that programs related to employment training and people awareness are being integrated, but the situation is critical. Humans do not make any random movement; everything serves the purpose of "adapting" to the systems and external conditions.

Apart from how intelligent an individual might be, the action still satisfies a general principle. In todays' society, this is a characteristic behaviour: "The ends justify the means". People want to have better security, feel safe, and take such actions for better means. But do they

know, understand, and adapt to what is better? While considering and analyzing the human side, it should also shield light from some critical factors related to cultural differences. Fukuyama explains why some societies do better than others, and he emphasizes the level of trust inherent in the society and social virtues differences between nations [101]. Thus, improving the results is needed to count, understand, and work with human behaviour and its influencing factors.

2.2 Understanding Culture and Differences: Albania vs. Hungary

The ecosystem in which people live is comprised of three broad systems: the physical, biological, and cultural [102]. Nature creates the physical and biological systems. At the same time, the cultural system considers the people's ideas and endeavors. A variety of the term "culture" has been suggested and contested in the existing literature [102], [103]. Taylor defines culture as "that complex hole which includes knowledge, belief, art, law, morals, custom, and any other capabilities and habits acquired by man as a member of society." [104] This definition includes psychological items with external ones. He explains that this would be problematic from a philosophical perspective because it cannot be characterized as natural. Other anthropologists have focused on artifacts and behaviours [105], [106].

"Culture is the man-made part of the environment" Herskovitz (1949, p. 17).

"Culture is the total shared, learned behavior of a society or a subgroup" Mead (1953, p. 22).

The artifacts and behaviour dimensions were combined in Malinowski's work. He defined culture as "a well-organized unity divided into two fundamental aspects - a body of artifacts and a system of customs" [107]. Later, the term took a semiotic turn that aimed at detailed interpretations. Geertz stressed that culture should be seen as a transmittable pattern interpreted through the meanings of symbols [108]. But this definition is not sufficient to trace the association between specific events in social groups. Individuals differ within a social group and follow his "thick description" that moves from the external focus to a psychological arena. The culture can be presented from the viewpoint of its members but does not consider psychological testing.

In 2001, a radical culture break from psychology shifted to “cultural materialism” that aims at generalization [109]. According to the cultural materialist, social practices cannot be explained through a thick description. Indeed, the factors that determine individuals’ social practices cannot be known. Accordingly, cultural differences can be explained by material factors from ecological to technological conditions without describing practices, history, or psychological states. Thus, semioticians and materialists remain in a debate about whether anthropology is related to humanities or science.

Cultural materialism has some drawbacks. In 1995, D’Andrade stated that “culture is often said to consist in rules. These rules are implicit because ordinary people can’t tell you what they are” [110]. According to this definition, both external items and the cognitive processes that interact with them should be considered when studying cultural differences. Additionally, other authors relate culture with the information that affects people's behaviour and can be widespread and represent a given social group [111]. Two theoretical perspectives have influenced the research on culture and personality, trait and cultural psychology [112]. Church et al. argue that even though these perspectives are seen as incompatible, integration is possible and essential for progress in this field.

The most important thing is that we as individuals should acknowledge the impact of the culture that shapes our perceptions, behaviours, family and friends, beliefs, and politics. As it can be seen, at one extreme, some authors do not consider the external items, and on the other hand, other definitions leave the psychology out. These different theoretical approaches can explain various cultural occurrences and sociological events. Nevertheless, none of the views is predefined as the “right” one. Also, they do not necessarily assume that analysts should be faithful to the informal understanding of the culture, but they can guide the research. For instance, a focus on behaviour can promote the examination of human activities. Attention to symbols can take, for example, language as a subject for study. A materialist approach might consider ecologic factors, and focusing on mental states can encourage psychological and inner factors testing.

While biology and the common nature of the people drive them to satisfy their needs, diversity in the physical and institutional environments they live in produces different ways of behaviour to fulfill their needs. Accordingly, there are drivers for cultural differences and

similarities across the nations. The two broad paradigms of cultural analysis are the emic versus etic approach [113]. The first paradigm assumes that dimensions of culture vary across countries. The second one, and more popular, relies on national cultural dimensions. Schwart, Hofstede, and House et al., state that the core characteristics of culture are considered universal and captured by a set of standard national culture dimensions [114], [115], [116].

Professor Geert Hofstede refers to culture as "the collective programming of the mind distinguishing the members of one group or category of people from others" [117]. His original dimensions included power distance (PDI), individualism vs. collectivism (IDV), masculinity vs. femininity (MAS), Uncertainty avoidance (UAI), and Long-term vs. Short-term orientation/pragmatic vs. normative. Another dimension - indulgence vs. restraint - was added later based on extensive research done by Professor Geert Hofstede, Gert Jan Hofstede, and Michael Minkov's suggestions [118]. In each dimension, the lowest possible score is 0, and the highest is 100.

To explore the drivers of Albania's culture relative to Hungarian culture, the 6-D model of Hofstede was applied [119]. The comparison between the two countries is represented in Figure 2.

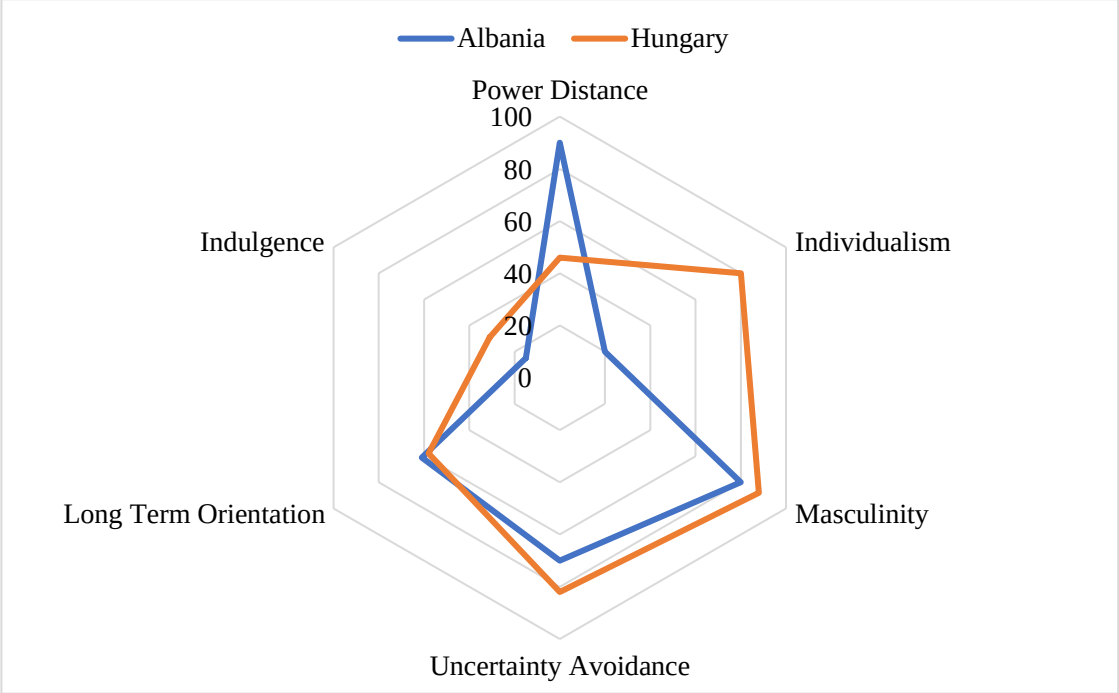

Figure 2: Countries comparison: Hofstede 6-D Model

- *Power Distance:* This dimension refers to the fact that the individuals within societies are not equal. In other words, it considers the culture's attitude towards inequalities among people - the extent to which less powerful members of a society accept that power is distributed unequally. Not surprisingly, Albania is shown with a high score of 90 and is considered a hierarchical society. Albanian people accept a hierarchical order where centralization is popular, subordinates expect to be told, and the ideal boss is a benevolent autocrat. Contrary to Albania, Hungary scores low (46), which means that power is decentralized, and managers count on their team members. Hungarians do not like to be controlled, and the communication with superiors is direct, informal, and participative. The essential characteristics of the Hungarian style are independence, hierarchy in line with convenience, equal rights, coaching leader, superior accessibility, management facilities, and empowerment.
- *Individualism vs. Collectivism:* The dimension of individualism addresses the degree of interdependence that society has among its members. Albania is classified as a collectivist society with a very low score (20), where loyalty is the key to maintaining solid relationships. This is shown in their long-term commitment to the group members, family, extended family, or other relationships. Members take responsibility for the other group members, and relationships are perceived in moral terms like a family link. On the other hand, with a high score of 80, Hungary is classified as an individualist society. Individuals are expected to take care only of themselves and their immediate family. In such societies, the offense can often cause guilt and low self-esteem. Business relationships are considered contracts with mutual benefit; hiring and promotion decisions are supposed to be based on meritocracy.
- *Masculinity vs. femininity:* This dimension addresses whether society wants to be the best (masculine) or like what they do (feminine). The results did not show a significant difference between the countries. Hungary scores only 8 points more than Albania's score of 80. Thus, both countries are considered "Masculine" societies. Albanians and Hungarians are proud of their successes and achievements in life, and they strive to be the best they can be. Conflicts are resolved between individuals, and the main goal is to "win."

- *Uncertainty Avoidance:* This dimension is related to how a society deals with the fact that what will come in the future can never be known. Uncertain avoidance focuses on whether individuals should try to control the future or just let it happen. In other words, it refers to the extent to which the members of a culture feel threatened by unknown situations and have created beliefs and institutions to avoid these. The results suggest that both countries have preferences for avoiding uncertainty. But, Hungary (UAI score 82) has more than Albania (UAI score 70). In these societies, time is money, people are hard-working and busy, innovation may be resisted, and security is crucial in motivation. Both countries keep rough codes of beliefs and behaviours. Also, there is an emotional need for rules even though they never seem to work. Decisions are supposed to be made carefully after analyzing the whole available information.
- *Long-term vs. Short-term Orientation:* This dimension represents how societies should maintain some links with their past while dealing with the challenges in the present and future. Additionally, it refers to how different societies prioritize long and short-term goals differently. Albania (61) and Hungary (58) are both considered to have a long-term orientation with a slight difference in scores. They are deemed pragmatic societies, and they believe that the truth depends on the situation, context, and time. Individuals can quickly adapt traditions to changed conditions and have a strong propensity to save and invest in the future.
- *Indulgence vs. Restraint:* The last dimension refers to how individuals control their desires and impulses based on how they were raised. When people show relatively weak control over their impulses, they are considered indulgent. On the other hand, the tendency toward relatively strong control over impulses refers to "Restraint". Albania (15) scores two times lower than Hungary (31). Therefore, Albanian and Hungarian cultures are shown as Restraints with some differences. Accordingly, Albanians have a relatively stronger tendency to cynicism and pessimism than Hungary. Unlike Indulgent, both societies do not spend much time on leisure and control their desires. Moreover, they are influenced by their social norms and might feel that not controlling impulses is wrong.

2.3 Technology Threat Avoidance Theory (TTAT) Approach

It is evident that cyber-attacks are rising, and they pose many challenges and risks for individuals and organizations. Due to this, the question that still prevails is what influences the peoples' behaviours not to protect adequately. Dinev et al. highlight the importance of studying users' motivations to adopt secure technologies and analyzing the factors influencing them [120]. Analyzing the behavioural factors that influence users' compliance to security policies at the organizational level has also been the other authors' focus [121] [122].

In psychology, several theories are commonly used to explain individuals' behavioural characteristics and the factors that affect their decisions to take protective or preventative actions towards IT threats [123], [124]. Rogers developed PMT (Protection Motivation Theory) in 1975. It assumes that the individual's motivation to protect from danger is related to cognitive factors such as threat severity, threat susceptibility, response effectiveness in preventing the threat, the response's cost, and the ability to execute the response [125], [126]. TTAT (Technology Threat Avoidance Theory) of Liang and Xue was based on the risk analysis literature of Baskerville [127] and other researchers in the field of health psychology [128], [129], [130] – by considering the two cognitive factors: copping appraisal and threat appraisal. Also, this theory proposes that the outcome of the threat appraisal is the users' perceived threat, defined by the perceived severity and susceptibility of the threat [131]. Additionally, this theory includes three factors that users consider in evaluating how avoidable can be a threat by a safeguard measure: effectiveness, cost, and self-efficacy.

The primary purpose of TTAT is that when individuals perceive a threat, they can be motivated to actively avoid it (by taking a safeguard measure) if they perceive it as avoidable by this measure. They can passively avoid the threat by behaving based on emotion-focused coping. It must also be noted that TTAT was explicitly designed for studying the factors that influence users to avoid IT threats by taking protective actions [132]. Regardless, the more they feel threatened by an IT risk, the more motivated they are to prevent them and behave more securely. Refining of this theory was suggested by Carpenter et al., where individual differences' effect on perceived threat was taken into account [133].

As this research aims to understand smartphone users' security motivation and behaviour towards IT threats, the theoretical approach of this dissertation is based on the principles of TTAT. Besides, this study aimed to compare two groups: Albanian users and Hungarian ones. Therefore, it was decided to shape the research around the idea of individual differences as well. The TTAT model is represented with some additive changes by considering the refined model by Carpenter et al.

2.3.1 Research Questions

The research questions were based on the factors that can affect the users' behaviour on using smartphone security technologies. Hence, it was of great interest to examine how they represented the users' security behaviours and smartphone practices. The main question that drove this research was: "How do the cognitive factors (copping and threat appraisal) and individual differences influence the Albanian and Hungarian users' security behaviour in smartphones?

The research model derived five specific research questions from the main question. The first research question integrated threat appraisal factors (perceived severity and susceptibility) and its outcome (perceived threat) that shape security motivation, leading to security behaviour. The second question aimed to investigate the effect of users' Perceived Threats on their motivation to defend against attacks and use smartphones' security technologies. The third research question has considered the three coping appraisal factors (Safeguard Effectiveness, Safeguard Cost, and Self-Efficacy) that shape Security Motivation, leading to Security Behaviour. The fourth question aimed to examine the influence of Security Motivation on users' behaviour using smartphones' security technologies. Finally, the fifth research question investigated the effect of risk and distrust propensity in users' perceived threat and the impulsivity impact in their motivation to use smartphones' security technologies. Based on these constructs, the research questions in this study are as follows:

- *Research question 1 (RQ1):* Do the Perceived Severity, Perceived Susceptibility, Risk, and Distrust propensity influence the users' Perceived Threats on smartphones?
- *Research Question 2 (RQ2):* Does the users' Perceived Threat influence their motivation to use smartphones' security technologies?

- *Research Questions 3 (RQ3):* Do the Safeguard Effectiveness, Safeguard Cost, Self-Efficacy, and Impulsivity influence users' motivation to use smartphones' security technologies?
- *Research Questions 4 (RQ4):* How do users' Security Motivation influence users' Security Behaviours?
- *Research Question 5 (RQ5):* Do the users' differences (Risk and Distrust Propensity and Impulsivity) influence their Perceived Threat and Motivation in using smartphones' security technologies?

2.3.2 Hypothesis 1 (H1)

Based on the prior literature of Oliver & Berger (1979) and Janz & Becker (1984) here, the perceived threat is related to user perception of smartphone's security risks; how harmful or dangerous can be an attack or malicious IT, and its influence on decision making (in this case, the motivation) [134], [129]. As proposed and explained by Liang and Xue in 2010, threat perception is shaped by two antecedents: perceived severity and perceived susceptibility. Perceived severity stands for users' subjective belief regarding the damage that a malicious IT could affect their devices and systems. Similarly, perceived susceptibility is related to users' subjective belief that malicious IT will probably affect their devices and systems. According to Burns et al., a high threat severity level motivates individuals to protect themselves [135]. This research supports the scholars' arguments and findings, and thus, it was hypothesized:

H1a: Perceived susceptibility of being attacked positively affects perceived threat in smartphones.

H1b: Perceived severity of being attacked positively affects perceived threat in smartphones.

2.3.3 Hypothesis 2 (H2)

Maslow and Mitzen define safety as a basic human need [136], [137]. Over the years, several authors confirmed the positive relationship between pleasant feelings and unpleasant feelings against security [126], [130], [138]. According to Liang & Xue, individuals' responses to health threats can be similar to their reactions to IT threats[131]. Also, Tu et al., and Posey

et al., found out that users that receive “signals” about a possible risk show a higher motivation in engaging in response actions [95], [139]. Supporting the arguments of the prior literature, it was hypothesized:

H2: Perceived threat positively affects security motivation in smartphones.

2.3.4 Hypothesis 3 (H3)

Here the safeguard effectiveness is defined in the context of smartphones security; if its application can be effective in using security technologies against threats. Bandura in 1982 and Janz and Becker in 1984 explained that the outcome of using a safeguard is the user perception that can be noted as similar to outcome expectancy and the health belief model [140], [129].

In 1984, Lazarus and Folkman developed the transactional stress model [141]. Copping was explained as a phenomenon that includes cognitive and behavioural responses to manage internal and/or external stressors [142]. When individuals feel safe and secure, they do not stress themselves to cope with the threats. Thus, a safeguard would make them feel more confident and adapt the security against the threats. Kroenke (2014) and Robertson (2020) confirm the relationship between safeguards, and threats in the IT field, and they argue that in order to avoid security threats, technical, data and human safeguards must be deployed [143], [144].

H3: Safeguard effectiveness positively affects security motivation in smartphones.

2.3.5 Hypothesis 4 (H4)

Liang and Xue (2009) stress that safeguard cost is related to physical and cognitive efforts such as money, time, inconvenience, and understanding level. Accordingly, the individuals compare benefits and costs before engaging in a behaviour. This, is confirmed by other studies in the field of health behaviour [129], [145]. So, before taking action, people are usually making a cost-benefit analysis. Albuquerque Junior et al. concluded that some public institutions are not deploying the necessary tools for protection because of the high costs involved [146]. Woon et al. highlighted that people would enable wireless network security

if its costs reduce [147]. Consequently, the higher the price/cost of a safeguard, the less motivation for users to use it.

H4: Safeguard cost negatively affects security motivation in smartphones.

2.3.6 Hypothesis 5 (H5)

Self-efficacy is defined as an individual's confidence to take a safeguard measure. Bandura argues that the behaviour will be predicted in any given instance by considering self-efficacy and outcome beliefs [140]. Agarwal et al., Compeau and Higgins, and Compeau et al. studied the relationship of self-efficacy with the IT adoption intent [148], [149], [150]. Other authors have also explained that if the users' level of self-efficacy increases, they will be more motivated to perform IT security behaviour [5], [4]. As a result, their motivation to avoid IT threats using a measure will be stronger.

H5: Self-efficacy positively affects security motivation in smartphones.

2.3.7 Hypothesis 6 (H6)

In the TTAT model, there is no difference between motivation and intention [132]. In this case, security motivation can be explained by the behavioural intention to use security technologies. Two cognitive theorists concluded that behavioural intention is a significant and strong predictor of actual behaviour [151], [152]. This relationship has been confirmed by other researchers as well [153]. Accordingly, Verkijika demonstrates the strength of the relationship between intentions and actual for single-action behaviours [154]. Other evidence in the literature supports the positive relation between security intentions and behaviour. It is adequate and enough evidence in the literature [11], [95], [13]. Thus, this study supported prior literature and hypothesized:

H6: Users' motivation to use smartphones' security technologies positively influences their security behaviour.

2.3.8 Hypothesis 7 (H7)

The effects of personality characteristics on cybersecurity behaviours have been in many IT researchers' attention [8]. In their studies, Giwah and Uffen et al. summarized that factors

affecting the actual usage of mobile devices' security technologies are very different. They depend on other external variables such as individuals' personality differences [7], [9]. Additionally, the researchers suggested future work to consider mobile device users' personalities in existing behavioural theories. Consequently, we can have a deeper and more comprehensive understanding of mobile users' IT security behaviour.

In the literature, it is shown that individuals' impulsivity, risk, and distrust propensities, influence their perceptions and decision-making [155], [156], [157]. Therefore, three more constructs are incorporated into the existing TTAT model. Consistent with the analysis and suggestions of Carpenter et al., this research includes the three constructs (Impulsivity, Risk, and Distrust Propensity) [133]. Since this study focuses on users' behaviour to use security technologies on smartphones, I found it relevant to examine how these three individuals' differences impact security threats and motivations that shape security behaviour in using smartphones' security technologies. Thus, the seventh hypothesis presumes that individual differences affect users' perceived threat and security motivation that shape smartphone security behaviour.

> *H7: Individual differences affect users' perceived threat and security motivations that shape their smartphone security behaviours.*

The hypotheses incorporated three constructs: impulsivity, risk propensity, and distrust propensity.

Impulsivity is a very complex concept. It refers to people's propensity to make decisions without considering the consequences [158]. According to Coutlee et al., impulsivity is the urge to respond spontaneously without thinking about the effects [159]. Moreover, it reflects the reduced ability to plan actions [160]. Evidence shows that individuals with a high level of impulsivity may get more benefits from the use of mobile internet features. Still, on the other side, they make minor security-sensitive decisions [96]. Also, Hadlington's results have demonstrated that impulsivity positively affects risky cybersecurity behaviours and highlight that individual differences may govern cybersecurity practices [156]. Hence, the higher the user's impulsivity, the less he will adopt and use security technologies.

H7a: Impulsivity negatively influences motivation to use the smartphone's security technologies.

Prior literature shows that risk propensity has had significant attention in the work of many scholars [161], [162], [163], [164]. The definition stands for an individual's tendency to get involved in risk or avoid it, and it can also change over time. Studies have demonstrated that differences in individuals' reactions and behaviours in risky situations depend on their risk propensity [165], [166]. This trait plays a significant role in understanding and applying policy settings in decision-making [167], [168]. If risk propensity is not considered, it can lead to challenges in practice [169].

