THESIS

Márk Huszár

2022

BUDAPEST BUSINESS SCHOOL

FACULTY OF INTERNATIONAL MANAGEMENT AND BUSINESS

INTERNATIONAL BUSINESS ECONOMICS

Full Time

East Asian Business Studies

CURRENT STATE OF IT SECURITY AWARENESS – CHALLENGES, RISKS AND EFFECTS GLOBALLY

Internal adviser: Dr. Éva Réka Keresztes

By Márk Huszár

VL2X9N

Budapest, 2022

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ATM	automated teller machine
CaaS	cybercrime-as-a-service
CD	compact disc
DDoS	Distributed Denial of Service
DoS	Denial of Service
DVD	digital video disc
GDP	gross domestic product
GDPR	General Data Protection Regulation
HHS	Health and Human Services
IBM	International Business Machines Corporation
IP	Internet Protocol
IT	information technology
MFA	multi-factor authentication
MNC	multinational corporation
NATO	The North Atlantic Treaty Organization
PHI	Protected Health Information
PIN	personal identification number
SIM	Subscriber Identity Module
SMS	Short Message Service
SSN	Social Security number
US	United States
USD	United States dollar
VPN	Virtual Private Network

LIST OF TABLES

LIST OF FIGURES

"There are only two types of companies – those that know they have been compromised, and those that do not know."

Dmitri Alperovitch, 2011

ABSTRACT

The digital revolution has become a part of our lives almost imperceptibly over the course of a few decades. Information technology surrounds us everywhere. In the interim, the frequency and severity of data breaches and cyberattacks also show an increasing trend. The thesis seeks to define the prevalent threats while providing an up-to-date summary and effective countermeasures that prove to be helpful on an individual level. Furthermore, the current state of IT security is analyzed to gain insight into the world of cybercrime, attacks against leading sectors and critical infrastructure, the level of human involvement, and the costs of all these burdens. Lastly, a survey about the individual awareness was conducted via primary research methods to amplify what have been uncovered beforehand.

Key words: data, data breach, IT security, awareness, cybercrime, cyberattack, security tools, human error, password

1. INTRODUCTION

This chapter serves as an introduction to the thesis. First, the background of the thesis subject is explained. Secondly, the research objectives are introduced, and the reviewed literature is presented. Lastly, the structure of the thesis is defined.

1.1 Background

The digital revolution has become a part of our lives almost imperceptibly over the course of a few decades. Information technology surrounds us everywhere. Communication, learning, and business all require knowledge of computers and programs. In addition, a vast amount of data has been created, increasing yearly (Statista, 2022). In today's world, the acquisition of user-level IT skills is essential.

Despite the numerous benefits, there are negative aspects that are often forgotten. The frequency and severity of data breaches and cyberattacks also show an increasing trend. The incredibly rapid development prevents safe adaptation and the awareness of dangers. The list of potential threats is constantly evolving. Nations and organizations have realized the importance of prevention and up-to-date countermeasures.

Regarding the field of IT security, legislation and corporate organizational culture are consciously trying to keep up, but only in a reactive manner. The phenomenon also harbours many dangers for users and individuals, who, however, have the fewest tools in their hands due to the lack of external help and attention. The availability of reliable IT security education outside the work environment could be better. In order to succeed, attackers target those without fundamental knowledge (IBM, 2022; Verizon, 2022).

1.2 Research objectives and research questions

The main objective of the research is to define the prevalent threats while providing an up-to-date summary and effective countermeasures that prove to be helpful on an individual level. Furthermore, the current state of IT security is analyzed via primary and secondary sources to understand better and precisely determine the level of awareness.

The objectives of the research are the following:

1. Define the challenges and dangers of IT security end-users are facing with and outline the possible solutions.
2. Examine, compare, and draw conclusion from the guidance and recommendations of several online sources promoting IT Security Awareness trainings, tips, practices and prevention.
3. Examine, compare and draw conclusion from various reports, papers and online sources related to the state of IT-security and security awareness (See **Section 1.3** for a detailed list).
4. Ascertain the actual, current knowledge and views of end-users related to IT security awareness by conducting primary research.

The main research questions to be addressed are:

1. What are the main challenges and dangers in IT security in the 2020s?
2. What can be learned in IT Security Trainings available online?
3. What is the current state of IT Security and Security Awareness?
4. Are humans really the weakest link? How aware individuals are?

1.3 Literature review

This study mostly relies on secondary sources. The data collected in the research comes from books by IT professionals, annual reports by renowned leading companies in the field of IT security, organizations promoting security awareness and various articles and blog entries that analyze IT-related materials.

