FH Vorarlberg
University of Applied Sciences

How cyber security is maintained in Austrian banks

Submitted in Fulfillment of the Degree of
Master of Art in Business (MA)

University of Applied Sciences Vorarlberg
International Management and Leadership

Submitted to
Kai Gammelin

Handed in by
Alisa Demidova

Dornbirn, 09.07.2021

Notice of Confidentiality

I hereby inform you that all information provided by research participants is confidential and will not be disclosed. The names of the banks of the participants, the auditor and the representatives of these organisations will not be disclosed as part of this work for reasons of strict confidentiality. In addition, no interview will be transcribed. The information provided was to be analyzed solely by the author and her supervisor, no third parties were involved.

Dedication

First of all I would like to thank Professor (FH) Dipl.-Ing. Wilfried Manhard, MBA for giving me the opportunity to study at University and supporting me through the research process. Thank you for all your help and motivation throughout my study.

Furthermore, I would like to express huge thanks to my supervisor Kai Gammelin, who made valuable contribution to this project as he guiding me through the confusing world of the cybersecurity, mentored me and gave me incredible support. Thanks to his expertise, advice, and support this project was possible.

Moreover, I would like to thank sincerely

… all my research participants who were not afraid and agreed to support me on this delicate and dangerous topic.

… professor Martin Doppler, with whom I took the first steps of this research area and carried out the research project in contextual studies "Computer science".

… process and change manager, Maria Galitskaia, director of IT Service, Alfred Olschnögger, Information Security and Compliance Manager, Veljko Lucic, who introduced me to the world of cybersecurity and got me so interested that I chose this topic for my research.

In addition, I would like to thank my family and my boyfriend, who supported me throughout my study, the preparation of the Master Thesis, and motivated me despite difficult times of restrictions and isolation.

Finally, I dedicate this study to all future researchers in the field of cultural influence on cybersecurity, and I hope that the topic will find resonance in the hearts and minds of many.

Abstract

The Title of the Master Thesis

“How cyber security is maintained in Austrian banks”

This paper gives an insight into how cybersecurity is built inside and outside banks in Austria. The research was conducted based on information received from bank representatives in Austria as well as on literature, participation in various kinds of online conferences, and so on. The main objective of this paper was to investigate the cybersecurity execution scheme and to consider the possible impact of the cultural factor on cybersecurity execution. Due to a force majeure situation like coronavirus, the author was able to obtain little information from participants, but even this helped to draw satisfactory conclusions and make recommendations to banks. Thanks to the vast amount of literature and research, confirmation of the factor under study was found, confirming the relevance of the work and the potential for further research.

Key words:

Cybersecurity, culture, organisational culture, social engineering, phishing, regulations, financial market, Schein, Trompenaar, Hall, Thomas, cultural background, awareness.

Contents

List of Figures

List of Tables

1. Introduction

"One worm may damage the whole cookery soup" (Vietnamese Proverb)

This Master thesis will provide the reader with insight into the peculiarities of cybersecurity in the financial sector in European Union (EU), and in particular in Austria, and will also suggest the importance of the cultural factor in cybersecurity. This paper will aim to explore the possible impact of cultural background on cybersecurity in order to further exploit the knowledge gained to maintain cybersecurity inside the companies and outside them too. The first chapter of this Master thesis dwells on the background of the topic under research – what the cybersecurity is, what factors, including these of the cultural background, contribute to it, its importance and the ways in which the cybersecurity of the financial sector in EU, especially in Austria, is different and unique.

1.1 Background

Every type of business has always been suffering from a variety of attacks since their creation. At the beginning, there were physical thefts which progressed into computer frauds as technology developed. Nowadays there is a new form of cancer on the body of business - cyber frauds. Companies of different levels are suffering from huge dents made in their budget and data. Hence the problem of protecting the intellectual property and fighting cybercriminals as it is becoming more sensitive. This attracts more and more interest of all companies, no matter what their size or the nature of industry is.

Cybersecurity, which often defined as "the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks"[1], very often extends beyond the organisational boundaries. In these volatile times, when much of any business is relegated to online venues, the cultural and human factor can play a critical role. The goal of these theses is to analyze the possible gaps that can be caused by this and try to suggest options to reduce them.

[1] (Kaspersky Lab, 2020)

Gradually, it has been discovered that the way a company maintains cybersecurity within its structure, on numerous occasions, relates to the company's country of origin.

The concept of cultural dependence was observed by different scientists, however these scientist were more focused on organisational and security culture. In M. Alnatheer and K. Nelson's published studies, "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context,"[2] were observed the security culture in Saudi Arabian organisations. Through their explorations, they established a chain of interdependence between the security culture and the organisational culture as well as the culture of the country in which the organisation operates. In other words, they tried to find a common link between all the kinds of cultures that can be in a working atmosphere.

Also, cyber culture is considered in a number of works in terms of Schein's framework[3], which will be describe more in details in second chapter. Like any culture, it has its own artefacts, values and assumptions. Based on the fact that cyber culture is part of organisational culture and an organisation is in the nutshell an association of people with different cultural backgrounds. Taking all of the above into account, we can conclude that all of these "cultures" need to work together in harmony to ensure stable and productive work.

1.2 Description of the problem

Before the start of the research project on computer science, the understanding of the importance of the problem was a bit vague and underestimated. With attacks and scams of all kinds, both on and off the Internet, companies need to consider all the possible causes of cybersecurity breaches. According to PwC 24th annual report 2021[4] CEOs all around the world find the cyber threats on the second place of the reasons which can be bad for the business growth within this year.

[2] (Nelson, December 2009)
[3] (Management Study HQ)
[4] (PwC, 2021)

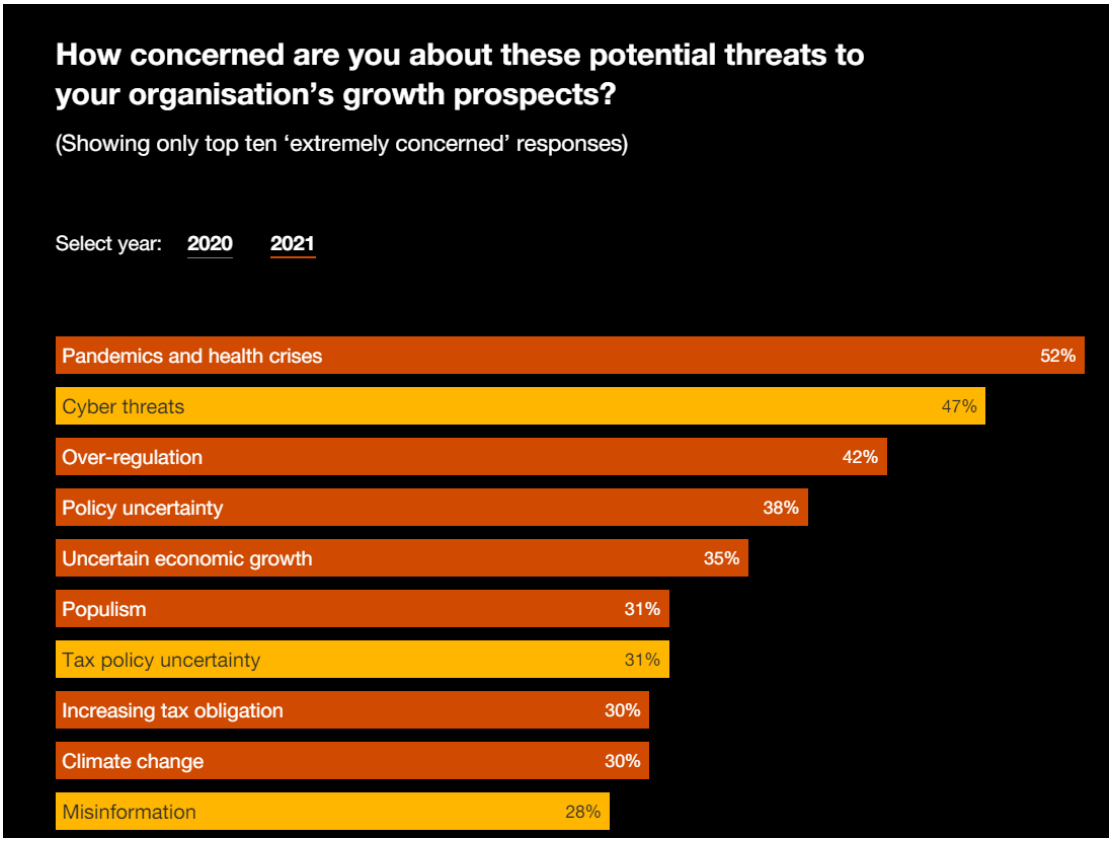


Figure 1. How concerned are you about these potential threats to your organisation's growth prospects? (Taken from the PwC CEO report 2021)

The other portal "Carnegie Service" published the timeline of the incidents[5], the target of which was the financial sphere. Therefore, realization of the weight of the problem has gained a well-defined shape. Every year more and more businesses around the world suffer from attacks of all kinds, and the financial sector is no exception. Hence, every bank and business should be prepared for potential threats and risks resulting from cyberattacks.

In the current situation with the coronavirus and the inability to work in a secure workspace, the threat of losing important data is increasing[6]. Cyber-hackers perceive the global pandemic as another opportunity for stepping up the criminal activity which makes the financial sector to seek all sorts of new protections and develop the risk management.

It would seem that in today's world, people would not be so quick to be duped by a phishing email about an unexpected inheritance or about winning a lottery that

[5] (Carnegie , 2007-2021)
[6] (AON Empower, 2020)

they have never participated in. Social engineering, like other scams, is evolving at an incredible rate and looking for relevant options to cheat. Such as fake World Health Organisation (WHO)[7] websites tracking the spread of coronavirus infection, infecting the devices on which they are opened. Not to mention that employees seek and expect information from their employer regarding their new schedule. They may receive a letter that looks perfectly adequate with information about the office with a timetable attached, but it was sent by hacker.

In times of general confusion, attacks such as voice calls (vishing) or SMS (smishing), which Kevin Mitnick[8] writes about in his book, can also play a good role for an attacker. Remote access from a home network or any other location where an internet connection is available also provides the ability to access important information on the employee's device, and then the entire internal network of the organisation[9]. There are even websites where you can see which devices are connected to the Internet and how secure they are. Even a printer or scanner can serve as an open door for a hacker.

VMware Carbon Black noted in their report "Global Threat Report. June 2020"[10] that attacks during the pandemic have increased dramatically (by about 91%).

Cybersecurity is a "complex challenge" for protecting your business from undesirable intervention both internal and external. "In fact, 80% of firms have seen an increase in cyberattacks 2020. Whereas due to pandemic, ransomware attacks rose 148% in March and the average ransomware payment rose by 33% to $111,605 as compared to Q4 2019."[11] According to the report which was conducted by Frank Downs, the Senior Director, Cybersecurity Advisory and Assessment Solutions, ISACA on November, 6th, "Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[12] This amount sounds more threatening than ever, especially as economies around the world are weakening.

In 2020 Baker McKenzie and Risk.net[13] developed a ranking of the most dangerous operational risks and published it on their report. "Operational risk is defined

[7] (Bannister, 2020)
[8] (Kevin D. Mitnick, 2002)
[9] (MalwareBytes, 2020)
[10] (VMware, 2020)
[11] (Dash, 2020)
[12] (Downs, 2020)
[13] (Risk.net, supported by Baker McKenzie, March 2020)

as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”[14] They could result in the suspension of any company's business activities for an indefinite period of time. Any irregularities without condition are detrimental to the business as a whole and have adverse consequences. However, according to the above study, this suspension occurs all the time, and brings adverse consequences. In addition, any charge can lead to both financial losses and loss of customer, partner, and reputation loyalty in general. If customers and partners cannot conduct their transactions in their preferred manner, they will eventually abandon a particular bank, and the reasons for any disruption will not be significant to them.

These risks are ranked below, and although according to research BIS Working Papers No 840 “Operational and cyber risks in the financial sector”[15] cyber-risks losses are not the most dangerous in context of operational risks losses, and according to data from March 2021 the number of operational loss events has now decreased, however, they still occur. Perhaps, this is largely due to the productive regulators and ongoing supervision. Despite the extra protection, cyber-risks losses still “account for up to a third of total operational value-at-risk”[16]. This paper will not deal separately with each operational risk. This example is presented to illustrate how dangerous any interference with a bank can be and how disruptive it can be to the business as a whole.

[14] (Storkey, November 2011)
[15] (Iñaki Aldasoro, 2020)
[16] (Iñaki Aldasoro, 2020)

A. Top 10 operational risks 2020		
Operational risk	2019	Change
#1 IT disruption	2	↑
#2 Data compromise	1	↓
#3 Theft and fraud	5	↑
#4 Outsourcing & third-party risk	6	↑
#5 Resilience risk	–	New entry
#6 Organisational change	4	↓
#7 Conduct risk	10	↑
#8 Regulatory risk	7	↓
#9 Talent risk	–	Re-entry
#10 Geopolitical risk	–	Re-entry

Figure 2.Change in operational risk grading in 2020 compared to 2019.[17]

IT disruption can act like a domino effect. It can start small and lead to total bankruptcy. This disruption can be either of a technical nature (breakdown, outdated software, etc.) or a hacker attack by any means possible, including social engineering.

The next risk could be "data compromise" - the loss of any data that could also cost the company money and reputation. Not only could the data be stolen, it could be resold to the dark net.

Theft and fraud also remain in the top three. As a senior risk manager at a global bank points out, with improved technology and customer-friendly systems, the ingenuity of criminals is increasing. In addition, it was suggested that due to the large number of regulations which oblige banks to collect and store huge amounts of personal data of customers and partners, the interest of criminals is also increasing.

The first three threats can be carried out by current employees as well as former employees or those about to leave the company, as this report discusses.

Outsourcing and third-party risk is certainly not an insignificant topic, as many banks use the services of various partners to perform different functions such as: data storage, IT system maintenance, software development, etc. In the event of a breach of this link, the client bank will have only one leverage - the contract, but there is no way to save itself from financial and reputational losses.

[17] (Risk.net, supported by Baker McKenzie, March 2020)

A new risk that came to attention in 2020 is a resilience risk. It is important to understand not only the rapid pace in which problems are detected, but also how quick all systems can be rebuilt so that they work at the same pace. McKensey pointed out in their report 2020[18] that it is very important to build sufficient and resilient system to be ready to any risks.

Regulatory risk includes the redundancy or insufficiency of certain regulations and rules. When operating in the international arena, different requirements, and laws of differing countries and/or unions come into force. Therefore, is always the possibility of confusion.

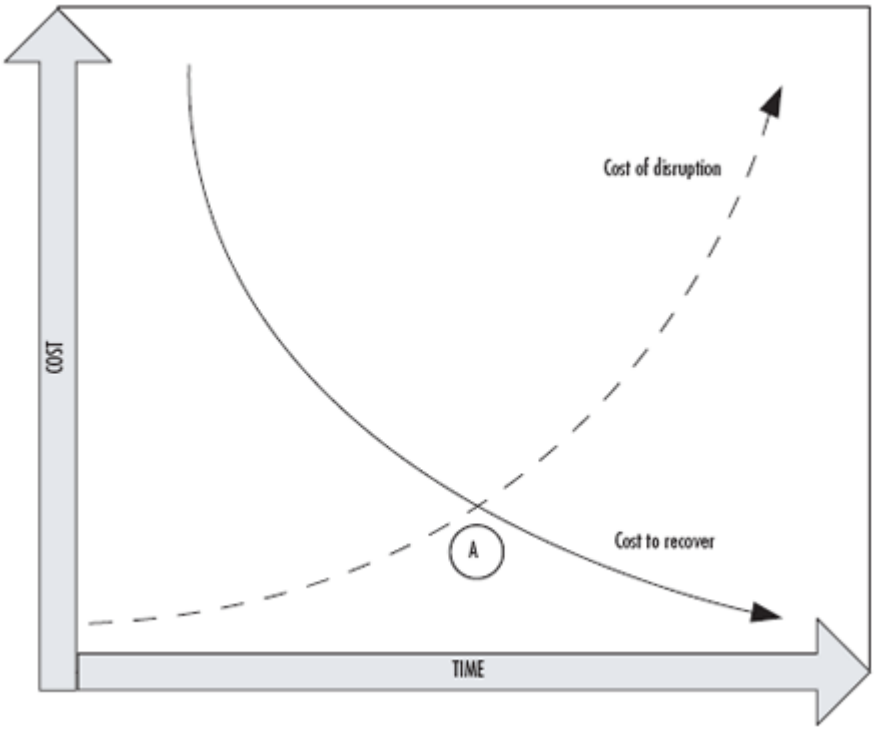


Figure 3. The interdependence of cost and time in the context of operational risk.[19]

As seen in the diagram above, the relationship between the time and cost of recovery and the cost of disruption is shown. Susan Snedaker[20] considers this to be an ideal balance. However, it is clear from the diagram how disruption costs increase

[18] (Susan Lund, 2020)
[19] (Snedaker, 2007)
[20] (Snedaker, 2007)

over time. According to Ian Storkey[21] the maximum response and recovery time is 72 hours, after which time the consequences can be irreversible.

In addition, just in June there was a webinar "EVENT: Ransomware 2021 Mid-Year Update: New Trends and Expert Insights" which also touched on the suspension of any business in the event of a ransom attack and the ethical way out of this situation.

In summary, the danger is not only the loss of data itself, but the time it takes to recover it, both financially and non-financially.

1.2.1 Human factor issues concerning the cyber-security

Any company, in any business, is made up of people who may be guided in their decision-making not only by their knowledge and skills, but also by the human factor and/or cultural background[22]. According to Kevin Mitnick[23], whose work contributed significantly to the development of this study, states that "… no technology in the world can protect a business"[24]. Therefore, cybersecurity should be studied and observed not only from a technical point of view, but also from a human and cultural perspective. The main treat of the cybersecurity could be not a hacker with laptop, but very skilled social engineer who can play easily with people's emotions and thoughts.

The author began this study before the coronavirus pandemic which it gave the research a slightly different character. According to previous studies by the Austrian Federal Economic Chamber (WKO), Austria had a previous shortage of qualified staff. According to their survey, a total of around 81% of all Austrian companies also felt the lack of skilled workers in their company in September 2020 despite the "Corona crisis". The Skilled Labor Radar 2020 also revealed that companies are suffering from skills shortages specifically in the IT environment, with computer security specialists, cloud storage specialists, network administration, etc. singled out[25]. Based on this data and personal experience with IT specialists, companies resort to hiring specialists from different countries, providing them with a workplace, accommodation, social guarantees, etc. This fact again refers us to a study by McKenzie and Risk.net,

[21] (Storkey, November 2011)
[22] (NOBLES, 2018)
[23] (Kevin D. Mitnick, 2002)
[24] (Kevin D. Mitnick, 2002)
[25] (HELMUT DORNMAYR, 2020)

in which they put "Talent risk" in ninth place. So the problem is not only relevant in Austria, but also worldwide.

With the advancement of technology, many gadgets and programs have emerged to prevent an attack. However, there remains one factor that will always be a danger to cybersecurity - humans. It will always be influenced by the environment, the human factor, as well as a significant cultural background. In this paper, the author wants to find the cultural background in cybersecurity compliance.

1.2.2 Cultural factor issues concerning the cyber-security

In my opinion, it is not a secret that different cultures and countries maintain and worry about safety in different ways. Some cultures, for example, the Russian one is more prone to taking measures only after the crises have occurred. A good case in point is a Russian proverb which describes this fact perfectly: “Пока гром не грянет, мужик не перекрестится” («If the thunder isn't roaring, the peasant won't cross himself»). Applying this proverb to the real life is not that difficult when we hear about the recent cyberattacks on Russian banks – over 75% of banks have proven their cybersecurity systems to be vulnerable. The most common reason for such incidents is the outdated software system, the irresponsibility of bank employees, and/or the fact that sensitive data is stored in the clear access and is not protected enough.[26] In 2018, the damage of such an ignorant approach to cybersecurity is estimated in staggering 44 million rubles (approximately 480 000 euro). However, the Central Bank of Russia has begun to develop recommendations aimed at financial institutions on how to protect data more effectively. All the things considered, this once again proves the point stated above – until there is no immediate threat, it is more likely that the company will not take more serious measures.

On the other hand, the Austrian culture is more focused on preventive measures. As the popular saying states “Des Faulen Werktag ist immer morgen, sein Ruhetag ist heute” or “Never put off till tomorrow what you can do today”. The Austrian Financial Market Authority launched a cybersecurity test which involved 10 different banks[27]. The results of the experiment prove higher levels of awareness among the companies of Austrian banking sector, effective cyber strategies and policies and

[26] (Inshakova, 2019)
[27] (CISOMAG, 2019)

the aptitude to adopt the cybersecurity improvements to be well prepared to fight off the potential cyber incidents. However, Austrian culture is heavily influenced with conservatism, which also contributes to the observance of cybersecurity.

1.2.3 Why Austria?

This Master Thesis focuses on Austria as its main contender for several reasons. One of the main reasons is that it was difficult to find any information on attacks on the financial sector in the country in question during the course of the research project.

The information provided in various sources about preventive measures against cyber-frauds taken by Austrian companies is limited. Is this because Austrian companies have got more mature security systems? Or is it that their tactics and strategies are different from the other countries? Maybe they are more focused on preventative measures? Or perhaps the question lies deeper and is related to the people's cultural background?

Austria is a small country with a fairly developed manufacturing, industrial, and financial sector. Especially the region that has been the focus of my work includes a large number of international companies which are market leaders in a variety of businesses. According to Federal Ministry of Austria "The Austrian banking system is a so-called universal banking system. The universal bank model offers significant potential for synergies and it allows for a high degree of risk mitigation as well as for flexible adaptation to changes in the financial environment."[28] There is no doubt that this type of business organisation cannot fail to attract attention. Furthermore, the impact of culture on security can be better assessed by submerging into the culture itself.

The Carnegie service[29] web-site provides a lot of information on the cyber-attacks in financial sphere all around the world, yet hardly any information on Austria can be found. This fact has caught my attention.

1.3 Research objective

[28] (FMA)
[29] (Carnegie , 2007-2021)

This paper will aim to explore the possible impact of cultural background on cybersecurity in order to further exploit the knowledge gained to maintain cybersecurity inside the companies and outside them too.

The usability will not be limited by the financial sphere only, but it could be applied for a variety of businesses with the international employees, customers and partners. Sustainable and resilient cybersecurity culture increases the stakeholders' loyalty and trust for the company, and it creates a better brand reputation, excluding all the possible cyber-attacks and data breaches. Also it will be useful for external auditors and regulatory authorities to design their future work with connection of this research project.

The main focus of this work is on the financial sector because it has at all times been the most coveted system for hacking[30]. Cyberthreats are constantly evolving, especially when it comes to the financial sphere. This sphere is considered to be one of the most vulnerable spheres in terms of cybersecurity. Banks have to think through the details of how to protect their clientele, partners at all levels and more importantly, their own business. Banks must be protected both internally and externally so that not to lose vulnerable information and, nonetheless, not to lose the company's face and customers' trust. In attempts to make their service as convenient as possible for clients, banks can often involuntarily provide another weak link in their security system. It is impossible to notice that the number of cyber incidents has grown rapidly over the last several years, especially with the coronavirus taking its toll on a huge number of businesses. "Of around 3,000 professionals surveyed in more than a dozen countries, 94% had suffered a data breach resulting from a cyber-attack. Organisations experienced an average of 2.17 breaches each, down from 3.4 in the report's previous edition – potentially because "more people are online and connected, and we have better tools to find the breaches," suggested McElroy, cybersecurity strategist".[31]

The financial sector is huge, because it includes not only banks, but also insurance companies, credit unions, savings and loans associations. Due to the fact that this sector is one the most vulnerable sectors, it is supposed to be well-protected and under the constant scrutiny of various financial institutions. There is a vast amount of different regulatory documentation that everyone involved in the field must follow. This

[30] (Cybersecurity education guides)
[31] (Bannister, 2020)

work focuses solely on banks in order to narrow down the number of supervisory bodies and mandatory documentation. Furthermore, only banks in Austria were taken into account, as other countries may have different regulations and supervisory authorities. In addition, due to the current situation with the coronavirus and the rather sensitive topic of the paper, the author was unable to gain access to banks in other countries, such as Russia for example. In addition, it is an important fact that banks strive to create a single safe space where they can operate smoothly and productively. By organising this space, they can stabilise the market and foster confidence both at home and abroad.

1.4 Research questions

The preliminary sources and literature overview has allowed to form the following primary research question and secondary research question:

How is the cybersecurity maintained by Austrian companies of the financial sector/ Is there the possible impact of cultural background on the cybersecurity maturity?

The problem under research is complex, thus the following sub-problems have been allocated:

- How do the banks maintain the cybersecurity in Austria:
    - Legal and regulatory requirements (EU and Austrian)
    - Internal policies
    - Risks and controls.
- Does the bank's view on computer security differ from that of
    - the supervisory authorities?
    - the software developers?
    - the external auditors?
- Is there a difference between the banks studied in the performance of computer security?
- Are there potential weaknesses in banks' computer security that could result from the influence of the cultural background?
- Are there the possible alternative ways to maintain the cybersecurity taking into consideration the cultural background?

1.5 Terminology and definitions

In the process of creating the thesis and studying the literature and sources, the following terminology has been used and emphasized.

According to one of the most famous transnational American companies which designs and sells network equipment cybersecurity (CISCO)"… is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes."[32]

"Confidential Information" is any information which is recognised by a company as prohibited for dissemination whether in written, electronic, oral or any other form (whether tangible or intangible). The disclosure of this information may negatively affect individual parts of the organisation, the organisation as a whole, as well as customers, partners, the company's prestige and, in the latter case, the possible loss of the brand.

According to the web-source "Investopedia" "risk management is the process of identification, analysis, and acceptance or mitigation of uncertainty in investment decisions."[33] In cyber security, this analysis does not only apply to tangible investments.

In the context of this study, "assets" refers to all information and other data, devices, and network with its components, etc. in an organisation's possession that support the information exchange, storage, and transmission activities of the enterprise. They are the primary target of an attack on an enterprise.

According to dictionary.com "hardware is the mechanical, magnetic, electronic, and electrical devices comprising a computer system, as the CPU, disk drives, keyboard, or screen." However, "Software is the programs used to direct the operation of a computer, as well as documentation giving instructions on how to use them" [34] .

[32] (CISCO)
[33] (KENTON, 2021)
[34] (Dictionary.com)

"The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Cloud servers are located in data centers all over the world. By using cloud computing, users and companies don't have to manage physical servers themselves or run software applications on their own machines."[35]

According to Kaspersky Lab "Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables."[36] This type of deception can be used with or without technology. The main method of influence is to play on the human or cultural factor. There is a huge number of techniques described by regulators, software developers, researchers in the field, etc.

One of the most common and widely used techniques is "phishing". "Phishing is a method of trying to gather personal information using deceptive e-mails and websites."[37] The principle is extremely simple, the victim receives an email with a link or attachment and once the link or attachment is opened the perpetrator has access to the victim's computer and then to the network as a whole. Two other variants of this attack work along similar lines - smishing (sending similar messages by text message) and vishing (sending similar messages by voicemail).

Malicious software (Malware) is an umbrella term that includes all possible dangerous software (viruses, Trojans, etc.) that can damage, destroy or steal confidential data.

Other terms will be introduced in this paper, the meaning of which will be disclosed as they apply to each individual case.

1.6 Delimitations

The following Master Thesis has two parts – theoretical and empirical. Both parts have limitations described in this section.