Nguyen and Kim studied the relationship of risk propensity and security technologies' protection efforts of the users exposed to many threats such as malware, data loss, and unauthorized access [170]. To protect themselves, they can use security technologies or practices. In line with the authors, a high-risk propensity user would be represented as less aware or conscious of threats. As a consequence, it would affect their motivation to use security technologies. Therefore, it was hypothesized:

H7b: Risk propensity negatively influences users' perceived threat in smartphones.

Distrust propensity has been defined as negative beliefs about another party's conduct [171]. Also, the authors showed that distrust has a negative effect on technology adoption. The importance of distrust is not limited to preventing individuals from experiencing negative consequences. Distrust prevails in many fields and events and can replace trust as a social mechanism to deal with risk [172], [173]. In a study of Hsiao, the distrust was explained as fear of technology adoption by analyzing it in different cultures [174]. Abelson et al. stressed that due to cybersecurity issues, several distinguished cryptographers had been involved in the debate concerning law enforcement's access to protect and secure data through different technological solutions [175].

Many actors such as governments, organizations, and developers have created backdoors in security measures. On the other hand, the system raises complex administration problems

and concerns about human rights and the rule of law. It is a case for discussion that distrust can influence the perceived risk/threat that later shapes security motivation.

Hence, it is hypothesized:

H7c: Distrust propensity positively influences users' perceived threat.

The research model used for this work is presented in Figure 3.

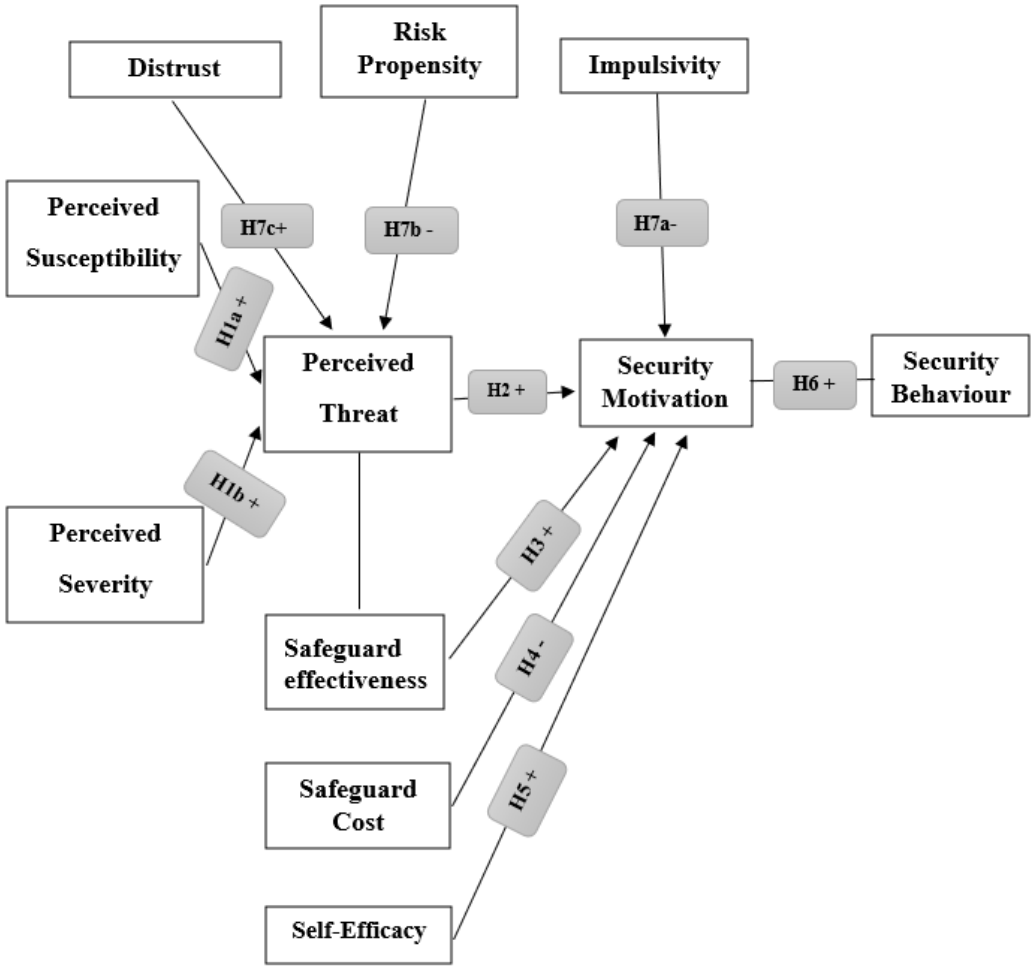

Figure 3: Research Model

3 METHODOLOGY AND DATA

This chapter provides an outline of the research methods followed in this study. It begins with the research design, the procedure chosen for this study, and its reasons. The instrument that was used for data collection is then discussed. The ethical considerations followed in the process, the participants' characteristics, and how they were sampled are also described. In addition, measures and the strategy used to analyze the data are discussed. Lastly, it offers the preliminary analysis of the study and model assumptions of partial least squares.

3.1 Research Design and Procedure

The research on smartphone security can evolve in different directions such as technical [176], behavioural [177], [156], [157] and policy-oriented [178]. Considering the aims of this research, the direction of this study is behavioural. The insights from the prior literature on IT security behaviour are applied to the smartphone context. The research methodology applied in this study could be in line with the positivist philosophy of research [179]. The authors [180] pointed out that a structured methodology should be applied to the research using quantitative methods, including statistical analysis. The aim was to obtain reliable, consistent, unbiased, and replicable results from other studies to present reality.

Fox and Burns highlight that positivism has been criticized for many reasons [180], [181]. It excludes sources deriving from human experiences, subjectivity from knowledge growth, and ignores opinions or intuition. This study has a behavioural orientation and describes the truth regarding the nature of selected groups and their complex behaviours. Therefore, to study the chosen groups' security behaviours, it was relevant to be guided by the post-positivism research philosophy, known as post-empiricism and methodological pluralism [182]. And in this work, besides providing descriptive information and statistical analysis concerning the samples, understanding complex actions and contributing to knowledge growth were essentials.

A survey instrument was employed to examine the revised TTAT model and the resulting hypotheses in this study. The research was carried out in three phases (Figure 4).

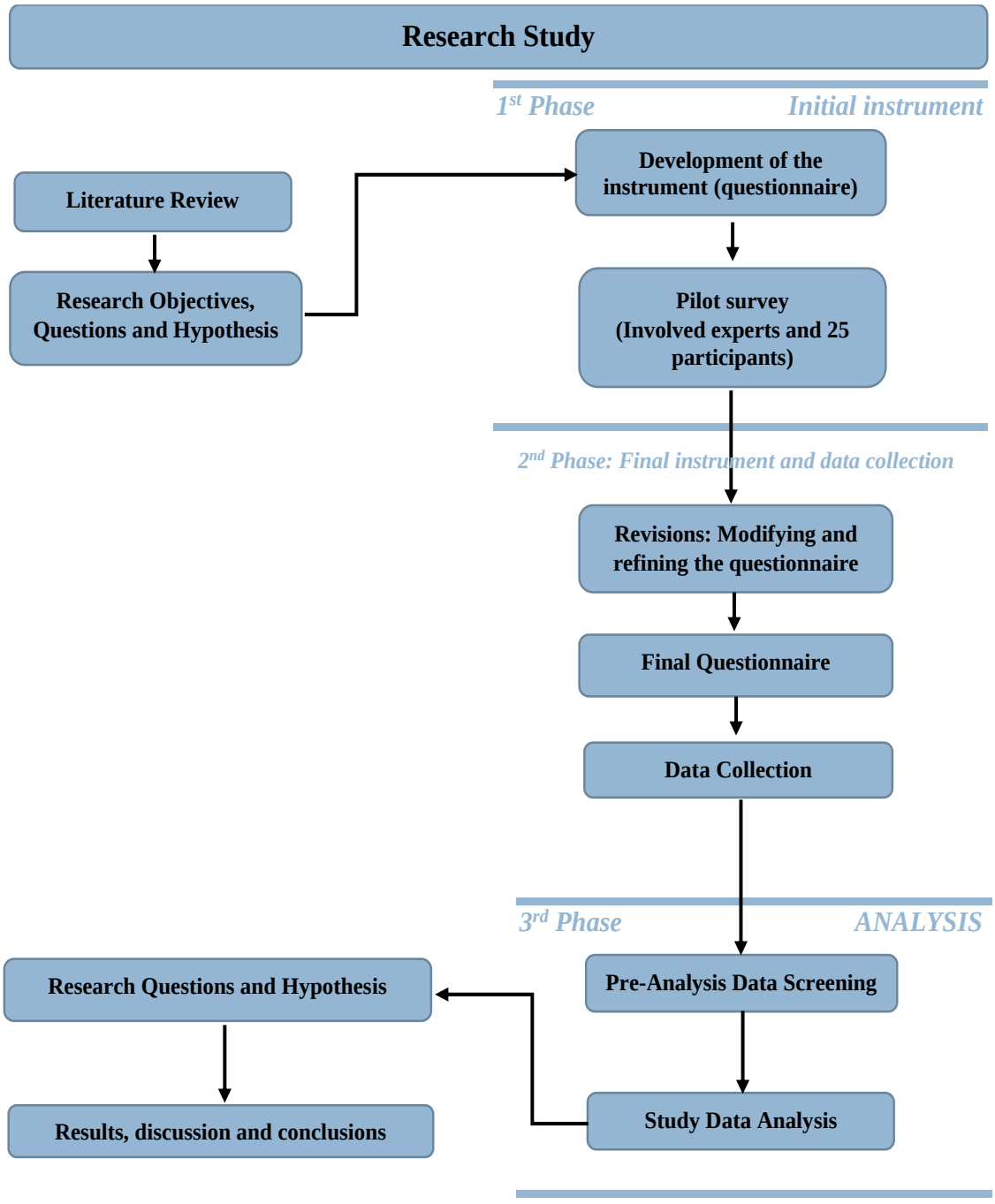

Figure 4: Research Methodology

In the first phase, an exploratory study was conducted. The relevant literature review regarding smartphone threats and empirical studies were examined to define the research questions and hypotheses. The questionnaire was developed based on validated measures from the existing TTAT model. The first version of the questionnaire was used to examine the usability and identify possible issues with the instrument.

In the second phase (confirmatory stage), the instrument was improved after conceptualizing constructs in the research model. The final survey instrument was developed, followed by the data collection process that addressed the research questions and hypotheses. In the last phase, the confirmatory study was conducted. The quantitative data were analyzed using descriptive statistics and Structured Equation Modelling (SEM) PLS. A preliminary analysis was performed for data accuracy in the third phase (data analysis). It was examined if the assumptions for conducting path analysis were satisfied, followed by the study data analysis.

3.2 Pilot Study

A pilot study was conducted to better use and apply the existing model. None of the constructs and respective items was changed. The TTAT model of Liang and Xue includes eight constructs: perceived susceptibility, perceived severity, perceived threat, perceived effectiveness, self-efficacy, security motivation, and security behaviour [132]. The revised TTAT model from Carpenter et al. (2019) contained the original constructs and three more: risk propensity, impulsivity, and distrust. They indicated that the four loadings of distrust did not load significantly on that construct; thus, their analyses were run without them [133]. Nonetheless, the pilot survey of this work considered all the constructs (from the original and revised model) and their items.

The reason was to pre-test and "try out" the instrument [183]. Also, adopting items is more efficient than developing them by yourself [184]. According to Straub (1989) and Creswell (2014), all measures should include items from prior research to ensure validity and reliability. If changes are made within the instrument, the validity and reliability should be re-established [185], [186]. Conducting a pilot survey and using all the constructs can warn about the main research; if the research protocols are not followed or the used model is not relevant or too complex. The pilot survey was conducted with 25 participants representing

the target population: individuals who use smartphones for business or personal reasons. It was developed using Google Forms and sent directly to colleagues, relatives, friends, and students. Many of the participants felt many of the questions were too repetitive. The feedback from the pilot test resulted in changes to the existing instrument. Some items within specific constructs and used scales had to be reconsidered for this study.

3.3 Final survey and data collection

After consulting with my advisors and for the purposes of this research, we realized that for a better understanding and to ensure validity, some of the items had to be changed and removed following the context of smartphones (Appendix II: Final questionnaire). The final web-based survey (in Google Forms) was appropriate for the present research. It allows the collection of many responses in different locations and is a handy method for testing the hypotheses [187].

The original language of it was English, and for better understanding, it was translated into Albanian and Hungarian languages. The survey contained three blocks of sections. The first one included demographic questions. The second section had questions about users' habits and practices in smartphones and security. The final and most important section included TTAT constructs and their respective items. The three forms (Albanian, English, and Hungarian) were active from October 26, 2020, until December 14, 2020. The electronic surveys were sent to the participants through email and social media platforms. Furthermore, two weeks later, a reminder message and invitation were sent to those who had not completed the survey.

Data captured from the electronic survey was automatically transferred into excel files. Using this method for collecting the data can reduce the potential for human error and minimize issues related to data accuracy [188].

3.4 Ethical considerations

The survey was conducted conform to the research practices based on fundamental principles of the European Commission and ALLEA for research integrity [189], [190]. It was made clear to the participants that their participation was voluntary and that their responses were used only for this study. The survey assured respondents of their anonymity and data

confidentiality. In addition, survey aims were clearly and honestly explained before, and it recognized the right of privacy, personal data protection, and freedom of movement.

3.5 Characteristics of the sample

The target samples for this study were individuals from less than 20 years old to more than 50 years old from Albania and Hungary. It was decided to consider also the international students studying and living in Hungary. A prerequisite for participation was that participants own a smartphone and use it for personal, business reasons, or both. The samples were randomly selected within the target countries. The demographics included age interval, gender, place of residence, place of growing up, level of education, monthly incomes, and employment status. Also, data related to users' habits and security in smartphone was gathered for a better profile understanding. Data consisted of: brand of smartphone, period of owning a smartphone, activity time on the internet during weekdays and holidays, the importance of social media accounts, if they have ever lost a smartphone, if they do let their smartphones in the other's hands, if they download apps only from official sites or untrusted ones as well, the number of installed apps, the frequency of changes in downloading apps and if in their knowledge the smartphones have been ever hacked.

3.6 Measures

To access all the constructs of the model were adopted previously validated measures. As mentioned before, they were modified based on the literature review and pilot test phase. At first, several items' wordings were changed to better fit the smartphone's security context. After the pilot phase, several constructs' items were dropped because they had related meanings among each other. The changes are represented in Appendix III.

The TTAT section of the survey consisted of three items to measure perceived susceptibility, eight items to measure perceived severity, two items to measure perceived threat, three items to measure safeguard effectiveness, six items to measure safeguard cost, five items to measure self-efficacy, three items to measure security motivation, and five items to measure security behaviour. Except for two security behaviours items, all the final items were adopted from Liang and Xue's work. The measures indicated 0.89 or greater Cronbach alpha coefficients. After the pilot phase, the two items included in the original study were not appropriate for a Likert-scale answer. Based on the evidence from the literature, the items

were not dropped or changed, but only the nature of the answer (Yes/No), and three additive ones were adopted from Claar and Johnson [191].

The survey's individual differences consisted of items that measure risk propensity, impulsivity, and distrust. To access them was considered the existing literature. Six risk propensity items were adopted from Nicholson et al., which presented a Cronbach alpha coefficient of 0.8 [192]. Also, and in line with the logic of their statements, two more items were added. The six items that comprised the distrust construct used by Ashleigh, Higgs, and Dulewicz showed greater Cronbach alphas greater than 0.7 [193]. The items proposed in the revised TTAT model [130] were adopted from Grasmick et al. [195] to access impulsivity. The authors indicated that impulsivity is one of the six self-control dimensions. The authors did not provide the reliability metrics even though all the items loaded significantly on the unidimensional factor.

The constructs measures were all adjusted to a six-point Likert scale (anchors: 1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = somewhat agree, 5 = agree, and 6 = strongly agree) with exception of security behaviour construct. The same Likert scale was used to access all the constructs with a consistent scale rather than a mixed one. The reasons for using a six-point Likert scale were found in the literature. As pointed out by Miller, the human mind can easily distinguish and memorize seven different categories and effectively focus on around six objects [194]. So, any increase in categories' number of responses beyond six or seven might be worthless. The neutral category was removed to avoid biases in measurement [195]. The mid-point can be attractive to respondents with no opinion. In addition, respondents that choose neutral are not truly neutral and therefore do not act as a transition group between the extremes [196], [197], [198]. The items within the security behaviour construct were changed to statements that required a Yes/No answer. Due to the nature and logic of the items, it is impossible to answer from strongly disagree to strongly agree.

3.7 Data analysis strategy

Considering this dissertation's aims and research model, Factor Analysis and Path Analysis in Structural Equation Modeling (PLS-SEM) were applied. The research phase of data analysis is comprised of three sections. The first part was conducted preliminary analysis for data accuracy and examined if the assumptions for conducting path analysis were satisfied. Path analysis involves the solution of multiple linear regression equations [199]. Therefore, the dependent variables must be distributed normally, and the relationships among the variables are assumed to be causal, linear, and additive. The second part presented descriptive statistics. Demographics, habits, and security practices within the smartphone context are introduced and explained. The third part tested the hypotheses by conducting a path analysis and explaining the research objectives, questions, and hypotheses. A summary of the research objectives, hypotheses, and applied tools is represented in Table 1.

Research objectives	Research Hypothesis	Related Theoretical Model and Applied survey questions	The research tools
O1: To introduce security and threats regarding smartphones.	-	Literature review: Chapter I – "Security and Smartphones"	Background sources.
O2: To gain insight into user behaviour of smartphone security and their using habits based on related research findings.	-	Chapter 2.1: Weakest Link-Human Factors importance Survey: Questions 8-20 related to users' habits and practices in smartphones and security.	-Background sources. -Descriptive statistics.
O3: To explore the research methods and theories for users' cyber-security motivations, threat perception, coping ability, and cybernetics.	-	Theoretical framework: Chapter 2.3 – TTAT Approach	-Background sources.
O4: To explain the samples used in the research model and define each users' group's cultural characteristics.	-	Cultural Differences: (AL-HU) - Chapter 2.2 Survey: Questions 1-7 related to demographics. - Chapter 4.1-4.3	-Hofstede 6-D Model -Descriptive statistics.
O5: To examine the influence of users' perceived threat and its two antecedents (perceived severity and perceived susceptibility) in users' security motivation in smartphones.	H1a: Perceived susceptibility of being attacked positively affects perceived threat in smartphones. H1b: Perceived severity of being attacked positively affects perceived threat in smartphones.	Liang and Xue (2009) TTAT Survey: Question 21 related to Perceived Susceptibility of getting a malicious IT (3 statements). Question 22 related to Perceived Severity of the threat consequences (8 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H2: Perceived threat positively affects motivation to use smartphone's security technologies.	Liang and Xue (2009) TTAT Question 23 related to Perceived Threat (2 statements).	-Durbin-Watson Test -Normal P-P Plot -Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).

O6: To examine the effects of safeguard measures (cost, effectiveness, and self-efficacy) in the users' motivation of using security technologies.	H3: Safeguard effectiveness positively affects motivation to use smartphone security technologies.	Liang and Xue TTAT model (2009) Question 24 related to Perceived Safeguard Effectiveness (3 items).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H4: Safeguard cost negatively affects motivation to use smartphone's security technologies.	Liang and Xue TTAT model (2009) Question 25: 6 statements referring to Perceived Safeguard Cost	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H5: Self-efficacy positively affects motivation to use smartphone security technologies.	Liang and Xue (2009) TTAT Question 26 refers to the Self-Efficacy construct (5 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
O7: To investigate users' security motivation and behaviour of using smartphones' security technologies.	H6: Users' motivation to use smartphones' security technology positively influences their behaviour of using smartphones' security technologies.	Liang and Xue (2009) TTAT Question 27 related to users' motivation in using security technologies (3 statements). Question 28 contains 5 (Yes/No) statements related to users' behaviours in using smartphone security tools/technologies.	-Durbin-Watson Test Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).

O8: To investigate the influence of individual's differences in motivation and behaviour of using security technologies.	H7a: Impulsivity negatively influences motivations to use the smartphone's security technologies.	Grasmick et al. (1993) Question 30 refers to impulsivity construct (4 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H7b: Risk propensity negatively influences motivation to use smartphone's security technologies.	Nicholson et al (2005) Question 29 refers risk propensity construct (8 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H7c: Distrust propensity negatively influences security motivation to use smartphone's security technologies.	Ashleigh, Higgs, and Dulewicz, (2012) Question 31 refers to Distrust construct (5 statements)	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
O9: To compare research results and highlight differences between Albanian and Hungarian users.	-	Research Results	Multigroup Analysis -AL vs. HU differences: β coef., p-values, t-values.

Table 1: The research objectives related to hypotheses, and the applied statistical tools

Before starting the analysis process, the raw data transferred in excel files were converted into a suitable format for decision-making and conclusions. Constructs and items were coded as indicated in Table 2.

Variable name	Variable Code	Items Code
Perceived Susceptibility	PSU	PSU1, PSU2, PSU3
Perceived Severity	PSE	PSE1, PSE2, PSE3, PSE4, PSE5, PSE6, PSE7, PSE8
Perceived Threat	PTH	PTH1, PTH2
Safeguard Effectiveness	SE	SEF1, SEF2, SEF3. SEF4. SEF5
Safeguard Cost	SCO	SCO1, SCO2, SCO3, SCO4, SCO5
Self-efficacy	SEF	SE1, SE2, SE3
Security Motivation	SM	SM1, SM2, SM3
Security Behaviour	SB	SB1, SB2, SB3, SB4, SB5
Impulsivity	IMP	IMP1, IMP2, IMP3, IMP4
Risk Propensity	RP	RP1, RP2, RP3, RP4, RP5, RP6, RP7, RP8
Distrust	DIST	DIST1, DIST2, DIST3, DIST4, DIST5

Table 2: Variables/Items names and Codes

The collected data was pre-analyzed for data screening, cleaning using IBM SPSS Statistics Software, and showing if data satisfied the requirements for conducting a multivariate analysis. Such analysis is important for ensuring the accuracy of the data and dealing with issues within response sets, missing data, and outliers or extreme values [200].