The research of Erdősi and Solymos (2018) in "IT biztonság közérthetően" [IT security in an understandable way] provides a consistent and wide-ranging description of the fundamental knowledge regarding cyberspace and its underlying threats. The book's authors identify and define the problems and recommend defensive practices in an accessible language. They touch upon more distinct concepts, e.g., data protection and regulations. Security tips were collected from 20 online sources handpicked by the researcher, including websites of IT and tech

companies, IT-related blog entries and articles (See Appendix for more details). Up-to-date secondary data collected from annual reports with regard to cybercrime and data breaches (IBM, 2022; Verizon, 2022; see also ForgeRock, 2022; Broadcom, 2021; Cyberedge Group, 2021) are given paramount importance. The reports elaborate on the factors of risk mitigation, the trends and tools used against organizations, and the state of security awareness and the economy that lies behind all this. Focusing on particular sectors, reports devote special attention to critical infrastructure (Thales, 2022), including Healthcare (Sophos, 2022), energy (DNV, 2021) and Finance (Varonis, 2022; IBM, 2022). Sources of factors influencing IT security are presented. Interpol's report on Covid-19 (2020) observes the effects of the virus on cybercriminal activities, teleworking and the shifts in trends. McGuire (2018) analyzes the size and activities of the cybercrime economy, and a deeper insight into the cybercriminal market and services is provided by Digital Shadows (2020).

1.4 Thesis outline

The research is introduced with the presentation of the background, research objectives and literature review. The following chapters define and review the concepts that serve as a base for both primary and secondary analysis. Next, the collected secondary data are presented, interpreted, and complemented with the findings of the primary analysis. The thesis concludes with a summary of the main points, answers to the research questions and suggests possible solutions.

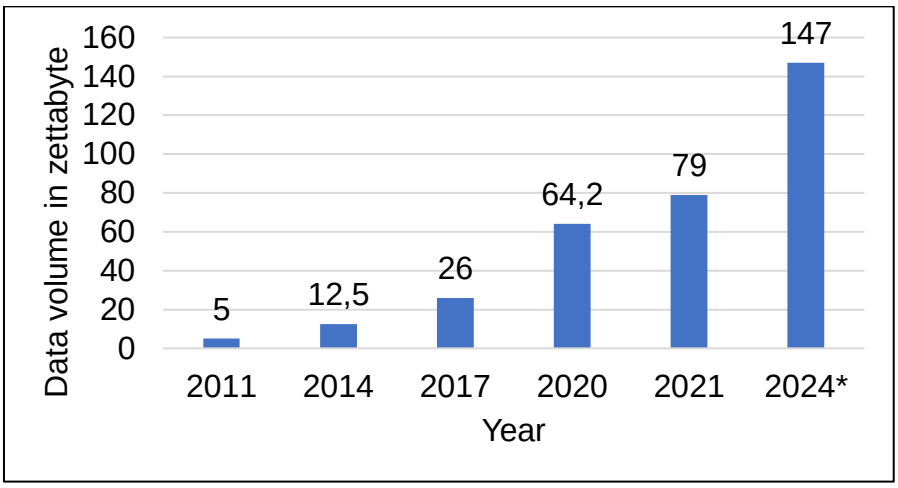
2. DATA AND ITS IMPORTANCE

In computer science, data is digital information which can be stored, moved or processed efficiently. Text, audio, images, and videos are all considered data, all of which are stored in binary form: single values from 1s and 0s (Vaughan, 2019).

Data surrounds us everywhere. The importance of data has been increasing for the last decades. As a result of the digital revolution, the world can collect and possess an unfathomable amount of data. According to Statista (2022a), worldwide data skyrocketed from 5 zettabytes to 79 zettabytes between 2011 and 2021, forecasting even higher numbers for the near future. One zettabyte equals a trillion (10^{12}) gigabytes.

Figure 1.

Worldwide data created, captured, copied and consumed, 2011 – 2021



Source: Statista, 2022a

Data has become a valuable and critical element of the business environment. It allows companies to measure, help the operations, the decision-making, and setting goals. However, the increased availability and value of data caught the attention of hackers as well. The more confidential data are out there, the more rewarding it is for the hackers to join in the end. Cybersecurity Ventures (2020) estimates that the cost of cybercrime will surpass 10 trillion USD annually by 2025.

3. DATA BREACHES

Defining a data breach (also data leak or data spill) is not a simple task – it does not enable unambiguous interpretation.

According to the US Department of Health and Human Services (2015), "data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Verbal, non-verbal, or written dissemination of confidential client data by a staff member may also be considered a data breach."

A data breach is not necessarily a cyberattack or a result of a cyberattack. While a cyberattack is an attempt to gain illegal access to a computer or computer system (Merriam-Webster, n.d.), a data breach occurs when protected or confidential data get disclosed without authorization.

This can be both intentional – an attack for harmful, damaging purposes – or unintentional – such as any kind of negligent behaviour regarding corporate data from an employee (Frankenfield, 2022).