The theoretical part contains analysis of literature sources devoted to the topic of cybersecurity. Theoretical framework is developed to describe cyber security organisation and oversight system in the EU and in Austria in particular. This chapter

[35] (Cloudflare)
[36] (Kaspersky Lab)
[37] (Fruhlinger, 2020)

will look at different studies on the organisation of computer security and the dangers of neglecting the importance of human and cultural factors. Furthermore, several cultural theories regarding computer security and a specific country, Austria, will be examined.

In the empirical part will be described in detail and analysed the questionnaires that were received from our participant banks, the auditor, and customers of the banks. In addition, each response was analysed in detail to get an overview of cyber security implementation, and perhaps find specific points for all companies to pay attention to. This analysis was conducted in terms of regulatory compliance as well as the cultural component. Due to the geographical location, the organisations under the analysis are situated in Austria.

Unfortunately, this work has got a lot of limitation due to the fact that all data is sensitive and cannot be made disclosed by organisations and of the coronavirus crisis, which has blocked access in many organisations.

In addition, it is important to note that computer security is highly influenced by the following legal requirements:

1) Legal regulatory requirements on different levels – they include a compliance of regulations on the banks' operation in the EU, in Austria and its regions.
2) International regulatory requirements (certifications) – here we can find a number of certifications, rules and conventions which are guided by various companies (for example, EC Council, ISACA, Offensive Security, (ISC)2, etc). It is vital to note here that each company might have and choose its own suitable certification to protect its structure.
3) Competitive Law of Austria - it promotes the fair business on any levels and for any company. Its implementation is controlled with the following institutions - The Upper Regional Court as Cartel Court, Federal Competition Authority and Federal Cartel Attorney.

   *This paper will only cover the first two points, as we have not dealt with any cases of legal regulation during the research.

1.7 The Structure of the Thesis

This paper aims to give an overview of the implementation of cybersecurity in the organisation, and in particular in the Austrian banking sector. It also allows us to reflect on a possible cultural dimension affecting security. The first chapter - introduction provides an overview of the cybersecurity situation in the world at present, the reasons for the choice of the study area, the main research question and the research objects are identified. The second chapter examines cybersecurity from different perspectives: legal and regulatory, human factors and cultural factors. An introduction to the region and the area of business under investigation is given. The third chapter presents the methodology used by the author to study and analyze cybersecurity in the financial sector. This chapter describes the types of questionnaires, the number of participants, and the risks and limitations that could not be overcome during this project. The fourth chapter provides an in-depth analysis of the information obtained from the study participants. A comparative analysis of the theoretical part and the real situation is also made.

1.8 Significance of the Study

After studying various regulations, reports from supervisory authorities in Austria and Germany, cyber security research worldwide and cyber security statistics, we can conclude that at this stage it is impossible to say that a company can be 100% protected against the possibility of attacks and intrusions into its internal network. This paper helps to look at cyber security from a slightly different perspective, considering not only the general organisational rules but also the cultural component. This can have a strong influence on employee behaviour, judgement, decision-making and communication with colleagues and management. Knowing the various techniques for analysing each employee's cultural background can significantly reduce the possibility of a successful hacker attack or reduce the percentage of employee error in the course of day-to-day duties.

1.9 Case study examples

Many studies in this field are based on a variety of case studies. In this subchapter, I would like to give some examples from the literature that can be found throughout.

Case study 1.

Kevin Mitnick has described a huge number of different case studies using social engineering in his books. The earliest case, and the most memorable, was that of Security Pacific National Bank in 1978. A hired IT employee doing back-up work and having access to information about bank transactions decided to take a share of the proceeds. The transactions required knowledge of a certain code, which was changed every day for security reasons. It was difficult for the staff to remember a new code every day, so they decided to write it down on a piece of paper and stick it on a board in the staff room. Knowing the necessary information about the company's internal procedures, the code for the transaction and knowing the lingo (professional language contained specific terminology), it was easy for an IT employee to transfer $10,200,000 to his Swiss bank account.

As this case study clearly shows, a lot depends on human and cultural factors. Excessive trust in people who may know the information and have a specialised vocabulary can give a false impression to employees and lead to dire consequences.

This example may be considered outdated, but knowing from personal experience many employees keep their login and password either under the keyboard or literally on the desk next to the monitor.

Case studies 2 and 3.

Information on this situation was found in a paper on employee fatigue from cybersecurity.[38]

An employee of a technology company participated in a survey as part of a study by Reeves et al. When asked about her perception of cybersecurity, however, she expressed the rather clear view that the department is "overzealous". She also resented the testing of her personal devices brought to work and said she easily fails to comply with cybersecurity regulations because she lacks respect for the cybersecurity department and its requirements.

This example clearly shows the employee's lack of awareness, and the absolute indifference of the cyber security department. A system can only be secure when both parties actively participate. I can also assume that the cyber security staff acts in a

[38] (A. Reeves, 2021)

rather formal and rigid manner, which is discouraged by the rest of the workforce. This may be due to a lack of communication between departments and a lack of awareness among all staff of the importance of the measures to be taken. There may also be a cultural aspect to this. Maybe the policy goes against the employee's cultural standards, which automatically makes it unacceptable and unnecessary for her.

This paper also looked at the experience of a cyber security officer who, in turn, trained other employees. His experience was also negative, as the training he was required to deliver was boring and uninformative. The material was provided by senior management who, according to the officer, was not particularly interested in the issue. As a result, after one of the incidents, the management simply changed for the damage, but demanded that things be fixed.

Here again there is a lack of employee communication within the company and an understanding of the damage that can be done to the company as a whole. As Mitnick[39] wrote, the company is willing to spend an incredible amount of money on a new coffee machine, but not on cybersecurity.

By looking at just these examples alone, you can imagine how many such cases can occur in day-to-day operations and can be potentially damaging to a company's business and reputation.

[39] (Kevin D. Mitnick, 2002)

2. Theoretical framework

A special feature of cyber security in the banking sector in EU, including Austria, is the large number of different regulations and requirements that each participant is obliged to follow. In this chapter, the author has tried to explore the views of various sources in order to gain sufficient insight into computer security from all possible perspectives: supervisors, software developers, auditors, and academic writings. In addition, various cultural and leadership theories will be considered to analyze their possible application to this study. Besides that, it should be noted that this study can only consider the recent sources of research on the development of cyber security and regulation in this area, as this area is inherently subject to change. In addition, adjustments and refinements have been significantly greater due to the international situation with coronavirus.

2.1 Overview of the regulations and authorities in financial sector.

The financial sector, like any other, is vulnerable to various attacks by hackers, so a well-functioning legal and regulatory framework must be in place to ensure safe operations. Given that the region we are looking at is in the EU, it is not only subject to regional requirements, but also to EU requirements. Here we look at the main supervisory bodies at different levels and provide a brief description of each.

2.1.1 EU level

Austria is part of the European Union (EU) and all business operating in its territory are subject to the regulations, documents, and conditions adopted by the EU. In addition to the regulations, there are supervisory bodies that assist various businesses to operate and verify their compliance with the generally accepted EU legislation.

There are two main regulatory institutions at this level which oversee and audit the financial sector: European Banking Authority and European Securities and Markets Authority.

"The European Securities and Markets Authority (ESMA) is an independent European Union (EU) Authority that contributes to safeguarding the stability of the EU's financial system by enhancing the protection of investors and promoting stable and orderly financial markets."[40] The main focus of the organisation is on risk assessment for the financial sector, productive interaction with other supervisory bodies in the sector, as well as direct supervisory activities. In addition, ESMA cooperates closely with another financial institution, European Banking Authority, which is described below. Both of these authorities issue various regulations and guidelines that all financial institutions must follow to ensure the safe operation of their business and the security of their customers and partners.

ESMA places great emphasis on the issue of computer security. In April 2019, two regulatory documents were launched on the topic of the cyber resilience testing requirements:

- Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector (JC 2019 26 from 10 April 2019)[41]
- Joint Advice of the European Supervisory Authorities to the European Commission on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector JC 2019 25 from 10 April 2019)[42]

One of the most important initiatives described in the document is the TLPT (threat intelligence led penetration testing) or TIBER-EU (EU-wide Threat Intelligence Based Ethical Red Teaming) testing. In other words, these are planned attacks on organisations, in our case banks, designed to help companies think through their future cybersecurity strategy. The introduction of these practices presents an opportunity for banks and the financial sector as a whole to more thoroughly identify, dis-

[40] (ESMA)
[41] (ESMA, 2019)
[42] (ESMA, 2019)

mantle and address gaps in their security, as well as develop preventative measures to avoid such breaches.

The TLPT test, which is conducted by "Red Teams", is a planned and controlled business cyberattack that identifies security weaknesses. They try to operate in a manner similar to that of real attackers, exploiting information available online and their techniques for finding possible access to sensitive information. There are cases where their inspection reveals that the company is not responding and is not monitoring the attack. They literally had access to all the information left unrecognized. However, this test is not a war in which there is a winner and a loser. On the contrary, the experience helps the company improve its cyber security system and close the gaps. A recent BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) report[43] discussed the initiative and raised concerns about the organisations carrying out this work. The Red Team gets access to all possible information, which could be used for gaining potential advantage.

"European Banking Authority (EBA) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector."[44] The headquarter is situated in Belgium. It was established on the 1st January in 2011 to promote "the European Single Rulebook" for all banking sectors to help all participants operate safely, successfully and in harmony across the EU. It is a very international organisation by itself, it includes "159 employees of 25 nationalities with more than 24 languages spoken"[45]. Perhaps this fact allows for the cultural specificities of each EU member state to be taken into account in ensuring the smooth and secure operation of the banking sector.

The last guideline compiled by the organisation was published on the 28th of November in 2019 EBA/GL/2019/04[46]. The document refers to other normative documents that must be taken into account when complying with this guideline. Also, it

[43] (BaFin, 2020)
[44] (EBA)
[45] (EBA)
[46] (EBA/GL/2019/04, 2019)

contains recommendations about cyber security for the financial market with the current situation taken into consideration. As mentioned earlier, most businesses have now moved online, which can be a factor in improving and speeding up communication and transactions, but it also increases the risk of cyber-attacks.

Although it is an oversight body, it can also be vulnerable to outside attacks. On 7th of March 2021 EBA became a target of an attack on its Microsoft Exchange Servers[47], which could have affected many organisations around the world. An investigation into the attack began immediately and new data protection measures were put in place. The organisation reported on the development of the situation on its website. This fact only confirms that no system is 100% secure and that there is always room for development and improvement.

We would like to point out in advance that the author uses reports and information from BaFin in this paper, even though the region under study is Austria. This type of regulator is authoritative and more experienced than the Austrian supervisory authority such as FMA. Based on their research it was possible to get a more detailed insight into the organisation of computer security in the EU.

Needless to say, these two organisations are not the only ones involved in standard-setting activities for the finance sector in EU, but they are amongst the main ones on which the author will rely in her thesis.

2.1.2 Austrian level

At the national level, there is a system of "supervisory hierarchy", which helps supervisory bodies to work effectively. This can be presented as a diagram which would also include internal audit. The internal circle is the bank's internal audit, which is also the third line of defence. The subsequent circles are external audits. The second circle is a bank auditor carried out by a different organisation. The third circle is a state commissioner, FMA/ ONB. Just the third tier is represented by government oversight bodies, namely: State commissioner with Federal Ministry of Finance (BMF), the

[47] (EBA, 2021)

Österreichische Nationalbank (ÖNB) and Financial Market Supervision in Austria (FMA).

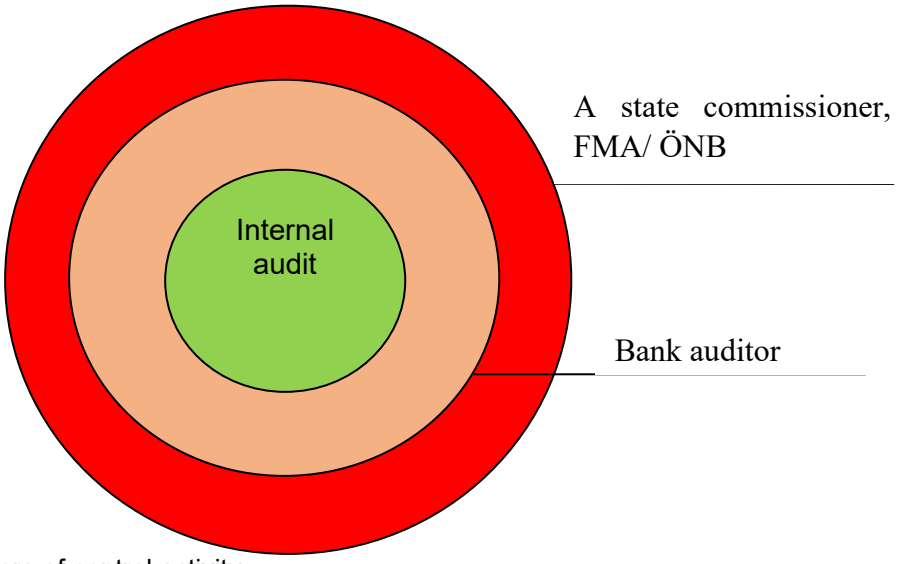


Figure 4. Layers of control activity.

State commissioner with Federal Ministry of Finance (BMF) is responsible for the legal conditions and legislation.

The functions of the Financial Market Authority are general: to supervise all kinds of activities in the financial sector, to monitor compliance with legal requirements, to maintain a transparent and fair operation in the sector, and to penalize failure to comply with requirements and to enforce compliance. The Österreichische National bank (ÖNB) is also responsible for the stability of the financial market and maintenance of supervisory functions, while also operatingas a bank.

The FMA and ÖNB have repeatedly conducted joint research within the framework of cyber security. One example of this cooperation is the first company stress test in 2019[48] to improve the security of the financial sector. In addition, it is worth noting that once again the focus was specifically on employees in the financial sector and the identification of possible security gaps related to the human factor. All research and recommendations for banks and their customers are published on the official FMA website. Understanding that they are responsible not only for firms and banks in the sector, but also for clients and partners, the FMA has developed a platform[49] to help anyone who is interested. On it, anyone can find useful information on

[48] (FMA, 2019)
[49] (FMA, 2021)

how to protect themselves, but can also contact experts, etc. Once again, this demonstrates how concerned the official supervisory authorities are about the security of the sector as a whole.

Apart from this, the FMA approves and makes mandatory any requirements for the safe operation of a business. For example, in official letter[50] was decided to make the application of three lines of defense framework in the financial sector mandatory.

2.1.3 Different standards

In addition to the bodies and standards presented above, there is also other regulation in the financial sphere such as the system for allocating responsibilities in cybersecurity. In January, 2013 The Institute of Internal Auditors (IIA) introduced a new type of dividing responsibilities and functions to maintain the cybersecurity into organisations in their position paper "The three lines of defense in effective risk management and control".[51]

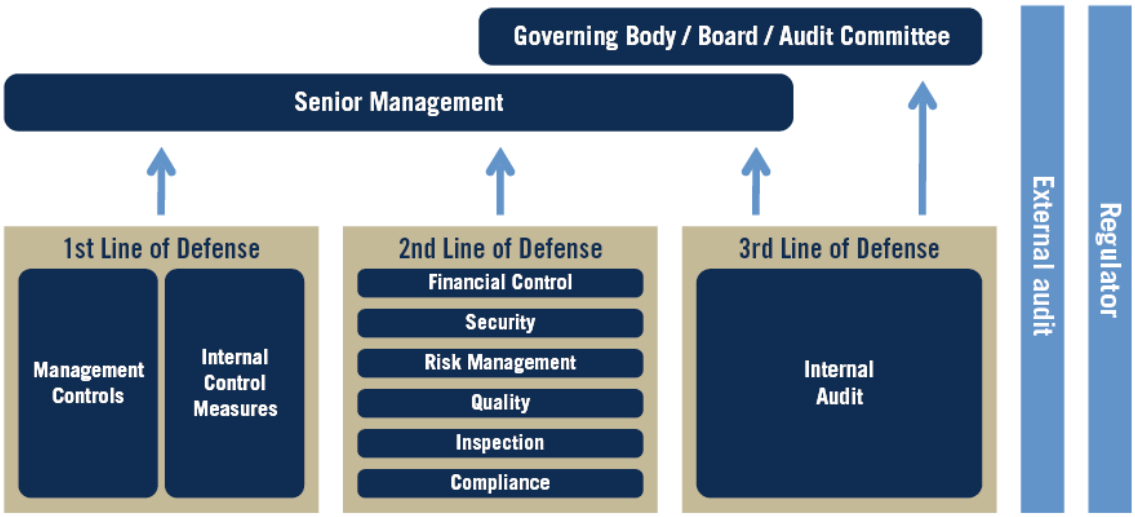


Figure 5. The three lines of defence model.[52]

To present the rather confusing system more illustratively, we can describe it as a "castle security framework".

[50] (Mag. Emilia Nemlig)
[51] (Auditors, 2013)
[52] (Auditors, 2013)

The first line is “the castle guards”. Their function is to take any possible measures to find the problem, and, solve it fast and effectively. Most of the time they are operational management or/ and IT specialists.

The second line of defense is “the watchmen on a tower”. They take the responsibility for predicting any possible risks, preparing preventive measures while regarding law, regulations, and financial risks. More often they are risk management departments, but it also could be an IT crew.

The third line of defense consists of “defense captains” (internal auditors). Their function is to control all lines and help them to operate properly. Also they are the bridge between the head of the company and cyber security responsible people.

This type of segregation of duties should have led to more effective work to address and avoid any cybersecurity breaches. However, over time this model has become a target of criticism as its application has been questioned. In 2015 The Financial Stability Institute published their Occasional Paper No 11 The “four lines of defense model”[53] for financial institutions, where they criticized the three lines model.

“Despite the enthusiastic embrace of the three-lines-of-defense model at major financial institutions over the past few years, the series of banking scandals that have occurred, and in which failures of internal control systems have played a role, have led to substantial financial losses and near-bankruptcies.” [54]

The reasoning for the system’s failure mainly underlies in the fact that the control is for the most part on the first line of defense, and, hence, there is the possibility of the human factor as a high level of risk taker can influence decision-making processes. Furthermore, not only may the second line lack the independence to act from the huge number of reports, but also it has been blamed for its lack of experience in recognizing threats, citing the long-standing speculative activities of Jérôme Kerviel, employee of Société Générale as an example.[55] This employee was on the second line and supported illegal speculation for more than 1 year. tracing this activity was diffi-

[53] (Isabella Arndorfer, 2015)
[54] (Isabella Arndorfer, 2015)
[55] (Isabella Arndorfer, 2015)

cult due to the fact that Kerviel skillfully gave false information that could not be challenged.

Obviously, we cannot judge whether the model has failed within Austria, as there is no information in their work if Austrian banks have failed using the model. However, there are several references to Austria in the document. For instance, some critical points regarding internal and external oversight, to which the document refers in general, were described in ÖNB's reporting in 2015[56].In addition, a paper on the importance of cooperation between external auditors and supervisors for more effective work on risks, bank safety assessments and so on was reviewed.[57]

In the model that has been recently proposed by the Financial Stability Institute, there is a fourth line of defense, which consists of external auditors. In their view, the introduction of a new party will help improve the existing model, making it safer and more efficient.

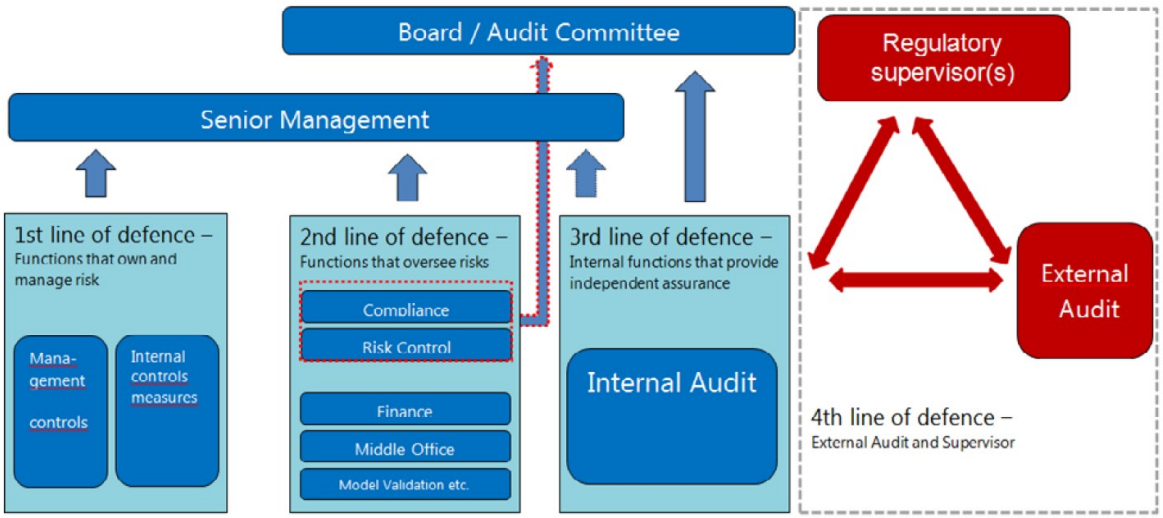


Figure 6. The four lines of defence model[58]

As we can see from comparison of the 2 models, FSI added more functions to 2nd line of defense and included 2 more players with new functions also.

[56] (LINCOLN, 2015)
[57] (EWALD NOWOTNY, 28 Stptember 2015)
[58] (Isabella Arndorfer, 2015)

In June 2019 IIA[59] has published a new and improved document on the three lines of defense with more detailed descriptions of each line's roles, responsibilities, accountabilities etc. They also commented on criticism of the model and suggested solutions to modernize it, but also advocated its continued use, but with some modifications. Undoubtedly, the model will change depending on the organisation and the business realities in which it operates, but IIAs are urged to stick to the main course of this model. In addition, they state that the model was originally developed for internal use only and did not take external audit into account, but this does not mean that it excludes it. Based on the above, an adequate model of the three lines of defense can be presented as follows:

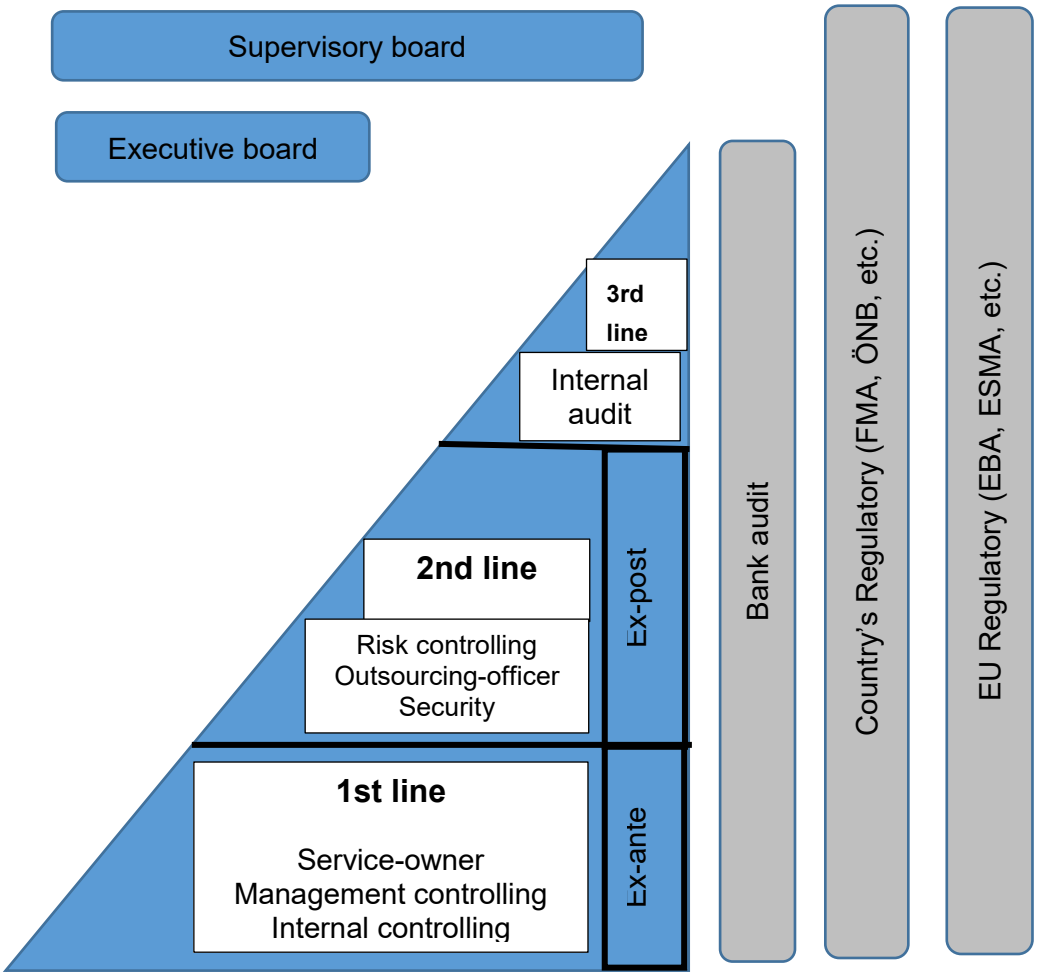


Figure 7. Three lines of defence (autor's perspective).

[59] (Jenitha John, 2019)

Ex-ante – represents primary data and situation analysis: observation, identification, comparison, data analysis. Ex-post - represents the subsequent analysis and further prediction of certain actions. In addition, ex-ante functions to check all possible clients and partners before giving them access to the system and to important information. Ex-post, on the other hand, will check the sufficiency and correctness of the checks carried out during the first line of defence. They are also responsible for carrying out drills and tests (phishing, for example) to confirm the correct operation of the first line of defence.

In addition to the above-mentioned regulatory authorities and banking regulations, organisations are also required to follow security requirements that apply to all types of business (ISO 27001, GDPR, etc.). According to a report by The Federal Financial Supervisory Authority (BaFin)[60] Germany, the financial sector must comply with a huge number of different rules and guidelines within EU and within individual countries, which can sometimes conflict with each other. In addition, if the organisation deals with clients and/or partners outside the EU, additional conditions are imposed as different legal requirements come into force. In order to ensure that these requirements do not conflict with each other, some international standards need to be agreed. As a result, some banks are obliged, among other things, to apply the General Data Protection Regulation (GDPR) - "is the toughest privacy and security law in the world"[61], which undoubtedly protects their rights in an international context but also imposes additional obligations.

In conjunction with things stated above, there is a number of mandatory and advisory certifications that banks must pass in order to do business. For example, ISO 27001[62] and ISO 27002[63]. According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system"[64], while ISO 27002 guides organisations in selecting, implementing, and managing controls on their cybersecurity risk environment—the controls on risks to the confidentiality, integrity, and availability of information in their information systems. "These Interna-

[60] (BaFin, 2020)
[61] (GDPR.eu, 2021)
[62] (ISO/IES 27001, 2005)
[63] (ISO/IES 27002, 2013-10-01)
[64] (TechTarget Contributor, 2009)

tional Standards have been developed to help organisations implement information security effectively"[65], while staying up to date with constantly changing development factors, both internal and external.

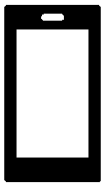
Another certificate that is also required for an organisation to conduct its business - ISO 9001[66]. It is a standard to which an organisation must adhere in order to perform a particular activity, which confirms the quality of the services provided. It also describes the legal and statutory requirements for the services/goods provided.

There is also one of the international standards that may be applied in relation to external auditing. ISAE 3402[67] is a recognized auditing standard. "The scope of ISAE 3402/SOC report is control over information technology and operational processes that affect an organisation's finances."[68] There are 2 types of report that are submitted to the auditor: Type 1 and Type 2. They differ solely in terms of function and the types of how and what the auditor examines. The frequency of the audit also varies from once a year to once every six months.