At first, the data sets were checked visually for errors and missing values. All the questions in the three surveys were marked as required to eliminate missing values, and participants had to select from a set of responses. In total, 593 responses were collected.

3.8 Outliers and extreme cases

The collected data were checked for possible outliers. Outliers are values or data points that are well below or above the other observation scores [201]. In an empirical study, Leys et al. pointed out that researchers often skip over-identifying outliers and lack knowledge about dealing with them during the data analysis process [202]. Outliers or extreme cases can distort the statistical analysis (mean, variance, standard deviation), or it can happen that they do not have a significant influence on the results. Different choices lead to distinct datasets, leading to inconsistent data analysis results. Consequently, the presence of extreme cases or outliers can lead to non-significant hypotheses. Hence, I decided to consider removing the outliers and extreme cases for better transparency in a multivariate analysis [205] and staying on the safe side.

3.8.1 Mahalanobis Distance

It was considered important the detection method and how to manage extreme cases. A well-known method used and suggested by many researchers for detecting multivariate outliers has been the calculation of the Mahalanobis Distance for each case [203], [204], [202]. Mahalanobis Distance is the distance of a case or a point from the center that is a point created by the means of all variables [205], [206]. The probability density of multivariate normal distribution was calculated to obtain the Mahalanobis Distance. According to the calculations in SPSS, five outliers with a p-value less than 0.001 were detected and removed: case with ID 35 (p=0.00091), 48 (p=0.00091), 162 (p=0.00088), 399 (p=0.00053), and 547 (p=0.0051). See for more Appendix IV, Table 19. As a result, 588 responses were kept for proceeding with data analysis.

3.8.2 Cook's Distance

Also, Cook's distance statistics were performed to check if influential points or significant extreme cases can affect the model [207]. The three dependent variables were checked, and from the results, the values were all below 1.0. For the Perceived Threat variable, depending on its ascendants (Perceived Susceptibility and Perceived Severity) and Risk and Distrust Propensity, the maximum Cook's Distance value was 0.111 (Table 3).

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.96027	6.17801	4.44303	.733394	588
Std. Predicted Value	-3.385	2.366	.000	1.000	588
Standard Error of Predicted Value	.041	.211	.084	.026	588
Adjusted Predicted Value	1.83950	6.18294	4.44300	.733799	588
Residual	-4.097067	4.039732	.000000	.946268	588
Std. Residual	-4.315	4.255	.000	.997	588
Stud. Residual	-4.363	4.318	.000	1.002	588
Deleted Residual	-4.188065	4.160496	.000030	.957495	588
Stud. Deleted Residual	-4.432	4.385	.000	1.006	588
Mahal. Distance	.104	28.073	3.993	3.363	588
Cook's Distance	.000	.111	.002	.009	588
Centered Leverage Value	.000	.048	.007	.006	588

a. Dependent Variable: PTH_AVG

Table 3: Cook's Distance Statistics for Perceived Threat

Depending on five variables (perceived threat, safeguard effectiveness, safeguard costs, self-efficacy, and impulsivity), the Security Motivation variable reached a maximum value of Cook's distance of 0.036 (Table 4).

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	.63251	5.04872	3.62868	.966086	588
Std. Predicted Value	-3.101	1.470	.000	1.000	588
Standard Error of Predicted Value	.057	.270	.121	.036	588
Adjusted Predicted Value	.62240	5.06458	3.62920	.965569	588
Residual	-3.950619	3.165127	.000000	1.240571	588
Std. Residual	-3.171	2.540	.000	.996	588
Stud. Residual	-3.182	2.551	.000	1.001	588
Deleted Residual	-3.978248	3.192343	-.000512	1.254659	588
Stud. Deleted Residual	-3.207	2.564	-.001	1.003	588
Mahal. Distance	.220	26.506	4.991	3.771	588
Cook's Distance	.000	.036	.002	.003	588
Centered Leverage Value	.000	.045	.009	.006	588

a. Dependent Variable: SM_AVG

Table 4: Cook's Distance Statistics for Security Motivation

In the last dependent variable, Security Behaviour depending on Security Motivation, Cook's distance values did not exceed 0.024 (Table 5). Since all the values were below 0.1, no significant outliers were found.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	.57201	.76629	.67415	.061095	588
Std. Predicted Value	-1.672	1.508	.000	1.000	588
Standard Error of Predicted Value	.009	.017	.012	.003	588
Adjusted Predicted Value	.56923	.76946	.67413	.061084	588
Residual	-.688577	.427989	.000000	.212778	588
Std. Residual	-3.233	2.010	.000	.999	588
Stud. Residual	-3.236	2.016	.000	1.001	588
Deleted Residual	-.689816	.430773	.000024	.213500	588
Stud. Deleted Residual	-3.263	2.022	.000	1.002	588
Mahal. Distance	.001	2.795	.998	.972	588
Cook's Distance	.000	.024	.002	.003	588
Centered Leverage Value	.000	.005	.002	.002	588

a. Dependent Variable: SB_AVG

Table 5: Cook's distance for Security Behaviour

3.9 Linearity

Multiple linear regression assumes that the independent variables collectively are linearly related to the dependent variable. Therefore, each independent variable is linearly related to the dependent variable.

To define the linearity between dependent and independent variables and to check if this assumption is satisfied, the scatterplots of the standardized residuals versus predicted values were examined for the three dependent variables: Perceived Threat (PTH), Security Motivation (SM), and Security Behaviour (SB). The graphs were assessed after generating Cook's distance statistics (Figures: 5, 6, 7), and they were inspected visually. From the figures below, the relationships are close to linear.

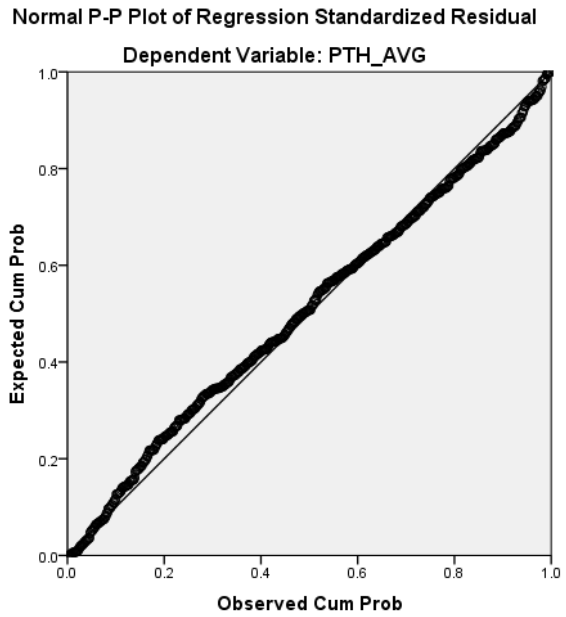

Figure 5: Normal P-P Plot of the Perceived Threat Dependent Variable

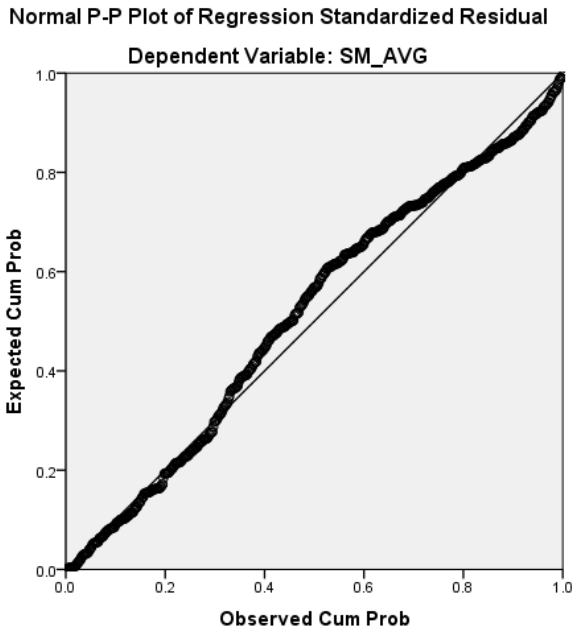

Figure 6: Normal P-P Plot of the Security Motivation Dependent Variable

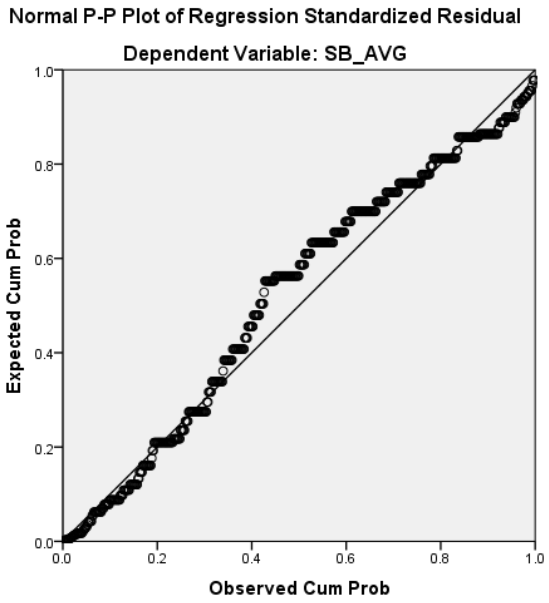

Figure 7: Normal P-P Plot of the Security Behaviour Dependent Variable

3.10 Independence of errors or cases: Durbin-Watson Test

The Durbin-Watson statistic test was used to access the independence of residuals of errors [206], [207]. The Durbin-Watson statistic can range from 0 to 4, but the value indicates no correlation between residuals is two or around two. After the test, results showed that the D-W statistic for the three dependent variables was around the value of 2, and respectively 2.048 (Table 6), 1.746 (Table 7), and 1.740 (Table 8). Consequently, the independence of errors' assumption was not violated.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.613[a]	.375	.371	.949509	2.048

a. Predictors: (Constant), DIST_AVG, PSU_AVG, RP_AVG, PSE_AVG

b. Dependent Variable: PTH_AVG

Table 6: Durbin-Watson Statistics Results for Perceived Threat variable

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.614[a]	.378	.372	1.245888	1.746

a. Predictors: (Constant), IMP_AVG, SE_AVG, SCO_AVG, SEF_AVG, PTH_AVG

b. Dependent Variable: SM_AVG

Table 7: Durbin-Watson Statistics Results for Security Motivation variable

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.276[a]	.076	.075	.212959	1.740

a. Predictors: (Constant), SM_AVG

b. Dependent Variable: SB_AVG

Table 8: Durbin-Watson Statistics Results for Security Behaviour variable

3.11 Normality

To check if the indicators meet the normality assumption, measures of kurtosis and skew were used [208]. Measures of kurtosis help identify if a curve is normal or abnormally shaped. A skewed curve is either positively or negatively skewed. Positively skewed curves show most scores below the mean, and negatively skewed curves are just the opposite. Both curves result in a normal asymmetrical curve. Both skew and kurtosis were analyzed through descriptive statistics. Acceptable skewness values should fall between − 3 and + 3, and the kurtosis range is appropriate from − 10 to + 10 when utilizing SEM [209]. The results for 11 variables of this study are represented in the table below (Table 9):

VARIABLES	Excess Kurtosis	Skewness	Observations
Distrust (DIST)	0.52	-0.462	588
Impulsivity (IMP)	-0.203	0.367	588
Perceived Severity (PSE)	0.692	-0.898	588
Perceived Susceptibility (PSU)	-0.92	0.25	588
Perceived Threat (PTH)	0.189	-0.725	588
Risk Propensity (RP)	-0.501	-0.264	588
Safeguard Cost (SCO)	-0.858	0.612	588
Safeguard Effectiveness (SE)	0.058	-0.731	588
Security Behaviour (SB)	-0.46	-0.378	588
Security Motivation (SM)	-1.047	-0.158	588
Self-Efficacy (SEF)	-0.835	-0.231	588

Table 9: Latent Variables (Descriptive)

The above values indicate that they fall into the pre-defined ranges, and we have a normal distribution of the data, and the normality assumption was not violated.

3.12 Multicollinearity

Another critical assumption is that multicollinearity should not exist. Factor analysis is an interdependency technique, and there should not be multicollinearity between the variables [210]. In this study, multicollinearity was checked with the help of the most widely used indicator, variance inflation factor (VIF) [211]. When the independent variables are not linearly related, the VIF indicates how strong the linear dependencies are and how often the variances of each regression coefficient are inflated due to collinearity. In other words, independent variables should not be highly correlated with each other; otherwise, they will lead to problems with understanding which variable contributes to the variance explained and technical issues in calculating a multiple regression model. It is widely assumed that a VIF value greater than 10 is potentially harmful. The values were examined, and all the variables had a VIF below 10, indicating that this assumption was fulfilled (Appendix III, Table 22).

3.13 Evaluation of the measurement model

An essential step in PLS-SEM analysis is to evaluate the outer model. This evaluation aims to determine how well the items load on the hypothetical construct [212]. For this purpose, the reliabilities of each item and variables, internal consistency, construct validity, convergent validity, and discriminant validity were assessed [213].

3.13.1 Reliability and Validity

To measure the internal reliability consistency and convergent validity, Cronbach's Alpha [214] and Average Variance Extracted (AVE) [215] were accessed in SPSS and SmartPLS 3 [216]. Cronbach's Alpha indicates how closely a set of items within the same construct is related. A good value should be from around 0.7 and above. AVE provides a measure of the variance's amount of a construct concerning the variance's amount due to measurement error. It represents how an item correlates positively with alternative items of the same construct. The criteria value is greater than 0.5.

Additionally, another measure was used to examine the internal consistency of latent variables (constructs): the composite reliability [217]. Table 10 shows the respective values for all the constructs. A value from around 0.7 and above is accepted.

CONSTRUCTS	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Perceived Severity (PSE)	0.945	0.948	0.955	0.724
Perceived Susceptibility (PSU)	0.909	0.913	0.943	0.847
Perceived Threat (PTH)	0.717	0.748	0.874	0.777
Safeguard Effectiveness (SE)	0.934	0.935	0.958	0.883
Safeguard Cost (SCO)	0.813	0.495	0.589	**0.326**
Self-Efficacy	0.875	0.921	0.908	0.671
Security Motivation (SM)	0.945	0.947	0.965	0.902
Distrust (DIST)	0.835	0.879	0.881	0.599
Impulsivity (IMP)	0.807	0.787	0.853	0.594
Risk Propensity (RP)	0.766	0.215	0.5	**0.22**
Security Behaviour (SB)	**0.366**	0.349	0.486	**0.249**

Table 10: Constructs Reliability and Validity

The problematic values are highlighted in red. Almost all the variables have shown a high level of internal consistency reliability (considering Cronbach Alpha coefficient) except security behaviour represented with the lowest reliability value. Therefore another coefficient was used to calculate the reliability of the security behaviour, and it was assessed using Kuder and Richardson Formula 20 [218]. It was decided to do so because it is related to the construct and items (variables) type [219]. As explained before, the security behaviour construct contained Dichotomous Items (Yes/No choice), where Yes is considered the best possible answer. The test statistic was performed by applying Kuder and Richardson Formula 20 (1) in Excel.

$$\rho KR20 = \frac{k}{k-1}\left(1 - \frac{\sum_{j=1}^{k} p_j q_j}{\sigma^2}\right) \quad (1)$$

k = 5 (number of items)

p_j = number of respondents who answered "Yes" in item j.

q_j = number of respondents who answered "No" in item j.

σ^2 = variance of the total scores of all the respondents answering the questions of Security Behaviour construct.

The ρKR_{20} result was 1.0, which means that the reliability level among the construct items was perfect. The calculations are shown in Appendix III (Table 20 and Table 21).

Risk propensity and safeguard effectiveness variables showed composite reliability values below 0.7 and AVE values below 0.5. According to the authors [220], [221], it is possible that a factor analysis can be conducted for evaluating the value of the constructs even though the outer loadings have an AVE below 0.5. Indicators with outer loadings values between 0.4 and 0.7 should be removed from the model if their removal results in an AVE increase [213]. Therefore, factor analysis was run, and it was found that 15 indicators did not load significantly as their value of outer loadings was <0.7 (Appendix III, Table 23).

It was considered for removal only the loadings that after their removal showed an increase in AVE: six items of Risk Propensity (RP1, RP2, RP3, RP5, RP6, RP8), three items of Safeguard Cost (SCO3, SCO4, SCO5), and two items of Security Behaviour (SB2 and SB3). Some indicators (RP7, SEF1, IMP 2, IMP3, SB4, and SB5) with outer loadings <0.7 were not removed because their removal did not show an increase in AVE. The new results concerning constructs' reliability and validity are presented in Table 11.

CONSTRUCTS	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Perceived Severity (PSE)	0.945	0.948	0.955	0.724
Perceived Susceptibility (PSU)	0.909	0.913	0.943	0.847
Perceived Threat (PTH)	0.717	0.748	0.874	0.777
Safeguard Effectiveness (SE)	0.934	0.935	0.687	0.883
Safeguard Cost (SCO)	0.804	0.848	0.958	0.833
Self-Efficacy (SEF)	0.875	0.921	0.908	0.671
Security Motivation (SM)	0.945	0.948	0.908	0.902
Distrust (DIST)	0.835	0.874	0.88	0.599
Impulsivity (IMP)	0.807	0.266	0.805	0.517
Risk Propensity (RP)	0.423	0.453	0.909	0.63
Security Behaviour (SB)	0.487	0.421	0.965	0.43

Table 11: Constructs Reliability and Validity after removing indicators that did not load significantly.

3.13.2 Discriminant Validity

The Heterotrait-monotrait (HTMT) ratio of correlation proposed by Henseler et al. was used [222]. Accordingly, the acceptable levels of discriminant validity are less than 0.90. Additionally, other authors suggest a threshold of 0.85 [208]. The HTMT values were assessed and are indicated in the table below (Table 12). None of them exceeded the value of 0.70.

CONSTRUCTS	**DIST**	**IMP**	**PSE**	**PSU**	**PTH**	**RP**	**SCO**	**SE**	**SB**	**SM**	**SEF**
Distrust (DIST)											
Impulsivity (IMP)	**0.245**										
Perceived Severity (PSE)	**0.288**	**0.073**									
Perceived Susceptibility (PSU)	**0.093**	**0.098**	**0.22**								
Perceived Threat (PTH)	**0.367**	**0.086**	**0.687**	**0.365**							
Risk Propensity (RP)	**0.425**	**0.236**	**0.187**	**0.135**	**0.334**						
Safeguard Cost (SCO)	**0.087**	**0.244**	**0.101**	**0.379**	**0.18**	**0.047**					
Safeguard Effectiveness (SE)	**0.24**	**0.038**	**0.462**	**0.273**	**0.619**	**0.265**	**0.204**				
Security Behaviour (SB)	**0.196**	**0.119**	**0.061**	**0.103**	**0.215**	**0.212**	**0.251**	**0.29**			
Security Motivation (SM)	**0.215**	**0.039**	**0.264**	**0.416**	**0.458**	**0.197**	**0.269**	**0.643**	**0.501**		
Self-Efficacy (SEF)	**0.219**	**0.093**	**0.323**	**0.09**	**0.386**	**0.161**	**0.231**	**0.313**	**0.142**	**0.279**	

Table 12: HTMT Values

4 RESEARCH RESULTS

This chapter report the main findings of the study based upon the applied methodology. At first, it presents the demographics of the samples and detailed information regarding the habits and practices of respondents in smartphones. Answers to the research questions are given, and results with regard to hypothesized statements are arranged in a logical sequence.

4.1 Demographics

The demographic characteristics of the study sample are represented in Table 13. The total number of the participants was 593, and after removing the outliers, only 588 responses were kept, of which 329 were from Hungary, 137 were from Albania, and 122 international students living in Hungary. The sample consisted of more men (N= 340, 57.8%) than women and people of Hungarian nationality (56%). The majority of respondents (N= 341, 58%) were between the age of 21 and 30. Around one-third of the sample (32.1 %) were grown up in a small city, followed by those in large (25.7%) and capital cities (26.2%).

A considerable number of the respondents (N=246, 41.5%) declared that they have a secondary education, and this was followed by around one-third that hold a Master's degree (N=176, 29.9%). A greater number (N=369, 62.8 %) were students, followed by 170 participants employed (28.9%). 40% of the participants (N=235) had less than 300 EUR/month incomes, and this was followed by around 18% (N= 108) getting 301-500 EUR/month, and by approximately 15% (N=90) with 1001 EUR/month or over and by 87 respondents that had 501-700 EUR/month incomes.

Variable	Frequency	Percent
Age		
<=20	99	16.8
21-30	341	58.0
31-40	89	15.1
41-50	32	5.4
>50	27	4.6
Gender		
Female	243	41.3
Male	340	57.8
Prefer to not say	5	0.9
Place of Growth		
Rural settlement	94	16.0
Small town	189	32.1
Large town	151	25.7
Capital of your country	154	26.2
Education		
Secondary	273	46.4
High School	34	5.8
Bachelor's Degree	87	14.8
Master's Degree	176	29.9
Ph.D./ Higher Degree	18	3.1
Employment Status		
Student	369	62.8
Employed	170	28.9
Unemployed	15	2.6
Self-employed	29	4.9
Retired	5	0.9
Monthly Incomes		
Under 300	235	40.0
301-500	108	18.4
501-700	87	14.8
701-1000	68	11.6
1001 or over	90	15.3

Table 13. Demographic characteristics of the study population N=588

4.2 Smartphone selection, usage purposes, and accounts importance

In the survey, users were asked about the smartphone's brand, smartphone usage purposes, and their most important accounts. The study results demonstrated that most Albanians (approximately 90%) use smartphones for business and personal purposes, and the rest only for personal purposes. On the other hand, almost half of Hungarians use smartphones for personal purposes (48.5%) and the other half for both reasons (51.5%). The fact that a considerable number of Albanian users bring their devices to work indicates that they can be more exposed to security threats.