- A dismissed worker prints a document about the customers of the company before leaving.
- An employee accidentally forwards confidential data to unauthorized recipients by having inserted a wrong address from clipboard.
- Someone smuggles out large amounts of secret data using a flash drive.
- An employee leaves the company phone, on which they store confidential e-mails.
- An employee sends internal data to himself by e-mail so that they can continue working from home.

In Frankenfield's interpretation, a data breach is defined as "unauthorized access and retrieval of sensitive information", despite being exposed and being attacked do not correspond. Nonetheless, the correlation is undeniable.

From a statistical standpoint, however, measuring the amount of data exposed and the level of exposition would be rather complicated. According to the data security company, Varonis data breach happens when thieves infiltrate the data systems and extract sensitive data (Sobers, 2022). In this paper, the latter definition will be used for further analysis of the available statistical data.

4. CYBERATTACKS AND HACKERS

A cyberattack can be defined as any attempt or activity targeting an individual or an organization with malicious intent. The goal can be achieved in very many ways. It can be simply the "breach of the information system" (Cisco, n.d.) or, to put it in greater detail, "steal, expose, alter, disable or destroy information" (IBM, n.d.). Although there is no argument about the illegality of cyberattacks, it is worth knowing that there is another similar term, cybercrime – "criminal activities carried out by means of computers or the internet" (Merriam-Webster, n.d.).

The individuals or organizations that launch these attacks are called hackers or cybercriminals. These people are well-versed in technology and able to penetrate and hack into IT systems. The analysis of the motivation behind the attacks has been touched upon by a multiplicity of past

researches and articles (IBM, n.d.; see also Erdősi & Solymos, 2018; Khagram, 2017). Based on that, this research divided the motives into the following 4+1 categories.

1. Financial benefit. – The hackers can profit from stealing useful information and resources (e.g., bank details) or from ransoming the victims in exchange of not to sell their classified, valuable data.
2. Destruction. – The attacker's main goal is to cause harm or reputational damage. These attacks are often personally motivated, (e.g., dissatisfied customers, former employees, competitors) primarily to seek vengeance or punishment by disrupting one's system.
3. Challenge and notoriety. – The desire of recognition and achievement motivates the hackers to compete against MNCs and their impenetrable security defenses. The expression *hacktivism* (hack + activism) is a form of civil disobedience for social or political purposes. Which can be the public humiliation of corporations via their defective security systems in order to generate noise and ultimately incite social and policy changes.
4. Espionage. – Hacking is a modern way and the future of spying. Not only on a corporate but on a governmental and international level. The possibility to gain such advantage over competitors (e.g., neutralizing their strategy or critical infrastructure) virtually, with minimal effort cannot remain unnoticed.
5. Ethical hacking. – Hacking with good intent. Hired by costumers to test the system and document the potential malfunctions.

Unfortunately, when it comes to hacking, the last category is much rarer than the above 4. The attacks are usually executed with the help of malicious software, but also a diverse range of other forms, which will be discussed in **Section 5**. of the research.

5. TYPES OF CYBERATTACKS

Cyberattacks are evolving at an alarming rate. The hackers are developing their software and methods, willing to remain one step ahead of the unsuspecting people. New ideas appear every day; therefore, providing an exhaustive list of attacks is almost impossible, but the research aims to collect the main and most common ones.

5.1 Malicious software

Malicious software, also known as "malware", is any kind of program that is planned to run on a computer without permission to steal or destroy the data on it. They are made and sent for

damaging purposes, to make the system vulnerable and inoperable. They can be further classified into sub-groups: ransomware, spyware, adware, Trojan and all kind of worms, viruses etc., being the most common types.

5.2 Viruses

Viruses are malicious programs that replicate themselves by connecting and modifying other files and programs. The viruses require a host program or file into which they writes their own code. It spreads rapidly via emails or downloads. It also needs human activation. The emails must be opened, the programs must be executed. Until then, the virus can stay in a dormant state (Latto, 2020).

5.3 Worms

Worms are often mixed up with viruses. They share similarities; however, the main difference between the two is that worms do not require host files or human activity. This attribute and their ability to replicate themselves can make them hidden and unnoticed for a very long time. They can spread even more rapidly than viruses, e.g., infecting all email contacts and so on, exponentially. The consequences can range from vexatious adverts to grave financial or infrastructure damage (Latto, 2020).

5.4 Trojan

Trojan or Trojan horse (named after the Ancient Greek legend) is a type of malware that is camouflaged in order to mislead the users of its legitimacy. It often hides inside seemingly harmless and authentic software, downloads, or email attachments; however, it does not replicate itself. Once it infects our systems and gets executed, it can cause various problems, from file corruption to serious data theft or system crashes.