Alongside with the standards and regulations necessary for the good functioning of a bank's internal system and its security, there are also additional requirements to protect direct customers, such as the Payment Services Directive 2 (PSD2)[69]. The main purpose is to protect customers when making any online payment transactions. PDS2 is closely connected with Strong Customer Authentication (SCA). There are three methods of customer authentication for all transactions:

Knowledge (something you know) – password, pin-code, etc.

[65] (Lack, 2019)
[66] (Koubek, 2019)
[67] (ISAE 3402, 2011)
[68] (ISAE 3402)
[69] (RAVELIN INSIGHTS, 2019)



Possession (something you have) – "reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device" (device, special electronic key, etc.)

Inherence (something that you are) – "biological and behavioural biometric" (fingerprints, face recognition, etc.)

Any financial institution providing financial transactions online and operating within the EU is required to follow this directive and SCA to verify customer identity using 2 or more of the above methods of authentication. The document EBA-Op-2019-06 on 21 June 2019[70] describes all the types in details to help banks to choose which will be suitable for them and for their customers.

Numerous banks operating in Austria are implementing this system quite enthusiastically. A good case in point is Sparkasse which previously used 3 methods of identification for a transaction:

- A mobile phone - the device from which the transaction is made. If the phone is changed, it needs to be re-registered in the bank's system.
- A fingerprint for logging into the app on the phone and accessing the accounts. Biometric login is not as easily susceptible to cyberattacks and all the valuable data is harder to retrieve.
- PIN for the corresponding transaction. However, in my experience, there has been a problem with multiple confirmation of the transaction, which has confused some clients. Nowadays, the bank with the new devices uses a 2-step identification system: design and facial recognition.

[70] (EBA-Op-2019-06, 2019)

*However, the bank customer can customize them directly to suit his or her needs. Confirmation of this information can be found in Appendix 1 “Survey of banks' clients”.

The author took the example of this bank, because I am currently their customer and can confirm this information personally.

In addition to the standards, requirements and regulations described above, there is a mandatory certification for all professionals involved in cybersecurity. There are 6 main companies responsible for training and examination the specialists in this field: ISACA, ISC^2, Offensive security, SANS GIAC, EC-Council, CompTIA. Every company has a huge range of certifications from technicians to management. Consequently, professionals in this field are required to have some form of certification as a proof of their competence and expertise.

As previously mentioned, there are a huge number of standards and regulations to which all types of business, and, especially, the financial sector must adhere and comply. Does this help to fully function without disruption or attack? There is no doubt that having regulations in place helps to build an adequate cybersecurity framework, but it is never a guarantee of 100% security. Moreover, Audit firm PwC has conducted its 24th Annual Global CEO Survey[71], in which Austria participated. According to their survey, over-regulation (38%), followed by cyber threats (26%), is the biggest concern for most companies. These statistics support the observation[72] that banks can be sometimes confused by the sheer number of mandatory regulations.

2.2 Auditors and software developers

To obtain a comprehensive assessment of the adequacy of system security and awareness of new threats, supervisory authorities alone are not sufficient. Many financial services firms and beyond use the services of audit firms such as PwC,

[71] (PwC, 2021)
[72] (BaFin, 2020)

Deloitte Austria, etc. Some companies provide reports and studies in the field of computer security, others provide penetration tests, others provide various statistics on the development of new technologies in the field or the most current threats, etc.

By engaging any third party and granting full or indirect access to company information, each organisation is exposed to additional risk. A number of EBA[73][74] and ESMA[75] regulations have been developed to assist banks in allocating responsibilities and rights between them and outsourcing companies.

Several documents provided by auditors were used in the preparation of this thesis, and the author also tried to obtain information from the so-called "Red Team".

CrowdStrike, Inc. has released its 2021 report[76] on the most dangerous malware threats. They have once again confirmed that 2020 and 2021 are tough years for the economy and business in general. In many ways, firms have been hit by attacks that were on the cusp of exploding pandemics, using social engineering, playing on people's panic. In the report, they identified the main countries that would make up the cybercrime organisations. It is interesting to note that none of the most dangerous organisations are found in EU. It is an unfortunate fact that their network is quite extensive and as people move into the digital world, the danger to any business increases dramatically.

Some audit companies also carry out so-called “planned attacks” on businesses, which help identify security weaknesses. The author mentioned them before as a TLPT or TIBER-EU testing. These attacks are exclusively overseen by company management and only certain employees are aware of them, allowing for the most effective test. They analyse different sources to get detailed information on the most recent attacks and threats. Each auditor then has a different tactic for working on these tests, which is further agreed upon with the customer.

[73] (EBA/GL/2019/04, 2019)
[74] (EBA/GL/2019/02, 2019)
[75] (ESMA)
[76] (CrowdStrike, 2021)

Initially, so-called teams are identified: Red, Blue and White. Each team has its own objective:

1) The red team must produce a successful hack.

2) The Blue team must prevent this hack.

3) The white team is the referee in this “battle”.

In other words, the white team makes sure that the competition is conducted correctly, that the rules are followed, that operational problems are solved, and at the end, they evaluate the success and give the result of the lesson learned. Sometimes the white team is called the “purple team”. In addition, there are more tiered similar tests, not just with the three main teams. The total number can be up to 6 teams[77], each with a narrower function, but the functions of the red and blue commands remain the same.

The red team has already been described before. The blue team is represented by protection specialists who can be brought in separately or before the red team for an initial network security check. Based on their analysis, initial conclusions are drawn to improve security measures and major gaps. A general conclusion is also drawn about the business' cyber security readiness. This group can be represented either by the firm's employees or by third parties.

Thanks to the consent of one of our participants, who also carries out the services of a planned attack, it is possible to get an idea of the process of this action. According to him, there is an initial discussion with the customer to determine the scope of the action covered by the attack authorisation, followed by reconnaissance and identification of the target. Obtaining information from the company comes in a variety of ways, but it is usually advisable to start the penetration tests with a black box phase (a type of testing where no internal company data and structure are known), then provide more information, when testers reach a stage where further research would be costly, skip that stage and move on to more productive testing.

[77] (MIESSLER, 2020)

The involvement of any third party organisation, such as software developers, auditors, cloud providers, etc., also entails operational risks. A huge contribution is also made by cybersecurity software developers such as Malwarebytes LAB, Duo Security, Inc., VMware, Inc., etc. There will be many references to their research and development in this paper. These companies provide the latest information on threats in the virtual world and the latest security trends and developments. They also provide a range of cybersecurity advice to companies and individuals alike.

2.3 Culture? Human factor? Or Both?

Despite the legal and technical security of businesses, there is always a factor that cannot be foreseen. The importance of the human factor has been addressed in the works of academics in 2009[78]. This can be considered a start, after which the human factor started to be considered from different perspectives: behaviour, psychology, culture and so on.

We have already touched on the relationship between organisational culture and security culture in the context of a country's culture[79] in chapter one. However, this theory will now be explored more substantively.

N. Gcaza, R. von Solms and J. van Vuuren "An Ontology for a National Cyber-Security Culture Environment"[80] wanted to change the "human's daily behaviour" using the ontology approach. "A security culture considers the social, cultural, ethical aspects of a user in order to change the overall security behaviour." In addition, this article refers to the Van Niekerk and von Solms[81] work, in which there is a clear view that "view the establishment of a culture as the "…key to managing the human factor".

In article "The Influence of Organisational Information Security Culture on Information Security Decision Making"[82] researchers emphasize the need to create a unified safety culture and implement it and make it a habit for the company as a

[78] (Herath, 2009b.).
[79] (Nelson, December 2009)
[80] (N. Gcaza, 2019)
[81] (Van Niekerk, 2010)
[82] (Kathryn Marie Parsons, 2015)

whole. However, they place great emphasis on the employee as the most important component for the stability of this culture. They also argue that employees can be "dangerous" to the organisation's overall security because of their "naivety". In my opinion, "naivety" in this context is not really the right word, but rather "trusting" and "open-minded" as characteristics of certain cultural traits.

Thomas Schlienger, Stephanie Teufel in their work "Information security culture. The Socio-Cultural Dimension in Information Security Management"[83] express a different opinion about employees. If the organisation wants to build a successful and secure security culture, it needs to stop perceiving employees as a threat and move them to the status of "assets". They consider a socio-cultural, people-centered approach "based on trust and partnership and accompanied by appropriate security technology", which will subsequently bring about the desired success in overall security.

The researchers were more focused to understand the employees' behaviour and the real reasons of their actions in the article "Information security culture: A Behaviour Compliance Conceptual Framework"[84]. The scientists divided participants into four groups according to their safety awareness and motivation to follow the rules: Knowing-Doing mode, Knowing-Not doing mode, Not knowing-Doing mode and Not knowing-Not doing mode. In my opinion, the most interesting and worthy of study categories are Knowing-Not doing mode and Not knowing-doing mode, as these are the ones where we can look for certain culturally influenced behavioural deviations.

Lee Hadlington's work[85] has looked at such aspects as Internet addiction and computer abuse, which he also inextricably links to the human factor and the impact on cybersecurity. In some cultures, the violation of any personal space, including the invasion of privacy, is unacceptable. For example, checking personal belongings such as laptops and/or phones in the context of performing cybersecurity can go against cultural values, which can lead to outright rejection. He insists on the need for employee awareness and the implementation of cybersecurity awareness on a daily-based level.

[83] (Thomas Schlienger, 2002)
[84] (Alfawaz, 2010)
[85] (Hadlington, 2017)

A. Reeves, P. Delfabbro, and D. Calic[86] have identified a very dangerous aspect of cybersecurity attitudes that employees can develop because of frequent training and education - cybersecurity fatigue. Several case studies were examined in which employees expressed misunderstanding and irritation about cybersecurity measures, providing further ground for investigating the human and cultural factor further.

"Information Security Culture: A Definition and A Literature Review"[87] confirms through its research that employees' "mistakes" can be caused by "people's attitudes and lack of awareness of security". In addition, this paper cites a valuable research that references Edgar Schein and his research into culture, organisational culture, and the application of his theories to cyber security culture. Certainly the work of Edgar Schein will be considered later in this chapter.

In the book "Advance in communicating, computing, networks and security. Volume 6" Paul Dowland and Steven Furnell[88] conducted a study of cyber security awareness with people from different countries (245 users from 35 countries). The aim of the study was to understand the dependence of people's actions on their culture, religion, age, gender, education, etc. This work served as a starting point for my research in computer science (contextual study).

Randall J. Boyle and Raymond R. Panko described in detail in their book "Corporate Computer Security"[89] possible threats that could come from employees. They may intentionally or unintentionally harm the safety of the organisation. An employee may make a mistake by providing access to information, but moreover, an employee may initiate an attack to achieve their personal goals (reinstatement, extortion, fraud, etc.).

The authors Ashleigh Wiley, Agata McCormac, Dragana Calic in their article[90] also look at the relationship between organisational and cybersecurity culture, but they also point out that it is not enough to improve just the management and technical part. They agree that national culture can play an important role. In addition, they touch on

[86] (A. Reeves, 2021)
[87] (Areej AlHogail, 2015)
[88] (Paul Dowland, 2009)
[89] (Randall J. Boyle, 2015)
[90] (Ashleigh Wiley, 2019)

the topic of punishment for non-compliance with cybersecurity. This topic is discussed in more detail in the article "The Influence of Organisational Information Security Culture on Information Security Decision Making"[91] on rewarding and punishing employees. In the end, the authors conclude that punishment is not an appropriate measure. This is not only true from a management and human factors perspective, but also from a cultural perspective. This type of control can go against some cultural standards or measurements and this can have extremely negative consequences.

As the role of employee is quite often reflected in the literature and research, it is worth considering some of the main attacks on staff. According to the common belief of many researchers and experts, and this fact was confirmed in a statistical study by Duo Security, Inc. that "Phishing is one of the most common threats hitting organisations".[92] MarkMonitor conducted a survey in 2017 regarding phishing attacks in various industries, and the first place was "Payment services," which directly includes banks.

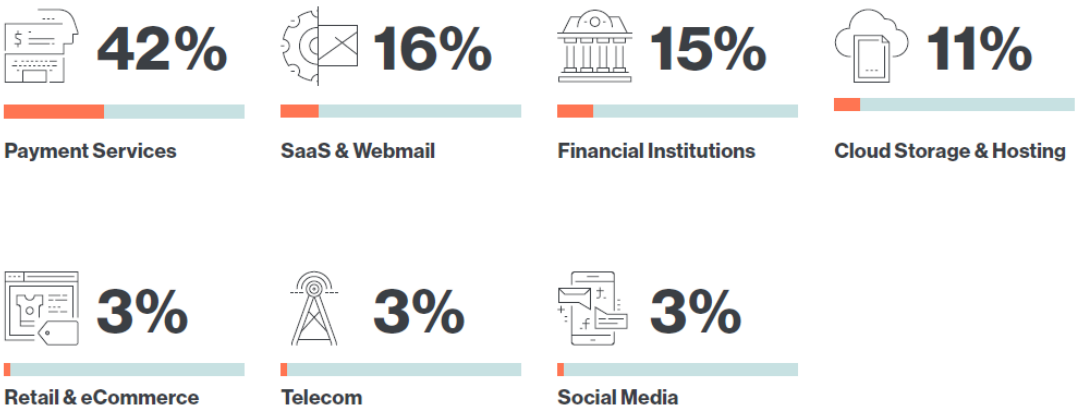


Figure 8. The most vulnerable areas for phishing. Source: APWG's Phishing Activity Trend Report, 4th Quarter, 2017[93]

There are three types of phishing attack scenarios outlined in this article, but according to many sources online, there are others. The goal of this attack is to gain ac-

[91] (Kathryn Marie Parsons, 2015)
[92] (Duo Security Inc.)
[93] (Duo Security Inc.)

cess to one computer, through which it will be possible to gain access to the entire network as well. What is striking is that despite the training and awareness of employees, 31% of the people who took part in their research will click on the link and 17% will also enter personal information.

According to Kaspersky Lab[94], one of the most prominent developers of anti-virus software and training, about 33.4 % of businesses suffer from social engineering, putting it at the top of the list compared to other dangers.

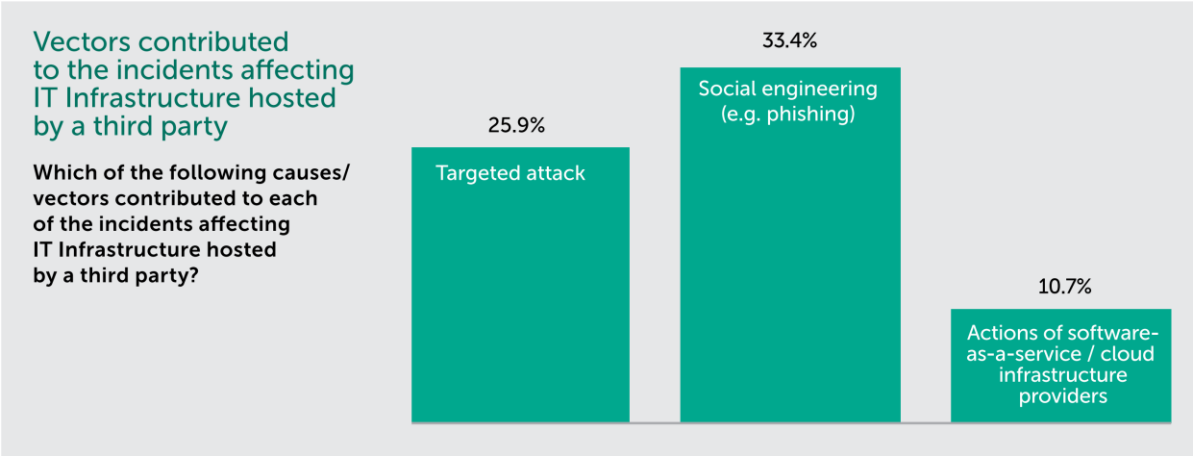


Figure 9. How could the social engineering be harmful for an organisation?[95]

Social engineering attacks are so successful because they play on human and cultural factors. Kevin Mitnick, in his book "Art of Defense"[96], cited a huge number of different cases that have nothing to do with technical security hacking. People duped by the attacker were very easily misled and did not realize that they were giving away any classified information. The situation aggravated with the international coronavirus pandemic, which provided even more ground for fraudsters. Cyber-attackers see the Covid outbreak as an opportunity to step up their illegal activities by exploiting the vulnerability of employees working from home[97] and capitalizing on people's strong interest in coronavirus-related news (e.g. malicious fake coronavirus related websites[98]). "What COVID-19 has created is effectively a huge monitoring challenge.

[94] (Kaspersky Lab, 2019-2020)
[95] (Kaspersky Lab, 2019-2020)
[96] (Kevin D. Mitnick, 2002)
[97] (AON Empower, 2020)
[98] (Anna Georgiadou, 2021)

Banks (and indeed all businesses) need to ensure that remote users are who they say they are, and that their behaviour is consistent with what would be expected. This is difficult when users may be logging in not only from company-issued laptops but also their personal phones, tablets and other devices. Usual BYOD (bring your own device) protocols that allow remote access only from one device may need to have been relaxed. In addition, staff are most likely not following their usual work patterns (logging on at circa 9am, logging out at circa 5pm) but may be working in bursts across different hours due to child care and other duties"[99]. In addition, employees can connect to the internal network not only from home but also from anywhere else where connectivity is available. (e.g. train, café, etc.). These networks should not be protected in any way[100].

As it has been already notices that all business shifted its activity on the internet, the business connection Business relationships have also started to be built online on specific social platforms, such as LinkedIn. According to Crowdstrike research[101], there have been many attacks on LinkedIn users in 2020. The attackers pretended to be representatives of various companies, rubbed in their trust, and then infiltrated the victims' computers. It is interesting to note that this social network is quite popular in the world (statistics can be cited), however, Austria is not even in the top 50 countries that actively use this social network[102]. According to statistics[103], the working population is 4,565,912. Only 24.5% of them are registered on LinkedIn. For 2019, the number has increased by 6.1%, which means a growing interest in the community. Consequently, Austria is becoming more active in the aforementioned social network LinkedIn and more vulnerable to attacks. In addition, this network can be used on the work computer, as it is designed to create new business connections around the world.

The examples of hacking and phishing can been seen from the very start of the pandemic. During this period, people were seeking information about the latest news about the spread of the pandemic, or were expecting emails about changes in working conditions (such as office closures and work from home)[104], and there are also cases

[99] (Judd Caplain, 2020-2021)
[100] (Anna Georgiadou, 2021)
[101] (CrowdStrike, 2021)
[102] (Tankovska, 2021)
[103] (Next Business Academy, 2019)
[104] (AON Empower Results, 2020)

of mass emails similar to billing, delivery information or a 'must see' email from a 'friend'[105].

The response to a particular link or letter can be dictated not only by learning, but also by an initial impulse that comes from a human factor and/or cultural background. It is impossible to consider any business in isolation from the culture of the country (employees) in which it operates. Some researchers have also tried to compare two or more cultures with each other by applying different theories, which will be discussed below. For example, researcher Anikó Tompos[106] in his work compared Bulgaria and Austria in the context of business relations. The author points out that studying these theories can be useful, but at the same time there is a great opportunity to immerse oneself in stereoscopy and hope for a positive outcome based solely on knowledge of cultural dimensions and standards. This point of view is correct, but critical thinking and analysis of the situation must always be present. Undoubtedly, one should be aware of these cultural theories, which help to analyse other people and one's own behaviour in particular. Relying solely on management theories, without taking into account the cultural specifics of partners, staff, customers, etc., is a huge risk of failure. The reason for failure will be simple, other people (cultures) may perceive a particular management decision differently, potentially leading to its misinterpretation and implementation.

2.4 Overview of the cultural theories and Austrian culture

„Culture consists in patterned ways of thinking, feeling and reacting, acquired and transmitted mainly by symbols, constituting the distinctive achievements of human groups, including their embodiments in artifacts; the essential core of culture consists of traditional (i.e. historically derived and selected) ideas and especially their attached values."[107]

There are many different cultural theories that can explain a person's behaviour based on his or her cultural background. However, there is always the danger of delv-

[105] (Banach, 2020).
[106] (Tompos, 2015)
[107] (Clyde, 1952)

ing into stereotypes. Hence, regardless of the cultural component, one cannot judge a person without bearing in mind their family background, educational background etc.

Much research has focused on the human factor in computer security decision-making, but the cultural factor has largely been omitted. According to research, management tools recognized as highly effective by one culture may be perceived quite differently by another culture, so the possible influence of the cultural dimension in any organisation should be taken into account[108].

Even though cyber security is whirling at a cosmic speed[109], and you only need to study the latest literature to get an up-to-date picture of what is happening in the field, academic works on culture produced decades ago remain as relevant as ever.

2.4.1 Schein

The organisational model[110] was developed in 1980 by a renowned American management professor. The model makes the culture more visible and transparent within any organisation or company. The most widely used cultural theory applied to cyber security culture is Edgar Schein's model of a culture. Schein divides all the mechanisms operating within an organisation into direct and indirect ones. Among the direct mechanisms there are opinions, status and appointments; indirect mechanisms do not influence the organisational culture directly, but the play a determinative role – they include formal guidelines, the visions of an organisation, corporate identity, design and rituals. He argues that every culture has its own artifacts, values and assumptions. It is most often presented as an iceberg with 3 parts.

[108] (Ksenia Keplinger, 2012)
[109] (CrowdStrike, 2021)
[110] (Management Study HQ)

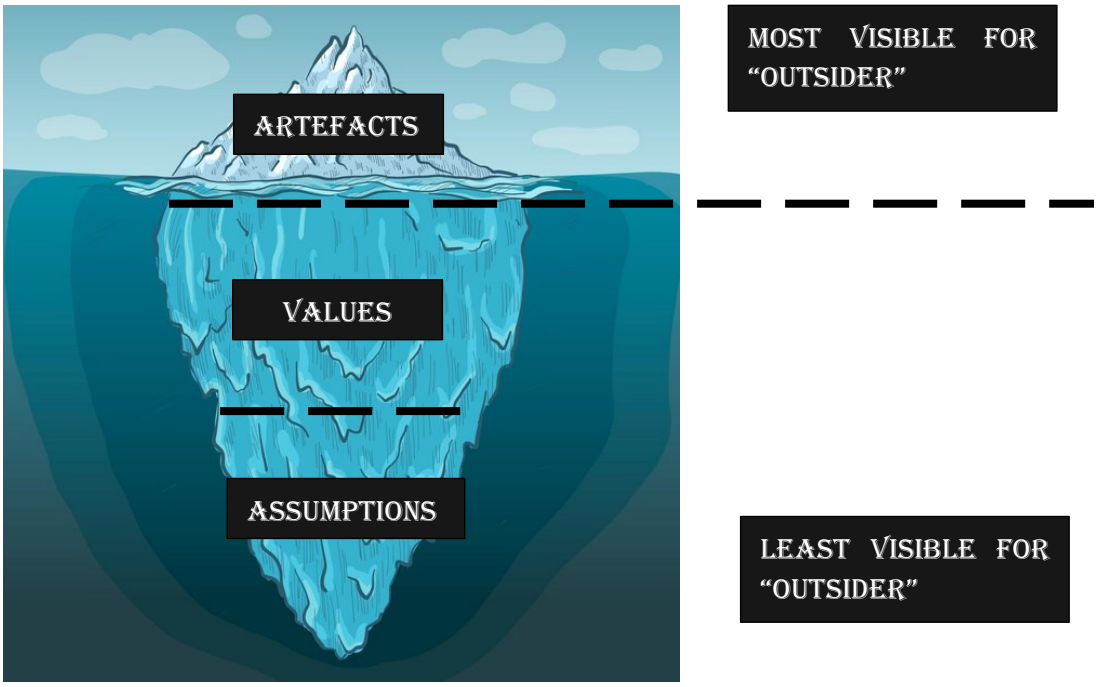


Figure 10. Edgar's Schein Organisation model (author's perspective).

Here artifacts are also a visible part of the culture that any outsider can notice. The value reflects everyone opinion about "how things should be". This dimension helps cultural individuals to define "situations and actions as desirable or not desirable". The assumption in this theory is an undeniable and unshakable belief. They form a kind of core of culture. Schein identified six kinds of assumptions:

1) Assumption about "truth". In other words, it is the presupposition of "what is truth" in all matters, the need to discover or conceal it.
2) Assumption about "time". In short, it is the importance of the time, its determination, etc.
3) Assumption about "space", including public and private space understanding, also understanding disruption of it and appreciation.
4) Assumption about "human's nature", which is responsible for the concept of good and evil in human nature, and whether it can be changed.
5) Assumption about "relationship inside the organisation", which idea is to understand how the work process should be structured, the relationship between rest and active work.

6) Assumption about “leadership”, including the definition of it, determination of the relationship boss/employee, concept of competitiveness inside and outside the organisation, etc.

Every culture in every manifestation can be analyzed according to this theory. It is possible to find artefacts, values and assumptions in national culture as well as in organisational and cyber security. The most important fact is to be able to bring all these cultures together and make the core of the common culture understandable and acceptable to all individuals. If we analyze every single corporate culture in a particular country, it will differ in some way from a similar organisation but in another country, or even in the same country. Their artifacts, values and assumptions may be radically different. It is necessary to consider the corporate culture in conjunction with the culture of the country in which it operates, as well as the cultural background of each individual employee.

2.4.2 Hofstede

Although some research papers, such as "Management accounting practices in a multicultural environment: evidence from Austria, Russia and the US"[111] argue that Hofstede’s approach is outdated and far from reality now, a website has been developed that provides a contemporary analysis of his work. Consequently, it is impossible to state with certainty that his approach cannot be used at present.

Geert Hofstede described in his works cultural dimensions’ approach for analyzing and comparing cultures. This chart illustrates Austria on the basis of the six cultural dimensions derived by Geert Hofstede[112].

[111] (Ksenia Keplinger, 2012)
[112] (Hofstede Insights)

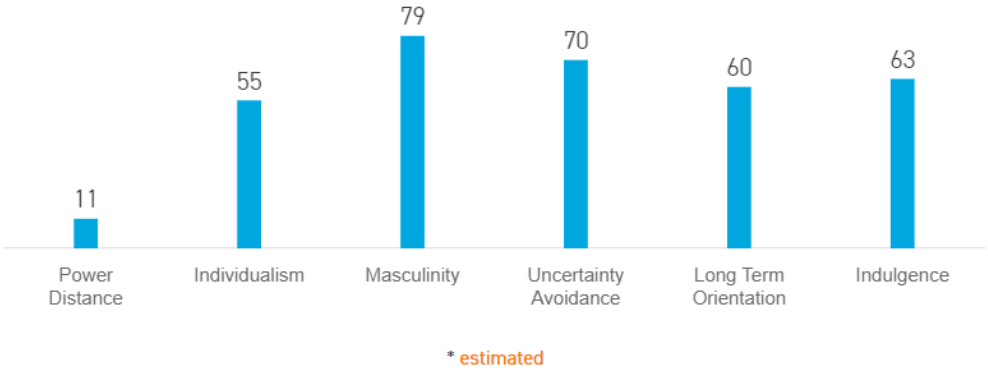


Figure 11. . Country Comparison: Austria according to Hofstede theory

The Hofstede theory is based on comparison of different cultures. The scale adopted in this study is from 0 to 100 where 50 is the average. Therefore, if the index is below 50 - the culture score is relatively LOW and vice versa.