The majority of Albanians (more than 60%) own an Apple smartphone, followed by around 30% that own a Samsung one, and the rest of the brands do not have a significant frequency. The Hungarian responses showed that about one-third (31.6%) own an Apple device, followed by Samsung (21.2%) and Huawei (21.2%) with the same percentage. On the other hand, Xiaomi smartphones were chosen by many Hungarians (17.6%), and the rest did not show significant frequencies.

There were differences between the two groups and their most important accounts. The most important account for most Albanians (55%) was Whatsapp, while more than half of Hungarian respondents did not use it at all. Around 60% of Hungarian respondents declared that the most important account is their email, and also 50% of Albanians reported that their email address has great importance to them. Approximately 40% of Hungarians responded that Facebook is very important to them, while only 5% of Albanians considered it very important. 30% of Albanians and only 15% of Hungarians gave great importance to their Instagram accounts. Both groups did not provide considerable importance to Messenger, Google Drive, Twitter, and Viber.

4.3 Habits and Practices

Respondents were required to give information about: internet activity with smartphones during weekdays and weekends, experience with the stolen device, leaving smartphones in the other peoples' hands, app downloading sites, experience with a hacked smartphone, number of apps on smartphones, and changes in frequency in apps (downloading a new one). Table 14 represents users' internet activity on smartphones during weekdays and weekends.

Besides, a comparison between the two main targets of this study (Albanian and Hungarians) is demonstrated.

Internet Activity		Albania	Hungary
During weekdays	*Less than 1 hour*	2.20%	6.90%
	1-2 hours	11.50%	18.50%
	2-3 hours	20.90%	26%
	3-4 hours	29.50%	22.40%
	5 hours or over	36.00%	26%
During weekends	*Less than 1 hour*	1.40%	8.10%
	1-2 hours	17.30%	20.60%
	2-3 hours	18.70%	26.90%
	3-4 hours	27.30%	22.70%
	5 hours or over	35.30%	21.80%

Table 14: Frequency of the users' internet activity (AL vs. HU)

Internet activity can be hijacked, and there is little that individuals can do about attacks at Internet Service Provider (ISP) level. Cookies that are small bits of text can be downloaded and stored by the browser users use, and they can track those web pages. Plugins may also track the activity across multiple web pages. Moreover, such tracking can go too far and be intrusive. For instance, a unique identifier is added to a cookie and used across different services on several marketing platforms.

Table 14 indicates that both groups are significantly active with their smartphones on the internet and posed to the threats. Still, Albanian users are more engaged than Hungarians in both cases (weekdays and weekends).

In response to the question “Do you let your smartphone in others’ hands?”, most of those surveyed in Albania and around one-third in Hungary trust others and let their devices to them. The participants were also asked if their smartphones had ever been lost. Albanians were shown as more careless than Hungarians: around 30% of Albanian users and only 17% of Hungarians answered that they had experienced it.

On the other hand, Albanian users seem to be more cautious about downloading sites than Hungarian ones. About 10% of Albanians and 24% of Hungarians seem careless because of downloading from non-official stores (i.e., App Store, Google Play).

Around half of the respondents have less than 20 installed applications in their smartphones in both groups and do not make frequent changes. Again about 50 % in both groups change (delete/install) apps to try new ones rarely/a couple of times per month or less frequently.

Moreover, respondents were asked if, according to their knowledge, their smartphone had ever been hacked. Half of Albanians declared "No," and more than one-third did not know. The rest (10%) were conscious that have experienced it. A considerable part of Hungarians (80%) was sure that have never experienced an attack on their smartphones, and only a vast minority (3%) had no knowledge if they had experienced it.

4.4 Testing hypotheses with all the valid data

The third and most important part of the questionnaire addressed questions related to research hypotheses. Hence, path analysis in PLS-SEM was applied to address the five research questions and seven hypotheses. As mentioned before, the relationships among independent variables and dependent variables were assessed by using SmartPLS 3.0.

Figure 8 shows the path coefficients along with R squared (R^2) within the variables of Perceived Threat, Security Motivation, and Security Behaviour. Path coefficients were used to measure the strength of the relationships between the variables, and they have range values between -1 and 1, and the p-values should be less than 0.05 [213]. Path coefficients closer to +1 indicate strong positive relationships, and closer to -1 indicate strong negative. If these values fall close to 0, the relationships are considered weak.

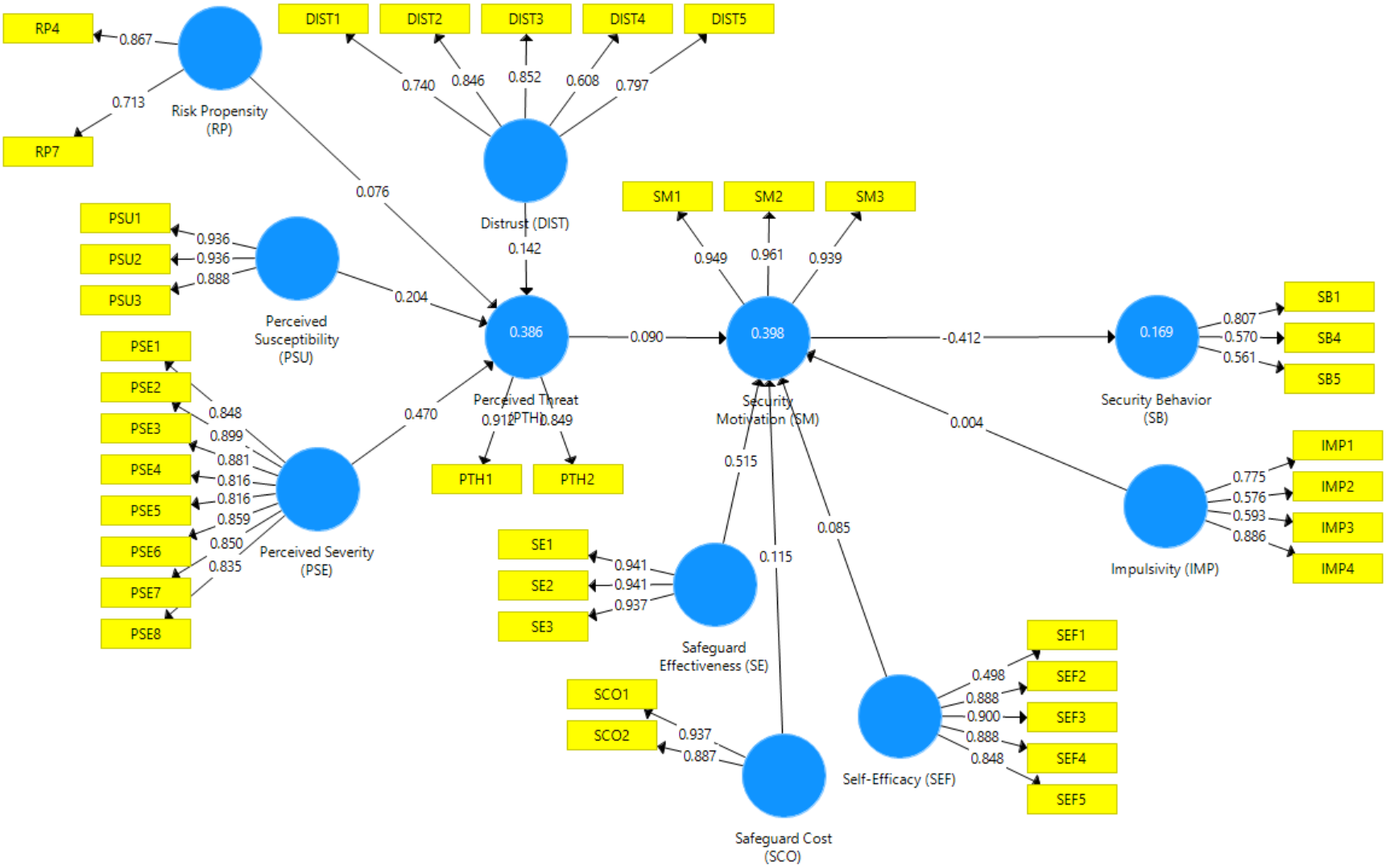

Figure 8: Partial Least Squares Structural Equation Modeling (N=588)

R^2 indicates the predictive accuracy of the model. Different scholars suggest different good R square variance values. A low R-square often might not be a problem in social sciences, where human behaviour cannot be accurately predicted. Hair et al. state that the acceptable level of R^2 depends on the research context. In disciplines like human behaviour, values of 0.20 are considered high, while in other contexts, that might not be significant [223], [224].

Therefore, here the R^2 values of 0.386 (PTH), 0.398 (SM), and 0.169 (SB) have been classified as substantial, substantial, and moderate. They indicate the amount of variance in the dependent variables that can be explained by their respective independent variables [213], [225].

The results presented in Figure 8 mean that:

- Perceived Susceptibility, Severity, Risk, and Distrust Propensity substantially explain 38.6% of the variance in Perceived Threat.
- Perceived Threat and Impulsivity substantially explain 39.8% of the variance in Security Motivation.
- Security Motivation moderately explains 16.9% of the variance in Security Behaviour.

In addition, t-statistics (two-tailed test) for significance testing of both inner and outer models was executed. Based on generated results, Perceived Susceptibility ($\beta=0.2$, $p<0.05$) has a positive but weak contribution to Perceived Threat. Perceived Severity ($\beta=0.47$, $p<0.05$) has a moderate positive contribution to Perceived Threat. So, H1a and H1b were supported. The other variable of Perceived Threat ($\beta=0.09$, $p<0.05$) positively influences Security Motivation, but the relationship is weak. The H2 was supported as well. Safeguard Effectiveness with a β coefficient of more than 0.5 and p-value less than 0.05 contributes to Security Motivation positively and close to significantly. Thus, the H3 is fully supported. Safeguard cost with a $\beta=0.12$ and p-value less than 0.05 has a weak contribution to Security Motivation. The H4 was assumed to be negative, but surprisingly, the relationship was positive. Self-Efficacy ($\beta=0.085$, $p<0.05$) positively affects the Security Motivation, and the relationship is considered weak. Hence, the H5 is supported.

Another surprising result was shown from the contribution of Security Motivation to Security Behaviour (H6). The relationship was confirmed, but the relationship resulted in moderately negative (β= - 041, p<0.05). Hypothesis 7 was not fully supported. The sub-hypothesis H7a (Impulsivity influence on Security Motivation) was not supported because the values of β and p did not satisfy the range. While, Perceived Risk showed a positive contribution to Perceived Threat (β=0.76, p<0.05). Even though the influence was not strong, it can be stated that sub-hypothesis H7b was supported. The last variable of Distrust showed a positive contribution to Perceived Threat as well (β=0.14, p<0.05). Thus, sub-hypothesis H7c was supported as well.

After testing the research model, table 15 summarizes the results where all the valid data (N=588) were considered.

Hypotheses	Paths	Path Coefficients (β)	t-values	p-values	SUPPORTED
H1a+	**Perceived Susceptibility (PSU) -> Perceived Threat (PTH)**	0.2030	6.0610	**0.0000**	**YES**
H1b+	**Perceived Severity (PSE) -> Perceived Threat (PTH)**	0.4710	10.0630	**0.0000**	**YES**
H2+	**Perceived Threat (PTH) -> Security Motivation (SM)**	0.0890	2.0840	**0.0370**	**YES**
H3+	**Safeguard Effectiveness (SE) -> Security Motivation (SM)**	0.5160	13.5270	**0.0000**	**YES**
H4-	**Safeguard Cost (SCO) -> Security Motivation (SM)**	0.1150	3.4300	**0.0010**	**(Yes but Positive relationship)**
H5+	**Self-Efficacy (SEF) -> Security Motivation (SM)**	0.0850	2.2460	**0.0250**	**YES**
H6+	**Security Motivation (SM) -> Security Behaviour (SB)**	-0.4110	12.4690	**0.0000**	**(Yes but Negative relationship)**
H7a-	**Impulsivity (IMP) -> Security Motivation (SM)**	0.0040	0.0660	**0.9480**	**NO**
H7b-	**Risk Propensity (RP) -> Perceived Threat (PTH)**	0.0760	2.1000	**0.0360**	**YES**
H7c+	**Distrust (DIST) -> Perceived Threat (PTH)**	0.1420	3.3240	**0.0010**	**YES**

Table 15: Research Results (Hypotheses, N=588)

4.5 Multigroup Analysis: Albania vs. Hungary

The multi-group analysis allows to test if pre-defined data groups have significant differences in their group-specific parameter estimates (e.g., outer weights, outer loadings, and path coefficients) [226]. SmartPLS provides outcomes of three approaches (path coefficients, t-value, and p-value) based on every group's bootstrapping results.

The groups have a significant difference for a p-value less than 0.05 and greater than 0.95 [225]. The significant differences were generated after the parametric test, assuming equal variances across the groups (Table 16).

Hypotheses	Paths	(β) -diff (GROUP_AL vs. GROUP_HU)	t-Value (|GROUP_AL vs GROUP_HU|)	p-Value (GROUP_AL vs GROUP_HU)
H1a+	Perceived Susceptibility (PSU) -> Perceived Threat (PTH)	-0.075	0.891	0.374
H1b+	Perceived Severity (PSE) -> Perceived Threat (PTH)	-0.229	2.027	0.043
H2+	Perceived Threat (PTH) -> Security Motivation (SM)	0.128	1.229	0.220
H3+	Safeguard Effectiveness (SE) -> Security Motivation (SM)	-0.154	1.647	0.100
H4-	Safeguard Cost (SCO) -> Security Motivation (SM)	-0.174	2.057	0.040
H5+	Self-Efficacy (SEF) -> Security Motivation (SM)	0.196	1.783	0.075
H6+	Security Motivation (SM) -> Security Behaviour (SB)	0.175	2.020	0.044
H7a-	Impulsivity (IMP) -> Security Motivation (SM)	0.045	0.369	0.712
H7b-	Risk Propensity (RP) -> Perceived Threat (PTH)	-0.099	1.092	0.275
H7c+	Distrust (DIST) -> Perceived Threat (PTH)	0.067	0.710	0.478

Table 16: Parametric Test (PLS Multi-Group Analysis)

The multi-group analysis demonstrated peculiarities between the two groups, specifically the influence of Perceived Severity to Perceived Threat, Safeguard Cost to Security Motivation, and Security Motivation to Security Behaviour. Perceived Threat in Smartphones of Hungarian users is influenced by both factors of threat appraisal (perceived susceptibility and severity). Albanian users' Perceived Threat is shown to be controlled only by the Perceived

Severity of being attacked by a threat. The cost of a safeguard against malicious software negatively influences the motivation of Hungarian users to use smartphone security technologies, but it does not affect the motivation of Albanian users. And lastly, the Albanian users intend to use smartphone security technologies, but this does not positively shape their security behaviour. The direction of this outcome differs from what was hypothesized, and in contrast to Hungarian users that are motivated and intend to use technologies against threats that lead to better security behaviour.

For a better understanding, groups were tested following the theoretical model. PLS Algorithm for Path Analysis was rerun for each group separately.

4.6 Results: Albania

In the case of Albania, only two hypotheses (H3+, H5+) and partially the first one (H1b+) were fully supported. Even though there is a relationship between Security Motivation and Behaviour, and the null hypothesis is rejected, the direction of this result is negative (β=-0322, $p<0.05$) and not positive as it was hypothesized.

Hence, the threat appraisal and coping factors cannot fully explain Albanian users' security motivations and behaviours in smartphone security. Also, the individual differences have not shown a significant effect. Therefore, the main research results for this group are as follows:

- Albanians perceive the threat in smartphones based only on the severity of an attack/threat and not its susceptibility. The more severe the nature of a threat, the more they will realize it. In addition, the study of this group failed to reject the null hypotheses for the influence of risk and distrust propensity. These variables did not affect the way Albanians perceive the threats in smartphones.
- Their intention or motivation to use security technologies against a threat in smartphones is influenced only by the effectiveness of safeguards and their efficacy in intending to use secure technologies. The cost of a safeguard against threats, the users' perceived threat, and their impulsivity do not affect their motivation to use security technologies.
- Albanians' intention and motivation to use technologies to secure smartphones do not lead to better security behaviours.

The results generated from the valid Albanian data (N= 137) are summarized in the table below (Table 17):

Hypotheses	Paths	Path Coefficients (β)	t-values	p-values	Supported
H1a+	**Perceived Susceptibility (PSU) -> Perceived Threat (PTH)**	0.098	1.253	**0.211**	**NO**
H1b+	**Perceived Severity (PSE) -> Perceived Threat (PTH)**	0.340	2.909	**0.004**	**YES**
H2+	**Perceived Threat (PTH) -> Security Motivation (SM)**	0.151	1.727	**0.085**	**NO**
H3+	**Safeguard Effectiveness (SE) -> Security Motivation (SM)**	0.403	4.314	**0.000**	**YES**
H4-	**Safeguard Cost (SCO) -> Security Motivation (SM)**	-0.087	0.976	**0.330**	**NO**
H5+	**Self-Efficacy (SEF) -> Security Motivation (SM)**	0.328	2.818	**0.005**	**YES**
H6+	**Security Motivation (SM) -> Security Behaviour (SB)**	-0.322	3.310	**0.001**	YES but Negative
H7a-	**Impulsivity (IMP) -> Security Motivation (SM)**	0.014	0.149	**0.882**	**NO**
H7b-	**Risk Propensity (RP) -> Perceived Threat (PTH)**	0.043	0.559	**0.576**	**NO**
H7c+	**Distrust (DIST) -> Perceived Threat (PTH)**	0.195	1.845	**0.066**	**NO**

Table 17: ALBANIA Hypotheses Results Summary (N=137)

4.7 Results: Hungary

In the case of Hungary, only H2 and partially H7 were not supported. How Hungarian users perceive smartphone threats does not affect their intention to use smartphone security technologies. Also, the impulsivity of users is not related to their motivation to use secure technologies in smartphones. This study's research questions and hypotheses show that the threat appraisal factors cannot fully explain Hungarian users' security motivation and behaviour. In contrast, the coping appraisal factors can fully explain their security motivation and behaviour. Furthermore, as it was hypothesized, Risk and Distrust Propensity influence how they perceive the threats in smartphones. The following highlights the main results for the Hungarian group:

- Hungarian users perceived threats based on perceived susceptibility and severity factors by showing a positive relationship (H1a+ H1b+). But their perceived threat does not shape motivation on using security technologies in smartphones.
- Risk and distrust propensity influence the Hungarian users' perceived threat. The more risks they take, the less chance they will perceive the threats in their smartphones. The more they distrust, the more they will perceive threats in their smartphones. Therefore, the null hypotheses were rejected, and both sub- hypotheses (H7b- and H7c+) were fully supported for this group.
- The three factors of copping appraisal (safeguard effectiveness, cost, and self-efficacy) explain their security motivation in smartphones, and the three hypotheses (H3+, H4-, and H5+) were fully supported.
- Lastly, the intention/motivation of Hungarian users to use smartphone security technologies positively shapes their security behaviour. Thus, the hypothesis (H6+) was supported.

The main results obtained from the Hungarian responses are set out in Table 18.

Hypotheses	Paths	Path Coefficients (β)	t-values	p-values	Supported
H1a+	**Perceived Susceptibility (PSU) -> Perceived Threat (PTH)**	0.197	4.760	**0.000**	YES
H1b+	**Perceived Severity (PSE) -> Perceived Threat (PTH)**	0.544	10.400	**0.000**	YES
H2+	**Perceived Threat (PTH) -> Security Motivation (SM)**	0.049	0.849	**0.396**	**NO**
H3+	**Safeguard Effectiveness (SE) -> Security Motivation (SM)**	0.550	11.054	**0.000**	YES
H4-	**Safeguard Cost (SCO) -> Security Motivation (SM)**	-0.097	2.142	**0.033**	YES
H5+	**Self-Efficacy -> Security Motivation (SM)**	0.107	2.147	**0.032**	YES
H6+	**Security Motivation (SM) -> Security Behaviour (SB)**	0.533	12.583	**0.000**	YES
H7a-	**Impulsivity (IMP) -> Security Motivation (SM)**	0.011	0.222	**0.824**	**NO**
H7b-	**Risk Propensity (RP) -> Perceived Threat (PTH)**	0.128	2.831	**0.005**	YES but positive
H7c+	**Distrust (DIST) -> Perceived Threat (PTH)**	0.128	2.987	**0.003**	YES

Table 18: Hungary Hypotheses Results Summary (N=329)

5 CONCLUSIONS

This section summarizes the main achievements, recommendations, limitations, and future work.

Security threats have also increased with the increased usage of smartphones, the internet, and apps for personal and work purposes. Technology alone cannot provide full support for security threats in smartphones. Information security involves protection and prevention, which implies users' interventions and behaviours. Hence, this work examined the role of behavioural science theories in understanding users' security intentions and behaviours in smartphones, how these theories can contribute to expanding research, and how the security risks can be reduced.

The primary purposes of the study were to identify the cognitive factors (threat and copy appraisal) and individual differences that influence users' motivations and behaviours in using security technologies in smartphones. For this reason, the revised TTAT model of Liang and Xue by Carpenter et al. that adopted PMT factors was applied. The TTAT model implements PMT's framework for detecting the main factors that lead to technology threat avoidance behaviour. This was achieved by exploring the relationship between threat appraisal factors (here, the threats posed in smartphones) and coping appraisal factors (here, security measures taken against threats in smartphones) and their role in motivating the use of protective measures that lead to security behaviours. In addition to the TTAT, and following Carpenter et al.'s suggestions, three more factors that considered individual differences were added: risk and distrust propensity influence on the threat appraisal, and impulsivity to the motivation in using protective measures for better security behaviour.