5.5 Ransomware

Ransomware is a program that is able to encrypt and lock data and demands ransom from users to return access. Unless the payment is made, it threatens the victims with the deletion of the documents. Ransomware often unknowingly infects systems via emails, links, and unreliable websites. There is no guarantee that the victims will be able to re-access the data even after paying the ransom. Ransomware has continuously been the number one cyberattack in recent years (IBM, 2022a).

5.6 Adware

Adware is free but unwanted software (or built-in software) which shows advertisements for users. The number of adverts is inconsistent and can vary from a slightly annoying 1-2 to an amount that completely covers the victims' screen. This generates revenue for the hackers for both the display and clicks (either intentional or unintentional).

5.7 Spyware

Spyware is software that sends information to attackers without the user's permission. It is designed to remain hidden and collect as much critical information as possible. It can list the websites visited by the users, access the cameras, and even monitor keystrokes to figure out passwords. With this data in their hands, the criminals can cause even more harm later, infecting the already vulnerable system with other malware.

5.8 DoS and DDoS attacks

With DoS and DDoS programs, cybercriminals can execute malicious network attacks. The program starts to communicate (e.g., with a website) and sends plenty of fake requests towards it, therefore overloading it. The site will be unable to respond to actual, regular users, or the attack might even crash the server because of the incoming traffic. DoS means Denial of Service, which is executed from one computer, while DDoS stands for Distributed Denial of Service and is sent from multiple computers.

5.9 Backdoor attacks and rootkits

Software often contains built-in modules that allow chosen individuals to access data or programs. These can be intentionally built-in by the creators or a result of programming vulnerability (Erdősi & Solymos, 2018). These backdoors can be used for attacks; that way, it is possible to get around the security system and remain completely hidden.

Rootkits are sophisticated malware and backdoor attacks that can hide at the level of the operating system and even get control over it. This level of access evades security measures because it cannot be controlled on a system level.

5.10 Botnet

The expression botnet comes from the combination of robot and network. A botnet is a group of connected (usually via online presence) computers or devices.

Once a computer gets infected with a "botnet carrier", the attacker will be able to take over control of the computer and its capabilities. After gathering as many as 1000 devices, hackers can use the combined power of these devices to execute dDOS attacks, generate spam emails or even mine cryptocurrencies (Baltazar, 2022).

6. OTHER FORMS OF ATTACK

There are other methods used by cybercriminals that do not necessarily demand the presence of software. However, the user's active or passive participation is crucial in this case as well.

6.1 Phishing

Phishing is a cyberattack that involves manipulation. The attackers send fake information via emails, texts, or phone calls. The goal is to deceive the users by pretending to be official and gain their trust to provide sensitive personal information for the hackers. One prevalent example is when the criminals are set up as official representatives of the victim's bank. Then, referring to a sudden, serious issue, they would demand bank credentials and passwords, insinuating that that is the only solution to protect assets (Efimenko, 2018).

Email remains the most prevalent channel for phishing. During phishing, the victim is misled to a page that looks extremely similar to the official website. With the use of false sites asking for identification, cybercriminals can steal the credentials and other data (username, password, sensitive financial or medical data) that individuals enter on the original website.

6.2 Pharming

Pharming is a more sophisticated way to steal the credentials of users. With the help of fraudulent links, the users are redirected to almost or entirely identically built-up websites. If the users are not aware of this, they will willingly type in their passwords and credentials. In that case, because of the diverted traffic of data, they have already become victims of data theft.

7. EVOLUTION OF DATA AND BREACHES

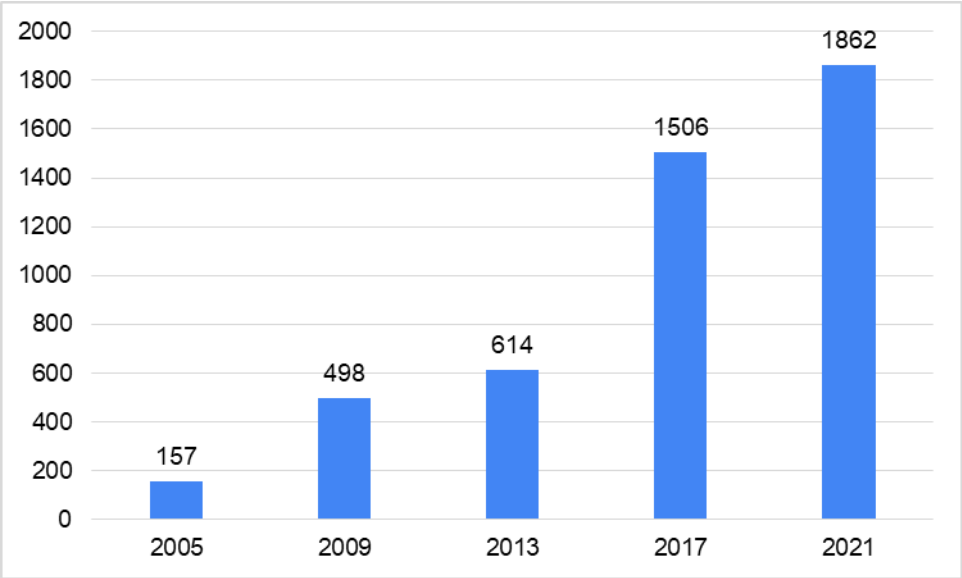
The history of data breaches does not go back a long time. It was only in the 2000s that companies started to leave behind paper records and digitalize their businesses, including data