From the Hofstede Insight on Austria, we can conclude that the Austrian culture is characterized as more democratic because the level of power distance equals 11. The Power Distance, which is the other way to describe hierarchical relationship within a business, is exceptionally low. The working atmosphere is conducive to an open dialogue as well as more acceptive of different viewpoints and opinions. Speaking of banking systems, most provinces have their own banks, sometimes with the main center in Vienna, however, it is not always so. Austria also has banks from other countries, which operate successfully in the country. The most striking example of power distance in the banking system is the use of ATMs. In Austria, a resident can withdraw money without paying any extra fees from any ATM near him. Banks do not try to show their superiority, but on the contrary, give the client the right to choose where and when to withdraw money. In this small and seemingly insignificant fact there is a hidden meaning, which affects all aspects, including cybersecurity.

Next dimension is responsible for the way in which society interacts between individuals: collectivism or individualism; whether an individual associates himself or herself with the concept of “I” or “we”. Austria scored 55 on this dimension, which

places it in a more individualistic society, in which the family will become more important than society as a whole. These societies are characterized by a greater self-awareness of the rules, the violation of which may lead to a loss of self-respect. Professionally, all relationships are based on mutual benefit. However, Hofstede states that "hiring and promotion decisions are supposed to be based on merit only, management is the management of individuals." However, according to my professional practice, there are cases in Vorarlberg where preference is not only based on professional merit but also on the applicant's closeness (friendship and family ties), especially in smaller villages and locations. However, this fact does not contradict the earlier point made about the importance of the family in individualistic societies.

Next dimension is "Masculine", but it is not about gender supremacy. This dimension has two levels:

1) High (Masculine), which is characterized as the presence of healthy competition in society, the desire to succeed and to be the best.

2) Low (Feminine), which focuses more on caring and improving the quality of life. Here, it is not accepted to be better than others.

According to Hofstede's data, Austrian society is at 79, and therefore the society is more focused on open competition, on achieving maximum success, etc. People in management positions are more likely to act decisively.

One more cultural dimension is the "Uncertainty avoidance" which according to Hofstede is described as how the less powerful members of society accept and expect an uneven power distribution. Conforming to his studies "…certain cultures are more risk-averse than others."[113] This could be the reason why the Austrian culture could be characterized as a low-risk acceptance culture. It is more typical for this culture to think about all the possible outcomes of the situation and to develop preventive measures. Consequently, sometimes precautions can be higher than a potential profit.

[113] (Hofstede, 1980)

Next dimension characterizes a society as either conservative, preferring to stick to established traditions and disdainful of change (low score), or innovative (pragmatically oriented), willing to change and adapt to new things (high score). Austria has a score of 60, which makes it a more pragmatic culture, but it still maintains an attachment to old traditions and patterns in both personal and professional life. The orientation of society is largely situation- and time-dependent, but society tends to save and invest.

The last dimension is based on how an individual can control his or her desires and emotions. In other words, how vividly members of a particular culture are prepared to demonstrate their emotions, feelings and experiences quite expressively. The two extremes of this dimension are "indulgence" or "restraint". Austria received a score of 63, which suggests that this culture is willing to enjoy life and give itself over to leisure activities completely. The society can be characterized as positive and optimistic.

This theory is general and does not mean that every individual person in society conforms to it. Hofstede gives a general description without going into detail about each person individually.

2.4.3 Trompenaars

Dutch interculturalist Fons Trompenaars presented his Dimensional model for cultures in 1993 in his work "Riding the Waves of Culture: Understanding Diversity in Global Business"[114]. He and a colleague, Charles Hampden-Turner, surveyed 40,000 employees from 40 countries. However, like with Hofstede, one cannot assign culture 100% to one or the other dimension. Each culture will occupy a different place on the scale of each dimension.

There are seven dimensions:

1) Universalism vs. particularism.

[114] (Fons Trompenaars, 2011)

This dimension determines the importance of professional or personal relationships in the culture. Universalism advocates equal treatment of all, regardless of family or friendship ties, while particularism values relationships more than rules. According to this theory, Austria belongs to universalism, which is once again confirmed by Hofstede's theory.

2) Individualism vs. communitarianism.

This dimension can be described as an individual's willingness and ability to work in a team or to rely more exclusively on themselves and their knowledge.

An individualistic culture focuses more on each individual's own decision making, on which his or her long-term future will depend. It is also characterized by taking responsibility for one's decisions.

A communitarian culture, on the other hand, is more inclined towards shared decision-making, which slows down the process as each participant tries to contribute. Austrian culture is characterized more as individualistic, as Hofstede has already written about.

3) Specific vs. diffuse.

In this context, this dimension can characterize the ability of cultural individuals to separate personal life from work. Some cultures focus on the separation of work and home, having a clear work and rest schedule. Others are not able to separate these two parts of their life because success can only be achieved when they are intricately linked. There is no doubt that the Austrian culture is the specific culture, because despite their desire to reach their goal and work towards success, they place great value on relaxation and family.

4) Neutral vs. affective.

This dimension is characterized by the ability and willingness to show emotion. A neutral culture may seem rather cold from the outside, as people try to contain their emotions, but continue to experience them internally. Representatives of affective cultures will be more likely to share their emotions both in the workplace and in their personal lives. Austria is more of a neutral culture, as exhibiting overly emotional behaviour can be viewed from a negative perspective.

5) Achievement vs. ascription.

This dimension can be described roughly as "given by birthright or earned", in other words in the culture of achievement an individual proves the status they have acquired by their knowledge, experience, achievements and skills. In subscription culture the individual receives their status according to certain patterns of society (age, position in the family society, etc.). In this culture the individual cannot challenge any decision of a superior in status, and unlike in the achievement culture, if they have a reasoned basis for doing so. The Austrian culture refers to a culture of achievement, as one earns status solely by oneself, regardless of social status or age.

6) Sequential time vs. synchronous time.

This dimension refers to the ability of a member of the culture to do something at the same time, or the sequence of actions is important, and, also, has a great importance for the value of time. In a sequential culture, all work is done in stages, with the timely completion of one stage moving on to the next stage. In this culture time is seen as a straight line. In a synchronous time culture actions can happen at the same time because time is flexible and not linear. Breaking timelines is unacceptable in a sequential culture, unlike in a synchronous culture where they can easily shift and vary.

Austrian culture is more of a sequential time culture. There are times in a professional activity when the answer to a question asked comes with a huge delay, but the reason for this delay is precisely because the individual follows all the other instructions consistently and then moves on to the new request.

7) Internal direction vs. external direction.

This dimension describes the relationship between society and the outside world. Internal cultures are convinced that they control the world around them and use it for their own purposes, organisational purposes, etc., in order to win conditionally. In outward-looking cultures people do not want to use the world around them, but rather to live in harmony with it. For a given culture, it is more important to focus on good relationships rather than competition and rivalry.

Austrian culture is more of an inner-directional culture, but not critically so. This conclusion can be drawn from Hofstede's dimensions in which the Austrian culture is "masculine", i.e. business is built on competition and getting the right result. However, despite this, based on the need to cooperate with other countries in maintaining cybersecurity, it cannot be said that Austria completely denies harmonisation with the outside world.

Despite the great influence of cultural background, we must not forget the human factor. Thus, it means that the leaders in different countries should be aware of not only the technical side of the question but also be prepared and work on the possible “weak points” of the cybersecurity – humans (employees and clients). No matter how much banks develop and establish the technical side of the issue, the human factor plays a big role. This aspect may depend on the cultural component as well as on the individual one. In fact, 52% of businesses admit that employees are their biggest weakness in IT security, with their careless actions putting business IT security strategy at risk[115].

2.4.4 Hall

Edward T. Hall[116] described the various cultural factors inherent in certain cultures. He identified four factors: time, context, space and information. The factor describing time divides crops into monochrome and polychrome. As with Trompenaars it is about the perception of time by different cultures and the sequence of actions.

A more interesting factor to pay attention to is the "context", or in other words the way information is transmitted. Hall divides cultures into High context communication and Low context communication. In High context communication cultures rarely is the message expressed in a direct manner. More often it is necessary to take in information "reading it between the lines", paying attention to non-verbal ways of communicating. In addition, this type of communication is more common in cultures with a strong intra-group connection, as some messages may be received without explanation or additional information. Low context communication cultures express the

[115] (Kaspersky Lab, 2017)
[116] (Changing minds.org)

information in maximum details because everything needs to be crystal clear and agreed upon in order to achieve the desired result. A task completed on time is much more important than a relationship. The Austrian culture can be characterized as a low-context culture. All documents developed and adopted in Austria try to explain all requirements and conditions in as much detail as possible so that there are no blind spots or gaps. In addition, when communicating in a business environment, the Austrians try to anticipate and stipulate all points in detail, leaving no room for conjecture or other interpretations.

The next factor that deserves attention is 'space', or each individual's perception of culture. There are cultures that are zealous about preserving their personal space and others that may be more comfortable with violating these boundaries. It is not just about the personal space of the office, the personal desk, the 'personal bubble', but also about minimizing the disturbance of others. Austria belongs to a culture that values and respects each individual's personal space, irrespective of his or her position.

And the last factor is responsible for the speed of information transfer. Austria refers to a culture with slow information transfer, as it has already been said before that culture is characterized by sequential actions and low context, which slows down the performance of certain functions.[117]

2.4.5 Alexander Thomas

There is a huge number of different cultural theories, which are divided into two branches of research: cultural dimensions and so-called cultural standards. Alexander Thomas (1996) was the founder of the cultural standards method[118]. His research was based on the work of Jean Paul Piaget (1962 and 1976) and Ernst Bosch (1980)[119]. This method refers no longer to measurements but rather to critical incidents that may occur during intercultural communication or workflow in an intercultural organisation. These incidents can be interpreted according to cultural standards that may affect both participants in the communication. Alexander Thomas defined this concept: "By cultural standards we mean all kinds of perceptions, thinking, judgments and actions

[117] (Lehrerfortbildungsservers Baden-Württemberg)
[118] (Schroll-Machl, 2010)
[119] (Gerhard Fink, 2005)

that in a given culture are regarded by the vast majority of people as normal, self-evident, typical and obligatory for themselves and others".[120]

Thomas conducted a series of interviews to identify one standard or another which, upon closer examination, overlap with the theories expressed by Hall, Trompenaars and Hofstede. For instance, the author of the article refers to the "German cluster" of cultures such as Germany, Austria, Switzerland, etc. that can be characterized as "assertiveness". However, this characterization can be perceived as a "Low context" dimension. In this paper, however, the author insists on the need to study cultural standards in critical situations in order to effectively manage and plan intercultural security, which is directly applicable to these theses. One of the cultural standards is belonging to the same culture, gender and/or age. It is possible to trace a more open and trusting, communication with a person of the same culture. In some cultures, respect for age and attitudes towards the person of the other sex may differ. Again, however, this approach cannot be completely different from cultural dimensions.

These basic theories are given to demonstrate the vastness of the various cultural dimensions and standards. In the present study the author will try to find possible corroborations of the cultural background in the responses of banks and the auditor. The study and consideration of cultural differences (dimensions and standards) can help to avoid possible negative incidents in the clash of interests, values of different cultures and lead to unfavorable consequences.

2.5 Overview of the region of study and financial sector there

Considering the fact that Austria is a small but fairly developed country, and that it is very rarely mentioned in attack statistics, it becomes quite an interesting subject of study. Is it that good and safe? In addition, the region is the author's current place of living, so studying from the inside can be much more productive than from the outside.

[120] (Gerhard Fink, 2005)

The Carnegie service[121] published the timeline of the incidents, the target of which was the financial sphere. Since 2017, over 200 attacks have been carried out and around 29 countries have been affected which means that the problem is becoming more global with more countries getting involved and it is up to date. Hence, every bank and business should be prepared for potential threats and risks resulting from cyberattacks. And as noted earlier, Austria is one of the countries that is not counted in these statistics.

Also, according to the Paul Bischoff research of the global cybersecurity level[122], it is obvious that Austria is one of the most powerful players on the world arena. In the current research the level of preparation for cyberattacks is estimated with the maximum score of 1,000, which is based on analysis made by Global Cybersecurity Index. The GCI includes:

- relevance to the five GCA pillars (legal, technical measures, organisational measures, capacity building measures, cooperation measures);
- relevance to the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data (GCI 2019. Report).

In this context Austria is fairly close to the ideal with the staggering score of 0,826.

Country	Score 2019	Score 2020	% of Mobiles Infected with Malware	Financial Malware Attacks (% of Users)	% of Computers Infected with Malware	% of Telnet Attacks by Originating Country (IoT)	% of Attacks by Cryptominers	Best Prepared for Cyberattacks	Most Up-to-Date Legislation
Spain	24.12	17.09	4.15	0.3	11.09	0.91	0.62	0.896	4
Portugal	32.79	16.91	4.36	0.2	12.79	0.11	0.54	0.758	5
Austria	25.76	16.63	3.01	0.3	8.13	0.05	0.21	0.826	3

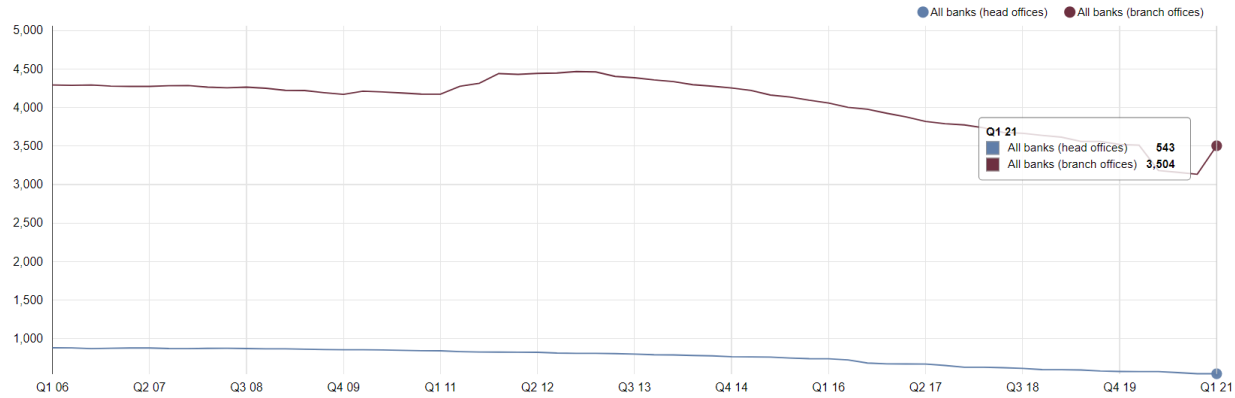
Table 1. Global cybersecurity ranking made by Paul Bischoff, Tech writer.

[121] (Carnegie , 2007-2021)
[122] (Bischoff, 2020)

Global Finance in November 2020 has identified the 50 safest banks in Europe[123] given the current dire situation around the world due to the Coronavirus. There is only one Austrian bank in this ranking, and it is not at the top of the list. However, the number of banks in Switzerland, which is one of the highest rankings, has fallen by 22% in eight years (from 312 to 246)[124]. Also despite the success of the German banking sector in 2019, which has increased its total assets in these times of crisis and has shown itself to be one of the safest, some banks such as Deutsche Bank have suffered from cuts in their branches and personal. The stock of this bank also plummeted[125]. In the Netherlands, the number of banks (44%) and offices (47%) also decreased between 2008 and 2018[126].

According to the Austrian National Bank[127], the total number of head office banks in Austria is 543 and branch offices – 3 504. Although the number of head offices and branch offices has declined since 2008, the country is still quite high. Can the number of banks be considered as an indicator of security?

Table 2. Number of banks by section in Austria. Developed by ÖNB



[123] (SANDERS, 2020)
[124] (Norrestad, 2020)
[125] (Norrestad, 2020)
[126] (Norrestad, 2020)
[127] (ÖNB, 2021)

3. Methodology

This research is designed to check the theory of cultural background influence on maintain cybersecurity. My research incorporates both qualitative and quantitative approaches. The initial plan was to involve as many banks, supervisors, auditors, software developers, clients, etc. as possible. However, the study received a large number of rejections due to coronavirus infection, difficulties in weakened business and over-employment of potential participants. In addition, the topic is quite sensitive and a small number of banks agreed to participate. Moreover, at the beginning of the development of this topic, it was planned to study specific situations of attacks on banks or staff reactions to potential dangers. However, this was also rejected as, once again, the topic is quite secret and there is no provision for a third party, which is the author, to disclose this information. Despite this fact being an obstacle to a more in depth and detailed study of the impact of the culture, it was confirmed that Austrian banks are seriously concerned about cybersecurity. On this basis, a literature review was carried out to get an overview of cybersecurity in general and then in the specific sector and region. The organisational structure of financial sector supervision in Austria was studied and the main bodies directly involved were examined. In addition, various academic papers on the topic of cross-cultural communication were studied in depth and different cultural theories were examined, which gave an insight into which cultural characteristics can influence cybersecurity.

An enquiry was sent to 15 banks operating in Austria and at least 4 banks were visited in order to arrange a meeting in person. After negotiations only a few banks agreed to participate. A questionnaire was sent to these banks (Appendix 2). This questionnaire was designed in such a way that it did not deal with sensitive topics but provided sufficient information for the study. Unfortunately, after the questionnaire was sent, some banks declined due to its strong specificity.

All participants refused to be interviewed, there was exclusive consent to answer one questionnaire. An attempt was made to do a bank staff survey, which was unsuccessful. In addition, supervisory authorities were tried to be involved in this study, one was even contacted by telephone. However, the result was again rejected. A questionnaire for software developers and auditors who carry out penetration tests has also been developed to get a comprehensive assessment of the cybersecurity situa-

tion. After companies agreed to take part in the study, a questionnaire was sent to them, but only one response was received.

Moreover, in order to confirm one of the theories, one express questionnaire was conducted online using the SmartSurvey system, which was successful. The data was reviewed, examined and presented in the Empirical framework chapter.

All data from the banks were entered analyzed manually.

Participant data are known exclusively by the author and her supervisor. No one else had access to the data and did not take part in the analysis. All banks' names, locations and names of survey participants are concealed. The names and numbers of the banks which used in this research are in random order.

Current research on cybersecurity in the financial sector, and beyond, was examined. The collection and analysis of data from various sources plays a major role in this paper. As cybersecurity is evolving rapidly, it was necessary to use only up-to-date data, particularly the coronavirus crisis.

3.1 Description of the bank's questionnaire

The questionnaire is used for the collection of general information about the cybersecurity in each bank, also for collecting feedback from the employees of the banks. Several versions of the questionnaire (for employees, for managers and for IT specialists) has been developed to provide more detailed information about cybersecurity, possible threats and general opinion about the system. The questionnaires have been designed and agreed upon with the supervisor before using them for the research.

In addition, the laws and regulations applicable to all areas of business, as well as those specific to the financial sector, will be studied in detail.

Below is a description and interpretation of the topics covered in the questionnaire, as well as an explanation of why certain aspects have been touched upon.

Questions "The organisation and its context" were included in the questionnaire to get an overview of legal and regulatory part of the cybersecurity framework which is used in this specific company. Also, there are some questions to learn about the division of the responsibilities in the companies. In addition, these questions reflect whether the bank complies with relevant regulatory requirements and various

standards, as well as the position of the department responsible for cybersecurity within the organisation.

Questions “Audit, Certification & Training” is aimed at examining and analyzing the preventive measures in place in the organisation. This topic is divided on “All employees”, “In the cybersecurity / IT area”, “Internal and External Audits” which gives us an indication of staff and management awareness of the cybersecurity. Moreover, the answers on these questions give an insight into the importance and frequency of training, which positions are required to participate, as well as the required certification and frequency of audits.

Questions “Make or Buy (Outsourcing)” is aimed at examining the maintaining cybersecurity by the company itself or outsource organisation. These questions show the extent to which a company does or does not trust a third party to perform certain cybersecurity functions. As already highlighted in chapter one, many of the risks precisely stem from the transfer of certain functions to third parties.

Questions “End-of-Life Technology & Actuality” are about the software and the hardware. The purpose of the questions was to find out the extent to which banks adhere to old traditions of storing and transmitting information. In addition, how important is it for them to make copies and the frequency of this process.

Questions “Risk Management & Risk Analysis” is designed to show how a company is prepared for any type of the attack, because the risk management and analyze is the key for protected system. This block was the most extensive as it includes all the possible dangers according to the participants. There was also an emphasis on getting threat information from other sources and analysing it. An important question was where companies see their future development in terms of cybersecurity. The answers to this question prompted the creation of another questionnaire (Appendix 1. Banks’ customers’ Survey).

Questions “Network procedures” were added to find out the difference in maintaining the cybersecurity in the organisation with multinational staff and with international partners and customers. With this block we wanted to look at possible problems with colleagues, partners or clients from different countries, which will also help to look at different cultural backgrounds.

3.2 Description of the customer’s questionnaire

This questionnaire has been designed solely to help bank customers understand the need for security. According to McAfee's 2021 report[128], individuals are still ranked 4th as Targeted Industry Sectors. This questionnaire was designed to look at cybersecurity from a different perspective. It was important to understand how often people use online banking, how aware they are of the possible dangers associated with it, and their satisfaction with the service provided. This questionnaire was sent to the social network Facebook, which is the main network for Austria according Statcounter (GlobalStatistics). 69,42% of the population which live in Austria prefer Facebook as a social media for interaction and business connection[129]. However, it was sent exclusively to expat groups. About 52 responses were received, the result of the questionnaire is presented in appendix 1. As mentioned earlier, the idea for this questionnaire emerged from an analysis of the banks' questionnaire. Based on the fact that the response was exclusively from people of non-Austrian culture, it was decided to conduct a study on the frequency of card use in one traditional bakery, whose customers are mostly Austrians.

3.3 Description of the auditor's questionnaire

This questionnaire was designed to get the perspective of companies on the other side of security. It was necessary to understand the views of auditors who check banks and other types of businesses on the adequacy of cybersecurity measures. This questionnaire was much smaller than for banks but touched on key points that might go against the banks' views. It was also divided into sections similar to the banks' questionnaire.

Questions "The organisation and its context" are intended to show their views on the vast number of regulations for banks, as well as their views on the organisation of the cybersecurity framework in banks.

Questions "Audit, Certification & Training" show their views on the frequency of training, the personnel to be involved, and the required certification. There was also a rather provocative question about their attitude towards hackers. Moreover, a number of questions were developed about their work as a "Red Team" for a planned bank attack.

[128] (McAfee Labs, 2021)
[129] (Statcounter, 2020-2021)

Questions “Make or Buy (Outsourcing)” are used for understanding their opinion in the usage of third-party assistance in maintaining the cybersecurity.

Questions “End-of-Life Technology & Actuality” were designed only for understanding their position according to the different types of storage data.

Questions “Risk Management & Risk Analysis” was designed to understand their views on the main threats to banks now, and whether the implementation of cybersecurity and attitudes towards it differ between countries and cultures.

3.4 Limitation of the research project

The study began by looking at the constraints and risks that may have arisen. All risks and limitations have been outlined in the research proposal. Thanks to predesigned solutions to these problems, they have been overcome. Unfortunately, not all were envisaged, since the author:

1) is a non-expert in the cybersecurity and the financial sector

2) is a foreigner, not a citizen of Austria or the EU

3) does not speak German fluently.

Based on this, the author cannot fully claim that the questionnaire was answered completely honestly and truthfully.

Nevertheless, thanks to a study of the literature, regulations and statistics, a result was obtained.

The question under study could attract further study or conduct the evaluation of the problem from different perspectives. Further development of this work could greatly help the financial sector and business in general. A noteworthy enhancement would be the addition of weighing factors to each question, which could potentially result into more exact and accurate output. A more in-depth study of cybersecurity and its relationship to the cultural framework could close the current themes of the dangers of social engineering exposure. A study of certain incidents and an employee survey or gamification on cybersecurity could yield much more results, but this type of research is not available now. It is important to study not only European cultures

but also those around the world, because, as previously stated, professionals may come from different countries with completely different backgrounds.

4. Empirical framework

There are many theories and practices on how exactly cybersecurity should be performed and how it will be effective. This chapter will look at the 5 banks that have agreed to participate in this study, as well as one auditor. The name, location, size etc. are not to be disclosed as agreed with the participants. In addition, the bank's customers were interviewed, without specifying names, locations, etc. This chapter aims to look at how cybersecurity is implemented and the extent to which banks comply with official requirements. In addition, we will try to find a cultural dimension to the implementation of cybersecurity in the financial sector.

At the beginning of this study there were a huge number of risks and limitations that the author identified, but under the influence of the coronavirus crisis, these have become at times almost impossible to overcome. It was lucky that the request on participation has received 5 replies from banks. In such a hard time for business few banks had responded to our request. Unfortunately, not all questions were possible to answer, but we gained an insight into the cybersecurity in banks in general. Of course, the author's aim was not only to interview bank specialists, but also other bank employees, as well as regulators, software developers, auditors, etc. Unfortunately, in the current situation many of the above authorities refused to help, due to the difficult business situation, as well as the heavy workload of the specialists and the rather sensitive topic of discussion. However, thanks to the openness of the supervisory authorities, it is easy to find the information you need on their websites and in their regulations. In addition, all the latest developments are informed immediately.

In this chapter the author will observe the banks' answers to the questionnaire, compare them with existing regulations, and try to find a cultural basis in the implementation of cyber security. In addition, the point of view of an Austrian auditing company will be considered in some issues, which will also give an insight into cybersecurity, but from a different angle. However, based on Alexander Thomas' theory there is no guarantee that the author received completely honest answers about the banks, as the author is of a completely different culture and, what is more, the questionnaire was written in a different language (English). According to Thomas' theory this can cause distrust in a person from another culture and not allow for full honesty.

Furthermore, the author is not a certified cyber security specialist and does not have a professional knowledge of German, which puts the author a priori in a low position in the perception according to Schein's theory. In other words, the author does not possess the necessary artefacts that are important for both Austrian and cyber security culture. This conclusion was reached based on an analysis of the surveys conducted, and comments left by participants: "the question is incorrectly posed", "not classifiable in the given answers", and so on.

Each section will be analysed in detail below, and compliance with normative standards as well as cultural theories will be identified.

4.1 The organisation and its context

At the outset, the author wanted to make sure that the banks under survey complied with all the rules and requirements of the regulatory authorities and followed the regulations issued by them. All banks comply a priori with the requirements of the supervisory bodies described earlier, such as the FMA and EBA. However, 50% also indicated compliance with international regulations such as GDPR, NIST, PSD2 etc. It means that at least 50% of banks have got an international connection and intercultural connections. Based on this fact, not only a huge number of regulatory and legal obligations are imposed on partners, but also cross-cultural communication and business practices will play a major role. In this difficult business situation, it was interesting to know if there are any requirements that are difficult to fulfil. The auditor confirmed this possibility and imagines that complexity can arise solely from the sheer number of requirements given. Knowing that, according to Hofstede, Austrian culture prefers to avoid the unknown, so it tries to prescribe as much as possible about official documentation. In addition, as the Austrian culture is a low-context culture, it is very important that all documentation is laid out as accurately and as orderly as possible.

Despite of this fact, Bank 2 replied “EBA Guidelines on ICT and security risk management is the most complicated to follow, because it is written in a very open style and there is much space left for interpretation”. The document is not a 100% framework and the absence of a requirement to undertake a certain action makes it difficult to enforce. According to Hofstede's theory of the 6 cultural dimensions, one of the dimensions is Uncertainty Avoidance. This dimension can be characterized as

society's desire to know or not know in advance the possible outcome, to control the future. Austria scores 70 on this dimension, which suggests that a given culture is more likely to follow a clear set of rules, as it is developed based on data analysis and research of the relevant authority. In addition, using international standards (GDPR) also protects the country from the possible unpredictability of the 'future'. In one of the questions, the author had veiledly included a checklist from ISO 27001 to test how responsibly banks are handling the new mandatory document.