A new instrument was developed by considering prior constructs and items of the revised TTAT model. At first, the data analysis was conducted using a large sample collected from smartphone users from Albania, Hungary, and international students living in Hungary. Accordingly, users' impulsivity did not show an effect on security motivation. Interesting results yielded from the positive impact of safeguard cost on users' security motivation and the negative influence of security motivation on security behaviour, which were hypothesized opposites. This study has demonstrated that these results can be accounted for in part by

different groups. Hence, the sample was divided into two groups based on their nationality (Albanian and Hungarian).

5.1 Main Research Achievements

This study's aims were achieved by answering five research questions. A quantitative method was employed to develop and validate the research model to answer the research questions. The methodology approach involved three phases. The first research question incorporated the two threat appraisals, perceived severity and susceptibility, and the outcome: users' perceived threat on smartphones. Also, it aimed to investigate the influence of risk and distrust propensity in users' perceived threats. Based on performed data analysis, susceptibility and severity regarding smartphones' threats positively influence their perceived threat in Hungary and partially in Albania.

The research results (strength of the paths) for the two groups are illustrated in Figures 9 and 10.

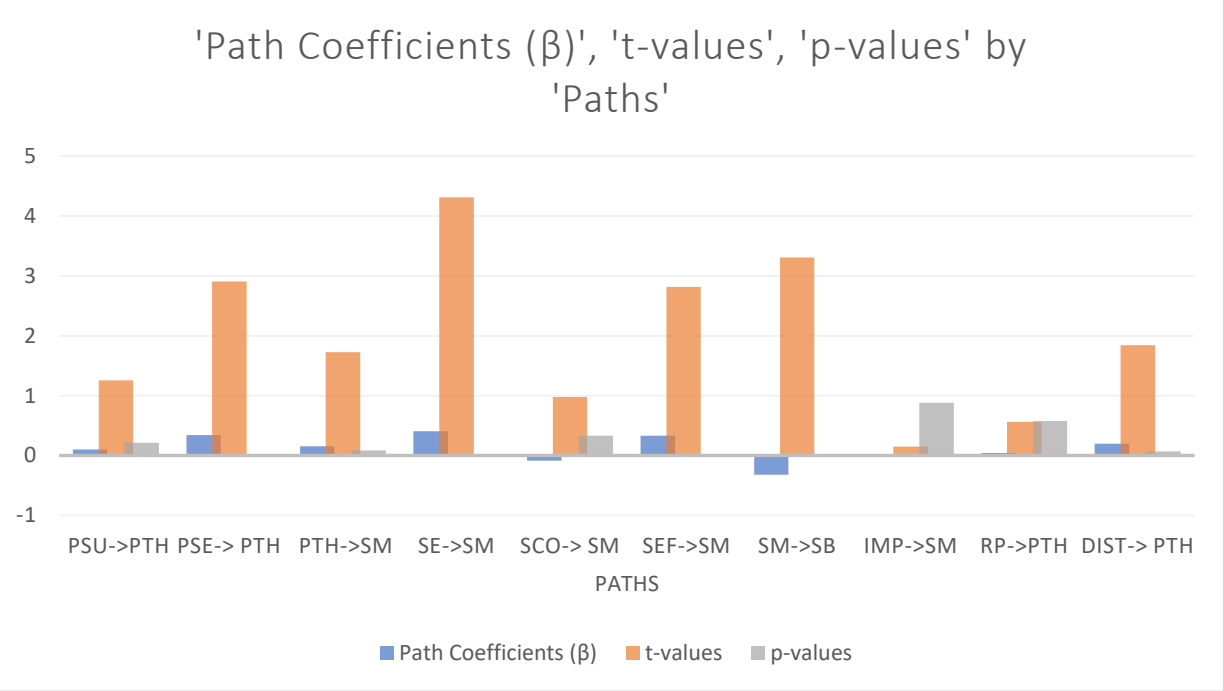

Figure 9: Albania - '(β)', 't-values', 'p-values' by 'Paths

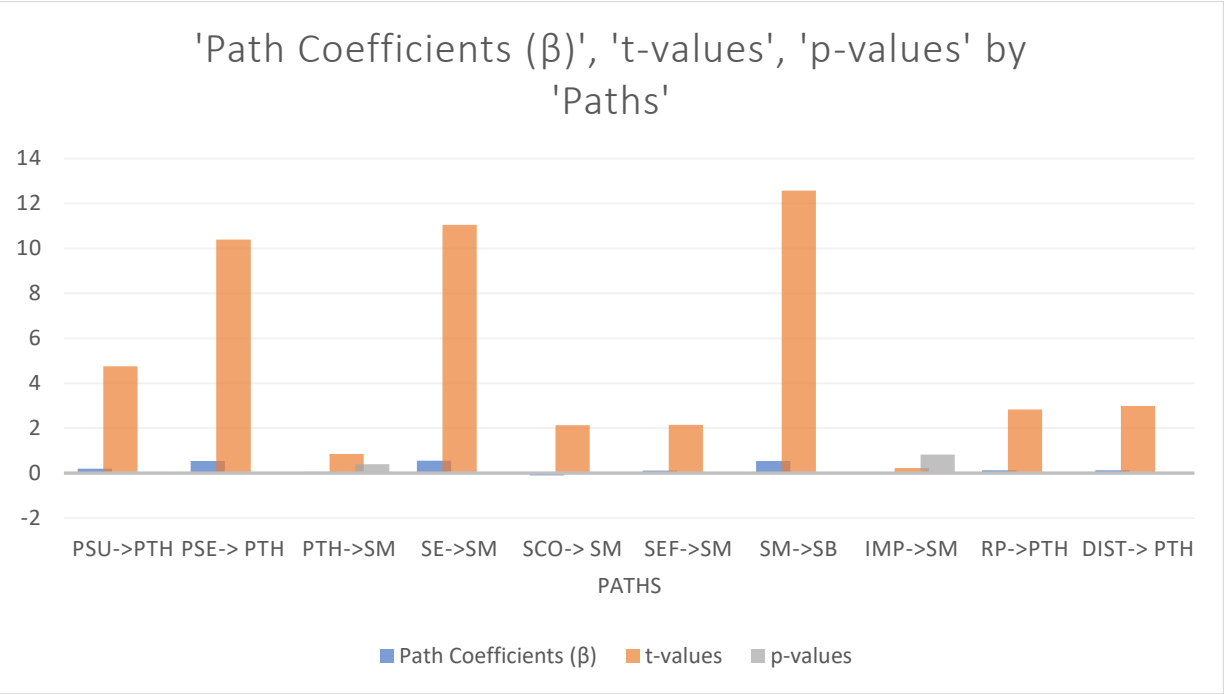

Figure 10: Hungary - (β)', 't-values', 'p-values' by 'Paths

Accordingly, the statements made are as follows:

Thesis 1a: There is a positive relationship between users' perceived threat susceptibility and perceived threat in smartphones, and this association is significant only in Hungary and not in Albania.

Thesis 1b: Users' perceived severity of being attacked positively affects smartphone perceived threat, and this association is stronger in Hungary than in Albania.

Published in: Kadena, 2017 [56]; Kadena 2018 [227].

The second research question addressed whether the users' perceived threat affects their motivation to use smartphone security technologies. The relationship was significant only in Hungary. Accordingly, the following statement was made:

Thesis 2: Users who receive "signals" regarding possible threats will be more motivated to use smartphones' security technologies, and this association was demonstrated significantly in Hungary and not in Albania.

Published in: Kadena, 2017 [228]; Kadena 2018 [227]; Kadena et al. 2022 [229].

The third research question incorporated copping appraisals (safeguard effectiveness and cost, and self-efficacy) on users' motivation to use smartphone security technologies. The results obtained from the analysis showed a positive influence of safeguard effectiveness and self-efficacy on users' motivation in using smartphone security technologies in both countries and a negative influence of safeguard cost on users' motivation only in Hungary. Therefore, the statements were formulated as follows:

Thesis 3: Smartphones' safeguard effectiveness positively affects users' motivation to use security technologies, and the association is stronger in Hungary than in Albania.

Published in: Kadena, Kovács, 2017 [71]; Kadena, Ruiz 2017 [84], Kadena, 2018 [230].

Thesis 4: The cost of safeguards regarding smartphone security negatively influences users' motivation to use security technologies in Hungary and not Albania.

Published in: Keszthelyi, Kadena, 2016 [82]; Kadena 2017 [56]; Kadena 2018 [231]; Holicza, Kadena, 2018 [232].

Thesis 5: Users' confidence to take a safeguard measure in smartphones contributes to better motivation in using smartphones' security technologies, which is more significant in Hungary than in Albania.

Published in: Kadena, 2018 [233]; Kadena, 2019 [83]; Kadena, 2020 [234].

The fourth research question examined users' motivation to use smartphones' security technologies in their security behaviours. Interestingly, the security motivation of users in smartphones showed a negative influence on security behaviours of Albanian users and a positive influence on security behaviours of Hungarian users:

Thesis 6: Users' intention to avoid threats and use smartphones' security technologies contributes to better security behaviours in Hungary but not Albania.

Published in: Kadena, 2018 [231]; Kadena, 2019 [235]; Kadena, Gupi 2021 [92].

The fifth research question focused on individual differences in users' perceived threats and their motivations to use smartphones' security technologies. In both countries, smartphone users' impulsivity did not impact their motivation for better security. Contrary to what was

hypothesized, risk propensity showed a positive relationship with the perceived threat in Hungary and no significant association in Albania. As hypothesized, users' distrust propensity positively influences their perceived threat in smartphones, but only in Hungary. Thus, the following statements were made:

Thesis 7a: Users' impulsivity in both countries does not contribute to their motivation in using smartphones' security technologies.

Thesis 7b: Users with high-risk tendencies in Hungary will feel more concerned with smartphone threats. While in Albania, there is no significant association between users' risk propensity and perceived threat.

Thesis 7c: Users' distrust tendencies contribute to a better understanding of smartphone security threats in Hungary and not Albania.

Published in: Kadena, 2017 [56]; Holicza, Kadena, 2018 [232]; Kadena, 2018 [236]; Kadena, Holicza, 2018 [23]; Kadena, 2019 [237]; Kadena, Pokorádi, 2020 [238].

This study can be of value and better serve to understand how users' smartphone security behaviours can be explained by cognitive factors and individual differences in different countries. As argued above, users' security motivations, behaviours, and practices had significant differences, which can be attributed to the individuals' cultural differences. This study has highlighted the importance of human behaviour in smartphone security. It can be considered a first step towards enhancing the understanding of two main groups: Albanian and Hungarian users.

The findings of this study make several noteworthy contributions to the TTAT original model of Liang and Xue and the original results that Carpenter et al. report in the TTAT revised model. An alternative approach was proposed by conducting a multi-group analysis to better explain the threat assessment process. Therefore, it can be it assists in understanding the different and mixed yielded results among different cultures. This work is relevant to the information security field and can be extended to the behavioural sciences. It can contribute to the emerging behavioural field of cultural differences and information security sciences.

5.2 Limitations and future work

This dissertation faced certain limitations. At first, the potential problem is that the scope of my study might have been too broad; it did not aim only to test the revised TTAT model but also to compare the two main groups included in the study. The refined study instrument was self-reporting rather than observing the users' intentions and behaviours. It provided insights into users' perceptions and did not capture their actual behaviours clearly. The collected data in number were appropriate for a comparative study between two countries (considering the population), but the sample sizes might be regarded as small. This suggests that conclusions based on the results should be drawn cautiously. Another limitation was the possibility that participants might not have been familiar with the smartphone security field and security terms used in the survey. This may have resulted in respondents' applying differing interpretations when completing the survey and consequently affecting the results.

There is a possibility that this study had insufficient identifiable individual differences from the sample groups of smartphone users. Therefore, an inadequate representation of the remaining population may affect the generalizability of these results. Another limitation is that the survey contained many items that can affect the accuracy of sample responses. Accordingly, several changes to the original TTAT instruments were made to improve the questions' clarity. These changes included modifying and dropping some of the prior items to fit the smartphone context better.

Additionally, scale changes were made, and throughout the instrument, only six-point Liker scales were used. This research showed that the measures exhibited adequate reliability and validity levels to support the findings. Nonetheless, these changes could have resulted in different interpretations of the research model constructs.

Behavioural theories have always been questioned for their integrity in IT [239]. This study highlights that attitude and intentions are essential predictors of behaviours and can increase users' motivation to behave securely. The items of the variables in this study were examined, and their strength had differences across different cultures. Based on the evidence from the data analysis and results, improvements are recommended for specific constructs. The failure of general items of risk propensity, safeguard cost, and security behaviour loadings indicate

the need to develop more specific items and technology-based scales suitable for use in the technology threat behaviour domain.

The differences between the two groups included in the research imply that further work is required. Future research can continue to explore the factors that influence users' security motivations and behaviours in smartphones by collecting data from other nations with similar cultures as Albania and Hungary. It can consider other constructs into the model to better explain individuals' security intentions and behaviours.

This study did not aim to examine smartphone users' security practices and habits. In-depth analysis is reserved for understanding better the root causes of the issues in the future. Nonetheless, the representative results of the study showed that the groups among each other have different approaches to using and securing their devices. The consequences of users' actions were related to users' threat perceptions, the lack of compliance with safeguards, security intentions, and some personality traits. Future research should develop a more comprehensive framework to integrate more personality traits and the cognitive factors discussed above and examine their influence on users' smartphone security motivations and behaviours.

5.3 Recommendations

The evidence from this study also offers some practical contributions. Nowadays, individuals need to be extra-cautious, and organizations should reinforce security measures. Results indicated that copping appraisal factors influenced the users' motivation and consequently their security behaviours in smartphones more than threat appraisal factors. Users' perceived threat will not always lead to better motivation in using smartphones' security technologies. This implies that more attention should be paid to increasing users' beliefs in the effectiveness of measures against smartphone threats and their confidence in performing these behaviours. Moreover, more effort should be made to reduce the costs of performing security behaviours, contributing to users' motivation to behave securely.

5.3.1 Translate awareness into action

Human error remains the weakest link in the security chain [12], [86]. Besides the antiviruses and other protective layers on computers and infrastructure, studies have shown that they do

not mitigate the security threats [3], [4], [5] completely. Therefore, organizations have already recognized that users' behaviours are responsible for security flaws and may pose significant risks to information security. For instance, in the case of Albania, lastly, data leakage has been a considerable concern. Over 600.000 personal data, including salaries, leaked because of internal infiltration and not an outside cyber-attack [240]. Albanian data protection legislation should put more effort into Information and Data Protection, following the best practices of its homologs in EU countries. Human factor knowledge and user-centered design principles would be helpful for security designers to produce more practical security solutions [241].

Increasing users' awareness through training materials and sufficient resources related to smartphone threats is recommended. Materials regarding security tools can be offered and explained with ease for better access and adoption. The information provided to the users against smartphone threats is suggested to highlight the costs of taking protective behaviours. Including proper behaviours and practices in accordance with users' culture can both be perceived to be effective. Consequently, the user can feel more confident in performing securely. Moreover, providing detailed information about how to implement smartphones' security technologies would make the security technologies more adaptive to the users. This can potentially increase their motivation and performance on security.

Understanding users' behaviour in smartphone security can better serve in designing cybersecurity solutions. Understanding the factors related to users' mobile security behaviours may contribute to technologies, policies, and procedures that effectively motivate people to behave more securely. Private and public organizations should encourage users to adopt smartphone security behaviours that promote safety against threats.

5.3.2 Applying computational cognitive methods

Applying cognitive training methods can be helpful to improve behavioural traits and enhance users' security behaviours. Companies should know the characteristics of their employees and customers and develop strategies to help users' security uncertainties and promote security behaviours.. Leaders and decision-makers should consider planning strategies and apply them in accordance with the users' behaviours [242]. Also, developers

and manufacturers should consider factors influencing human behaviours and form unique strategies to ensure that systems have maximum security [237], [229].

Computational cognitive methods can be used to predict the behaviour of attackers or systems users' [243], [244]. For instance, social engineering attacks on conversation data like phone calls (call locations and conversations' details) can be detected by using network models [245]. Moreover, special attention should be paid to the reliance on recency and frequency of cyberattacks [246].

5.3.3 Multi-disciplinary research for better cybersecurity strategies

When developing strategies that promote protective behaviours, individual differences and other factors hidden in national differences can be utilized. A fundamental requirement to address cyber threats, should be considered the increase of countries' capacities. This work highlights cybersecurity needs structure, approach, and technical capacities improvements. Future systems, especially those belonging to the critical infrastructure, are suggested to follow European strategic priorities in cybersecurity [247].

Research should focus on understanding how individuals adopt and use new technology and how risk is perceived. A strong collaboration of economics, social disciplines, and technology experts is needed. Such multi-disciplinary research can serve in modeling and designing better future solutions in the digital world. Moreover, simulation experiments (i.e., artificial intelligence) can create more awareness and a greater understanding of the unconscious and intuitive reactions to threats.

References

[1] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *Commun. Surv. Tutorials, IEEE*, vol. 15, pp. 446–471, Jan. 2013, doi: 10.1109/SURV.2012.013012.00028.

[2] ENISA, "Cyber Europe 2010 Report ," 2011. Accessed: Apr. 07, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/ce2010report.

[3] N. Leavitt, "Mobile Security: Finally a Serious Problem?," *Computer (Long. Beach. Calif).*, vol. 44, no. 6, pp. 11–14, 2011, doi: 10.1109/MC.2011.184.

[4] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008, doi: https://doi.org/10.1016/j.chb.2008.04.005.

[5] B.-Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, pp. 815–825, 2009.

[6] A. Alhogail, A. Mirza, and S. Bakry, "A comprehensive human factor framework for information security in organizations," *J. Theor. Appl. Inf. Technol.*, vol. 78, pp. 201–211, Aug. 2015.

[7] A. D. Giwah, "User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory," in *SoutheastCon 2018*, 2018, pp. 1–5, doi: 10.1109/SECON.2018.8479178.

[8] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt, *Personality and IT security: An application of the five-factor model*, vol. 6. 2006.

[9] J. Uffen, N. Kaemmerer, and M. Breitner, "Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures," *J. Inf. Secur.*, vol. 04, pp. 203–212, Jan. 2013, doi: 10.4236/jis.2013.44023.

[10] R. Crossler and F. Bélanger, "An Extended Perspective on Individual Security

Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument," *SIGMIS Database*, vol. 45, no. 4, pp. 51–71, Nov. 2014, doi: 10.1145/2691517.2691521.

[11] F. Belanger and R. E. Crossler, "Dealing with digital traces: Understanding protective behaviors on mobile devices," *J. Strateg. Inf. Syst.*, vol. 28, no. 1, pp. 34–49, 2019, doi: https://doi.org/10.1016/j.jsis.2018.11.002.

[12] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Human Behav.*, vol. 69, pp. 437–443, Apr. 2017, doi: 10.1016/j.chb.2016.12.040.

[13] R. Xu, R. M. Frey, E. Fleisch, and A. Ilic, "Understanding the impact of personality traits on mobile app adoption – Insights from a large-scale field study," *Comput. Human Behav.*, vol. 62, pp. 244–256, 2016, doi: https://doi.org/10.1016/j.chb.2016.04.011.

[14] H. Shinoda, "The Concept of Human Security : Historical and Theoretical Implications," in *IPSHU English Research Report Series No.19. Conflict and Human Security: A Search for New Approaches of Peace-building*, no. 19, 2004, pp. 5–22.

[15] R. S. Post, A. A. Kingsbury, and D. A. Schachtsiek, *Security Administration: An Introduction to the Protective Services*. Butterworth-Heinemann, 1991.

[16] UNDP, *Human Development Report*. 1994.

[17] E. Rothschild, "What is Security?," *Daedalus*, vol. 124, no. 3, pp. 53–98, 1995, doi: 10.1016/b978-159749168-6/50005-x.

[18] D. A. Baldwin, "The concept of security," *Rev. Int. Stud.*, vol. 23, no. 1, pp. 5–26, 1997, doi: 10.1017/S0260210597000053.

[19] R. Fischer, E. Halibozek, and G. Green, *Introduction to Security*. Butterworth-Heinemann, 2006.

[20] G. Manunta, "What is Security?," *Secur. J.*, vol. 12, no. 3, pp. 57–66, 1999, doi: 10.1057/palgrave.sj.8340030.

[21] D. Brooks, “What is security: Definition through knowledge categorization,” *Secur. J.*, vol. 23, pp. 225–239, Jul. 2010, doi: 10.1057/sj.2008.18.

[22] Joint Chiefs of Staff, “Cyberspace Operations,” in *Joint Publication 3-12 Cyberspace Operations*, 2018, pp. 1–11.

[23] E. Kadena and P. Holicza, “Security Issues in the Blockchain(ed) World,” in *2018 IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI)*, Nov. 2018, pp. 211–216, doi: 10.1109/CINTI.2018.8928212.

[24] Cryptomusem, “Enigma History,” 2012. https://www.cryptomuseum.com/crypto/enigma/hist.htm (accessed Aug. 24, 2020).

[25] A. Hodges, “Alan Turing,” in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed. 2002.

[26] A. L. Rusell, “OSI: The Internet That Wasn’t - IEEE Spectrum,” *IEEE Spectrum*, Jul. 30, 2013. https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt (accessed Apr. 07, 2021).

[27] J. P. Anderson, “Computer Security Technology Planning Study (Volume I),” Washington, 1972.