storage. Privacy Right Clearinghouse's database of data breach chronology began in 2005. Their report contains more than 100 entries from the first year, including major breaches with more than 1 million accounts compromised. Various sectors were affected, including Finance, manufacturing and even education (Privacy Rights, n.d.).

Similar to data usage, the number of data breaches has been increasing ever since. Both the quality and quantity of data available online importantly improved. Likewise, cybercriminals developed, and their repertoire revamped. According to Statista (2022b), the number of data incidents in 2005 was 157. In 2021 the number of breaches skyrocketed to 1862, increasing almost twelvefold.

Figure 2.

Number of annual data breaches in the United States



Source: Statista, 2022b

8. SECURITY AWARENESS

The online presence of companies and their data, combined with the constantly evolving technology and recent challenges such as Covid-19, all play into the hands of the perpetrators of cyberattacks. Rapid IT solutions changes often leave behind negligent employees with out-of-date security knowledge.

Security awareness can be defined in many different ways. It is a process and a goal at the same time. In a perfect world, with well-planned and implemented policies and procedures, companies aspire to create the most secure environment possible (Sellers, 2010). The process includes training, informative emails, and even internal surveys. The security department of a company is responsible for introducing effective measures.

Also, security awareness is the knowledge (or lack of knowledge) of individuals obtained from the above-mentioned processes. This knowledge is required by many organizations formally. Internal tests help companies to evaluate the effectiveness and the level of awareness.

Furthermore, it can be a strategy or a countermeasure. When it comes to defence against cyberattacks and security breaches, it is not necessarily the billion-dollar IT security equipment but rather the often underestimated individual behaviour and the so-called "human factor" (which I will expand upon later in **Section 9.2**) that play a huge role in success. Even the most secure systems can go haywire at a (wrong) push of a button. Reducing human error is one of the critical elements to mitigating risks.

9. RISK MITIGATION

9.1 Individuals' role and responsibility

When it comes to keeping data and IT systems safe, users (individuals) play a crucial role because they are the ones who really use them on a daily basis. They are responsible for creating data, sending it across networks, storing it in various IT devices or media, and finally erasing it if necessary. In light of the foregoing, we can conclude that any management, operator, expert, or external party who has access to the organization's data is a user. Anyone with access to your home's information technology infrastructure, whether family, friends, or acquaintances, counts as a user.

9.2 The human factor

Individuals have become the number one target for cybercriminals. According to Verizon's Data Breach Investigation Report (2022), 82 per cent of all data breaches can be linked to some kind of human error last year. This proves that security awareness training is a key element in reducing human risk. Employees of larges companies are more likely to take part in well-planned, practical security awareness training, but even these companies have difficulties combatting cyberattacks.

In Cyberedge Group's 2021 Cyberthreat Defense Report, according to the surveyed companies, the two most serious deficiencies that hinder adequate defence are the low level of awareness among employees and the lack of skilled personnel who could provide that knowledge. On a scale of 1 to 5, these two scored 3.73 and 3.70, respectively. The two are closely related. If there is no one in the company to take IT security and awareness education into their hands, then no improvement can be expected from the employees. Moreover, these issues have been existing for many years. It is also a problem that the employees of most companies receive security training only once, usually when they join the company. Unfortunately, this knowledge and vigilance can wear out quickly without updates, and it can also easily become outdated as new threats and features arise.

Figure 3.