In order to establish a secure system and to avoid unknowns as much as possible, each bank must have precise policies, procedures and controls in place. Unfortunately, we did not find absolute uniformity on this issue, however, we did confirm the fact that banks claim to adhere to all the requirements of the latest ISO 27001 document and try to keep their system secure. Banks have a precise delineation of what the procedures, policies and controls are. The main point was for us to check how seriously they take the issues we have described. The survey showed that the banks comply with all official requirements without question, or at least that they have regulatory documents in place.

Every bank that took part in our survey reported that they have a dedicated computer security department, which is solely responsible for ensuring secure operations. The auditor stand for that IT department is supposed to be responsible for the cybersecurity, unless the bank has a specific cybersecurity department which can check both business risks and technical risks.

Also they confirmed applying The Three Lines of Defense model. As indicated earlier, the FMA has issued an order to apply this model, despite its criticism. Unfortunately, none of the banks answered us what their departments' functions and we cannot predict them. Nevertheless, Prof. Flemming Ruud, PhD, CPA (Norway)[130] mentioned that for financial market it is sometimes very hard to divide the functions between the lines, which has been proven by Bank 5, which mentioned that IT security department is defined as 1st line of defense and evaluation ongoing to define 1,5 line control framework. Considering that cybersecurity specialists only come into action after the first line of defense, it may raise concerns according to critics of this model. As previously described, there is a high probability that the first line of de-

[130] (Prof. Flemming Ruud, November 2019)

fense may be played by human and/or cultural factors and an attack will not be prevented. The danger is that people from different cultures may have different perceptions of risk and either accept risks or find them unacceptable. In addition, as Hall wrote, different cultures have different perceptions of 'space'. Some cultures cannot violate another person's space, e.g. addressing some safety issue to another person, perhaps a higher ranking person. This can also be seen in the key of the Power Distance dimension or the cultural standard of 'loss of face' or cultural standard by Thomas "maintaining and giving face"[131]. In addition, as stated earlier in the theoretical section, different cultures can be individual or communitarian according to Trompenaars, which can influence their decision-making. For example, some cultures can make a decision without regard to the opinion of another person.

The auditor also believes that "It's an abstract concept that helps design your security, but it is not necessary, as long as you understand the basic principles". In other words, for them, if the system is designed in a different way, it is also acceptable as long as it works without errors and successfully repelled attacks.

4.2 Audit and Certification & Training

In order to avoid such a situation, as indicated in many papers, continuous training, tests and information campaigns are necessary, but it is also important to carry out research on the workforce and their cultural background.

With new types of viruses, attacks and scams increasing daily, how often do you need to train specialists and other staff to make your system as secure as possible?

"According to a survey conducted by MindTake on behalf of techbold in January 2020, 60 percent of all companies with more than 31 employees in Austria had an IT security incident in the last two years. The three main causes, with a share of almost 45 percent of respondents, were a technology failure, hacker attacks (40.6 percent) and employee error or ignorance (34.8 percent)."[132]

80% of the banks answered that they perform trainings, awareness campaigns, test etc. monthly, but 20% - quarterly. If we apply the worldwide practice of trainings, according to statistics designed by Shanhong Liu in 2020 about the frequency of cybersecurity trainings for employees in different organisations in USA. 29% of re-

[131] (Gerhard Fink, 2005)
[132] (Schultz, 2020)

spondents confirmed proceeding tests only once per year.[133] The regulations described earlier do not specify the frequency of training, only that frequency is important. Perhaps based on the fact that attacks and attackers develop on a daily basis, banks prefer to choose the most correct course of action - monthly. This type of training should not interfere with the work process, but at the same time should be aimed at preventing possible new attacks. In addition, there is a view that training should be tailored to each position, taking into account possible job specifics and the functions performed. This approach will help to identify the smallest security gaps in the day-to-day work of a position[134]. In addition, knowing that people of a certain culture can sometimes be guided by the first impulse of that culture, it is important to take this fact into account when planning and delivering training. For example, it is possible to apply the tool as Cultural Adaptability Profile (CAP)[135] designed by researchers, experts in global mobility and L&D specialists. This tool will help provide a behavioural assessment of actions in a given situation, as well as providing insight into how adapted a person is to the culture in which he or she works.

As discussed in various research papers, such as (e.g. comparing Austria and Bulgaria, Austria, USA and Russia[136]), different cultures react and act differently, as people are indirectly or directly influenced by their culture. Some cultures may be naïve (from the work on naïveté) or overly trusting[137], may rely too much on their education and act rather risky[138] etc. For example, if we consider the dimension of ignorance avoidance in Hofstede's theory, some cultures (e.g. Austria) will try to calculate all possible steps and plan their actions safely, unlike other cultures (e.g. the US), which may be characterized as "risk-takers". Training is therefore very important in order to reduce the possible influence of the cultural background.

Every bank mentioned the mandatory phishing training and overall awareness of information security. As previously stated, social engineering is one of the main methods of infiltrating a company[139]. It is still quite successful to this day because of the human and cultural factor. This fact brings us to the next question that was asked to the banks about the positions of staff who participate in trainings. In the chart men-

[133] (Liu, 2020)
[134] (Antipov, 2016)
[135] (Smith, 2020)
[136] (Ksenia Keplinger, 2012)
[137] (Kevin D. Mitnick, 2002)
[138] (Kathryn Marie Parsons, 2015)
[139] (WRIGHT, 2016)

tioned below it can be seen which positions are mandatory to participate in trainings and which sometimes do not participate at all.

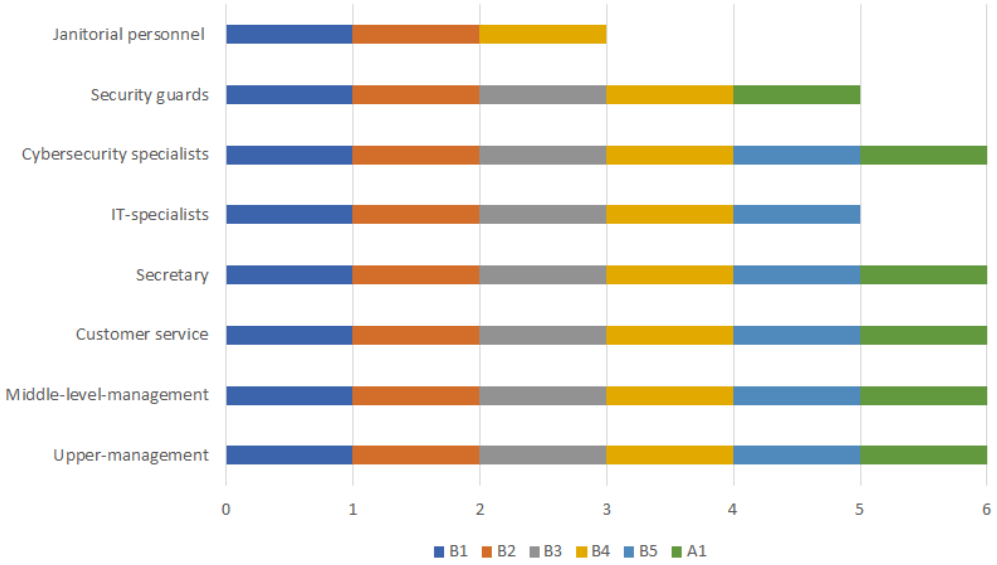


Figure 12. What type of personnel is taking part in trainings?

Interestingly, 2 banks and the auditor excluded janitorial personnel and one bank also excluded security guards. So why is it so important to include all possible personnel who may be in the building in the training? According to Kevin Mitnick and his book "Art of deception", social engineering can theoretically unlock any door, even a very well-guarded one, by influencing seemingly insignificant areas. In one of the chapters, he gave an example, how fraudsters can gain access to your information without resorting to sophisticated software, purely by playing on the human factor. “Dumpster diving” is one of the thing one attack that seems incredibly odd, however, could be a real threat to information if neither the staff nor the cleaners make sure that crucial documents are completely destroyed. “The lower the position in the organisation, the more serious the training should be”, - said bank 4. There is also a fairly clear cultural influence here. As mentioned earlier, some cultures do not separate work from private life, and for a member of that culture, an 'employee' coming in late at night can be perceived as perfectly adequate. Given that cultures can be more generous and for them relationship building is more important than business relationships, there is again a danger of being attacked by social engineers.

A rather surprising answer was received from the auditor, that the specialists should not take part in the training either. Could this be an overestimation of the experience and education of the specialist? According to Schein, they already have the necessary knowledge and judgement (artefacts, values and assumptions) and would not need this training. However, overestimating one's capabilities and skills is exactly what leads to mistakes[140].

Mitnick[141] has pointed out many times in his book the importance for the social engineer of knowing 'lingo' both within the organisation and narrowly specialized. That is, even he potentially pointed to one important artifact of culture (corporate and cybersecurity). Furthermore, knowing this "lingo" and being able to apply it correctly can create false assumptions (according to Schein's theory), which literally opens all doors in the organisation.

Crowdstrike in its report informed that there is now a tendency for criminals "to adapt the letter to the language of the target country and manipulate the victims emotionally in order to increase the number of infections"[142]. It follows that even deceivers are actively applying Schein's theory of the 3 levels of culture to carry out their activities more effectively. They show that they are armed with a specific artefact (lingo) and can get access to vulnerable and important information easily.

In addition, a fraudster could gain access to the building after the main staff has finished working, telling the janitorial personnel or security that he/she has forgotten an important document at the workplace. This has happened and is described in the Mitnick's book[143]. It is not a minor fact that this position is most often held by non-Austrian origin people who can be easily misled due to their low position and cultural background. Returning again to the article "Information security culture: A Behavioural Compliance Conceptual Framework"[144], where the authors have divided employees into 4 categories. They repeatedly point out the need for employees to be aware and informed in order to put them all in the same Knowing-Doing mode, re-

[140] (Kathryn Marie Parsons, 2015)
[141] (Kevin D. Mitnick, 2002)
[142] (CrowdStrike, 2021)
[143] (Kevin D. Mitnick, 2002)
[144] (Alfawaz, 2010)

gardless of their position. Moreover in a lot of articles confirmed that the employee awareness increases overall security[145].

An important question was whether the employees' and the banks' certification. How is it important to have specific certification for work in general? Bank 4 informed us that they don't think that certification is a guarantee of a high level of awareness and professionalism in the cybersecurity. Also, a person without any certification can work more sufficiently. However, as already described in the theoretical part, any culture can be analyzed according to Schein's theory. Cybersecurity culture has the same artefacts, values and assumptions. It was important to understand whether this theory applied to banks. Appropriate certification and education can also be viewed in terms of obligatory cultural artifacts of both organisational culture and Austrian culture as a whole. Artifacts are a visual representation of culture. By having certain artifacts, such as a certificate, an individual can be considered part of a given group. However, education and work experience can be seen as a 'Value' of culture. In other words, it is a representation of "how things should be done". Moreover, certification, experience and education may be among the reasons for hiring an employee regardless of his or her cultural background. However, according to research "The Influence of Organisational Information Security Culture on Information Security Decision Making"[146], the presence of these artefacts may play against the company. Professionals may overestimate their experience and skills. Again, more research is needed into each individual's culture.

According to the survey, all specialists and bank employees have relevant education, work experience, certification according to their position, etc. In addition to this, banks are obliged by regulation to have various certificates such as ISO 27001, ISO 9001, ISAE 3402 and so on.

Despite this, no bank posts its certificate on its website, compare to other businesses, which update their information immediately after receiving a certificate. Why don't banks show this information?

There is a perception that hackers or cybercriminals are lazy. This opinion was expressed by Arne Schönbohm, Präsident, Bundesamt für Sicherheit in der Informati-

[145] (Thomas Schlienger, 2002)
[146] (Kathryn Marie Parsons, 2015)

onstechnik (BSI)[147]. A similar view was expressed by Chris Baraniuk[148] in his article for the BBC in 2017 and Dan Stoy[149], Solutions Specialist in his recommendations for Coordinate System Solutions, Ltd in 2018. The main idea behind this inference is that nowadays it is very easy to find software to help you break into any system. Also, the widespread use of social engineering, which essentially requires no in-depth knowledge of the technical side of things. From this we can conclude that hackers would rather launch an attack on a poorly defended target than attack a business with a potentially good system against breaches. Hackers, like any other experts, do research on a potential target to understand weaknesses and strengths. In our electronic world, the first instance would, of course, be the website. Having discovered a particular document on it, and given the fact that they can be "lazy", will a specific attack be devised, or will the perpetrator find a different target? On the other hand, a bank operating in a particular country is required to have the appropriate certification, and demonstration or non-demonstration will in no way play a role in a hacker's desire to attack a particular bank. Taking into account the fact that one of the main methods was and still is social engineering, despite all possible certifications; the individual is still very vulnerable. This fact is confirmed by the previously reported statistics on the effectiveness of phishing attacks, which CISCO claims in its article to be a "low-effort, successful method"[150].

It is also worth considering the fact that sometimes hackers may not be criminals. For example, if you consider another book by Kevin Mitnick, "The Art of intrusion"[151], where in the first chapter he describes a money affair done simply by good technicians who just wanted to test themselves and their professionalism. It was a kind of challenge for them, not a way to get rich, but they came out winners and with quite a lot of money.

According to the CrowdStrike report[152], on the rise of crime and their minute-by-minute technological advances, the statement that "hackers are lazy" can be questioned. It must be borne in mind that criminals can use a variety of methods and one should not expect that providing or not providing a certificate can protect a company

[147] (BaFin, 2020)
[148] (Baraniuk, 2017)
[149] (Stoy, 2018)
[150] (Duo Security Inc.)
[151] (Kevin D. Mitnick, 2006)
[152] (CrowdStrike, 2021)

from any threats. Therefore, in my opinion, one cannot say for sure whether hackers are lazy or not.

This fact has been confirmed by Bank 4 which favors the publication of the certificates online. According to the specialist, even if you do not provide a copy of the certificate on your website, you indirectly write about them in various articles or blogs. Much more dangerous may be the job descriptions exhibited by your human resources department which may indicate what knowledge and what software a particular professional should have. With this information, an attacker can infer how he or she will conduct a successful attack.

From the auditor's point of view, banks should display their certificate on their website because “the primary purpose is publicity. You can have good security without a certificate.” Showing the certification, you just conform that you protected what can increase trust from partners (existing and potential). Moreover, they commented the idea about “lazy hackers”. Do they think some hackers are lazy? Yes, but not all of them. Hackers are aware that all certification has limitations and loopholes, so they can circumvent it knowing or not knowing it exists. They also divide hackers who are hunted for "big fish" and those who are just "just showing off or trying something new".

Cultural bias can play a huge negative and positive role in analyzing the actions of particular employees. Based on this fact, the analysis should try to "switch off" one's own culture or have a third independent party (from a totally different culture) to independently assess an incident or employee's behaviour.

Based on the facts described above, it is obvious to think that banks should to audits of their system periodically, that’s why the questions about external and internal audit were designed. According to the fact that every bank in Austria is obliged to follow “the three lines of defense” framework, they have to plan and carry out periodic checks both internally and externally. There is no specific timeframe required, only that they are supposed to be periodical. The frequency of the audits only mentioned in ISAE 3402. Our participants confirmed 40% maintain internal audit once a year, 40% half-year and 20 % periodically. Absolutely the other picture with external audit – 60% answered “yearly”, 20% half-year and 20% periodically. Internal audit occupies the third line of defense and external audit could theoretically occupy the fourth line,

as described in the work of Isabella Arndorfer, Andrea Minto which criticizes the current system.[153].

As LoD has already been criticized by various experts and resources (confirmation in the theoretical chapter), the problem with the third line of defense may be that they may not recognize the high level of risk, and concentrate on other areas, which may reduce the effectiveness of this line. Based on this, if internal audits take place only once a year, a number of potentially high-risk areas may be missed due to too infrequent inspections[154].

Of course, a large number of frequent checks can reduce performance, hence a more efficient and quicker way to check the safe operation of all protection lines and the system as a whole should be developed.

4.3 Make or Buy (outsourcing) and End-of-Life & Actuality

Perhaps because cyber security threats are evolving quite rapidly, banks sometimes make use of third parties. 60% of the banks surveyed use third-party assistance with various cyber security issues, while 40% try to use their own resources exclusively.

According to Hofstede's theory, Austrians prefer to avoid the unknown in business, and they also try to achieve maximum results. Resorting to third parties who are professionals in their business is quite logical and culturally validated. In addition, a contract with all third parties is as detailed as possible (low-context), in which all rights, obligations and restrictions are stipulated.

We were asked whether companies use the standard software or whether they completely/partially modify it to suit themselves. This question was needed to understand how easy it would be for fraudsters to gain access by knowing what software a particular bank uses. As was the case in the most high-profile Iranian Natanz facility attack case[155], where the attackers were able to find out the exact details of the software and deal a devastating blow to the entire enterprise. Most interestingly, despite the fairly secure facility, the attackers obtained the information through photographs

[153] (Isabella Arndorfer, 2015)
[154] (Bruce, 2017)
[155] (Dashlane, 2018)

of journalists that were taken during the president's visit to the facility. The photos caught some of the computer screens where the main software was running.

Also, according to Bank 4, there were cases where a software developer could leave a 'logic bomb', so it was important to understand the extent to which they had access to company data. As Mitnick's book[156] pointed out earlier, the hacker may sometimes not be a criminal, but an ordinary technician who wanted to test his skills to the fullest.

In the banks' responses, it is possible to trace a pattern of the answers according to the cultural basis. Some answers are quite extensive describing the maximum functions of the third party (low context), while others are "all according to the contract and the law" (high context). Moreover, as previously stated, the author is an outsider to the company, to cybersecurity and to Austrian culture in general. Therefore, there is a certain lack of the necessary “artefacts” and trust as towards a representative of a different culture.

Based on the fact that we needed to understand how cybersecurity is performed in general, the banks were also asked a bit about the technical and organisational system. In addition, banks were asked about the frequency of updates of the system and only 2 banks indicated a specific timeframe, as opposed to others which answered rather vaguely: "Timely", "depending on criticality of the processed data" and bank 5 mentioned the system of “Patch Management Life Cycle”. It is the type of systematically updating of the software[157].

As one software developer writes, keeping up to date will help improve your cybersecurity system. An outdated system is an unnecessary opportunity for a hacker. The attacker can easily track down a system bug and use it to launch an attack. In addition, software updates lead to stable operation, bring any improvements and improve performance[158].

As Mitnick wrote in his book[159], and as software developers and researchers repeatedly point out, one of the dangers may be obsolete equipment accessing the Internet that has been implanted into a company's internal network. There are a num-

[156] (Kevin D. Mitnick, 2006)
[157] (Broadcom, 2021)
[158] (Symanovich, 2021)
[159] (Kevin D. Mitnick, 2002)

ber of publicly available sites where anyone can easily find information about possible hardware connected to the network and whether it is protected or not. With this information a hacker can easily break into the outdated equipment and gain access to all network. When asked about the frequency, we received different data. Some banks gave specific timeframes, while others took a more analytical approach, such as life cycle asset management. This approach helps companies analyze their equipment and decide on its performance and applicability in the current operating environment. However, the question remains to what extent this analysis takes into account resilience to cyber-attacks. Perhaps the equipment is evaluated solely on the basis of technological criteria, without cyber security risk management.

Given that the technology world is evolving quite rapidly, it was important to understand whether the company had old equipment that could potentially become a weak link in cyber security. As a result, 60% have equipment that is 10-20 years old, which is quite obsolete. 20% were evasive, and only 20% reported that equipment is being replaced all the time. This bank tries to upgrade every 3-5 years to comply with all security measures. According to the technical specialists, the hardware supposed to be replaced at least once per 5 years[160].

Could there be a cultural subtext in the use of obsolete equipment? If something works well, there is no point in constantly replacing it and wasting the budget.

“Cyberspace is growing rapidly, as new connected devices, networks, services and data emerge. This brings changes in the scale not only of networks, but also of data volumes, storage capacity, processing systems and the knowledge space that we collectively create. The scale of cyberspace is already difficult for most to conceptualize.” (World economic forum 2020). Because of the huge amount of data that banks have to store, there is a need for either additional hardware devices, or so-called “cloud” storage. In its research, Blancco Technology Group concluded that many companies continue to use legacy equipment to store information. The study involved 600 participants from various countries, including Europe. They concluded that two out of five companies spend more than $100,000 on storing information on hardware devices, which can pose security risks[161].

[160] (Kill, 2017)
[161] (Spadafora, 2019)

According to Kaspersky Lab statistics, the financial sector is in third place for cloud storage usage[162].

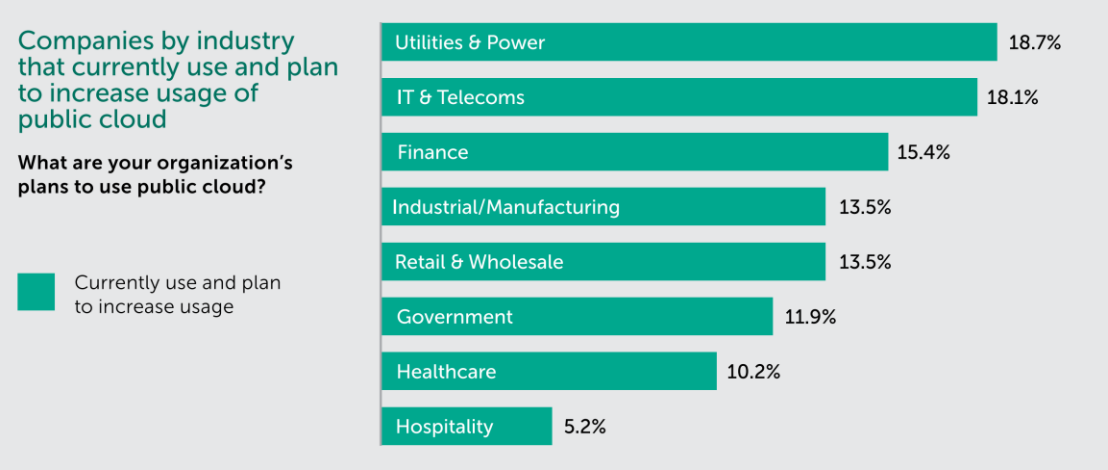


Figure 13. Usage of cloud storage[163].

In addition to increasing the company's capacity, this storage facility also carries certain risks. Sometimes you have to deal with a data service provider that is on the other side of the world, which brings with it certain regulatory, legal and cross-cultural challenges. Regardless of size, businesses (21%) are storing sensitive data on the cloud, according to Kaspersky Lab, putting them at risk. Data security is the responsibility of both service providers and the companies themselves. According to their statistics, the majority of data leakage incidents (33%) are caused by social engineering (most often phishing). Despite research into cloud storage and major security breaches, most companies cannot be completely confident in their service provider. This fact only speaks to a lack of awareness among companies themselves. Also, only 39% of SMBs and 47% of large enterprises have taken steps to protect data in cloud spaces, meaning that the remainder are shifting the responsibility for keeping their data secure to the provider. Kaspersky Lab sees the future in storing information in the cloud, but insists that staff training is mandatory and that a sufficiently secure system must be developed.

Despite research in this area, two out of five banks still prefer only hardware for storing information, three out of five use both types of information storage. One of them stated the need to move 100% to cloud storage because "it is the future". From a

[162] (Kaspersky Lab, 2019-2020)
[163] (Kaspersky Lab, 2019-2020)

cultural perspective, the use of hardware could be a sign of avoidance. Cloud storage brings a huge amount of risk and additional regulatory requirements to the organisation and perhaps some banks prefer to avoid additional blind spots. In addition, more often than not, the cloud storage providers are located outside Austria, which also makes them from a different culture, which violates some cultural standards (Alexander Thompson). Last but not least, as previously described, Austrian culture embraces the new, but with the preservation of the old. Perhaps that is why some companies try to switch to a new kind of information storage, but still stick to the "tried and tested way".

According to research by leading software development company Malwarebytes LAB[164], due to the current coronavirus situation and the mass shift of companies to home office, cloud storage may increase in popularity. Based on research conducted by the self-styled online freelancing platform Upwork they concluded that "By 2028, research shows 73 per cent of all departments will have remote workers."[165] Consequently, security must extend far beyond the company. Employees can use their personal devices at home or anywhere in the world, while still being connected to the internal network. Employees may also save work files on personal cloud storage, which may not be secure enough, and so on[166].

With cloud storage, you always have access to your information wherever you are, but that does not mean that any kind of storage of your information does not need to be backed up. Data backup is the process of backing up important information on any type of hardware or cloud, which the company then has access to in case the information is stolen or lost. Another Norton software vendor insists on systematizing the process, because in the event of data loss, ransomware attack or other mishap, the company can recover much of the data[167].

There are several ways of carrying out this process. Two out of five banks reported a daily process, one bank did not indicate any specific term, one bank reported that "period depending on the specific business requirements for the various applications/services" and only bank 4 indicated a specific GFS data retention ("Grandfather-father-son"), which is used in business as well as in ordinary life. This type of backup

[164] (MalwareBytes Labs, 2020)
[165] (Upwork (UPWK), 2019)
[166] (MalwareBytes Lab, 2020)
[167] (Chivers, 2021)

is based on creating backups in a specific period of time. "The GFS backup rotation technique is a popular method of data backup, allowing combining full and partial copying to different media for both reducing backup time and enhancing storage security."[168]

Table 3. Example of the GFS framework[169].

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1 Father	2 Son	3 Son	4 Son	5 Son	6
7	8 Father	9 Son	10 Son	11 Son	12 Son	13
14	15 Father	16 Son	17 Son	18 Son	19 Son	20
21	22 Father	23 Son	24 Son	25 Son	26 Son	27
28	29 Father	30 Son	31 Son	Son	Grandfather	

Once again, there is no concrete guidance from the supervisory authorities on how this process should be structured. Several reasons are possible, one of which could be to give banks the freedom to do so without locking them into a particular structure, thereby giving hackers the opportunity to calculate and plan an attack at the right time. Also it could be an example of one of the cultural standards is that absolute autonomy in decision-making can be accepted if nothing else is prescribed. However, some banks do prefer to use some techniques which have proven to be effective, i.e. have earned their status as effective.

From the above, we can conclude that outsourcing is not an easy topic and certainly carries a huge amount of risk. From the other hand, thanks to the fact that there are domestic and international laws within the EU, it has become safer to use third parties. However, outsourcing will always carry operational and other risks. In the event of any interruption, the bank itself will bear the financial and other losses, as they are the main (financial) service provider. Of course, additionally all conditions can be spelled out in agreements and laws, but in my opinion every bank should have a plan B in case one of the outsourcing partners fails. In addition, we did not get a specific answer about auditing third-party companies. The banks responded with gen-

[168] (Handy Backup)
[169] (Handy Backup)

eral phrases such as "according to the contract", "within the law", "almost every day" etc.

4.4 Risk Management & Risk Analysis

As stated by BaFin[170] in its article, the EBA and EIOPA have repeatedly pointed to the importance of risk management for the financial market, and in particular the assessment of each company's risk. According to the survey, all banks have a system for assessing risk tolerance, but only three out of five that are willing to accept security risks depending on its level. Banks 3 and 4 reported that the most frequent calculation is based on the value and likelihood of the risk.