[28] B. Middleton, “The 1980,” in *A History of Cyber Security Attacks: 1980 to Present*, 1st ed., Florida, USA: Taylor & Francis Group, 2017, pp. 3–33.

[29] S. B. Lipner, “The Birth and Death of the Orange Book,” *IEEE Ann. Hist. Comput.*, vol. 37, no. 2, pp. 19–31, 2015, doi: 10.1109/MAHC.2015.27.

[30] H. J. Highland, “A history of computer viruses — Introduction,” *Comput. Secur.*, vol. 16, no. 5, pp. 412–415, 1997, doi: https://doi.org/10.1016/S0167-4048(97)82245-6.

[31] B. Middleton, “The 2000,” in *A History of Cyber Security Attacks: 1980 to Present*, 1st ed., Florida, USA: Taylor & Francis Group, 2017, pp. 66–99.

[32] E. Kaděna, “The use of smartphones in surveillance,” in *Management, Enterprise and Benchmarking in the 21st Century*, 2018, pp. 170–179.

[33] E. Kaděna and A. Kerti, “Security Risks of Machine-to-Machine Communications,”

HÍRVILLÁM = SIGNAL BADGE, vol. 8, no. 1, pp. 95–115, 2017.

[34] E. Kadena, H. P. D. Nguyen, and L. Ruiz, “Mobile Robots: An Overview of Data and Security,” in *Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP*, 2021, pp. 291–299.

[35] ISO/IEC, “ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary,” 2018. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (accessed Aug. 17, 2020).

[36] A. Neumann, N. Statland, and R. Webb, “Post-processing audit tools and techniques,” in *Proceedings of the NBS Invitational Workshop*, 1977, pp. 11–3; 11–4, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf.

[37] J. Andress, “Chapter 1 - What is Information Security?,” in *The Basics of Information Security*, J. Andress, Ed. Boston: Syngress, 2011, pp. 1–16.

[38] A. M. Shabut, K. T. Lwin, and M. A. Hossain, “Cyber attacks, countermeasures, and protection schemes — A state of the art survey,” in *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, 2016, pp. 37–44, doi: 10.1109/SKIMA.2016.7916194.

[39] Oberlo, “How Many People Have Smartphones? ,” 2020. https://www.oberlo.com/statistics/how-many-people-have-smartphones (accessed May 12, 2021).

[40] S. O’Dea, “Smartphone users 2020,” *Statista*, Mar. 31, 2021. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (accessed May 12, 2021).

[41] K. Cheng, M. Gao, and R. Guo, “Analysis and Research on HTTPS Hijacking Attacks,” in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, 2010, vol. 2, pp. 223–226, doi: 10.1109/NSWCTC.2010.187.

[42] T. Koutny, “Detecting Unauthorized Modification of HTTP Communication with Steganography,” in *2010 Fifth International Conference on Internet and Web Applications and Services*, 2010, pp. 26–31, doi: 10.1109/ICIW.2010.12.

[43] J. Lee and S. Jung, “Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G network,” 2012.

[44] R. Elz and R. Bush, “Clarifications to the DNS Specification RFC - Proposed Standard,” Jul. 1997. Accessed: Mar. 31, 2021. [Online]. Available: https://datatracker.ietf.org/doc/rfc2181/.

[45] D. Atkins and R. Austein, “Threat Analysis of the Domain Name System (DNS) RFC 3833 ,” Aug. 2004.

[46] T. Chomsiri, “HTTPS Hacking Protection,” *21st Int. Conf. Adv. Inf. Netw. Appl. Work.*, vol. 1, pp. 590–594, 2007.

[47] J. Singh and V. Grewal, “A Survey of Different Strategies to Pacify ARP Poisoning Attacks in Wireless Networks,” *Int. J. Comput. Appl. (0975 – 8887)*, vol. 16, no. 11, pp. 25–28, 2015.

[48] E. Rescorla and A. Schiffman, “The Secure HyperText Transfer Protocol RFC 2660,” Aug. 1999.

[49] A. R. Chordiya, S. Majumder, and A. Y. Javaid, “Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools,” in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, May 2018, pp. 438–443, doi: 10.1109/EIT.2018.8500144.

[50] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou, “User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols,” in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Jan. 2015, pp. 239–244, doi: 10.1109/CCNC.2015.7157983.

[51] A. Smith, “Strange Wi-Fi spots may harbor hackers: ID thieves may lurk behind a hot spot with a friendly name,” *Dallas Morning News, Kn. Ridder Trib. Bus. News, Washington, DC May*, vol. 9, 2007.

[52] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, “A Survey of Mobile Malware in the Wild,” in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2011, pp. 3–14, doi: 10.1145/2046614.2046618.

[53] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android Permissions: User Attention, Comprehension, and Behavior,” 2012, doi: 10.1145/2335356.2335360.

[54] S. Motiee, K. Hawkey, and K. Beznosov, “Do Windows Users Follow the Principle of Least Privilege? Investigating User Account Control Practices,” 2010, doi: 10.1145/1837110.1837112.

[55] Y. Wang, K. Streff, and S. Raman, “Smartphone Security Challenges,” *Computer (Long. Beach. Calif).*, vol. 45, pp. 52–58, Dec. 2012, doi: 10.1109/MC.2012.288.

[56] E. Kadëna, “Smartphone Security Threats,” in *Management, Enterprise and Benchmarking in the 21st Century*, Jan. 2017, pp. 141–160.

[57] H. Bigdoli, *Handbook of Information Security, Threats, Vulnerabilities, Prevention and Management. Volume 3*. Hoboken: John Wiley & Sons, Inc., 2006.

[58] C. Gao and J. Liu, “Modeling and Restraining Mobile Virus Propagation,” *IEEE Trans. Mob. Comput.*, vol. 12, no. 3, pp. 529–541, Mar. 2013, doi: 10.1109/TMC.2012.29.

[59] Mcafee, “Mobile Threat Report 2016,” 2016.

[60] Cisco Systems Inc., “Cisco Annual Security Report,” 2014.

[61] Juniper, “Juniper Networks Third Annual Mobile Threats Report,” 2012.

[62] A. Ghosh, P. K. Gajar, and S. Rai, “Bring your own device (BYOD): Security risks and mitigating strategies,” *J. Glob. Res. Comput. Sci.*, vol. 4, no. 4, pp. 62–70, 2013.

[63] E. Koh, J. Oh, and C. Im, “A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment,” *Lect. Notes Eng. Comput. Sci.*, vol. 2210, Mar. 2014.

[64] C. Rose, “BYOD: An Examination Of Bring Your Own Device In Business,” *Rev. Bus. Inf. Syst.*, vol. 17, p. 65, May 2013, doi: 10.19030/rbis.v17i2.7846.

[65] O. E. Yeboah-Boateng, “Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA),” Institut for Elektroniske Systemer, Aalborg Universitet, 2013.

[66] B. Causey, “How to Conduct an Effective IT Security Risk Assessment,” 2013. Accessed: Apr. 02, 2021. [Online]. Available: https://security.vt.edu/content/dam/security_vt_edu/downloads/risk_assessment/strategy-how-to-conduct-an-effective-it-security-risk-assessment_2411470.pdf.

[67] E. Yeboah-Boateng and P. M. Amanor, “Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices,” 2014.

[68] A. Karygiannis and L. Owens, “Wireless Network Security: 802.11, Bluetooth and Handheld Devices,” 2002.

[69] J. Bourne, “Malware and ‘connection hijacking’ remain biggest BYOD risks, report warns,” *Enterprise CIO News*, Sep. 05, 2016. https://enterprise-cio.com/news/2016/sep/05/malware-and-connection-hijacking-remain-biggest-byod-risks-report-warns/ (accessed Apr. 03, 2021).

[70] P. Ruggiero and J. Foote, “Cyber Threats to Mobile Phones Mobile Threats Are Increasing,” 2011. Accessed: Apr. 03, 2021. [Online]. Available: http://www.symantec.com/connect/blogs/phishers-have-.

[71] E. Kadëna and T. Kovács, “The need for BYOD security strategy,” *Hadmérnök (XII)*, vol. XIII, no. 4, pp. 138–145, 2017.

[72] J. Chen, “COVID-19: Cloud Threat Landscape,” *Palo Alto Networks*, 2020. https://unit42.paloaltonetworks.com/covid-19-cloud-threat-landscape/ (accessed Apr. 05, 2021).

[73] T. Thornburgh, “Social Engineering: The ‘Dark Art,’” in *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, 2004, pp. 133–135, doi: 10.1145/1059524.1059554.

[74] T. Jordan and P. Taylor, “A Sociology of Hackers,” *Sociol. Rev.*, vol. 46, no. 4, pp. 757–780, Nov. 1998, doi: 10.1111/1467-954X.00139.

[75] K. D. Mitnick and W. L. Simon, “Security’s Weakest Link,” in *The Art of Deception: Controlling the Human Element of Security*, USA: John Wiley & Sons, Inc., 2003.

[76] Zimperium, “COVID-19 Mobile Threats Against Remote Workers,” *zLabs*, Apr. 2020. https://blog.zimperium.com/covid-19-threats-against-mobile-remote-workers-what-enterprises-need-to-know/ (accessed Apr. 05, 2021).

[77] IBM, “Understanding the mobile threat landscape in 2019,” 2019.

[78] Deloitte, “COVID-19 Global Cyber risks: Is a major cyberattack looming?,” Jun. 2020. Accessed: Apr. 14, 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-cyber-covid-19-deloitte-global-cyber-covid-executive-briefing-issue-8release-date-6-3-2020-vf.pdf.

[79] Interpol, “Global Landscape on Covid-19 Cyberthreat,” 2020.

[80] L. Porta, “Analysis: Internet traffic related to coronavirus - the good and the bad,” *Wandera*, 2020. https://www.wandera.com/analysis-covid19-internet-traffic/ (accessed Apr. 06, 2021).

[81] A. Keszthelyi, “About Passwords,” *Acta Polytech. Hungarica*, vol. 10, pp. 99–118, Jan. 2013.

[82] A. Keszthelyi and E. Kadëna, “Misunderstanding how Passwords Work,” in *11th International Conference on Mangement, Enterprise and Benchmarking (MEB 2016)*, 2016, pp. 83–92.

[83] E. Kadena, “Password Selecting Habits,” in *RAJNAI ZOLTÁN KIBERBIZTONSÁG – CYBERSECURITY 2.*, Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 161–175.

[84] E. Kadëna and L. Ruiz, “Adoption of biometrics in mobile devices,” in *Proceedings*

of FIKUSZ Symposium for Young Researchers, 2017, pp. 140–148.

[85] M. O'Neill, "The Internet of Things: do more devices mean more risks?," *Comput. Fraud Secur.*, vol. 2014, no. 1, pp. 16–17, 2014, doi: https://doi.org/10.1016/S1361-3723(14)70008-9.

[86] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, Apr. 2009, doi: 10.1057/ejis.2009.6.

[87] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Comput. Secur.*, vol. 25, no. 1, pp. 27–35, Feb. 2006, doi: 10.1016/J.COSE.2005.12.004.

[88] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/J.COSE.2013.12.003.

[89] E. Schultz, "The human factor in security," *Comput. Secur.*, vol. 24, no. 6, pp. 425–426, Sep. 2005, doi: 10.1016/J.COSE.2005.07.002.

[90] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security : Individual , Culture and Security Environment," Edinburgh (AUSTRALIA), 2010. doi: 10.14722/ndss.2014.23268.

[91] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective," *Procedia - Soc. Behav. Sci.*, vol. 147, Aug. 2014, doi: 10.1016/j.sbspro.2014.07.133.

[92] E. Kadena and M. Gupi, "HUMAN FACTORS IN CYBERSECURITY: RISKS AND IMPACTS," *Secur. Sci. J.*, vol. 2, no. 2, pp. 51–64, 2021, doi: 10.37458/ssj.2.2.3.

[93] M. Alohali, N. Clarke, S. Furnell, and S. Albakri, *Information security behavior: Recognizing the influencers*. 2017.

[94] M. M. Ratchford and Y. Wang, “BYOD-Insure: A Security Assessment Model for Enterprise BYOD,” in *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, 2019, pp. 1–10, doi: 10.1109/MOBISECSERV.2019.8686551.

[95] Z. Tu, O. Turel, Y. Yuan, and N. Archer, “Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination,” *Inf. Manag.*, vol. 52, Mar. 2015, doi: 10.1016/j.im.2015.03.002.

[96] D. Jeske, P. Briggs, and L. Coventry, “Exploring the relationship between impulsivity and decision-making on mobile devices,” *Pers. Ubiquitous Comput.*, vol. 20, no. 4, pp. 545–557, 2016, doi: 10.1007/s00779-016-0938-4.

[97] H. Romer, “Best practices for BYOD security,” *Comput. Fraud Secur.*, vol. 2014, no. 1, pp. 13–15, 2014, doi: https://doi.org/10.1016/S1361-3723(14)70007-7.

[98] P. Steiner, “Going beyond mobile device management,” *Comput. Fraud Secur.*, vol. 2014, pp. 19–20, Apr. 2014, doi: 10.1016/S1361-3723(14)70483-X.

[99] E. Kadena, “Albania: Earthquake shock of the 26th November 2019,” *Natl. Secur. Rev. Period. Mil. Natl. Secur. Serv.*, vol. n/a, no. 1, pp. 54–72, 2020.

[100] R. H. Thaler, *Quasi Rational Economics (Google eBook)*. New York: Russell Sage Foundation, 1994.

[101] F. Fukuyama, *Trust: The Social Virtue and the Creation of Prosperity*. London: Penguin Books, 1995.

[102] A. L. Kroeber and C. Kluckhohn, “Culture: a critical review of concepts and definitions.,” *Pap. Peabody Museum Archaeol. Ethnol. Harvard Univ.*, vol. 47, no. 1, pp. viii, 223–viii, 223, 1952.

[103] J. R. Baldwin, S. L. Faulkner, M. L. Hecht, and S. L. Lindsley, Eds., “Redefining culture: Perspectives across the disciplines.,” *Redefining culture: Perspectives across the disciplines.* Lawrence Erlbaum Associates Publishers, Mahwah, NJ, US, pp. xxiii, 260–xxiii, 260, 2006.

[104] E. B. Tylor, “Primitive culture: Researches into the development of mythology,

philosophy, religion, language, art and custom, Vol. 1, 3rd American from 2nd English ed.," *Primitive culture: Researches into the development of mythology, philosophy, religion, language, art and custom, Vol. 1, 3rd American from 2nd English ed.* Henry Holt and Company, NY, US, pp. xii, 502–xii, 502, 1889, doi: 10.1037/12987-000.

[105] M. J. Herskovits, *Man and his works; the science of cultural anthropology.* Oxford, England: Alfred A. Knopf, 1949.

[106] M. Mead, *The Study of Culture at a Distance*. Chicago: University of Chicago Press, 1953.

[107] B. Malinowski, "Culture," in *Encyclopedia of the Social Sciences*, vol. 4, E.R.A. Seligman, Ed. New York: MacMillan, 1931, pp. 621–646.

[108] C. Geertz, *The interpretation of cultures*. New York: Basic Books, 1973.

[109] M. Harris, *Cultural Materialism: the Struggle for a Science of Culture*. Walnut Creek, CA: AltaMira Press, 2001.

[110] R. D'Andrade, *The Development of Cognitive Anthropology*. Cambridge: Cambridge University Press, 1995.

[111] P. J. Richerson and R. Boyd, *Not by Genes Alone: How Culture Transformed Human Evolution*. Chicago, IL: University of Chicago Press, 2005.

[112] A. T. Church *et al.*, "Cultural Differences in Implicit Theories and Self-Perceptions of Traitedness: Replication and Extension With Alternative Measurement Formats and Cultural Dimensions," *J. Cross. Cult. Psychol.*, vol. 43, no. 8, pp. 1268–1296, Dec. 2011, doi: 10.1177/0022022111428514.

[113] S. Venaik and P. Brewer, "The Common Threads of National Cultures," *Australas. Mark. J.*, vol. 23, no. 1, pp. 75–85, Feb. 2015, doi: 10.1016/j.ausmj.2014.12.001.

[114] S. H. Schwartz, "Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries," in *Advances in experimental social psychology*, vol. 25, Elsevier, 1992, pp. 1–65.

[115] G. Hofstede, *Culture's consequences: Comparing values, behaviors, institutions and*

organizations across nations. Sage publications, 2001.

[116] R. J. House, P. J. Hanges, M. Javidan, P. W. Dorfman, and V. Gupta, *Culture, leadership, and organizations: The GLOBE study of 62 societies*. Sage publications, 2004.

[117] G. Hofstede, *Cultures and Organizations: Software of the Mind.* New York: McGraw-Hill, 1991.

[118] G. Hofstede, G. J. Hofstede, and M. Minkov, *Cultures and Organizations: Software of the Mind*, 3rd ed. New York: McGraw-Hill, 2011.

[119] Hofstede Insights, "Country Comparison." https://www.hofstede-insights.com/country-comparison/albania,hungary/ (accessed Apr. 16, 2021).

[120] T. Dinev, J. Goo, Q. Hu, and K. Nam, *User behavior toward preventive technologies - cultural differences between the United States and South Korea.* 2006.

[121] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Comput. Secur.*, vol. 24, no. 2, pp. 124–133, 2005, doi: https://doi.org/10.1016/j.cose.2004.07.001.

[122] E. Albrechtsen, "A qualitative study of users' view on information security," *Comput. Secur.*, vol. 26, no. 4, pp. 276–289, 2007, doi: https://doi.org/10.1016/j.cose.2006.11.004.

[123] C. Matt and P. Peckelsen, "Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 4832–4841, doi: 10.1109/HICSS.2016.599.

[124] B. Hanus and Y. "Andy" Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 2–16, Jan. 2016, doi: 10.1080/10580530.2015.1117842.

[125] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975, doi:

10.1080/00223980.1975.9915803.

[126] J. E. Maddux and R. W. Rogers, “Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change,” *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983, doi: https://doi.org/10.1016/0022-1031(83)90023-9.

[127] R. Baskerville, “Risk analysis: an interpretive feasibility tool in justifying information systems security,” *Eur. J. Inf. Syst.*, vol. 1, no. 2, pp. 121–130, Mar. 1991, doi: 10.1057/ejis.1991.20.

[128] ROGERS and R. W., “Cognitive and Physiological process in fear appeals and attitude change : A revised theory of protection motivation,” *Soc. Psychophysiol.*, pp. 153–176, 1983, Accessed: Aug. 26, 2020. [Online]. Available: http://ci.nii.ac.jp/naid/10030147332/en/.

[129] N. K. Janz and M. H. Becker, “The Health Belief Model: A Decade Later,” *Health Educ. Q.*, vol. 11, no. 1, pp. 1–47, Mar. 1984, doi: 10.1177/109019818401100101.

[130] N. Weinstein, “Perceived Probability, Perceived Severity, and Health-Protective Behavior,” *Health Psychol.*, vol. 19, pp. 65–74, Feb. 2000, doi: 10.1037/0278-6133.19.1.65.

[131] H. Liang and Y. Xue, “Avoidance of information technology threats: A theoretical perspective,” *MIS Q. Manag. Inf. Syst.*, vol. 33, no. 1, pp. 71–90, 2009, doi: 10.2307/20650279.

[132] H. Liang and Y. Xue, “Understanding security behaviors in personal computer usage: A threat avoidance perspective,” *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010, doi: 10.17705/1jais.00232.

[133] D. Carpenter, D. Young, P. Barrett, and A. Mcleod, “Refining Technology Threat Avoidance Theory,” *Commun. Assoc. Inf. Syst.*, vol. 44, pp. 380–407, Jan. 2019, doi: 10.17705/1CAIS.04422.

[134] R. L. Oliver and P. K. Berger, “A Path Analysis of Preventive Health Care Decision Models,” *J. Consum. Res.*, vol. 6, no. 2, pp. 113–122, Sep. 1979, doi: 10.1086/208755.

[135] A. J. Burns, C. Posey, T. L. Roberts, and P. Benjamin Lowry, “Examining the relationship of organizational insiders’ psychological capital with information security threat and coping appraisals,” *Comput. Human Behav.*, vol. 68, pp. 190–209, 2017, doi: https://doi.org/10.1016/j.chb.2016.11.018.

[136] A. H. Maslow, “A theory of human motivation.,” *Psychol. Rev.*, vol. 50, no. 4, pp. 370–396, 1943, doi: 10.1037/h0054346.

[137] J. Mitzen, “Ontological Security in World Politics: State Identity and the Security Dilemma,” *Eur. J. Int. Relations*, vol. 12, no. 3, pp. 341–370, Sep. 2006, doi: 10.1177/1354066106067346.

[138] M. A. Moon, M. J. Khalid, H. M. Awan, S. Attiq, H. Rasool, and M. Kiran, “Consumer’s perceptions of website’s utilitarian and hedonic attributes and online purchase intentions: A cognitive–affective attitude approach,” *Spanish J. Mark. - ESIC*, vol. 21, no. 2, pp. 73–88, 2017, doi: https://doi.org/10.1016/j.sjme.2017.07.001.

[139] C. Posey, T. Roberts, and P. Lowry, “The impact of organizational commitment on insiders’ motivation to protect organizational information assets,” *J. Manag. Inf. Syst.*, vol. 32, pp. 179–214, Aug. 2015.

[140] A. Bandura, “Self-efficacy mechanism in human agency.,” *Am. Psychol.*, vol. 37, no. 2, pp. 122–147, 1982, doi: 10.1037/0003-066X.37.2.122.

[141] R. S. Lazarus and S. Folkman, *Stress, Appraisal, and Coping*, 1st ed. Springer Publishing Company, 1984.

[142] A. Biggs, P. Brough, and S. Drummond, “Lazarus and Folkman’s psychological stress and coping theory.,” in *The handbook of stress and health: A guide to research and practice.*, Wiley-Blackwell, 2017, pp. 351–364.