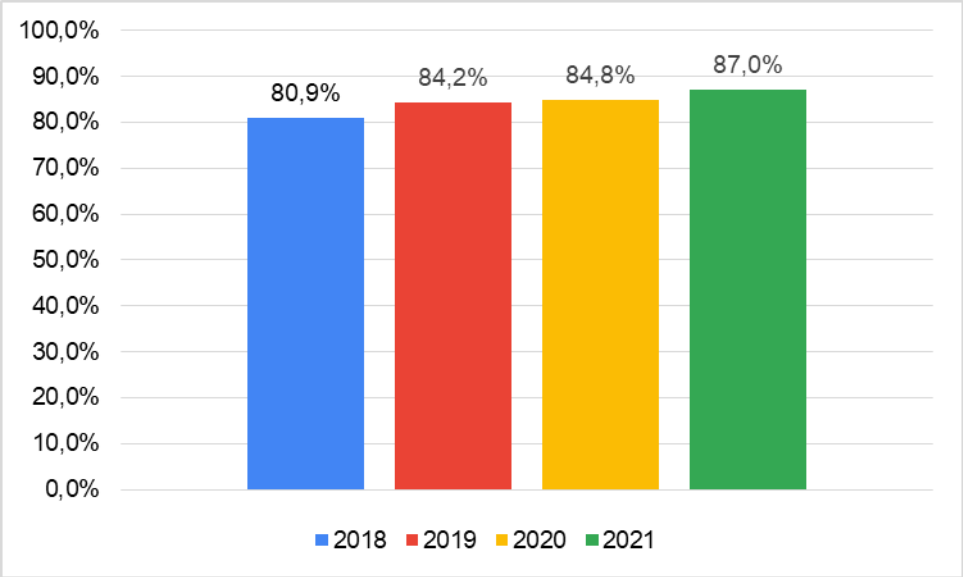
Barriers to Establishing Effective Defenses (scale of 1 to 5, 5 being most serious)

Source: 2021 Cyberthreat Defense Report, Cyberedge Group, LLC.

Secondly, the shortage of specialists with security expertise is becoming more and more significant. In 2021, 87% of the survey participants gave feedback that they did not have sufficient capacity to fill these positions. That affects almost 9 out of 10 companies. This number has increased continuously in recent years, but in 2021 a significant jump of 2.2% can be seen, and 87 per cent is an all-time high. The answers to this are not to be found in career changes or resignations. Covid and the resulting sudden huge demand for remote work have placed a significant burden on security professionals. They also had to secure a completely separate remote access system instantaneously. That gives even more devices to check, a larger attack surface in the midst of new threats.

Figure 4.

Percent of organizations experiencing a shortfall of skilled IT security personnel



Source: 2021 Cyberthreat Defense Report, Cyberedge Group, LLC.

However, on an individual level, outside the working environment, helplessness and vulnerability are even more prominent. Many people lack basic or user-level computer skills, which leaves them even more deceivable and exposed to hackers.

Security training and tips for individuals are available in grand quantities on the Internet, free of charge. In this research, 20 websites were handpicked to collect and analyze the best practices against data breaches. The sites include articles from prestigious IT-security companies, government, banking and educational websites, and blog posts from semi-professional cybersecurity webpages. (See Appendix for the entire list.) The findings do not intend to prioritize certain techniques over others but rather to measure the frequency and publicity of those.

Table 1.

Security tips handpicked from IT websites

Security tip	**Incidence (out of 20)**
Use strong passwords, password managers, reset password	17
Enable 2-step verification/ multi-factor authentication (MFA)	15

Update software	17
Back up data	9
Use antivirus software, firewalls, and other IT-security tools	11
Acquire basic IT-security-knowledge	12
Have a reaction plan in case of infection	7
Be careful with public WIFI	7
Reduce cyber footprint	7
Protect mobile devices	5

Source: self-edited, 2022

9.3 Creation of a secure environment

The gap between low and high security, which is typically quantified by the number of security incidents, must be understood in view of the fact that full (100%) security is impossible to achieve. That is to say, if there are fewer security incidents, then security is improved. We cannot assume that our IT systems will remain incident-free without protection for an extended period of time in light of the current condition of global threats. Therefore, security should not be considered an annoying necessity but rather a way to guarantee the success of operations.

When it comes to safety, the principle of uniformity should be kept in mind. It indicates that the defence must be constructed so that all its elements have the same strength – requisite measures to establish functional security. Every defence has its own vulnerabilities and can only be as effective as its weakest link. As with any attack, the attacker will look for weak points in the defence and focus their efforts where they will have the largest impact with the least amount of work. When we factor in need to ensure the confidentiality, integrity, and availability of the IT resources (data, technologies, apps) we employ, it becomes abundantly evident what we must do to ensure security (Erdősi & Solymos, 2018).

9.4 Passwords

A password is a secret string of characters. It is used for data protection – with passwords, and it is possible to verify whether the user has the right to access it or not. Passwords can contain numbers, letters (both uppercase and lowercase), special characters, and symbols.

Choosing a strong password is a key element when protecting against cyber criminals. In the author's research, 17 out of 20 sources advised that using strong passwords, password managers, and password resetting is an effective security tip. Hackers cracking the user's password is one of the most frequent types of data breaches. The Consumer Identity Breach Report of ForgeRock (2022) shows that the number of usernames and passwords compromised is more than 2 billion. Hackers' main method to find out passwords is a strategy called brute force attack. This often involves the usage of tools and bots that go through all the possible combinations. A list of common weak passwords such as ("123456" or "password") are also tested. The weaker the password, the lesser time is needed to crack through. According to Hive Systems' research about passwords (2022), any password less than seven characters can be stolen with a brute force attack.