Risk assessment can more than ever be linked to a cultural basis. As pointed out by Alexander Thomas in his book[171], the same goal can be pursued differently by different cultures and the acceptance/unacceptance of risk plays a huge role. For example, if both cultures want to succeed at something, the goal will be the same, but the tools and actions used to achieve it may be dramatically different. However, in this case it is not possible to confine oneself solely to Hofstede's dimension of 'Uncertainties avoidance', the work of all scholars presented in this thesis, especially Alexander Thomas, must be taken into account, because he views cultural specificities from a slightly different angle.

One of the most important questions in the questionnaire was where companies see the general root causes for cybersecurity risks and we got the following chart. If the bank responded that it is the category that is dangerous, it is highlighted in red in the table. If the category is not dangerous, it is highlighted in green.

Table 4. What is the general roots cause for cybersecurity risks?

	IT (hard and software)	Employees	Processes	External impact
B1				
B2				
B3				

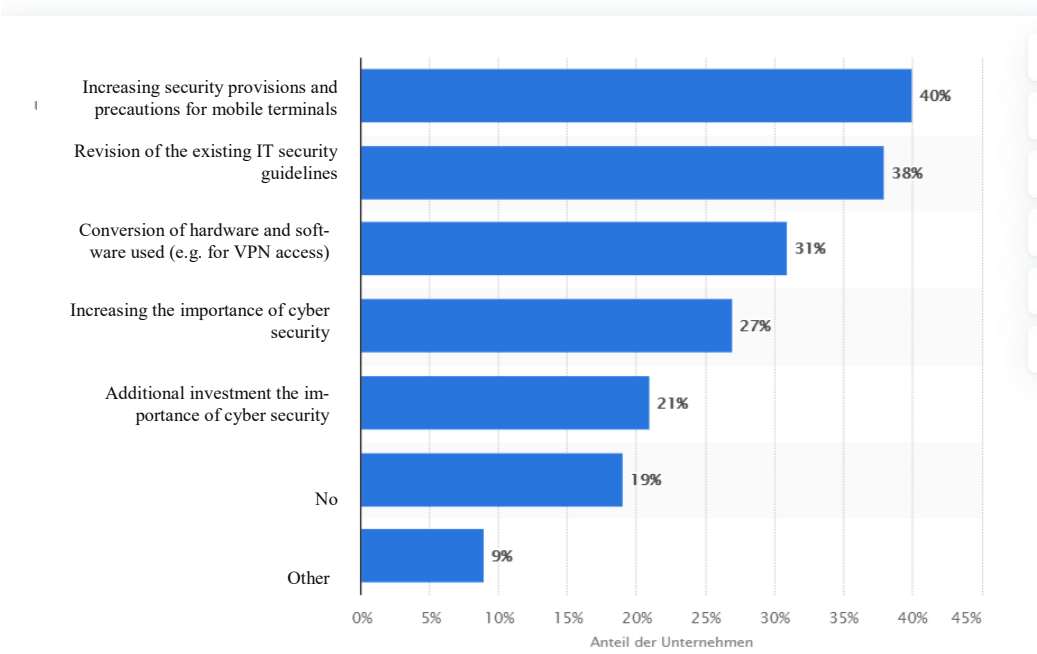
[170] (BaFin, 2020)
[171] (Schroll-Machl, 2010)

B4				
B5				

Although different banks see causes in different areas, but all agreed that 100% of the threat will always come from company employees. In other words, despite the development of security in general, the human factor remains one of the most dangerous. This means that research in this area remains important and our attempt to find different cultural patterns in behaviour can help banks reduce risk in this area. Unfortunately, our employees' questionnaire was rejected due to confidentiality concerns. However, I insist that a detailed examination of the possible bases for a decision can fundamentally change cyber security.

Deloitte Austria and the SORA research institute verified a survey of companies in 2020 on their future course of development after the pandemic. As a result, one of the most important aspects was the rethinking of existing cyber security. With this in mind, it was important for the survey to get the banks' perspective on which area of security they would like to focus more on. Two of the five reported that all of the following areas were important to them, one bank planned to focus on third-party action, one bank said it was important to review internal assets, and only one refrained from commenting.

Table 5. What data and information security measures will you focus on in the future against the background of Covid-19?



Again, this fact is supported by the fact that we have received many rejections to take part in this work, as banks and other organisations are now very focused on building as secure a system as possible.

Assuming that banks find employees to be one of the main root causes for cyber security risks, it was important to understand what the most important mistakes are that put them in this position. We cited the most common mistakes made by employees, such as disclosing information to third parties, phishing, etc. In support of this fact, Kaspersky Lab studies show the percentage of employees who concealed an attack.[172]

[172] (Kaspersky Lab, 2017)

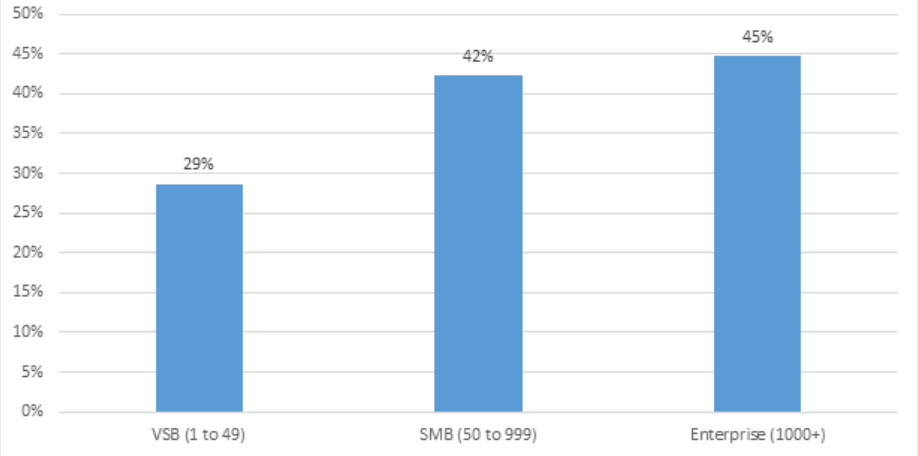


Figure 14. Percent of businesses where employees hide cybersecurity incidents (by segments). Source: IT Security Risks Survey 2017, global data

However, according to the prose, the result below, mistakes occur or can occur very rarely. From which a few theories can be made:

1) Companies are not completely honest, as admitting an error by their employee can lower their credibility.

2) Companies are not prepared to confirm this fact, as it would go against Schein's values.

3) Companies trust their employees because they have a professional relationship (Masculine culture according to Hofstede's dimensions).

4) Companies can "lose their faces" what will be against the cultural standards of the culture, etc. according to Alexander Thomas.

The validity of this information can only be verified by furthermore in-depth research of each individual bank from the inside.

Below is a chart of the most dangerous threats to banks according to them.

Table 6. The main threats for banks' cybersecurity

	Internal (social engineering)	Direct attack by an employee	Internet of Things (printers, modems, etc.)	Update the system	Hackers' attack	Former employee direct attack or using social engineering	External equipment	Customers	Partners
B1									
B2									
B3									
B4									
B5									

From the table, we can clearly see the 3 main dangers are "social engineering", "Hackers' attacks" and "External equipment", while two of these can be dealt with exclusively by technical means, the first is exclusively at the human level. However, a hacker attack also involves a great deal of human error of any kind and type of attack. How correctly it will be assessed as dangerous or non-dangerous, how quickly it will be informed, etc.

Staff awareness will always be of paramount importance. Every culture perceives information and the need for it differently, but it is important for many cultures to understand why they need to fulfil certain responsibilities or requirements[173].

Unfortunately, in the following example I cannot give the name of the participant, but I can tell you that it is a former bank employee in Russia. The bank in question is headquartered in the European Union. Employees have been given a list of what they can and cannot do. One of the points was that they are not allowed to use their personal USB flash cards in the workplace. The employee did not understand the strangeness of this requirement and considered it unreasonable a priori. Based on this small case, we can say that there was no structured training and the root causes of the requirements were not explained to the staff. Furthermore, some cultures do not separate personal life from work, as indicated in Trompenaar's work. Consequently, using

[173] (Alfawaz, 2010)

something personal in the workplace is not unacceptable to them, nor is working outside the workplace and outside working hours.

Given that many information leaks are caused by human error, it was important to clarify what then is the main threat to business. All banks confirmed that it is an internal threat, such as phishers. In addition, three out of five banks confirmed a possible IoT threat and a failure to update the system in a timely manner. Even though these banks indicated that updates are "timely" and "when it's necessary". From which we can conclude that this process of updating the system needs to be reviewed and a specific frequency for each program needs to be adjusted. In addition, since they are indicating a possible attack through different hardware, the long-term hardware usage policy should also be reviewed. One bank has equipment that has been in use for more than 20 years, which makes it insecure.

Being aware of the latest news and new types of attacks is very important, as it has already been stated many times, society is increasingly moving into the digital world and cyber security is becoming the number 1 topic. Naturally, banks also want to get the latest news, so they use certain sources. According to data received from them, they fully analyze their own experience, most also rely on data received from auditors and official supervisory bodies, and most prefer to receive data from other sources, for example OSINT (Open Source Intelligence) or FS-ISAC, etc. Bank 4 reported that it trusts its peers, white hackers and software developers more than official supervisory bodies. In his/her opinion, information from them is more reliable and closer to the working situation than from official sources. In addition, we did not get a specific answer about auditing third-party companies. The banks responded with general phrases such as "according to the contract", "within the law", "almost every day" etc.

While it is important to get information from different sources, it is not unimportant to get it in a timely manner, to analyze it and to draw certain conclusions. Only one bank said how it analyses the information it receives, the others simply said that certain specialists do it and the analysis is done according to certain areas of work. Bank 5 reported on those levels of evaluations that exist for the analysis in their Security Operations Center.

1st Level: false-positive evaluation (is a result that indicates the presence of a condition even when it does not exist).

2nd Level: deep analysis on the threat/incident

3rd Level: Escalations and countermeasures.

The results on the frequency of receiving information were a bit confusing as bank 4 indicated daily, bank 2 indicated weekly, bank 3 indicated monthly, bank 1 and 5 indicated as appropriate. Perhaps there is no definite structure to this question as it is not defined in the official documentation and each bank decides for itself which period is more appropriate.

Like any other business, banks need to plan any changes or improvements for the coming year. We decided to find out which aspects they plan to pay particular attention to. The companies see improvement in all areas of business, but Bank 2 and Bank 3 see no need to improve "Customer's service including app". Despite what FMA sees as a threat to security, it is the customers[174]. They have developed an additional website to help bank customers take preventative measures against cyberattacks, especially when using mobile apps. In addition, one bank reported that people try to download the bank's apps from pirated fake websites or apps, particularly seen by android users. Although Austrians according to Hofstede avoid uncertainty, they are also according to cultural characteristics quite complacent.

In order to be credible and to obtain data solely within Austria, we developed a small questionnaire and sent it to various sources, mainly social media. The result was impressive, as the questionnaire received a response from 52 people; hence the issue of improving the quality of applications is not unimportant. We would also like to point out that the questionnaire was specifically aimed at expat groups, i.e. potentially people from a different culture.

People in the 30-40 age group participated more actively in the survey (45.10%). In addition, we confirmed the fact that people currently prefer to use cards rather than cash. 69.23% chose this form of payment as the most acceptable, however, 28.85% still use both card and cash. This practice is possible due to the realities that not all of EU and not everywhere can be paid by card. The current practice is that

[174] (FMA, 2021)

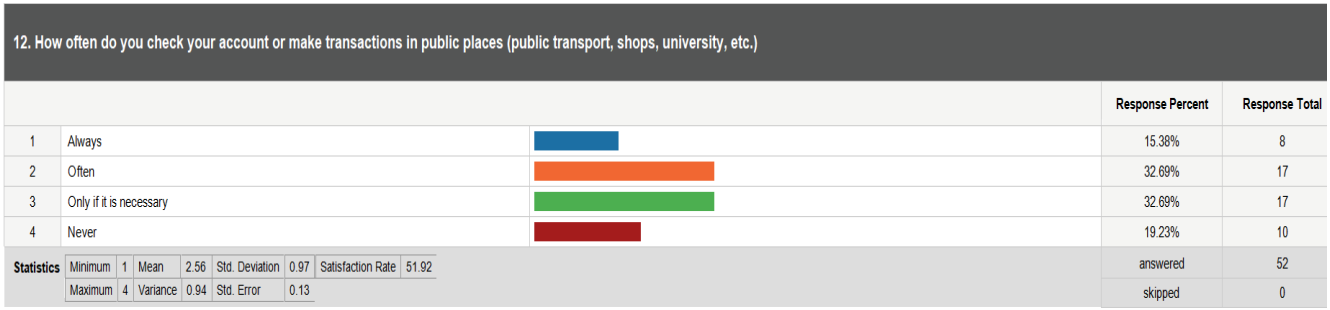
people use the services of more than 1 bank, as confirmed by the survey data 44.23% are clients of two banks and 94.23% have a banking application installed.

Although all banks offer 2 types of authentication, there are responses where users turn off one type due to inconvenience of use.

One type of authentication is 'what you have', which can be a device, phone number etc. but only 51.92% inform the bank of its change. Perhaps some banks have an automatic notification system for changes.

We also looked at what methods and how many users use to access and authenticate, which may be useful for banks in the future. So far all methods are within the scope of EBA legislation[175].

Knowing social engineering techniques such as “shoulder surfing” (the situation when the attacker sits next to you in a public place and checks what you are doing with you device) or using an unsecured network in a public place (café, restaurant, etc.) to steal data, it was asked how often people check their accounts in public places, and the results can be seen in this diagram.



12. How often do you check your account or make transactions in public places (public transport, shops, university, etc.)

		Response Percent	Response Total
1	Always	15.38%	8
2	Often	32.69%	17
3	Only if it is necessary	32.69%	17
4	Never	19.23%	10

Statistics								answered	52
	Minimum	1	Mean	2.56	Std. Deviation	0.97	Satisfaction Rate	51.92	skipped	0
	Maximum	4	Variance	0.94	Std. Error	0.13			

Figure 15. Answers the question from the Bank's clients questionnarie (Appendix 1)

It turns out that almost 48% of those surveyed could be a potential victim of a social engineer. 32.69% answered "only if necessary", which allows us to add them to the percentage already indicated earlier.

As discussed in the theoretical part, banks, software developers, as well as supervisory authorities are constantly informed about new threats and how to protect against them. Participants were asked the question “Have you read all the precautions that the bank publishes on its website to protect customers from all sorts of scams?" and it turned out that only 32.7% were interested in the security issue. Perhaps this

[175] (EBA-Op-2019-06, 2019)

percentage will change the banks' view on further improving cybersecurity for customers, as they are still one of the security threats.

In addition, 30 participants out of 52 gave detailed answers to the question about improving the app and the online payment system. This fact confirms that they have something to say and can give banks useful information that banks can use in the future.

However, I repeat that this survey was conducted amongst predominantly people from other cultures. Conducting another small survey on the preferred method of payment, it was found that only 16% of customers of one traditional bakery pay by card. This fact allows us to conclude that Austrians predominantly prefer cash to cards, which confirms one of the cultural traits - the preservation of an old and tried and tested method. In addition, according to people, cash allows them better control over their spending. Based on this study, the reasons for the reluctance to develop customer service are obvious. However, it is not possible to give an absolute answer as no research has been done on the customer base and the percentage of Austrian customers compared to customers from other countries has been identified.

According to the banks' responses, they have taken all possible measures to protect themselves against malware attacks, which is probably confirmed by the previously cited statistics, which do not include Austria. Again, the Crowdstrike report[176] does not provide specific information about the attack on Austrian banks, but it is interesting that the developers of the most dangerous malware are in Russia, China, North Korea, etc. Is it possible to characterize this one on a cultural basis? Perhaps one of the cultural standards is to take a dominant position. All three states have a strong military power and in the present digital world they need to take the same position. Furthermore, these countries are characterized as collectivist in contrast to Austria[177]. Although in Austria the dimension of masculinity prevails, but also individualism, so it is much more important for someone to achieve success related exclusively to the life of the individual rather than society as a whole.

4.5 Network procedures

[176] (CrowdStrike, 2021)
[177] (Hofstede Insights)

This section received the smallest number of answers and useful information, as some banks chose not to answer questions. Our interviewees not only operate within Austria but also abroad, hence they are actively involved in cross-cultural communication both internally and with partners and customers. Of course, some banks refrained from commenting on which countries they work with. However, more than half of the banks admitted that they work with other parts of the EU. This type of cooperation is safe for them as it is conducted within a single regulatory framework, in which, if there can be any disagreements, the parties will still be guided by EBA and ESMA rules and laws. Importantly, a bank in each part of the European Union must comply with the requirements of its own country, but as the banks have assured us, no law or requirement is conflicting or contradictory.

In addition, according to banks cyber security culture is totally integrated in organisational culture. Based on the fact that "…that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of a group"[178]. which confirms that culture is organized by people. Also researchers in cross-cultural management have highlighted that culture is learned and shared from a group member to another group member. Consequently, without knowledge and the right mechanism to transfer and share it, it is impossible to build a harmonious culture.

Theoretically, we can conclude that cybersecurity culture is not built on a sufficient level, so there is still a problem of individuals not understanding what they can and cannot do.

Despite the rather positive picture, three out of five banks admitted to having some difficulties in interacting with staff at different locations. Therefore, in spite of all the rules and regulations, the human and cultural factor is still a cornerstone and needs to be further explored.

Thanks to the response of an auditor who has worked on several continents and with different cultures, we can confirm that the influence of the cultural factor is quite strong. Furthermore, he pointed out that “different attitudes to risk on the one hand, and personal responsibility or accountability on the other.” If we turn to Erin

[178] (Tylor, 1920)

Meyer's work 'The Cultural Map'[179], where she repeatedly reiterates that despite the human element, every individual is subject to cultural influences. It is not possible to establish good and productive business relationships just by taking the human factor into account. By assessing a person's behaviour, you will be in terms of their culture, so that it can lead to a dead end or a breakdown in the relationship. Knowing that attitudes towards risk come from a cultural background as well as from responsibility mixed with the human factor, we can conclude that this paper is relevant.

[179] (Meyer, 2014)

5. Analyses of findings and discussion

Having studied the academic literature, the work of various academics, software developers, auditors, as well as the regulatory documentation of supervisory bodies, we can conclude that the banking sector must be as secure as possible against any kind of attack. A great number of measures are taken to ensure that the whole sector operates efficiently and smoothly. No specific examples of attacks or break-ins in the Austrian banking sector were found by the author, however, the question remains open.

The survey gave an idea of what an almost perfect cybersecurity should look like, as small gaps were found that need to be corrected.

However, the author sees a discrepancy in the adoption and harmonization of cultures (organisational, cultural, national). Many auditors and researchers say in their reports repeatedly that it is necessary to study the human factor to create a safe space, and this factor is inextricably linked with the cultural framework. Various techniques need to be applied to examine all possible variables to improve cybersecurity. Calvin Nobles[180] ones again confirmed that an improvement of the trainings will not help totally mitigate the risk of human factor as many managers think.

Coffey[181] argues that existing training and education programs are not designed for end-users and may later prove ineffective. Therefore, it is necessary to design these trainings taking into account all possible factors, including both human and cultural.

[180] (NOBLES, 2018)
[181] (Coffey, 2017)

6. Discussion

The cybersecurity is one of the main topics in business environment nowadays and I had little idea how big problem was before I started my research project on computer science. A huge number of academics and analysts from around the world are currently studying the topic from completely different angles. As outlined in the first chapter, the security of systems in general includes not only the technical side, but also the human factor, which has previously been poorly considered. Researchers have begun to pay more attention to the integration of organisational culture and cybersecurity culture.

A study of the literature and the surveys conducted leads to the conclusion that the influence of the human and cultural factor is attracting more and more attention. Based on the fact that despite all the technological advances in the world, people are still the main danger in cybersecurity. Their actions, behaviour and pleasant decisions can determine the future of a company and its reputation. As described in the work of cross-cultural scholars, culture can influence all areas of society, so when an analysis of sources found many potential markers of this influence on cybersecurity, the theory was confirmed. Of course, the human factor also has an impact, but by examining the cultural factor, there is the potential to reduce the overall risk. Studying the impact of different cultures on decision-making and incorporating this into cybersecurity culture, training and simply everyday life is likely to help companies work more effectively.

As has already been mentioned, this paper has certain limitations which could not be overcome. However, it can be a basis for further research in this field. In addition, the limitations include the danger of stereotyping in the analysis of culture and the danger of one's own culture influencing the plausibility of assessing another culture[182].

The methodology has been chosen absolutely correctly, however, the questionnaire can be modified and supplemented to provide more detailed information on cultural influences. It is very important to obtain data from bank employees as well, which will help to gain a deeper understanding of the influence of culture on the decision-making process. The sample size is rather small, but gave a general idea of cybersecurity in the financial sector. Of course, if there is an opportunity to work further

[182] (Tompos, 2015)

on this project, as many auditors and software developers as possible should be involved. Unfortunately, the author realizes that it is not possible to involve the supervisory authorities again for confidentiality reasons.

7. Conclusion.

In every aspect of professional and personal life, an individual may feel influenced by his or her cultural background. Most studies have built on cross-cultural comparisons, but due to the dilettante topic covered in this paper, this has been quite difficult. In addition, as I am an "outsider" to Austrian culture and am not a bank employee, it was not possible to reveal much information. In addition, many important documents that could and could play a critical role in this study are published in German, which also makes full immersion difficult. The EU financial sector is unique in general, and in terms of cybersecurity in particular.

There are supervisory bodies for the entire EU, as well as for each individual country, but they also have an assistant function:

- They prepare a huge amount of documentation in order to protect companies, their customers and partners;
- Interact productively with each other;
- Provide assistance and support to clients, etc.

After attending a webinar "EVENT: Ransomware 2021 Mid-Year Update: New Trends and Expert Insights" where the situation in America was mainly discussed, I can conclude that this mechanism is not well established there.

Furthermore, such a system is necessary not only to maintain a good structure within each organisation, but also for the country and the EU as a whole. With such a system of full inclusion and interaction, supervision bodies demonstrate to other countries that their financial sector is well protected.

Based on the fact that the supervisory and regulatory authorities are constantly conducting various studies, facilitating conferences, helping bank customers, and issuing new documents on cybersecurity, it is safe to say that cybersecurity concerns exist. They try to anticipate all possible risks and dangers that a business may face. Can this introduce constraints and difficulties in business? As I am not an employee of the bank, I cannot answer it.

The author posed two research questions: How the cybersecurity is maintained by Austrian companies of the financial sector / Is there the possible impact of cultural background on the cybersecurity maturity?

The first question was answered quite successfully, this paper gives an insight into the cybersecurity of 5 banks in Austria, of course detailed data was not obtained, but it can be a confirmation that banks take security very seriously.

In answering the second question, the author had not only to analyse the questionnaires but also to compare them with different cultural theories. After examining 5 banks operating in Austria, we were able to find signs of cultural influences on cyber security, but this analysis cannot be considered in-depth. Unfortunately, we were not able to fully conduct cross-cultural research because we did not have access to the internal culture of the organisation. As Anikó Tompos states in his research of the Austrian and Bulgarian cultures[183] "cross-cultural comparative research revealing differences and similarities in norms and values of national cultures, and the manifestations of these orientations in practices and behaviour, helps people from different cultures to understand and successfully deal with the difficulties arising from different views of what is considered good and rational, for example".

In order to build a well-protected system, it is necessary to understand the way each individual part works. It is not possible to set up a system by trying to judge everyone by one criterion. If there are people from different cultures in the organisation, it is necessary to do a cultural analysis and understand the possible primary reactions to different situations in order to develop an effective operating plan.

The underappreciation of human factors in cybersecurity illustrates a gap between theoretical research and organisational practices regarding information security (NSTC, 2016)[184].This development of this research can, in my opinion, help banks to minimise the influence of cultural (and possibly partly human) factors as much as possible.

Although all professionals claim that cybersecurity culture is fully embedded in the organisational culture, there are still cases where security professionals consider the rest of the staff to be 'below' themselves because they do not possess certain arte-

[183] (Tompos, 2015)
[184] (Council, 2018)

facts, values, and assumptions. If this happens, can we say that one culture is embedded in another. There needs to be a more substantive development of the training program and the inclusion of all staff in maintaining cybersecurity.

Crowdstrike reports that there is a visible trend of "big fish" attacks in the financial sector shifting from banks to cryptocurrencies. However, this topic will not be dealt with in this paper, as it is quite extensive and has its own regulatory and legal frameworks. This example has only been given to show how huge the financial market is and also how huge the risk is in any of its sections, especially nowadays when we are slightly moving to the digital environment.

It is not only culture that dictates perceptions and reactions to information, but also human qualities. However, making employees aware of the need for certain measures can alleviate these rough edges. By explaining why a method is necessary, there may be a chance to reduce the human/cultural factor[185]. However, the characteristic of impulsivity can be dictated not only by human factors, but also by culture, as some cultures are a priori impulsive according to the Trompenaars theory.

The financial sector and beyond may want to look more closely at human nature, rather than just the technical side of things, after examining this work. Several recommendations can be highlighted:

1) In order to identify possible security gaps and identify genuine employee reactions, it is not sufficient to conduct surveys in the usual way, as the answers will be those that security requires, but the reality may be different from what is desired[186].

2) Examine employee cultures using all possible theories and tools. For example, the Hofstede team presented a large number of different applications on their website to help simplify and improve the process

3) Do not fall into stereo typicality when analyzing. This can be a basic mistake when ideas about culture and its characteristics are based on stereotypes that were formed quite a long time ago and that differ from scientific studies of cultures or that hyperbolize the cultural characteristics.

[185] (Hadlington, 2017)
[186] (Hadlington, 2017)

4) Do not forget the possible human factor. As can be seen in various works, a person may come from a particular culture and be influenced by it, but sometimes their actions may be dictated by their upbringing, family background, education, the environment that he/she was raised in, work experience and so on[187].

5) Develop trainings with the above requirements in mind, as well as the responsibilities of the employees. In other words, the training should be as close as possible to what the employee does every day and what difficulties he or she may encounter.

6) Trainings should be designed more in a gaming way. This type will help to engage the employee more than the instructed or formal type. “Tell people – and they may forget… show them – they may remember… but involve them and they will understand” (Confucius).

7) Explain in detail and in simple terms how important cybersecurity is and what the consequences might be. As seen in many works, people simply do not understand why they have to comply with security requirements, and some consider them excessive.

8) Do not perceive employees as a threat and try to prevent possible undesirable actions with various measures, including punishment.

9) To have a clear understanding of what information is subject to disclosure and what is not. In support of this, I would like to give you an example. A human resources officer, when drafting a position description for an IT employee, indicated which system the company uses. This information can be very useful to hackers and put the entire company at risk.

In addition, in the course of our work, we have come to the conclusion that it is safe to put the certification on the bank's website. Firstly, it demonstrates to clients and the bank's partner that the bank is secure, and secondly, it can be a guarantee that a "lazy" hacker will not carry out an attack on the bank. However, as the auditor pointed out, there are loopholes in every system, so certification cannot be a guarantee of 100% security. It is much more dangerous not to train and inform your employees.

[187] (Hadlington, 2017)

Also, banks need to find a balance between outsourcing services and in-house services. As the trend shows, many banks are planning to move to cloud storage, which also imposes a huge amount of risk. Perhaps plan B should be considered, if one of the storage facilities is suspended, it should be possible to reconnect the other storage facility.

With a slightly different approach to the human and cultural factor, it is possible to achieve an unexpectedly positive result. The process will be labour and time consuming but will provide an excellent basis for further productive and safe work. The dangers associated with people's reactions will occur all the time. Covid 2019, due to which threats of attacks on people have increased because they are anxious and lost, is not the only possible danger. It is impossible to predict which criminal trends or force majeure circumstances may occur in the future. To be prepared for an ever-changing world, you need to think through all the options you have to protect your company and your business as a whole.