[143] D. Kroenke, *MIS Essentials*, 4th ed. Pearson, 2014.

[144] B. Robertson, “Technical, data, and human safeguards against security threats,” 2020. https://sites.google.com/site/bus141benrobertson/technical-data-and-human-safeguards-against-security-threats (accessed Aug. 28, 2020).

[145] I. M. Rosenstock, “The Health Belief Model and Preventive Health Behavior,” *Health Educ. Monogr.*, vol. 2, no. 4, pp. 354–386, Dec. 1974, doi: 10.1177/109019817400200405.

[146] A. E. de Albuquerque Junior, E. M. dos Santos, A. E. de Albuquerque Junior, and E. M. dos Santos, “ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH INSTITUTES,” *J. Inf. Syst. Technol. Manag.*, vol. 12, no. 2, pp. 289–315, May 2015, doi: 10.4301/S1807-17752015000200006.

[147] I. Woon, G. Tan, and R. T. Low, *A Protection Motivation Theory Approach to Home Wireless Security*. 2005.

[148] R. Agarwal, V. Sambamurthy, and R. M. Stair, “Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy—An Empirical Assessment,” *Inf. Syst. Res.*, vol. 11, no. 4, pp. 418–430, Aug. 2000, [Online]. Available: http://www.jstor.org/stable/23011046.

[149] D. R. Compeau and C. A. Higgins, “Computer Self-Efficacy: Development of a Measure and Initial Test,” *MIS Q.*, vol. 19, no. 2, pp. 189–211, Aug. 1995, doi: 10.2307/249688.

[150] D. Compeau, C. A. Higgins, and S. Huff, “Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study,” *MIS Q.*, vol. 23, no. 2, pp. 145–158, Aug. 1999, doi: 10.2307/249749.

[151] I. Ajzen, “The theory of planned behavior,” *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1991, doi: https://doi.org/10.1016/0749-5978(91)90020-T.

[152] I. Ajzen and M. Fishbein, “Understanding Attitudes and Predicting Social Behavior,” 1980.

[153] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User Acceptance of Information Technology: Toward a Unified View,” *MIS Q.*, vol. 27, no. 3, pp. 425–478, Aug. 2003, doi: 10.2307/30036540.

[154] S. F. Verkijika, “Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret,” *Comput. Secur.*, vol. 77, pp.

860–870, 2018, doi: https://doi.org/10.1016/j.cose.2018.03.008.

[155] S. Churchill and D. Jessop, “Spontaneous implementation intentions and impulsivity: Can impulsivity moderate the effectiveness of planning strategies?,” *Br. J. Health Psychol.*, vol. 15, pp. 529–541, Oct. 2009, doi: 10.1348/135910709X475423.

[156] L. Hadlington, “Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours,” *Heliyon*, vol. 3, no. 7, Jul. 2017, doi: 10.1016/j.heliyon.2017.e00346.

[157] L. Hadlington, “The ‘human factor’ in cybersecurity: Exploring the accidental insider,” in *Psychological and Behavioral Examinations in Cyber Security*, 2018, pp. 46–63.

[158] C. R. Cloninger, T. R. Przybeck, and D. M. Svrakic, “The Tridimensional Personality Questionnaire: U.S. Normative Data,” *Psychol. Rep.*, vol. 69, no. 3, pp. 1047–1057, 1991, doi: 10.2466/pr0.1991.69.3.1047.

[159] C. G. Coutlee, C. S. Politzer, R. H. Hoyle, and S. A. Huettel, “An Abbreviated Impulsiveness Scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11.,” *Archives of Scientific Psychology*, vol. 2, no. 1. American Psychological Association, Huettel, Scott A.: Center for Cognitive Neuroscience, Duke University, Box 90999, Durham, NC, US, 27710, scott.huettel@duke.edu, pp. 1–12, 2014, doi: 10.1037/arc0000005.

[160] J. H. Patton, M. S. Stanford, and E. S. Barratt, “Factor structure of the Barratt Impulsiveness Scale.,” *Journal of Clinical Psychology*, vol. 51, no. 6. John Wiley & Sons, US, pp. 768–774, 1995, doi: 10.1002/1097-4679(199511)51:6<768::AID-JCLP2270510607>3.0.CO;2-1.

[161] K. R. MacCrimmon and D. A. Wehrung, “Characteristics of Risk Taking Executives,” *Manag. Sci.*, vol. 36, no. 4, pp. 422–435, Apr. 1990.

[162] S. B. Sitkin and A. L. Pablo, “Reconceptualizing the Determinants of Risk Behavior,” *Acad. Manag. Rev.*, vol. 17, no. 1, pp. 9–38, 1992, doi: 10.2307/258646.

[163] M. Keil, L. Wallace, D. Turk, G. Dixon-Randall, and U. Nulden, “Investigation of risk

perception and risk propensity on the decision to continue a software development project," *J. Syst. Softw.*, vol. 53, pp. 145–157, Aug. 2000, doi: 10.1016/S0164-1212(00)00010-8.

[164] K. Sullivan, "Corporate managers' Risky behavior: Risk taking or Avoiding?," *J. Financ. Strateg. Decis.*, vol. 10, no. 3, pp. 63–74, 1997.

[165] J. G. March and Z. Shapira, "Variable risk preferences and the focus of attention.," *Psychol. Rev.*, vol. 99, no. 1, pp. 172–183, 1992, doi: 10.1037/0033-295X.99.1.172.

[166] G. M. Frankfurter, E. G. McGoun, and K. C. H. Chiang, "Practical Views of Risk-Taking," *J. Invest.*, vol. 10, no. 4, pp. 30 LP – 40, Nov. 2001, doi: 10.3905/joi.2001.319484.

[167] S. B. Sitkin and L. R. Weingart, "Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity," *Acad. Manag. J.*, vol. 38, no. 6, pp. 1573–1592, 1995, doi: 10.2307/256844.

[168] K.-T. Hung and C. Tangpong, "General Risk Propensity in Multifaceted Business Decisions: Scale Development," *J. Manag. Issues*, vol. 22, no. 1, pp. 88–106, Aug. 2010, [Online]. Available: http://www.jstor.org/stable/25822517.

[169] E. Bendoly, K. Donohue, and K. L. Schultz, "Behavior in operations management: Assessing recent findings and revisiting old assumptions," *J. Oper. Manag.*, vol. 24, no. 6, pp. 737–752, Dec. 2006, doi: 10.1016/j.jom.2005.10.001.

[170] Q. Nguyen and D. Kim, *Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives*. 2017.

[171] J. Lee, J.-H. Ahn, and B. Park, "The Effect of Repetition in Internet Banner Ads and the Moderating Role of Animation," *Comput. Hum. Behav.*, vol. 46, no. C, pp. 202–209, May 2015, doi: 10.1016/j.chb.2015.01.008.

[172] M. Deutsch, *The Resolution of Conflict*. Yale University Press, 1973.

[173] J. B. Rotter, "Generalized expectancies for interpersonal trust.," *Am. Psychol.*, vol. 26, no. 5, pp. 443–452, 1971, doi: 10.1037/h0031464.

[174] R. Hsiao, “Technology fears: Distrust and cultural persistence in electronic marketplace adoption,” *J. Strateg. Inf. Syst.*, vol. 12, pp. 169–199, Oct. 2003, doi: 10.1016/S0963-8687(03)00034-9.

[175] H. Abelson *et al.*, “Keys under doormats: mandating insecurity by requiring government access to all data and communications,” *J. Cybersecurity*, vol. 1, no. 1, pp. 69–79, Sep. 2015, doi: 10.1093/cybsec/tyv009.

[176] Z. Fang, W. Han, and Y. Li, “Permission based Android security: Issues and countermeasures,” *Comput. Secur.*, vol. 43, pp. 205–218, 2014, doi: https://doi.org/10.1016/j.cose.2014.02.007.

[177] A. Mylonas, A. Kastania, and D. Gritzalis, “Delegate the smartphone user? Security awareness in smartphone platforms,” *Comput. Secur.*, vol. 34, pp. 47–66, 2013, doi: https://doi.org/10.1016/j.cose.2012.11.004.

[178] A. H. Mark and P. P. Karen, “Mobile device security considerations for small- and medium-sized enterprise business mobility,” *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 97–114, Jan. 2014, doi: 10.1108/IMCS-03-2013-0019.

[179] M. R. De Villiers, “Models for Interpretive Information Systems Research, Part 1: IS Research, Action Research, Grounded Theory - A Meta-Study and Examples,” in *Mora, M., Gelman, O., Steenkamp, A. L., & Raisinghani, M. (Eds.). Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems*, IGI Global, 2012, pp. 222–237.

[180] N. J. Fox, “Post-positivism,” in *The SAGE Encyclopaedia of Qualitative Research Methods*, L. Given, Ed. London: Sage, 2008.

[181] R. B. Burns, *Introduction to research methods*, 4th ed. Australia: SAGE Publications Ltd, 2000.

[182] F. Waismann, *Causality and Logical Positivism*. Springer, 2011.

[183] T. L. Baker, *Doing social research*. New York: McGraw-Hill, 1994.

[184] M. N. K. Saunders, P. Lewis, and A. Thornhill, *Research methods for business*

students. Harlow, Essex, England: Pearson Education Limited, 2016.

[185] D. W. Straub, “Validating Instruments in MIS Research,” *MIS Q.*, vol. 13, no. 2, pp. 147–169, Jan. 1989, doi: 10.2307/248922.

[186] J. W. Creswell, *Research design : qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, California: SAGE Publications, 2014.

[187] S. A. Samani, “Steps in Research Process (Partial Least Square of Structural Equation Modeling (PLS-SEM)),” *Int. J. Soc. Sci. Bus.*, vol. 1, no. 2, pp. 55–66, Oct. 2016, Accessed: Jan. 24, 2021. [Online]. Available: www.ijssb.com.

[188] D. P. Bachmann, J. Elfrink, and G. Vazzana, “Tracking the Progress of E-mail Versus Snail-Mail,” *Mark. Res.*, vol. 8, no. 2, pp. 31–35, 1996.

[189] European Commision, *Ethics for researchers*. Luxembourg, 2013.

[190] ALLEA - All European Academies, *The European code of conduct for research integrity*. Berlin: Berlin-Brandenburg Academy of Sciences and Humanities, 2017.

[191] C. L. Claar and J. Johnson, “Analyzing Home PC Security Adoption Behavior,” *J. Comput. Inf. Syst.*, vol. 52, no. 4, pp. 20–29, Jun. 2012, doi: 10.1080/08874417.2012.11645573.

[192] N. Nicholson, E. Soane, M. Fenton-O’Creevy, and P. Willman, “Personality and Domain-Specific Risk Taking,” *J. Risk Res.*, vol. 8, Mar. 2005, doi: 10.1080/1366987032000123856.

[193] M. Ashleigh, M. Higgs, and V. Dulewicz, “A new propensity to trust scale and its relationship with individual well-being: Implications for HRM policies and practices,” *Hum. Resour. Manag. J.*, vol. Vol 22, pp. 360–376, Nov. 2012, doi: 10.1111/1748-8583.12007.

[194] G. A. Miller, “The magical number seven plus or minus two: some limits on our capacity for processing information.,” *Psychol. Rev.*, vol. 63 2, pp. 81–97, 1956.

[195] M. Maness, P. Sheela, S. Balusu, and A. Pinjari, “When Neutral Responses on a Likert Scale Do Not Mean Opinion Neutrality: Accounting for Unsure Responses in a Hybrid

Choice Modeling Framework," 2018.

[196] G. Kalton, J. Roberts, and D. Holt, "The Effects of Offering a Middle Response Option with Opinion Questions," *J. R. Stat. Soc. Ser. D (The Stat.*, vol. 29, no. 1, pp. 65–78, Jan. 1980, doi: 10.2307/2987495.

[197] A. Baka, L. Figgou, and V. Triga, "'Neither agree, nor disagree': A critical analysis of the middle answer category in Voting Advice Applications," *Int. J. Electron. Gov.*, vol. 5, pp. 244–263, Jan. 2012, doi: 10.1504/IJEG.2012.051306.

[198] P. Sturgis, C. Roberts, and P. Smith, "Middle Alternatives Revisited: How the neither/nor Response Acts as a Way of Saying 'I Don't Know'?," *Sociol. Methods Res.*, vol. 43, no. 1, pp. 15–38, Sep. 2012, doi: 10.1177/0049124112452527.

[199] D. L. Streiner, "Finding Our Way: An Introduction to Path Analysis," *Can J Psychiatry*, vol. 50, no. 2, pp. 115–122, 2005.

[200] L. Yair, *Assessing the Value of E-Learning Systems*. Information Science Publishing, 2006.

[201] G. S. Maddala, "Outliers," in *Introduction to Econometrics*, 2nd ed., New York: MacMillan, 1992, p. 89.

[202] C. Leys, M. Delacre, Y. L. Mora, D. Lakens, and C. Ley, "How to classify, detect, and manage univariate and multivariate outliers, with emphasis on pre-registration," *Int. Rev. Soc. Psychol.*, vol. 32, no. 1, pp. 1–10, 2019, doi: 10.5334/irsp.289.

[203] C. A. Mertler and R. V. Reinhart, *Advanced and multivariate statistical methods: Practical application and interpretation*, 6th ed. Taylor and Francis, 2016.

[204] C. Leys, O. Klein, Y. Dominicy, and C. Ley, "Detecting multivariate outliers: Use a robust variant of the Mahalanobis distance," *J. Exp. Soc. Psychol.*, vol. 74, pp. 150–156, Jan. 2018, doi: 10.1016/j.jesp.2017.09.011.

[205] P. C. Mahalanobis, "On test and measures of group divergence : theoretical formulae," *J. Proc. Asiat. Soc. Bengal*, vol. New series, no. 4, pp. 541–588, 1930, Accessed: Mar. 02, 2021. [Online]. Available: http://localhost:8080/xmlui/handle/10263/1639.

[206] P. C. Mahalanobis, “On the generalised distance in statistics,” in *Proceedings of the National Institute of Sciences of India*, 1936, pp. 49–55, Accessed: Mar. 01, 2021. [Online]. Available: https://insa.nic.in/writereaddata/UpLoadedFiles/PINSA/Vol02_1936_1_Art05.pdf.

[207] R. D. Cook, “Detection of Influential Observation in Linear Regression,” *Technometrics*, vol. 19, no. 1, pp. 15–18, 1977, Accessed: Mar. 02, 2021. [Online]. Available: http://www.stat.ucla.edu/~nchristo/statistics100C/1268249.pdf.

[208] R. Kline, *Principles And Practice Of Structural Equation Modeling*. 2010.

[209] S. Brown, “Measures of Shape: Skewness and Kurtosis,” Oct. 26, 2020. https://brownmath.com/stat/shape.htm (accessed Mar. 16, 2021).

[210] E. S. Vasu and P. B. Elmore, “The Effect of Multicollinearity and the Violation of the Assumption of Normality on the Testing of Hypotheses in Regression Analysis,” Washington, D.C., Mar. 1975.

[211] W. Yoo, R. Mayberry, S. Bae, K. Singh, Q. Peter He, and J. W. Lillard, “A Study of Effects of MultiCollinearity in the Multivariable Analysis.,” *Int. J. Appl. Sci. Technol.*, vol. 4, no. 5, pp. 9–19, Oct. 2014, Accessed: Mar. 11, 2021. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/25664257.

[212] J.-M. Becker, K. Klein, and M. Wetzels, “Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models,” *Long Range Plann.*, vol. 45, no. 5, pp. 359–394, 2012, doi: https://doi.org/10.1016/j.lrp.2012.10.001.

[213] J. Hair, G. T. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 1st ed. Thousand Oaks, CA: Sage, 2014.

[214] L. J. Cronbach, “Coefficient alpha and the internal structure of tests,” *Psychometrika*, vol. 16, no. 3, pp. 297–334, Sep. 1951, doi: 10.1007/BF02310555.

[215] C. Fornell and D. F. Larcker, “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *J. Mark. Res.*, vol. 18, no. 1, p. 50, Feb. 1981, doi: 10.2307/3151312.

[216] C. M. Ringle, S. Wende, and J.-M. Becker, “SmartPLS 3.” SmartPLS, Bönningstedt, 2015, Accessed: Mar. 16, 2021. [Online]. Available: http://www.smartpls.com.

[217] M. Brunner and H.-M. SÜβ, “Analyzing the Reliability of Multidimensional Measures: An Example from Intelligence Research,” *Educ. Psychol. Meas.*, vol. 65, no. 2, pp. 227–240, Apr. 2005, doi: 10.1177/0013164404268669.

[218] G. F. Kuder and M. W. Richardson, “The theory of the estimation of test reliability,” *Psychometrika*, vol. 2, no. 3, pp. 151–160, 1937, doi: 10.1007/BF02288391.

[219] N. L. Ritter, “Understanding a Widely Misunderstood Statistic: Cronbach’s α,” New Orleans, Feb. 2010.

[220] R. P. Bagozzi, Y. Yi, and L. W. Phillips, “Assessing Construct Validity in Organizational Research,” *Adm. Sci. Q.*, vol. 36, no. 3, p. 458, Sep. 1991, doi: 10.2307/2393203.

[221] R. Silva, C. Ringle, D. Silva, and D. Bido, “Structural Equation Modeling with the SmartPLS,” *Rev. Bras. Mark.*, vol. 13, pp. 56–73, Sep. 2014.

[222] J. Henseler, C. M. Ringle, and M. Sarstedt, “A new criterion for assessing discriminant validity in variance-based structural equation modeling.,” *J. Acad. Mark. Sci.*, vol. 43, no. 1, pp. 115–135, 2015, doi: 10.1007/s11747-014-0403-8.

[223] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. New York: Routledge, 1988.

[224] R. F. Falk and N. B. Miller, *A primer for soft modeling.* Akron, OH, US: University of Akron Press, 1992.

[225] J. Hair, M. Sarstedt, C. M. Ringle, and S. P. Gudergan, *Advanced Issues in Partial Least Squares Structural Equation Modeling (PLS-SEM)* , 1st ed. SAGE Publications, Inc, 2017.

[226] M. Sarstedt, J. Henseler, and C. Ringle, “Multi-Group Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results,” *Adv. Int. Mark.*, vol. 22, pp. 195–218, Jan. 2011, doi: 10.1108/S1474-7979(2011)0000022012.

[227] E. Kadena, “Smartphone Security Awareness and Practices of Users in Albania,” *J. Aware.*, vol. 3, no. Special, pp. 14–81, 2018, doi: 10.26809/joa.2018548618.

[228] E. Kadena, “Necessity of BYOD Security Strategy,” in *LIX. Georgikon Napok. A múlt mérföldkövei és a jövő kihívásai: 220 éves a Georgikon*, Z. B. Nagy, Ed. Keszthely, Hungary: Pannon Egyetem Georgikon Mezőgazdaságtudományi Kar, 2017, pp. 198–204.

[229] E. Kadena, S. Kocak, K. Takácsné György, and A. Keszthelyi, “FMEA in Smartphones: A Fuzzy Approach,” *MATHEMATICS*, vol. 10, no. 3, p. 513, 2022, doi: 10.3390/math10030513.

[230] E. Kadena, “The adoption of Blockchain in Mobile Devices: Challenges and Opportunities,” in *2. International Conference on Awareness*, Canakkale: Rating Academy, 2018, pp. 421–426.

[231] E. Kadena, “Lack of cybersecurity education,” in *Współczesne problemy zarządzania, obronności i bezpieczeństwa. T. 2*, Z. Tadeusz and I. Horzela, Eds. Warsaw, Poland: Akademia Sztuki Wojennej, 2018, pp. 83–90.

[232] P. Holicza and E. Kadëna, “Smart and Secure? Millennials on Mobile Devices,” *Interdiscip. Descr. Complex Syst.*, vol. 16, no. 3-A, pp. 376–383, Sep. 2018, doi: 10.7906/indecs.16.3.10.

[233] E. Kadena, “Security in Home Automation,” *BÁNKI KÖZLEMÉNYEK*, vol. 1, no. 1, pp. 5–25, 2018.

[234] E. Kadena, “Password Selecting Habits,” in *Eight International Scientific Web-conference of Scientists and PhD. students or candidates*, Z. Rajnai, P. Schmidt, and P. Jurik, Eds. Budapest, Hungary: Óbuda University, 2020, pp. 164–176.

[235] E. Kadena, “Blockchain integration into mobile devices,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 195–201.

[236] E. Kadena, “Human error and latent conditions in mobile devices. Reducing risks through FMEA,” in *III.International Rating Academy Congress on Applied Sciences*,

Lviv: Rating Academy, 2018, pp. 8–13.

[237] E. Kadena, “Security of mobile devices in the view of Swiss Cheese Model,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 176–183.

[238] E. Kadena and L. Pokorádi, “HUMAN ERRORS IN MOBILE DEVICES,” in *European Smart, Sustainable and Safe Cities Conference 2020 : Abstract Book*, D. Tokody and Z. Nyikes, Eds. Budapest, Hungary: Óbudai Egyetem, 2020, p. 18.

[239] T. Sommestad, H. Karlzén, and J. Hallberg, “The sufficiency of the theory of planned behavior for explaining information security policy compliance,” *Inf. Comput. Secur.*, vol. 23, no. 2, pp. 200–217, Jan. 2015, doi: 10.1108/ICS-04-2014-0025.

[240] S. Coble, “Albania’s Prime Minister Issues Data Leak Apology - Infosecurity Magazine,” Dec. 24, 2021. https://www.infosecurity-magazine.com/news/albanias-prime-minister-issues/ (accessed Mar. 22, 2022).

[241] M. Sasse and I. Flechais, “Usable Security Why Do We Need It? How Do We Get It?,” in *Security and Usability: Designing secure systems that people can use*, Sebastopol, US: O’Reilly, 2005, pp. 13–30.