Table 2.

Time it takes a hacker to brute force your password in 2022

Number of characters	Numbers only	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24k years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Source: Hive Systems, LLC, 2022

To create impenetrable passwords the following guidelines should be borne in mind.

1. Use as many characters as possible. – The longer the password, the more difficult it is to break through.
2. Add uppercase characters, numbers, symbols. – It augments the total number of combinations as well.
3. Do not include personal data or common ideas in passwords. – It could facilitate the efforts of the criminals by getting an alternative to brute force attacks.
4. Do not use the same password twice. – Once one of your passwords get compromised, it is more likely that the hackers will attempt to enter with that at different locations.
5. Reset/update password regularly. – Every time the password is updated, the ticking clock of a possible brute force break through will also reset.
6. Be aware that passwords do not guarantee total safety. – Having a strong password is a great first line of defense, however it is advised to combine it with other security measures such as password managers and two-factor authentication tools (See **Section 9.5 and 9.6** for more details).

Users often have the wrong idea of what a strong password really is. It is easy to forget that what can be very complicated for the human eye and memory is a child's play with computers and password-cracking programs. The working principle of brute force tools is that the software tries all possible combinations of characters as a password. If we choose a four-letter word, it does not matter whether our password is dogs, doGs, D0gs or doG$. Because of its brevity, the program will quickly reach the end of all existing combinations and cracks the code. To the human eye, however, the jumbled, illogical use of special characters can cause confusion and easily lead to mixing or forgetting the password. We can defend against such an attack most effectively if we choose a long but easy-to-remember password. With the combination of four simple four-letter words, we can give computers thousands of years of work, while the human brain can process the image created from this in seconds and preserve it for a long time.

9.5 Password managers

A password manager is an encrypted application that generates and stores all the different passwords of a user. These passwords are protected by one exceptionally strong password, the so-called "master password". By using a password manager, the user only needs to memorize that one code and access the rest via the application (Erdősi & Solymos, 2018). Memorization of passwords can be tiring. Nowadays, people have such a huge number of accounts that using different passcodes at every different site or application is almost impossible to remember

successfully. A NordPass survey from 2020 revealed that an average user has about 100 passwords. Unfortunately, laziness and the threat of forgetfulness drive people to choose incredibly weak, easy-to-guess, and often personal credentials, therefore giving excellent chances for criminals (Williams, 2020). Password manager applications have their risk as well – in case one forgets the master key or gets stolen, it is possible to lose all of your sensitive data in one attempt.

9.6 Multi-factor authentication (MFA)

Multi-factor authentication (also known as two-factor authentication or two-step verification) is a security process to strengthen your personal accounts even more. As the name suggests, this method requires two (or even more) authentication factors to verify and validate the user's identity. One single password cannot guarantee 100 per cent safety; however, adding one extra layer of protection can make the hackers' life much more difficult. Rountree (2011) distinguished three factors of authentication.

1. Knowledge-related factors. – For example, a password or any kind of personal identification number.
2. Possession-related factors. – Such as a bank card, SIM card, or other physical tokens.
3. Identity-related factors. – Unique, biometric identity, such as the face, voice, or fingerprint recognition.

The more factors are combined, the more secure the data will be. Luckily, multi-factor authentication is more and more popular, and all combinations can be demonstrated with real-life examples.

- 1. + 2.: Withdrawing money from an ATM. It requires a bank card (possession), but also the PIN (knowledge).
- 1. + 3.: New-generation smartphones are often equipped with fingerprint scanners. You can choose this option in online banking applications. Therefore, the first layer of protection is your banking credentials (knowledge), and as a second layer they are strengthened with your fingerprints (identity).
- 2. + 3.: Getting an SMS (possession [of a SIM card]) on a phone with face recognition unlock (identity).
- 1. + 2. + 3. – Combining all of the above, such as money withdrawal paired with fingerprint approval from smartphone.

Using two-step verification is usually mandatory for services such as online banking or the stock market, but it can be added to most email service providers, e-commerce pages and even to social media. Rountree also points out that two-factor authentication is not the same as dual authentication. MFA is the combination of two different factors, while dual authentication is the repetition of the same factor twice (e.g., using two passwords in a row), which is less effective than the former method. In the security tips research, MFA has appeared 15 times out of 20, making it the third most recommended tip. Most of the time, it was mentioned combined with passwords.