References

“FMA und OeNB testen in einem Planspiel die Reaktionsfähigkeit des österreichischen Bankensektors auf Cyber-Attacken“ [Journal]. - [s.l.] : https://www.fma.gv.at/fma-und-oenb-testen-in-einem-planspiel-die-reaktionsfaehigkeit-des-oesterreichischen-bankensek, 1. July 2019.

A. Reeves P. Delfabbro, and D. Calic Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue [Journal] // SAGE. - January-March 2021. - DOI: 10.1177/21582440211000049.

Alessandro Oltramari Diane Henshel & Mariana Cains, Blaine Hoffman Towards a Human Factors Ontology for Cyber Security [Journal] // STIDS. - 2015.

Alfawaz Salahuddin and Nelson, Karen and Mohannak, Kavoos Information security culture : a behaviour compliance conceptual framework [Journal] // QUT Digital Repository. - Brisbane, Australia : Research Gate, 2010.

Anna Georgiadou Spiros Mouzakitis, Dimitris Askounis Working from home during COVID-19 crisis: a cyber security culture assessment survey [Journal] // Security Journal. - 4. February 2021. - https://doi.org/10.1057/s41284-021-00286-2.

Antipov Andrei Security Awareness Course Design Best Practices [Online] // Infosec. - 1. April 2016. - https://resources.infosecinstitute.com/topic/security-awareness-course-design-best-practices/#:~:text=Besides%2C%20some%20regulations%2C%20such%20as,days%20is%20the%20general%20recommendation.

AON Empower Results Cyber Risk Implications of the Coronavirus Outbreak [Journal]. - 2020.

AON Empower Results Social Engineering Attacks And COVID-19 [Online] // AON Empower Results. - January 2020. - https://www.aon.com/cyber-solutions/thinking/social-engineering-attacks-and-covid-19/.

Areej AlHogail Dr. Abdulrahman Mirza Information Security Culture: A Definition and A Literature Review [Konferenz]. - Saudi Arabia : Research Gate, 2015. - DOI: 10.1109/WCCAIS.2014.6916579.

Ashleigh Wiley Agata McCormac, Dragana Calic More than the individual: Examining the relationship between culture and Information Security Awareness [Journal] // Computers & Security. - Edinburgh, Australia : Elsevier Ltd., 7. October 2019. - 88 (2020) 101640.

Auditors The Institute of Internal THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL [Journal] // IIA Position Paper. - [s.l.] : The Institute of Internal Auditors, January 2013.

Authority European Banking Annual report 2019 [Bericht]. - Luxembourg : Publications Office of the European Union, 2020. - ISBN 978-92-9245-659-7.

BaFin Cybersicherheit eine Herausforderung für Staat und Finanzwirtschaft [Journal] // BaFin Perspektiven. - 2020.

Banach Zbigniew The Dangers of Social Engineering Attacks [Online] // Netsparker. - 10. April 2020. - https://www.netsparker.com/blog/web-security/social-hacking-social-engineering-attacks/#:~:text=Cybercriminals%20can%20use%20a%20wide,victims%20to%20perform%20dangerous%20actions.

Bannister Adam “Remote working during coronavirus pandemic leads to rise in cyber-attacks, say security professionals” [Online] // The Daily Swig. Cybersecurity news and views. - 14. July 2020. - https://portswigger.net/daily-swig/remote-working-during-coronavirus-pandemic-leads-to-rise-in-cyber-attacks-say-security-professionals.

Baraniuk Chris News reports and pop culture continually paint cyber-criminals as cunning and devious hackers, with almost magical computer skills. Is that actually true? [Online] // BBC. - 26. July 2017. - https://www.bbc.com/future/article/20170726-why-most-hackers-arent-sophisticated.

Bischoff Paul Which countries have the worst (and best) cybersecurity? [Online] // Comparitech. - 24. March 2020. - https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

Bös Bernhard Doctoral thesis "Managers’ perceptions of organizational cultures in Austria" [Buch]. - [s.l.] : WU Vienna University of Economics and Business, 2009.

Broadcom Patch Management Life Cycle [Online] // CA CLIENT AUTOMATION - 14.0. - 12. May 2021. - https://techdocs.broadcom.com/us/en/ca-enterprise-software/business-management/clarity-client-automation/14-0/using/dsm-web-console/patch-management/patch-management-life-cycle.html.

Bruce Steve Internal audit: three lines of defence model explained [Online] // ICAS. - 6. November 2017. - https://www.icas.com/professional-resources/audit-and-assurance/internal-audit/internal-audit-three-lines-of-defence-model-explained.

Carnegie Timeline of Cyber Incidents Involving Financial Institutions [Online] // Carnegie Endowment for International Peace. - 2007-2021. - https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide.

Changing minds.org Hall's cultural factors [Online] // Changing minds.org. - http://changingminds.org/explanations/culture/hall_culture.htm.

Chivers Kyle Data backup: Why it’s important plus strategies to protect your information [Online] // Norton. - 25. February 2021. - https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html.

CISCO What is cybersecurity? [Online] // Cisco web-site. - https://www.cisco.com/c/en/us/products/security/what-is-

cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of,or%20interrupting%20normal%20business%20processes..

CISOMAG Austrian Banks well prepared to handle cyber threats: FMA [Online]. - 4. July 2019. - https://cisomag.eccouncil.org/austrian-banks-well-prepared-to-handle-cyber-threats-fma/.

Claire La Fleur Blaine Hoffman, C. Benjamin Gibson, Norbou Buchler Team performance in a series of reional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization [Journal] // Computers & Security. - United States : Elsevier Ltd., 17. February 2021. - 104 (2021) 102229.

Cloudflare What is the cloud? [Online] // Cloudflare. - https://www.cloudflare.com/learning/cloud/what-is-the-cloud/.

Clyde Kroeber Alfred L. andKluckhohn Culture: A critical review of concepts and definitions [Journal] // Peabody Museum of Archaeology & Ethnology. - [s.l.] : Harvard University, 1952.

Coffey J. W. Ameliorating sources of human error in cybersecurity: technological and human-centered approaches. [Konferenz] // The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola (pp. 85-88).. - 2017.

Commvault Grandfather-Father-Son (GFS) Data Retention [Online]. - https://documentation.commvault.com/commvault/v11/article?p=11635.htm.

Council National Science and Technology Networking and Information Technology Research and Development Program. Ensuring Prosperity and National Security. [Online]. - 3. March 2018. - https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.

CrowdStrike Inc. Global Threat Report [Journal] // CrowdStrike, Inc.. - 2021.

Cybersecurity education guides Cyberdefense in the Financial Services Industry: Securing the Vault [Online] // Cybersecurity education guides. - https://www.cybersecurityeducationguides.org/finance/.

Dash Siddhant 5 Biggest Cyber Attacks of 2020 (So Far) [Online] // Security Boulevard. - 8. November 2020. - https://securityboulevard.com/2020/10/5-biggest-cyber-attacks-of-2020-so-far/.

Dashlane The Virus That Saved The World From Nuclear Iran? STUXNET / Prod. Show The Infographics. - 2018 .

Dictionary.com [Online]. - https://www.dictionary.com/browse/software.

Downs Frank Top Cyberattacks of 2020 and How to Build Cyberresiliency [Online] // ISACA. - 6. November 2020. - https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency.

Duo Security Inc. CISCO Phishing. A mdern Guide to an Age-Old Problem [Journal] // Duo Security Inc..

EBA Cyber-attack on the European Banking Authority [Online] // The European Banking Authority. - 07. March 2021. - https://www.eba.europa.eu/cyber-attack-european-banking-authority.

EBA EBA at a glance [Online] // The European Banking Authority. - https://www.eba.europa.eu/about-us/eba-at-a-glance.

EBA/GL/2014/13 Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) [Journal]. - 19. December 2014.

EBA/GL/2017/10 Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) [Journal]. - 27. July 2017.

EBA/GL/2017/11 Guidelines on internal governance [Journal]. - 21. 03 2018.

EBA/GL/2019/02 Final Report on EBA Guidelines on outsourcing arrangements [Artikel]. - 25. February 2019.

EBA/GL/2019/04 FINAL REPORT. EBA Guidelines on ICT and security risk management [Journal]. - 29. November 2019.

EBA-Op-2019-06 Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 [Journal]. - 21. June 2019.

ESMA ESMA IN BRIEF [Online] // The European Securities and Markets Authority. - https://www.esma.europa.eu/about-esma/esma-in-brief.

ESMA Guidelines on outsourcing to cloud service providers [Artikel] // Final Report. .

ESMA JC 2019 25 // Joint Advice of the European Supervisory Authorities To the European Commission on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sec. - April 10, 2019.

ESMA JC 2019 26 // Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector. - 10. April 2019.

EWALD NOWOTNY Governor of the Austrian National Bank speech at the conference Supervisors and Auditors Building a Constructive Relationship [Konferenz]. - Vienna : [s.n.], 28 Stptember 2015.

Expert Program management Trompenaars Cultural Dimensions – The 7 Dimensions of Culture [Online]. - https://expertprogrammanagement.com/2017/10/trompenaars-cultural-dimensions/.

FMA Financial Market Supervision in Austria [Online] // The Financial Market Authority. - https://www.fma.gv.at/en/financial-market-supervision-in-austria/.

FMA FMA and OeNB test the Austrian banking sector’s ability to react to cyber attacks [Online] // The Austrian Financial Market Authority. - 01. July 2019. - https://www.fma.gv.at/en/fma-and-oenb-test-the-austrian-banking-sectors-ability-to-react-to-cyber-attacks/.

FMA Let's talk about money [Online]. - 20. January 2021. - https://redenwiruebergeld.fma.gv.at/en/beware-of-financial-scams/.

FMA Structure of the Austrian Financial Sector [Online] // Federal ministery Republic of Austria. - https://www.bmf.gv.at/en/topics/financial-sector/structure-of-the-austrian-financial-sector.html.

Fons Trompenaars Charles Hampden-Turner Riding the Waves of Culture: Understanding Diversity in Global Business [Buch]. - [s.l.] : Nicholas Brealey Publishing, 2011. - Third edition. - ISBN: 978-1-90483-838-8.

Fruhlinger Josh What is phishing? How this cyber attack works and how to prevent it [Online] // CSO. - 4. September 2020. - https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.

Gammelin Kai Lernende Risiko - und Wissenorganisation [Journal] // Diebank. - July 2016. - S. pp 42 - 45.

GDPR.eu Complete guide to GDPR compliance [Online] // GDPR.eu. - Proton Technologies AG, 2021. - https://gdpr.eu/.

Gerhard Fink Marcus Kölling, Anne-Katrin Neyer The cultural standard method [Journal] // EI Working Papers Nr. 62. - Vienna, Austria : [s.n.], March 2005.

Gez Doron Top 5 Cyber Threats Facing Banks in 2020 [Online] // Hub Security. - 20. January 2020. - https://hubsecurity.io/top-5-cyber-threats-facing-banks/.

Hadlington Lee Human factors in cybersecurity; examining the link between Internat addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours [Journal] // Heliyon 3. - [s.l.] : Elsevier, 29. June 2017. - e00346.

Handy Backup Grandfather Father Son Backup Scheme [Online]. - https://www.handybackup.net/grandfather-father-son-backup.shtml.

HELMUT DORNMAYR MARLIS RECHBERGER Demand for/Lack of Skilled Labour in Austria in 2020 [Journal] // ibw research brief. - December 2020. - Issue No. 108. - ISSN 2071-2391.

Herath T., Rao,H.R. Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. [Journal]. - [s.l.] : Eur.J.Inf.Syst.18(2), 2009b.. - S. 106–125.

Hofstede Geert Culture’s Consequences: International Differences in Work-related Values [Journal]. - Newbury Park, CA : Sage Publications, 1980.

Hofstede Insights COUNTRY COMPARISON [Online] // Hofstede Insights. - https://www.hofstede-insights.com/country-comparison/austria,russia/.

Iñaki Aldasoro Leonardo Gambacorta, Paolo Giudici, Thomas Leach BIS Working Papers No 840 Operational and cyber risks in the financial sector [Journal] // Bank for intrenational settlement / Hrsg. Department Monetary and Economic. - February 2020.

Inshakova Olga “Three-quarters of Russian banks are vulnerable to cyberat-tacks” [Online] // International Forum. Security and Safety Technologies. - 11. July 2019. - https://eng.tbforum.ru/blog/three-quarters-of-russian-banks-are-vulnerable-to-cyberattacks.

Isabella Arndorfer Andrea Minto Occasional Paper No 11. The “four lines of defence model” for financial institutions [Journal] // Financial Stability Institute. - [s.l.] : Bank for International Settlement, December 2015. - ISSN 1020-9999 (online).

ISAE 3402 Implementation [Journal]. - [s.l.] : ISAE3402.CO.UK, RISKLANE LTD.

ISAE 3402 INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS (ISAE) 3402. [Journal]. - [s.l.] : ASSURANCE REPORTS ON CONTROLS AT A SERVICE ORGANIZATION, 15. June 2011.

ISO/IES 27001 Information technology - Security techniques - Information security management systems - Requirements. - 2005. - SN ISO/IEC 27001:2013 en.

ISO/IES 27002 Information technology — Security techniques — Code of practice for information security controls [Journal]. - 2013-10-01.

Jenitha John Mark Carawan, Greg Grocholski, Trygve Sørlie, Shannon Urban, Beili Wong, Charlie Wright Three Lines of Defense [Journal] // IIA EXPOSURE DOCUMENT. - [s.l.] : The Institute of Internal Auditors, June 2019.

Johan van Grieken Bert Truyman Managing Risk from Every Direction. Take control of third-party risk with third-party assurance reporting [Journal] // Deloitte. - Belgium : [s.n.], March 2018.

Judd Caplain Charles A. Jacco Key cyber risks for banks during COVID-19 [Online] // KPMG. - 2020-2021. - https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html.

Kardonup Lizzie “The 6 Types Of Cyber Attacks To Protect Against In 2019” [Online] // Pagely. - 20. November 2019. - https://pagely.com/blog/cyber-attacks-in-2018/ .

Kaspersky Lab The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within [Online] // Kaspersky Daily. - 2017. - https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

Kaspersky Lab Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns [Online] // Kaspersky Lab. - 2019-2020. - https://www.kaspersky.com/blog/understanding-security-of-the-cloud/.

Kaspersky Lab What is Cyber Security? [Online]. - 2020. - https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

Kaspersky Lab What is Social Engineering? [Online]. - https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering.

Kathryn Marie Parsons Elise Young, Marcus Antanas Butavicius, Agata McCormac,Malcolm Robert Pattinson, Cate Jerram The Influence of Organizational Information Security Culture on Information Security Decision Making [Journal] // Journal of Cognitive Engineering and Decision Making. - [s.l.] : Human Factors and Ergonomics Society, June 2015. - N. 3 : Bd. Vol. 9. - S. pp. 117-129. - DOI: 10.1177/1555343415575152.

KENTON WILL Risk Management in Finance [Online] // Investopedia. - 1. March 2021. - https://www.investopedia.com/terms/r/riskmanagement.asp#:~:text=Key%20Takeaways-,Risk%20management%20is%20the%20process%20of%20identification%2C%20analysis%2C%20and%20acceptance,return%20in%20the%20investment%20world.&text=Alpha%20is%20a%20measure%20of,ar.

Kevin D. Mitnick William L. Simon The Art of Deception [Buch]. - Indianapolis, Indiana : Wiley Publishing, Inc., 2002. - ISBN: 978-0-7645-4280-0.

Kevin D. Mitnick William L. Simon The Art of Intrusion [Buch]. - Indianapolis, Indiana : Wiley Publishing Inc., 2006. - ISBN 13: 978-0-471-78266-7, ISBN 10: 0-471-78266-1 .

Khatri Prem “The importance of cyber security in banking” [Online]. - 25. September 2019. - https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/.

Kill Greg When to Update and Replace Your Company’s Computers [Online] // Integracon technologies. - 20. June 2017. - https://integracon.com/when-to-update-and-replace-your-companys-computers/#:~:text=Keep%20Your%20Tech%20in%20Check,every%205%20years%20or%20so..

Koubek Dr. Anni ISO 9001 [Online] // Quality Austria. - 2019. - https://www.qualityaustria.com/produktgruppen/qualitaet/iso-9001/.

Ksenia Keplinger Birgit Feldbauer-Durstmueller, Christine Mitter MANAGEMENT ACCOUNTING PRACTICES IN A MULTICULTURAL ENVIRONMENT: EVIDENCE FROM AUSTRIA, RUSSIA AND THE US [Journal] // SSRN Electronic Journal FROM AUSTRIA, RUSSIA AND THE US. - Austria : [s.n.], January 2012. - DOI: 10.2139/ssrn.2009635.

Lack Ben What is the ISO 27002 Standard? [Online] // Reciprocity. - 6. August 2019. - https://reciprocitylabs.com/resources/what-is-the-iso-27002-standard/.

Lehrerfortbildungsservers Baden-Württemberg Edward T. Hall. Four distinguishing features [Online] // Lehrerfortbildungsservers Baden-Württemberg. - https://lehrerfortbildung-bw.de/u_berufsbezogen/wahl/fb1/kompcult/culpat/hall.htm.

LINCOLN FREREJACQUE AND Financial supervisors & external auditors: partnering for financial stability // Centre for Financial Reporting Reform (CFRR) / Redakt. Bank Austrian National. - Vienna : [s.n.], 28. September 2015.

Liu Shanhong Employee cyber security awareness training frequency in organizations in the United States as of 2018 [Online] // Statista. - 1. April 2020. - https://www.statista.com/statistics/949179/united-states-training-frequency-security-awareness/.

Mag. Emilia Nemlig Mag. Martin Konrad Official letter about Internal Revision [Bericht]. - Vienna : FMA.

Maijoor Steven Ref: FinTech Action Plan - ICT / cybersecurity topics and cloud outsourcing [Bericht]. - 10 April 2019. - ESMA50-164-2193.

MalwareBytes Enduring from home: COVID-19's impact on business security (final report) [Journal]. - USA : [s.n.], 2020.

MalwareBytes Lab RemoteSec: achieving on-prem security levels with cloud-based remote teams [Online]. - 13. March 2020. - https://blog.malwarebytes.com/business-2/2020/03/remotesec-achieving-on-prem-security-levels-with-cloud-based-remote-teams/.

MalwareBytes Labs SMB cybersecurity posture weakened by COVID-19, Labs report finds [Online]. - 8. September 2020. - https://blog.malwarebytes.com/reports/2020/09/smb-cybersecurity-posture-weakened-by-covid-19/.

Management Study HQ Edgar Schein's Model of Organizational Culture [Online] // Management Study HQ. - https://www.managementstudyhq.com/edgar-schein-model-theory.html.

McAfee Labs Threat report [Journal]. - [s.l.] : McAfee, April 2021.

Meyer Erin The Culture Map [Buch]. - New York : Public Affairs, 2014. - ISBN 978-1-61039-276-1 (INTL PB), ISBN 978-1-61039-671-4 (INTL EB).

MIESSLER DANIEL The Difference Between Red, Blue, and Purple Teams [Online]. - 4. April 2020. - https://danielmiessler.com/study/red-blue-purple-teams/.

N. Gcaza R. von Solms and J. van Vuuren An Ontology for a National Cyber-Security Culture Envirinment [Journal]. - South Africa : Research Gate, 2019.

Nelson M. Alnatheer and K. A Proposed Framework for Understanding In-formation Security Culture and Practices in the Saudi Context [Konferenz] // Proceedings of the 7th Australian Information Security Management Conference. - December 2009. - S. pp. 6-17.

NetApp What Is Backup and Recovery? [Online] // NetApp. - https://www.netapp.com/data-protection/backup-recovery/what-is-backup-recovery/#:~:text=The%20purpose%20of%20the%20backup,or%20accidental%20deletion%20of%20data.

Next Business Academy LinkedIn usage data and statistics for Austria - August 2019 [Online] // Next Business Academy. - 28. August 2019. - https://nextbusinessacademy.nl/en/2019/08/28/linkedin-statistics-and-data-for-austria-2019/.

Nicholson F. THREE LINES OF DEFENSE: REPORT ON THE PUBLIC EXPOSURE FINDINGS JUNE-SEPTEMBER 2019 [Journal].

NIST Glossary [Online] // (National Institution of Standards and Technology). - https://csrc.nist.gov/glossary.

NOBLES Calvin Botching Human Factors in Cybersecurity in Business Organizations [Journal] // Sciendo / Hrsg. pp.71-88. - USA : HOLISTICA, 2018. - Issue 3 : Bd. Vol 9. - DOI: 10.2478/hjbpa-2018-0024.

Norrestad F. Number of banks in the Netherlands 2008-2019 [Online] // Statista. - 16. November 2020. - https://www.statista.com/statistics/586998/total-number-of-banks-in-the-netherlands/.

Norrestad F. Total assets of German banks 2000-2019 [Online] // Statista. - 25. November 2020. - https://www.statista.com/statistics/273085/total-assets-of-german-banks-since-2003/.

Norrestad F. Total number of banks in Switzerland 2011-2019 [Online] // Statista. - 9. November 2020. - https://www.statista.com/statistics/646515/total-number-of-banks-switzerland-europe/#statisticContainer.

ÖNB Number of banks [Online] // ÖNB. - 2021. - https://www.oenb.at/en/Statistics/Standardized-Tables/Financial-Institutions/Banks/Number-of-Banks.html.

Paul Dowland Steven Furnell Advances in Communications, Computing, Networks and Security, Volume 6 [Buch] / Hrsg. School of Com-puting Communications and Electronics. - [s.l.] : University of Plymouth, 2009. - ISBN: 978-1-84102-258-1.

Prof. Flemming Ruud PhD, CPA (Norway) Reflections on the Three Lines of Defence [Konferenz] // Internal Audit Service, European Commission. - Brussels : [s.n.], November 2019.

PwC A leadership agenda to take on tomorrow [Journal] // 24th Annual Global CEO Survey. - [s.l.] : PwC, 2021.

Randall J. Boyle Raymond R. Panko Corporate Computer Security [Buch]. - USA : Pearson Education, 2015. - fourth edition. - ISBN-10: 1-292-06045-X, ISBN-13: 987-1-292-06045-3.

RAVELIN INSIGHTS PSD2 and strong customer authentication [Online] // RAVELIN. - 2019. - https://www.ravelin.com/insights/ultimate-guide-psd2-strong-customer-authentication?utm_term=payment%20services%20directive%202&utm_campaign=PSPs+-+Europe&utm_source=adwords&utm_medium=ppc&hsa_ver=3&hsa_grp=54439236202&hsa_kw=payment%20services%20directiv.

Risk.net, supported by Baker McKenzie Top 10 op risks 2020 [Journal]. - March 2020.

Salacuse Jeswald W. “The top ten ways that culture can affect international negotiations” [Online] // IVEY business journal. - March/April 2005. - https://iveybusinessjournal.com/publication/the-top-ten-ways-that-culture-can-affect-international-negotiations/.

SANDERS DAVID Top 50 Safest Banks In Europe 2020 [Online] // Global Finance. - 23. November 2020. - https://www.gfmag.com/magazine/november-2020/2020-50-safest-banks-europe.

Schroll-Machl Alexander Thomas / Eva-Ulrike Kinast /Sylvia Handbook of Intercultural Communication and Cooperation [Buch]. - Göttingen : Vandenhoeck & Ruprecht GmbH & Co. KG, 2010. - 2nd Revised Edition. - ISBN Print: 978-3-525-40327-3 — ISBN E-Book: 978-3-647-40327-4.

Schultz Eva Ursachen für IT-Security-Vorfälle in KMU in Österreich 2020 [Online] // Statista. - 21. February 2020.

Security RSI IT SECURITY FRAMEWORKS: WHAT YOU NEED TO KNOW [Online]. - 3. January 2019. - https://blog.rsisecurity.com/it-security-frameworks-what-you-need-to-know/..

service Moody's Investors Government of Austria – Aa1 Stable [Journal]. - 17. September 2019.

Smith John Your Cultural Adaptability Profile (CAP) [Journal] // Hofstede Insights. - 21. September 2020.

Snedaker Susan Understanding security risk management: Recovery time requirements [Online] // TechTarget. - 30. August 2007. - https://searchitchannel.techtarget.com/feature/Understanding-security-risk-management-Recovery-time-requirements.

Spadafora Anthony Organisations waste resources storing useless IT hardware [Online] // Techradar. - 24. January 2019. - https://www.techradar.com/uk/news/organisations-waste-resources-storing-useless-it-hardware.

Statcounter Social Media Stats Austria [Online] // Statcounter. - May 2020-2021. - https://gs.statcounter.com/social-media-stats/all/austria.

Storkey Ian Operational Risk Management and Business Continuity Planning for Modern State Treasuries [Bericht] / Fiscal Affairs Department ; INTERNATIONAL MONETARY FUND. - November 2011. - H12, H60, H63, H83.

Stoy Dan Hackers are Lazy – Why Are You Making Life Easy for Them? [Online] // Corporate Business Systems, Ltd.. - 1. August 2018. - https://www.coordinated.com/blog/hackers-are-lazy-why-are-you-making-life-easy-for-them.

Supervision Basel Committee on Banking Cyber-resilience: Range of practices [Journal] // Bank for International settlement. - December 2018. - ISBN 978-92-9259-228-8.

Supervision Basel Committee on Banking Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches [Journal] // Bank for international settlements. - June 2011.

Susan Lund James Manyika, Jonathan Woetzel, Edward Barriball, Mekala Krishnan, Knut Alicke, Michael Birshan, Katy George, Sven Smit, Daniel Swan, Kyle Hutzler Risk, resilience, and rebalancing in global value chains [Online] // McKinsey and Company. - 6. August 2020. - https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains.

Symanovich Steve 5 reasons why general software updates and patches are important [Online] // NortonLifeLock. - 23. January 2021. - https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html#:~:text=Software%20updates%20do%20a%20lot%20of%20things&text=These%20might%20include%20repairing%20security,is%20running%20the%20latest%20version..

Tankovska H. Leading countries based on LinkedIn audience size as of January 2021 [Online] // Statista. - 10. February 2021. - https://www.statista.com/statistics/272783/linkedins-membership-worldwide-by-country/.

TechTarget Contributor ISO 27001 [Online] // TechTarget. - September 2009. - https://whatis.techtarget.com/definition/ISO-27001.

Thomas Schlienger Stephanie Teufel INFORMATION SECURITY CULTURE. The Socio-Cultural Dimension in Information Security Management [Journal] // iimt - international institute o/management in telecommunications. - University of Fribourg (CH) : [s.n.], 2002. - 10.1007/978-0-387-35586-3_46.

Tompos Anikó Austrian and Hungarian values and norms in cross-cultural management research [Journal] // Impresa Progetto. - 2015. - n. 3 - 2015. - ISSN 1824-3576.

TRANSLATIONS DAY The Relationship between Language and Culture Defined [Online]. - 11. May 2018. - https://www.daytranslations.com/blog/language-and-culture/.

Tylor E. B. Primitive Culture. Researches into the development of mythology, philosophy, religion, language, art and custom [Buch]. - London : John Murray, 1920. - 4th edition.

Upwork (UPWK) Third Annual “Future Workforce Report” Sheds Light on How Younger Generations are Reshaping the Future of Work [Online]. - 5. March 2019. - https://www.upwork.com/press/releases/third-annual-future-workforce-report.

Van Niekerk J.F. & Von Solms, R. Information-security culture: A management perspective. [Journal] // Computers & Security. - 2010. - 29. - S. pp.476–486.