[242] E. Kadena, “Assessing risks in mobile devices by using fmea,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 184–194.

[243] V. D. Veksler, N. Buchler, B. E. Hoffman, D. N. Cassenti, C. Sample, and S. Sugrim, “Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users,” *Front. Psychol.*, vol. 9, 2018, doi: 10.3389/fpsyg.2018.00691.

[244] V. D. Veksler, N. Buchler, C. G. LaFleur, M. S. Yu, C. Lebiere, and C. Gonzalez, “Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior,” *Front. Psychol.*, vol. 11, 2020, doi: 10.3389/fpsyg.2020.01049.

[245] H. Sandouka, A. J. Cullen, and I. Mann, “Social engineering detection using neural networks,” in *2009 International Conference on CyberWorlds*, 2009, pp. 273–278.

[246] Z. Maqbool, P. Aggarwal, V. S. C. Pammi, and V. Dutt, “Cyber Security: Effects of Penalizing Defenders in Cyber-Security Games via Experimentation and Computational Modeling,” *Front. Psychol.*, vol. 11, 2020, doi: 10.3389/fpsyg.2020.00011.

[247] ENISA, “Analysis of the European R&D Priorities in Cybersecurity,” 2018.

[248] CISA, “What is Cybersecurity? | CISA,” May 06, 2009. https://us-cert.cisa.gov/ncas/tips/ST04-001 (accessed May 11, 2021).

[249] P. Lavrakas, “Encyclopedia of Survey Research Methods.” Thousand Oaks, California, 2008, doi: 10.4135/9781412963947 NV - 0.

[250] R. Netemeyer, W. Bearden, and S. Sharma, “Scaling Procedures.” SAGE Publications, Inc., Thousand Oaks, California, 2003, doi: 10.4135/9781412985772.

List of Tables

List of Figures

Appendix I: Definition of main terms used in the study.

The most important terms used in this study are represented and defined in the literature as follows:

Smartphone – a portable device that contains mobile telephone and computing functions.

Cybersecurity – the state of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information [248].

Construct – a characteristic or the subject matter that can be measured or observed using survey questions [249].

Construct items – survey items included in a construct that covers a particular topic [250].

Perceived Severity – subjective belief of an individual regarding the negative consequences of an event or outcome [129].

Perceived Susceptibility – individual's subjective perception of being affected from a risk [129].

Perceived Threat – perceived severity and perceived susceptibility of a "dangerous" or risky condition [129], [212].

Security Motivation – behavioural intention to use security technologies [132], [151], [152].

Security Behaviour – individuals' actual behaviour - usage of security technologies against threats [132].

Impulsivity – the urge to respond spontaneously without thinking about the consequences. [159]. It reflects the reduced ability to plan actions [160].

Risk Propensity – an individual's tendency to get involved in risk or avoid it [161], [162], [163].

Distrust Propensity – negative beliefs about another party's conduct [171].

Appendix II: Final questionnaire

Questionnaire about users' practices and behaviours on smartphones' security

Hello!

I am Kadëna Esmeralda, a Ph.D. student in Hungary. I am working on a study about users' practices and behaviours on smartphones' security. Your information is confidential and very important for my thesis. I would like to ask your help in filling out this questionnaire. It takes only 10-12 mins.

Thank you in advance!

1. **Your Age: ***
   - < =20
   - 21-30
   - 31-40
   - 41-50
   - >50

2. **Gender: ***
   - Female
   - Male
   - Prefer to not say

3. **Your place of residence (Country, City)*: _____**

4. **Where did you grow up? *:**
   - Rural settlement
   - Small Town
   - Large Town
   - Capital of your country

5. **Your education: ***
   - Secondary School
   - High School
   - Bachelor's Degree
   - Master's Degree
   - Ph.D./ Higher Degree

6. **You are: ***

- Student
- Employed
- Unemployed
- Self-employed
- Retired

7. **Approximately what is your monthly income (in Eur): ***

- Under 300
- 301-500
- 501-700
- 701-1000
- 1001 or over

8. **Do you regularly use a smartphone? ***
   - Yes
   - No

9. **What brand of smartphone do you use?***
   - Apple
   - Google
   - HTC
   - Huawei
   - Lenovo
   - LG
   - Motorola
   - Nokia
   - Samsung
   - Sony
   - Xiaomi
   - Other:_____

10. **How long have you owned a smartphone?***

- 5 months or less
- 1 year
- 2 years
- 3 years
- 4 years
- 5 years or more

11. **For what purposes are you using your smartphone? ***

- Personal
- Business

- Both

12. How long are you active with your smartphone on the internet on an average day? *

- Less than 1 hour
- 1-2 hours
- 2-3 hours
- 3-4 hours
- 5 hours or over

13. How long are you active with your smartphone on the internet on weekends and holidays? *

- Less than 1 hour
- 1-2 hours
- 2-3 hours
- 3-4 hours
- 5 hours or over

14. How important are the below-mentioned systems for you? *

Please indicate using a 6-point scale (1: don't use it, 2: ot important at all; 3: I don't think is important; 4: It can be importan; 5: Important 6: Very important):

- Personal e-mail account
- University/Business e-mail account
- Facebook
- Messenger
- Instagram
- Google Drive
- Twitter
- WhatsApp
- Viber
- Other:_____

15. Have you ever lost your smartphone? *

- Yes
- No

16. Do you let your smartphone in the others' hands? *

- Yes
- No

17. Your applications are downloaded: *

- Only from official stores
- From other sites as well

18. Has your smartphone ever been hacked (i.e., virus, malware…)? *

- Yes
- No
- I don't know

19. How many apps have you installed on your smartphone?

- <20
- 20-40
- 40-60
- 60-80
- >80

20. How frequently do you make changes (e.g. try out new apps regularly)?

- Daily
- A couple of times per week
- Rarely/a couple of times per month
- Less frequently

21. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement about: Perceived Susceptibility of getting a malicious IT*

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)

- My chances of getting malware/virus are great
- There is a good possibility that my smartphone will have malware/virus
- I feel malware/virus will infect my smartphone in the future

22. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement about: Perceived Severity of the threat consequences*

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)

- Malware/virus would steal my personal information from my smartphone without my knowledge
- Malware/virus would invade my privacy
- Malware/virus could record my Internet activities and send it to unknown parties
- My personal information collected by malware/virus could be used to commit crimes against me
- Malware/virus would slow down my Internet connection
- Malware/virus would make my smartphone run more slowly
- Malware/virus would cause system crash on my smartphone from time to time
- Malware/virus would affect some of my smartphone programs and make them difficult to use

23. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement about: Perceived Threat: *

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)

- Malware/virus poses a threat to me
- It is risky to use my smartphone if it has malware/virus

24. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Safeguard effectiveness*

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)

- Anti- (malware/virus) software would be useful for detecting and removing malware/virus
- Anti-(malware/virus) software would increase my performance in protecting my smartphone from malware/virus
- Anti-(malware/virus) software would enable me to search and remove malware/virus on my smartphone faster

25. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Safeguard cost* *(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)*

I don't have anti-(malware/virus) on my smartphone because …

… I don't know how to get an anti-(malware/virus) software

… Installing anti-(malware/virus) software is too much trouble.

… I don't want to pay for the license/paying for the license is expensive

… It slows down my smartphone

… It runs out my battery quicker

… other_____

26. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Self-Efficacy *

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)

I could successfully install and use anti-(malware/virus) software if …

… I had never used a package like it before

… I had seen someone else doing it before trying it myself

… someone else helped me get started

… I had a lot of time to complete the job

… I had just the built-in help facility for assistance

27. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Security motivation* *(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 somewhat agree, 5 = agree, and 6 = strongly agree)*

- I intend to use anti-(malware/virus) software to protect my smartphone from the threats
- I predict I would use anti-(malware/virus) software to protect my smartphone from the threats
- I plan to use anti-(malware/virus) software to protect my smartphone from the threats

28. Please answer with Yes or No to the following statements: Security Behaviour*

- I use an anti-(malware/virus) software on my smartphone.
    - Yes
    - No
- I use password protection on my smartphone.
    - Yes
    - No
- I use biometric protection on my smartphone.
    - Yes
    - No
- I use software updates on my smartphone whenever they are available.
    - Yes
    - No
- I use operating system updates on my smartphone whenever they are available.
    - Yes
    - No

29. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Risk Propensity*

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4= somewhat agree, 5= agree, and 6 = strongly agree)

- I engage in risky health related behaviors (e.g., smoking, poor diet, high alcohol consumption)

- I engage in risky career related behaviors (e.g., quitting a job without another to go to)
- I take safety risks (e.g., fast driving, cycling without a helmet)
- I never make decisions that are contrary to the regulatory framework
- I take financial risks (e.g., gambling, risky investments)
- Success makes me take higher risks
- I only take strategic financial risks; risk-taking should meet the outcomes expected from the investment
- I often think about doing things that I know society would disapprove of

30. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Impulsivity*

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = somewhat agree, 5 = agree, and 6 = strongly agree)

- I often act on the spur of the moment without stopping to think.
- I don't devote much thought and effort to preparing for the future.
- I often do whatever brings me pleasure here and now, even at the cost of distant goals.
- I'm more concerned with what happens to me in the short run than in the long run.

31. Please indicate, using a 6-point scale, how much you either agree or disagree with each statement: Distrust Propensity*

(1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = somewhat agree, 5= agree, and 6 = strongly agree)

- I have little faith in other people's promises
- In these competitive times, I have to be alert; otherwise, others will take advantage of me
- People are primarily interested in their own welfare despite what they say
- People who act in a friendly way towards me are disloyal behind my back
- People are only concerned with their own well-being

Thanks for your participation!

Appendix III: Instrument changes

Questions, constructs and items from the existing survey	Questions, constructs and items in the final survey of this research
Perceived susceptibility • It is extremely likely that my computer will contain malware in the future. • The chances of getting malware on my system are great. • There is a good possibility that my computer will contain malware at some point. • There is a good chance that there will be malware on my computer at some point in the future.	**Perceived susceptibility** • My chances of getting malware/virus are great. • There is a good possibility that my smartphone will have malware/virus. • I feel malware/virus will infect my smartphone in the future.
Perceived severity • Malware could steal personal information from my computer without my knowledge. • Malware could invade my privacy • My personal information collected by malware could be misused by cyber criminals. • Malware could record my Internet activities and send it to unknown parties. • My personal information collected by malware could be subjected to unauthorized secondary use. • My personal information collected by malware could be used to commit crimes against me. • Malware could slow down my Internet connection. • Malware could make my computer run more slowly. • Malware could cause my systems to crash from time to time. • Malware could affect some of my computer programs and make them difficult to use.	**Perceived severity** • Malware/virus would steal my personal information from my smartphone without my knowledge. • Malware/virus would invade my privacy. • Malware/virus could record my Internet activities and send it to unknown parties. • My personal information collected by malware/virus could be used to commit crimes against me. • Malware/virus would slow down my Internet connection. • Malware/virus would make my smartphone run more slowly. • Malware/virus would cause system crash on my smartphone from time to time. • Malware/virus would affect some of my smartphone programs and make them difficult to use.
Perceived threat • The consequences of getting malware on my computer threaten me. • Malware is a danger to my computer. • It would be dreadful if my computer was infected by malware. • It would be risky to use my computer if it had malware.	**Perceived threat** • Malware/virus poses a threat to me. • It is risky to use my smartphone if it has malware/virus.
Perceived effectiveness • Computer security software would be useful for detecting and removing malware. • Computer security software would increase my ability to protect my computer from malware. • Computer security software would enable me to search and remove malware on my computer faster. • Computer security software would enhance my effectiveness in finding and removing malware on my computer. • Computer security software would make it easier to search for and remove malware on my computer.	**Perceived effectiveness** • Anti- (malware/virus) software would be useful for detecting and removing malware/virus. • Anti-(malware/virus) software would increase my performance in protecting my smartphone from malware/virus. • Anti-(malware/virus) software would enable me to search and remove malware/virus on my smartphone faster.

• Computer security software would increase my productivity in searching and removing malware on my computer.	
Safeguard cost • I don't have security software on my computer because I don't know how to get it. • I don't have security software on my computer because it may cause problems with other programs on my computer • I don't have security software on my computer because installing it is too much trouble.	**Safeguard cost** ***I don't have anti-(malware/virus) on my smartphone because …*** • … I don't know how to get an anti-(malware/virus) software • … Installing anti-(malware/virus) software is too much trouble. • … I don't want to pay for the license/paying for the license is expensive • … It slows down my smartphone • … It runs out my battery quicker • Other …….
Self-efficacy • I could successfully install and use computer security software if there was no one around to tell me what to do. • I could successfully install and use computer security software if I had never used a package like it before. • I could successfully install and use computer security software if I only had the software manuals for reference. • I could successfully install and use computer security software if I had seen someone else do it before trying myself. • I could successfully install and use computer security software if I could call someone for help if I got stuck. • I could successfully install and use computer security software if someone helped me get started. • I could successfully install and use computer security software if I had a lot of time to complete the task. • I could successfully install and use computer security software if I only had the built-in help facility for assistance. • I could successfully install and use computer security software if someone showed me how to do it first. • I could successfully install and use computer security software if I had used a similar package before.	**Self-efficacy** ***I could successfully install and use anti-(malware/virus) software if …*** • … I had never used a package like it before • … I had seen someone else doing it before trying it myself • … someone else helped me get started • … I had a lot of time to complete the job • … I had just the built-in help facility for assistance
Security motivation • I intend to use computer security software to avoid malware breaches. • I use computer security software to avoid malware breaches. • I plan to use computer security software to avoid malware.	**Security motivation** • I intend to use anti-(malware/virus) software to protect my smartphone from the threats. • I predict I would use anti-(malware/virus) software to protect my smartphone from the threats • I plan to use anti-(malware/virus) software to protect my smartphone from the threats
Security behavior	**Security behavior**

• I run computer security software regularly to remove malware from my computer. • I update my computer security software regularly.	• I use an anti-(malware/virus) software on my smartphone. (Yes/No) • I use password protection on my smartphone. (Yes/No) • I use biometric protection on my smartphone. (Yes/No) • I use software updates on my smartphone whenever they are available. (Yes/No) • I use operating system updates on my smartphone whenever they are available. (Yes/No)
Risk propensity • I engage in risky recreational activities (e.g., rock-climbing, scuba diving) • I engage in risky health related behaviors (e.g., smoking, poor diet, high alcohol consumption). • I engage in risky career related behaviors (e.g., quitting a job without another to go to). • I take safety risks (e.g., fast driving, cycling without a helmet). • I take financial risks (e.g., gambling, risky investments). • I take social risks (e.g., standing for election, publicly challenging rules or decisions).	**Risk propensity** • I engage in risky health related behaviors (e.g., smoking, poor diet, high alcohol consumption). • I engage in risky career related behaviors (e.g., quitting a job without another to go to). • I take safety risks (e.g., fast driving, cycling without a helmet). • I never make decisions that are contrary to the regulatory framework. • I take financial risks (e.g., gambling, risky investments) • Success makes me take higher risks. • I only take strategic financial risks; risk-taking should meet the outcomes expected from the investment. • I often think about doing things that I know society would disapprove of.
Impulsivity • I often act on the spur of the moment without stopping to think. • I don't devote much thought and effort to preparing for the future. • I often do whatever brings me pleasure here and now, even at the cost of distant goals. • I'm more concerned with what happens to me in the short run than in the long run.	**Impulsivity** • I often act on the spur of the moment without stopping to think. • I don't devote much thought and effort to preparing for the future. • I often do whatever brings me pleasure here and now, even at the cost of distant goals. • I'm more concerned with what happens to me in the short run than in the long run.
	Distrust • I have little faith in other people's promises • In these competitive times, I have to be alert; otherwise, others will take advantage of me • People are primarily interested in their own welfare despite what they say • People who act in a friendly way towards me are disloyal behind my back • People are only concerned with their own well-being.

Appendix IV: Assumptions for Factor and Path Analysis

- **OUTLIERS (Applying Mahalanobis Distance in SPPS)**

Case_ID	PMAH_1
547	**0.00051**
399	**0.00053**
162	**0.00088**
35	**0.00091**
48	**0.00091**
239	0.00122
339	0.00122
261	0.00258
518	0.00258
429	0.00536
436	0.00536
192	0.00536
585	0.00536
424	0.00603
152	0.00603
228	0.00603
151	0.00603
469	0.00603
546	0.00603
123	0.00665
58	0.00665
302	0.00665
.....	.....

Table 19: P-values (Mahalanobis distance) and removed cases.

- **Kuder and Richardson Formula 20 (in Excel): Security Behavior (5 items) reliability calculation**

	Item 1	Item 2	Item 3	Item 3	Item 4	Item 5
Total no. of "Yes" responses	147	543	452	396	439	
p	0.25	0.92347	0.76871	0.67347	0.7466	
q	0.75	0.07653	0.23129	0.32653	0.2534	
pq	0.1875	0.07067	0.1778	0.21991	0.18919	0.84507

Table 20: KR20 Calculations

k	5
∑pq	0.84507
Var (s^2)	4.31587
KR20	**1.0**

Table 21: Security Behaviour Reliability coefficient (KR20)

- **VIF Values <10**

	VIF
DIST1	**1.592**
DIST2	**1.965**
DIST3	**2.333**
DIST4	**1.689**
DIST5	**2.387**
IMP1	**1.393**
IMP2	**1.656**
IMP3	**1.993**
IMP4	**1.862**
PSE1	4.081
PSE2	**5.711**
PSE3	4.109
PSE4	**2.564**
PSE5	3.121
PSE6	4.045
PSE7	3.753
PSE8	3.396
PSU1	3.844
PSU2	3.725
PSU3	**2.420**
PTH1	**1.453**
PTH2	**1.453**
RP1	**1.333**
RP2	**1.503**
RP3	**1.752**
RP4	**1.136**
RP5	**1.603**
RP6	**1.532**
RP7	**1.268**
RP8	**1.394**
SB1	**1.002**
SB2	**1.054**
SB3	**1.075**
SB4	**1.715**
SB5	**1.744**
SCO1	**1.907**
SCO2	**2.203**
SCO3	**1.613**
SCO4	3.222

SCO5	3.218
SE1	4.168
SE2	4.025
SE3	3.668
SEF1	**1.334**
SEF2	3.059
SEF3	3.081
SEF4	**2.859**
SEF5	**2.260**
SM1	4.625
SM2	**5.768**
SM3	4.182

Table 22: VIF Values

- **OUTER LOADINGS**

	Distrust (DIST)	Impulsivity (IMP)	Perceived Severity (PSE)	Perceived Susceptibility (PSU)	Perceived Threat (PTH)	Risk Propensity (RP)	Safeguard Cost (SCO)	Safeguard Effectiveness (SE)	Security Behavior (SB)	Security Motivation (SM)	Self-Efficacy
DIST1	**0.740**										
DIST2	**0.846**										
DIST3	**0.852**										
DIST4	**0.607**										
DIST5	**0.796**										
IMP1		**0.775**									
IMP2		**0.574**									
IMP3		**0.592**									
IMP4		**0.887**									
PSE1			**0.848**								
PSE2			**0.899**								
PSE3			**0.881**								
PSE4			**0.816**								
PSE5			**0.816**								
PSE6			**0.860**								
PSE7			**0.850**								
PSE8			**0.835**								
PSU1				**0.936**							

PSU2				0.936							
PSU3				0.888							
PTH1					0.907						
PTH2					0.855						
RP1						0.019					
RP2						-0.160					
RP3						-0.395					
RP4						0.731					
RP5						-0.236					
RP6						0.247					
RP7						0.523					
RP8						-0.148					
SB1									0.809		
SB2									0.023		
SB3									-0.028		
SB4									0.560		
SB5									0.545		
SCO1							0.931				
SCO2							0.814				
SCO3							0.295				
SCO4							0.102				
SCO5							0.059				
SE1								0.941			
SE2								0.941			
SE3								0.937			
SEF1											0.498
SEF2											0.888
SEF3											0.900
SEF4											0.888
SEF5											0.848
SM1										0.949	
SM2										0.962	
SM3										0.938	

Table 23: Outer Loadings

Acknowledgments

First and foremost, I would like to praise and thank God that I have finally accomplished the thesis!

Besides my efforts, the success of this work depends on the encouragement and guidelines of many others. I am very grateful to the Stipendium Hungaricum programme for awarding me the Ph.D. scholarship in 2017. I want to express my deep and sincere gratitude to my supervisor Dr. András Keszthelyi. Without his encouragement, guidance, and kindness since my Masters' studies, this Ph.D. thesis would not have materialized. I would also like to thank him for his friendship and his great sense of humor. Gratefully acknowledges and greatest appreciation to my co-supervisor, Prof. Dr. Katalin Takács-György, for generously giving encouragement, suggestions, guidance, and valuable inputs throughout this research. Her vision, dynamism, and motivation have deeply inspired me.

Special gratitude to the Head of the Doctoral School, Professor Lívia Cveticanin for her support and kindness since I started the Ph.D. studies. Profound gratitude to the Dean of Donát Bánki Faculty of Mechanical and Safety Engineering, Zoltán Rajnai. Thank you for your trust, encouragement, support, confidence, and assurance! My sincere thanks also go to all the professors and staff of Óbuda University that have been very supportive and collaborative with me during all these years.

Special words of gratitude go to my Ph.D. colleagues and friends who have been a major source of support during this long process. I am also very grateful to my students, friends, colleagues, and everyone that took the time to fill my survey. Without their contribution, the findings of this research would not have been possible.

Last but not least, I am grateful to the most important people in my life. Gratitude to my parents, Minushe and Skënder, to my sister Xhuli, to my brother Benard, and to my nephews Enis and Luis. Thank you for your patience, understanding, and giving me the extra strength and motivation to get things done!