Veiga Dr Adéle Da A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument [Konferenz] // SAI Computing Conference 2016, London, UK. - South Africa : [s.n.], July 13-15, 2016. - S. pp 1006-1015. - 978-1-4673-8460-5.

VMware Inc. Global Threat Report. Extended enterprise under threat [Journal]. - June 2020.

WRIGHT JORDAN The trouble with phishing [Journal] // Duo Security, Inc.. - 2016 .

Appendix

List of Appendixes

Appendix 1. Banks customers‘ survey

1. Gender

			Response Percent	Response Total
1	Male		38.46%	20
2	Female		61.54%	32
3	Intersex		0.00%	0

Statistics										
	Minimum	1	Mean	1.62	Std. Deviation	0.49	Satisfaction Rate	30.77	answered	52
	Maximum	2	Variance	0.24	Std. Error	0.07			skipped	0

2. Age

			Respon-se Per-cent	Respon-se Total
1	younger than 20		0.00%	0
2	20-30		31.37%	16
3	30-40		45.10%	23
4	40-50		11.76%	6
5	50-60		11.76%	6
6	older than 60		0.00%	0

Statis-tics										
	Mini-mum	2	Mean	3.04	Std. Devia-tion	0.95	Satisfaction Rate	40.78	answered	51
	Maxi-mum	5	Vari-ance	0.9	Std. Error	0.13			skipped	1

3. Which payment method do you prefer?

		Response Percent	Response Total
1	Cash	1.92%	1
2	Card	69.23%	36
3	Both	28.85%	15

Statistics								
	Minimum	1	Mean	2.27	Std. Deviation	0.48	Satisfaction Rate	63.46
	Maximum	3	Variance	0.24	Std. Error	0.07		

answered	52
skipped	0

4. How many banks do you have accounts in?

		Response Percent	Response Total
1	One bank	28.85%	15
2	Two banks	44.23%	23
3	More than two	26.92%	14

Statistics								
	Minimum	1	Mean	1.98	Std. Deviation	0.75	Satisfaction Rate	49.04
	Maximum	3	Variance	0.56	Std. Error	0.1		

answered	52
skipped	0

5. Do you have mobile banking apps installed?

		Response Percent	Response Total
1	Yes	94.23%	49
2	No	5.77%	3

Statistics								
	Minimum	1	Mean	1.06	Std. Deviation	0.23	Satisfaction Rate	5.77
	Maximum	2	Variance	0.05	Std. Error	0.03		

answered	52
skipped	0

6. Do you need a password to access your app?

		Response Percent	Response Total
1	Yes	82.35%	42
2	No	17.65%	9

Statistics								
	Minimum	1	Mean	1.18	Std. Deviation	0.38	Satisfaction Rate	17.65
	Maximum	2	Variance	0.15	Std. Error	0.05		

answered	51
skipped	1

7. Does your app require fingerprint or facial recognition to access it?

		Response Percent	Response Total
1	Yes	60.78%	31
2	No	29.41%	15

7. Does your app require fingerprint or facial recognition to access it?

			Response Percent	Response Total
3	Other (please specify):		9.80%	5

Statistics									
	Minimum	1	Mean	1.49	Std. Deviation	0.67	Satisfaction Rate	24.51	answered 51
	Maximum	3	Variance	0.45	Std. Error	0.09			skipped 1

Other (please specify): (5)

1	04/05/2021 15:02 PM ID: 165762402	Second authentication sent by sms
2	04/05/2021 16:05 PM ID: 165770394	MFA
3	04/05/2021 18:38 PM ID: 165783881	Optional
4	05/05/2021 19:47 PM ID: 165882086	it doesn't require, but I chose this option voluntarily
5	06/05/2021 23:04 PM ID: 166007635	It doesn't require but i always opt to use it

8. Do you have to notify the bank in any way when you change your phone (device or number)?

			Response Percent	Response Total
1	Yes		51.92%	27

8. Do you have to notify the bank in any way when you change your phone (device or number)?

		Response Percent	Response Total
2	No	15.38%	8
3	I don't know	32.69%	17

Statistics								
	Minimum	1	Mean	1.81	Std. Deviation	0.9	Satisfaction Rate	40.38
	Maximum	3	Variance	0.81	Std. Error	0.12		

answered	52	
skipped	0	

Comments: (4)

1	04/05/2021 15:53 PM ID: 165768749	I only have the two factor app my bank requires for internet banking. No app banking. No where to say this so putting this info here.
2	04/05/2021 16:05 PM ID: 165770340	Just vor the VISA Card
3	05/05/2021 09:53 AM ID: 165812888	Only the number, I do not need to notify but I have to make sure to change it in my profile.
4	06/05/2021 08:07 AM ID: 165902576	I'd do it anyways

9. Does your bank use any other type of authentication (SMS with password, special question, etc.)?

		Response Percent	Response Total
1	Yes	63.46%	33
2	No	36.54%	19

9. Does your bank use any other type of authentication (SMS with password, special question, etc.)?

									Response Percent	Response Total
Statistics	Minimum	1	Mean	1.37	Std. Deviation	0.48	Satisfaction Rate	36.54	answered	52
	Maximum	2	Variance	0.23	Std. Error	0.07			skipped	0

10. If yes, which ones?

		Response Percent	Response Total
1	Open-Ended Question	100.00%	33

1	04/05/2021 10:28 AM ID: 165731375	Sms
2	04/05/2021 11:21 AM ID: 165737401	It uses another app to verify the transactions or also sms.
3	04/05/2021 12:37 PM ID: 165746323	Mobile TAN
4	04/05/2021 13:07 PM ID: 165749756	Identification App
5	04/05/2021 13:40 PM ID: 165753281	Verification through banking app on mobile
6	04/05/2021 13:49 PM ID: 165754263	SMS
7	04/05/2021 14:18 PM ID: 165757522	It remembers the Browser I use for Online Banking and from time to time I have to confirm the browser using TAN

10. If yes, which ones?				
			Response Percent	Response Total
8	04/05/2021 15:02 PM ID: 165762402	Sms with password		
9	04/05/2021 15:28 PM ID: 165765624	SMS with password		
10	04/05/2021 15:47 PM ID: 165768020	Special word, password & a special number		
11	04/05/2021 15:53 PM ID: 165768749	Mobile tan		
12	04/05/2021 16:05 PM ID: 165770375	S-Identity (seperate authentication app)		
13	04/05/2021 16:05 PM ID: 165770394	SMS with PIN; MFA		
14	04/05/2021 18:38 PM ID: 165783881	Pin, Username, tan		
15	04/05/2021 18:51 PM ID: 165784619	sms, password		
16	04/05/2021 19:29 PM ID: 165786907	SMS with password; notification to write code		
17	05/05/2021 07:55 AM ID: 165802685	SMS		
18	05/05/2021 08:52 AM ID: 165806791	SMS w/ passwd		
19	05/05/2021 09:26 AM ID: 165810153	Special questions. Authenticator app.		
20	05/05/2021 09:53 AM ID: 165812888	ATC number		

10. If yes, which ones?				
			Response Percent	Response Total
21	05/05/2021 13:55 PM ID: 165844337	SMS, TAN		
22	05/05/2021 16:13 PM ID: 165861146	SMS		
23	05/05/2021 18:01 PM ID: 165872379	yes 2FA when using a browser or new device		
24	05/05/2021 19:47 PM ID: 165882086	not sure, because I don't use it. But I think SMS for sure.		
25	05/05/2021 22:47 PM ID: 165892533	Password and if I want more security I can use an application that my bank created to login in my mobile bank.		
26	06/05/2021 06:18 AM ID: 165898690	Special questions		
27	06/05/2021 07:34 AM ID: 165900920	SMS code		
28	06/05/2021 08:23 AM ID: 165903579	SMS with password and notification		
29	06/05/2021 10:52 AM ID: 165919318	Special question		
30	06/05/2021 14:43 PM ID: 165956513	OTP ONE TIME PASSWORD BY SMS		
31	06/05/2021 20:47 PM ID: 165999431	code sending by sms or email		
32	06/05/2021 23:04 PM ID: 166007635	All , but i use 2 factor for these types of accounts always. So I utilize an authentication app as well for code generation		
33	07/05/2021 22:15 PM ID: 166081943	Push-message		

10. If yes, which ones?

	Response Percent	Response Total
	answered	33
	skipped	19

11. When carrying out a transaction, does your bank ask

			Response Percent	Response Total
1	Confirmation with password		50.00%	26
2	Confirmation with finger print or facial recognition		50.00%	26
3	No extra confirmation		7.69%	4
4	Other (please specify):		23.08%	12

Statistics						
	Minimum	1	Mean	2.03	Std. Deviation	1.07
	Maximum	4	Variance	1.15	Std. Error	0.13

answered	52
skipped	0

Other (please specify): (12)

1	04/05/2021 11:21 AM ID: 165737401	Verification in another app with another password
2	04/05/2021 13:07 PM ID: 165749756	Confirmation via Identification App and SMS
3	04/05/2021 13:40 PM ID: 165753281	Verification through banking app on mobile
4	04/05/2021 14:18 PM ID: 165757522	It sends me an SMS with TAN

11. When carrying out a transaction, does your bank ask

			Response Percent	Response Total
5	04/05/2021 15:47 PM ID: 165768020	My English bank is finger print. My Austrian bank has a separate app for signing		
6	04/05/2021 15:53 PM ID: 165768749	Mobile tan		
7	04/05/2021 16:05 PM ID: 165770394	SMS with PIN		
8	04/05/2021 18:44 PM ID: 165784178	QR code / photo tan		
9	05/05/2021 09:26 AM ID: 165810153	Confirmation with authenticator app or sms		
10	05/05/2021 13:55 PM ID: 165844337	TAN		
11	05/05/2021 22:47 PM ID: 165892533	Extra confirmation from another application		
12	06/05/2021 11:25 AM ID: 165924326	Using a separate app S Identity		

12. How often do you check your account or make transactions in public places (public transport, shops, university, etc.)

			Respon-se Per-cent	Respon-se Total
1	Always		15.38%	8
2	Often		32.69%	17
3	Only if it is necessary		32.69%	17

12. How often do you check your account or make transactions in public places (public transport, shops, university, etc.)

		Response Percent	Response Total
4	Never	19.23%	10

Statistics									
	Minimum	1	Mean	2.56	Std. Deviation	0.97	Satisfaction Rate	51.92	answered 52
	Maximum	4	Variance	0.94	Std. Error	0.13			skipped 0

13. Have you read all the precautions that the bank publishes on its website to protect customers from all sorts of scams?

		Response Percent	Response Total
1	Yes	23.08%	12
2	No	65.38%	34
3	Not interested	1.92%	1
4	I get this information from other sources	9.62%	5

Statistics									
	Minimum	1	Mean	1.98	Std. Deviation	0.8	Satisfaction Rate	32.69	answered 52
	Maximum	4	Variance	0.63	Std. Error	0.11			skipped 0

14. Are you satisfied with your bank's service, including the apps?

			Response Percent	Response Total
1	Very satisfied		30.77%	16
2	Satisfied		51.92%	27
3	Neutral		15.38%	8
4	Dissatisfied		1.92%	1
5	Very dissatisfied		0.00%	0

Statistics									
	Minimum	1	Mean	1.88	Std. Deviation	0.72	Satisfaction Rate	22.12	answered 52
	Maximum	4	Variance	0.53	Std. Error	0.1			skipped 0

15. What do you think should be improved in banking applications? In this question, please do NOT specify your bank or hint at your bank.

		Response Percent	Response Total
1	Open-Ended Question	100.00%	30

1	04/05/2021 11:21 AM ID: 165737401	I think the app is too complicated and the design is not very good. It's also a little annoying that saving or presenting transactions is complicated.
2	04/05/2021 12:37 PM ID: 165746323	Can be made more user friendly. Make it more ""Single click"".
3	04/05/2021 13:07 PM ID: 165749756	One bank has a good app an website, the other bank has an ugly old style app and website, confirmation via sms feels old.
4	04/05/2021 13:33 PM ID: 165752557	Love my app. I pay with my phone, for years!!
5	04/05/2021 13:40 PM ID: 165753281	-

15. What do you think should be improved in banking applications? In this question, please do NOT specify your bank or hint at your bank.			Response Percent	Response Total
6	04/05/2021 13:49 PM ID: 165754263	I think my bank does an okay job. I don't know what i would do differently		
7	04/05/2021 14:18 PM ID: 165757522	I dont use mobile applications, since I dont trust them (have no particular reason though). Secondly - what if I lose my phone? I do my transactions from a computer at home.		
8	04/05/2021 14:52 PM ID: 165761371	Push notifications immediately after every transaction		
9	04/05/2021 15:02 PM ID: 165762402	Option to select the language		
10	04/05/2021 15:47 PM ID: 165768020	N/A		
11	04/05/2021 16:05 PM ID: 165770340	It should be easier for people who have internet but no smartphone.		
12	04/05/2021 16:39 PM ID: 165774127	To be able to use mobile banking app and do the transaction on same device		
13	04/05/2021 18:38 PM ID: 165783881	User experience!		
14	04/05/2021 18:44 PM ID: 165784178	To be able to do the same transactions that are possible to do on a computer		
15	04/05/2021 19:29 PM ID: 165786907	Feeling of security: not always I feel safe online to use the app. Possibilities: not possibilities are available in the app and you would need to log in in the website		
16	04/05/2021 23:40 PM ID: 165797777	More choices of how monthly expenditure can be viewed. The overview can be confusing.		
17	04/05/2021 23:59 PM ID: 165798005	Multilingual options for foreigners in the app and in the communications.		

15. What do you think should be improved in banking applications? In this question, please do NOT specify your bank or hint at your bank.

			Response Percent	Response Total
18	05/05/2021 07:55 AM ID: 165802685	I actually like my banking app. So nothing.		
19	05/05/2021 09:26 AM ID: 165810153	Fully homomorphic encryption to protect personal data.		
20	05/05/2021 09:53 AM ID: 165812888	nothing		
21	05/05/2021 18:23 PM ID: 165874447	Faster transaction between different banks		
22	05/05/2021 22:47 PM ID: 165892533	I wouldn't change anything for the moment, I'm satisfied with my banking application.		
23	06/05/2021 07:34 AM ID: 165900920	Popularize the QR code payment		
24	06/05/2021 08:07 AM ID: 165902576	Lack of payments categorisation in the mobile app. OCR improvement would be an advantage.		
25	06/05/2021 08:23 AM ID: 165903579	In some of the apps, for example Bank Austria the app is not logical.		
26	06/05/2021 10:52 AM ID: 165919318	payment for all services, without exception		
27	06/05/2021 14:43 PM ID: 165956513	Better rewards for customers and cashback		
28	06/05/2021 20:47 PM ID: 165999431	Voice recognition, facial or do fingerprint		
29	06/05/2021 23:04 PM ID: 166007635	Budgeting is something they always have.. But it's always limited. And easier and quick ways of categorizing your transactions.		
30	07/05/2021 22:15 PM ID: 166081943	I like the app from my bank		

15. What do you think should be improved in banking applications? In this question, please do NOT specify your bank or hint at your bank.		
	Response Percent	**Response Total**
	answered	30
	skipped	22

Appendix 2. The Questionnaire for banks

Master's thesis: Alisa Demidova

"How cyber security is maintained in Austrian companies."

International management and leadership

FH Vorarlberg, Dornbirn, Austria.

Dear Sir/ Madam,

I'm the student of FH Vorarlberg, Master's program "International management and leadership" and conducting the research of maintain cybersecurity in financial sphere. I have chosen this sphere of business because it is considered to be one of the most vulnerable spheres in terms of cybersecurity. Banks have to think through the details of how to protect their clientele at all levels.

The main focus of work is cultural background aspect of maintain cybersecurity. I would like to explore how cybersecurity is done in financial sphere; however, I will not address "prohibited" or confidential topics.

All materials and research will be used exclusively as part of the scientific work. The paper will not name the company or the names of the participants in the study. No personal information about participants will be disclosed. All received information will be analyzed only by me. If participants indicate their willingness to avoid their results being made publicly, I will do it immediately.

Questionnaire:

The organization and its context

- What of the legal and regulatory requirements are the most complicated to follow and why?

- Are there policies (p) and controls (c) in place to provide management direction in view of:

mobile device, USB flash cards and teleworking	Choose the correct option
user access to the network controlled	Choose the correct option
rights for the access to the specific information	Choose the correct option
physical access to the building (duty and off-duty hours/days)	Choose the correct option
security of information transferred within or outside of the organization	Choose the correct option
development of software	Choose the correct option
new employee's screening	Choose the correct option
information security responsibilities and duties for current employees	Choose the correct option
information security responsibilities and duties for employees who terminate or change employment (former employees)	Choose the correct option

prevent unauthorized physical access and damage to information and information processing facilities	Choose the correct option
prevent loss, damage, theft or compromise of assets and interruptions to operations	Choose the correct option
the process of assigning, creating and changing passwords and access keys to various information	Choose the correct option
for the use of cryptography and key management	Choose the correct option
installation of any software by users without approval or control by specific department	Choose the correct option
to maintain the security of information transferred within or outside of the organization	Choose the correct option
determine what kind of information is vulnerable	Choose the correct option
regularly reviewed for technical compliance with policies and standards	Choose the correct option

- Which department is responsible for cybersecurity? Choose the correct option ☐Other _____
- Is this department part of the Choose the correct option Line of Defense
- When the cybersecurity responsibility and control procedures are allocated to the 1st LoD
- When the cybersecurity responsibility and control procedures are allocated to the 2nd LoD

Audit, Certification & Training

- **All employees**

- How often do you perform an awareness campaigns, tests (e.g. phishing), or training? Choose the correct option
- What are the main contents of the initiatives?
- What types of personal is taking part in trainings?

ɔper-level management	Choose the correct option
ddle-level management	Choose the correct option
ıstomer service	Choose the correct option
·cretary	Choose the correct option
·specialists	Choose the correct option
ybersecurity specialists	Choose the correct option
·curity guards	Choose the correct option
nitorial personnel	Choose the correct option

her_____ Choose the correct option

- **In the cyber security / IT area**

➢ What kind certification a bank employee must have?

➢ Which certificates does your bank have (e.g. ISAE 3402, DIN EN ISO 27001)? Why these ones?

➢ Do you post them online? Choose the correct option

➢ Please explain

- **Internal and External Audits**

➢ How often Internal Audit checks the cybersecurity or parts of it? Choose the correct option

Comments:

➢ How often External Audit checks the cybersecurity or parts of it? Choose the correct option

Comments:

Make or Buy (Outsourcing)

➢ Do you try to maintain your cyber security Choose the correct option

➢ **If external support / service provider is used:**
- Which parts are outsourced?
- Why you have outsourced parts of your cyber security?
- Do you plan to change it and why?

➢ How do you monitor the third-party provider and the outsourced parts?

End-of-Life Technology & Actuality

➢ Software development company:

- Do you use some standard software, or they have changed it for you? Choose the correct option
- If “yes”, how much the software has changed from the original version? Choose the correct option

- What are the software's designer's responsibilities?

- Who controls the software and how?

- How often do you do updates? Choose the correct option

➢ Hardware development:

- How often do they update the hardware (buy new, repair some parts and so on)? Choose the correct option

Comments:

- Which department is responsible for the hardware audit?

- Do you have any equipment (computers, laptops, printers and so on) which are running and has got access to the network? Choose the correct option Other_____
- Do you use that hardware to store the information or they prefer "cloud"(external cloud services)? Choose the correct option Other_____
- If you use "cloud", what kind of information you prefer to storage there?

- Is there a procedure for creating backups? Choose the correct option
- Is there a defined backup period? Choose the correct option
- Is there a process for assigning access rights for backup creation, access and management?

Risk Management & Risk Analysis

➢ Are information security risks compared to the established risk criteria and prioritized? Choose the correct option

➢ What level of the risk you can determine as acceptable?

➢ Is documented information about the information security risk assessment process available? Choose the correct option

➢ What are the general root causes for cyber security risks? (you can "tick" few options)

☐IT (hard or software)
☐Employees
☐Processes
☐External impacts

- How do you prevent cyber security risks (please describe)?

- Where do you think that further improvements are necessary to defend your bank? (you can "tick" few options)

☐External equipment (e.g. ATM)
☐Internal equipment (e.g. firewalls, computer, printers)
☐Employees (honest and dishonest mistakes)
☐Customers
☐Other third parties (please describe)
External third-party fraudsters
☐cyber access
☐physical access

- How do you solve this problem?

- What are the most common employee's mistakes that were determine as threat for cybersecurity?

ishing e-mails	Choose the correct option
sclose confidential information (information about customers, information about transactions, identification numbers of the employees and so on)	Choose the correct option
sclose non-confidential information (telephone numbers of a branch, names and telephone numbers of the employees or managers and so on)	Choose the correct option
e unprotected device	Choose the correct option
anned attack of a former worker	Choose the correct option
her:	Choose the correct option

- What is the main threat for your cybersecurity? (you can "tick" few options)

☐Internal
Social engineering (including phishing attack):
☐Direct attack by an employee

	☐Internet of Things (printers, modems, etc.) ☐Update of the system ☐ External ☐Hackers' attack ☐Former employee direct attack or using social engineering ☐External equipment ☐Customers ☐Partners
➢ How do determine the possible threats? (you can "tick" few options)	☐Reports from different auditors ☐Reports from official auditors like FMA ☐Reports threats from own experience ☐Other_____
➢ How does the process of analysis designed?	
➢ How often do you get the information about the most common threats? ➢ How do you update the data base of threats?	Choose the correct option
➢ Is this analyzing influence of the design of trainings? ➢ If "yes", how?	Choose the correct option
➢ How does trainings effective?	Choose the correct option
➢ Do you have strategies to improve the system? (you can "tick" a few options)	☐Hardware ☐Software ☐Social engineering ☐Improvement external equipment ☐Customer's service including app ☐Other_____
➢ Does the information security risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISMS, and are risk owners identified?	Choose the correct option
The malware attacks	
➢ Is there protection against malware?	Choose the correct option
➢ Are information, software and systems subject to back up and regular testing?	Choose the correct option
➢ Is there a procedure to investigate, analyse and plan to prevent such attacks in the future?	Choose the correct option
Network procedures	

➢ Is there any difference between your banks in the different locations?	Choose the correct option Other_____
➢ How does the cybersecurity culture is implemented to the organizational culture?	Choose the correct option
➢ Do you have international partners, employees, customers?	Choose the correct option
➢ If “yes”, where are they from?	Choose the correct option
➢ Does the work process change when a foreign partner / customer / employee is involved?	Choose the correct option
➢ Do they apply their regulatory requirements (country, region, union)?	Choose the correct option
➢ How do you deal with these requirements conflict with your regulatory requirements (country, region, union)?	
➢ Are there policies and agreements in place to protect information assets that are accessible to suppliers, and is the agreed level of information security and service delivery monitored and managed, including changes to provision of services?	Choose the correct option

Thank you for your time, consideration and for your support!

Once the data has been collected and analyzed, the result can be sent to you immediately.

Best regards,

Alisa Demidova.

ade9590@students.fhv.at

+4367763033041

Appendix 3. The Questionnaire for auditors and software developers

Master's thesis: Alisa Demidova

"How cyber security is maintained in Austrian companies."

International management and leadership

FH Vorarlberg, Dornbirn, Austria.

Dear Sir/ Madam,

I'm the student of FH Vorarlberg, Master's program "International management and leadership" and conducting the research of maintain cybersecurity in financial sphere. I have chosen this sphere of business because it is considered to be one of the most vulnerable spheres in terms of cybersecurity. Banks have to think through the details of how to protect their clientele at all levels.

Questionnaire:

The organization and its context
➢ There is an opinion that banks have to follow huge amount of different regulations and norms. Do you think that the legal and regulatory requirements are complicated to follow for the companies and why?
➢ Which department should be responsible for cybersecurity and why? Choose the correct option ☐Other _____
➢ What line should cybersecurity professionals be on?
➢ Do you think that concept of 3 Lines of Defense is sufficient enough for protection of a company and why?
Audit, Certification & Training
• **All employees**
➢ How often do you perform an awareness campaigns, tests (e.g. phishing), or training for the companies? Choose the correct option
➢ What are the main contents of the initiatives? What do you check more often?
➢ What types of personal should taka part in trainings?
ıper-level management Choose the correct option
ddle-level management Choose the correct option
ıstomer service Choose the correct option
ɛcretary Choose the correct option

·specialists Choose the correct option
'bersecurity specialists Choose the correct option
:curity guards Choose the correct option
nitorial personnel Choose the correct option
her_____ Choose the correct option

- **In the cyber security / IT area**

➢ What kind certification a bank employee must have?

➢ Which certificates does your bank have (e.g. ISAE 3402, DIN EN ISO 27001)?

➢ Do you think they should post them online? Choose the correct option

➢ Please explain

➢ A relatively recent article from BaFin claims that "Hackers are lazy", explaining that they will not attack banks that have undergone certain certifications. Do you agree with this statement?

➢ Is it true that hackers often take the easier route?

➢ If this statement is true, then why are there more and more dangerous, hard to trace viruses?

- **Internal and External Audits**

➢ How often should Internal and External Audits check the cybersecurity or parts of it? Choose the correct option

Comments:

You are using “red team” framework to help the companies find some gaps in their cybersecurity.

➢ How do they find you?

➢ How do you choose the area you will attack?

➢ Does the company provide you with information?

➢ Are you based on the latest research on the most common attacks?

- If “yes”, do you use official resources like FMA, EBA, ESMA reports or something else?

- How effective it can be for them?

Make or Buy (Outsourcing)

- What is the best way for the companies to maintain the cybersecurity? Choose the correct option
- **Why:**

- How do the companies supposed to monitor the third-party provider and the outsourced parts?

End-of-Life Technology & Actuality

- Hardware development:

- Is it safe to use “cloud” storage or is it better to store everything on hard drivers?

- Why?

Risk Management & Risk Analysis

- What are the general root causes for cyber security risks? (you can “tick” few options)
  - ☐IT (hard or software)
  - ☐Employees
  - ☐Processes
  - ☐External impacts
- What are the most common employee's mistakes that were determine as threat for cybersecurity?

ishing e-mails	Choose the correct option
sclose confidential information (information about customers, information about transactions, identification numbers of the employees and so on)	Choose the correct option
sclose non-confidential information (telephone numbers of a branch, names and telephone numbers of the employees or managers and so on)	Choose the correct option
e unprotected device	Choose the correct option
anned attack of a former worker	Choose the correct

	option
her:	Choose the correct option

- What is the main threat for your cybersecurity? (you can "tick" few options)

☐Internal

Social engineering (including phishing attack):

☐Direct attack by an employee

☐Internet of Things (printers, modems, etc.)

☐Update of the system

☐ External

☐Hackers' attack

☐Former employee direct attack or using social engineering

☐External equipment

☐Customers

☐Partners

- How often do you get the information about the most common threats? Choose the correct option
- How do you update the data base of threats?

- Is there a realistic way to fully protect against Social Engineering attacks?

- Do you think that people with different cultural backgrounds have different attitudes to cybersecurity?

- If "yes", why and how?

Thank you for your time, consideration and for your support!

Once the data has been collected and analyzed, the result can be sent to you immediately.

Best regards,

Alisa Demidova.

ade9590@students.fhv.at

+4367763033041

Statement of Affirmation

I hereby declare that all parts of this thesis were exclusively prepared by me, without using resources other those stated above. The thoughts taken directly or indirectly from external sources are appropriately annotated. This thesis or parts of it were not previously submitted to any other academic institutions and have not yet been published.

Dornbirn, 09. July 2021

Alisa Demidova, M.sc