9.7 Software updates

Updates are tied for first place, appearing 17 times out of 20 in the research. Updating software means that the user agrees to the modifications (usually made and initiated by the software developers) in order to fix or improve it. From an IT-security standpoint, software updates are essential to reduce, remove and avoid vulnerabilities. Hackers can capitalize both on the unintentional errors made by the developers and the technological limitations caused by an outdated version of the software. The tactics and tools of cybercriminals have constantly been evolving; however, unpatched (not updated) software is not changing at all; therefore, sooner or later becomes obsolete. Users are reluctant to commit themselves to the updates mainly because of their doubts and fears of negative consequences, changes in functionality and also the expenses of money and time (Salamun, 2018). On the other hand, updates could provide more than just increased security. New features, improved efficiency, increased speed, and better system compatibility are all convincing arguments.

All hardware, such as phones, televisions, smart devices, and even Wi-Fi routers, contain a so-called firmware program that controls the device. These are programs that were written by the developers, often years in advance, and their vulnerabilities become apparent over time. Therefore, it is of the utmost importance that the firmware on home network devices is up-to-date and free of known security flaws. The most recent firmware versions can be obtained from the manufacturer. If not, we may fall victim to an attack even if we have strong encryption and believe we have done everything possible to ensure security (Erdősi & Solymos, 2018).

9.8 Data back-ups

A data backup, by definition, is a copy of important information that is stored in a different location. With data back-ups, the user is able to access or regain data in case of a data loss.

There are many types of data losses, and it is not necessarily related to cyberattacks. People lose data through frozen computers, stolen mobile phones, and forgetting to press save buttons. However, the ones related to security are malicious attacks, especially the infamous ransomware. Ransomware is designed to damage users that do not have any back-ups. In that case, the victims are more likely to pay out the ransom, as that is the only chance to get back confidential, sensitive, or personal data. On an individual level, it might include family photos, videos, music, emails, documents etc.

A survey made by Backblaze (2021) found that about 20% of users never back up data on their computers. Even though data awareness greatly improved compared to the 35% in 2008, this still needs improvement. There are different ways to defend against data loss, and the best solution usually depends on the amount of data.

1. Removable media. – Portable devices such as CDs, DVDs, pen drives and external hard drives that can be easily removed from and plugged into computer devices to transfer information. The storage capacity can reach from hundreds of megabytes up to terabytes (10^6 MB).
2. Cloud services. – Connected servers from all around the world that have Internet access are referred to as the Cloud. Cloud servers are able to provide practically unlimited storage capabilities for users. This way, they do not have to worry about physical copies; all data can be accessed virtually via the Internet. Possibly the most famous ones, Google Drive and Microsoft OneDrive, are platforms made for personal cloud storage.
3. Non-digital physical copies. – Sometimes non-digital copies of assurance, invoices, bank statements, medical results etc., are worth preserving. However, if people do not wish to have documents piled up at home, this should be limited to the most crucial data only.

Keeping data at two or more locations is called data redundancy. This redundant state can be achieved by using at least two different data storage solutions. The more locations the users choose to save data, the less vulnerable they are. Non-digital assets cannot be stolen by cybercriminals. On the other hand, cloud data will remain accessible even after a domestic fire incident. The combination of multiple copies, locations and solutions is the best strategy people could aim for (Stouffer, 2022).

9.9 Antivirus, firewall and other security tools

Security tools can provide extra layers of protection against threats and help users to stay safe. In addition, demo versions for testing, and some of them are available free of charge completely. Antivirus software is designed to detect, isolate (put in quarantine) and remove malicious programs and viruses. When talking about computer systems, the term "quarantine" refers to a locked repository where no data or processes can be accessed or run. Files that have been quarantined can be restored if absolutely necessary, but this should be done sparingly. The main justification for quarantining such software is that anti-virus software is unable to successfully disinfect it, rendering it necessary to isolate it from the rest of the operating system. These software are made against existing threats; therefore, updating and using the latest version of these programs are important to maximize safety. An outdated version of the software or the virus definition can create a false sense of security, which is also a risk possibility.

Firewalls can filter and analyze the incoming and outgoing data, and according to the settings, they do not allow for certain suspicious files to open or run. For individuals, the possession of a personal firewall is advisable. The personal firewall is a software that enables or disables network communication and the running of applications. The firewall runs on the user's personal computer; it can be a software installed by the end-user or the part of the operating system. The ultimate goal of the firewall is to prevent unauthorized access according to the personalized rules and limitations set up by the individuals. Other tools include anti-spyware software (detecting threats such as password stealing) and password managers (See **Section 9.5**). These programs can function independently, but complex security systems with the combination of various security tools (e.g., web filtering, antivirus softwares, data encryption) are accessible as well. This combined solution is often referred as endpoint protection or endpoint security. Security tools scored 11 out of 20 in the author's research (St-Hilaire, 2018; Erdősi & Solymos, 2018).

9.10 Security knowledge

Without fundamental knowledge about the threats and defensive tools, users can never reach a comprehensive level of awareness and security. Strong passwords and impenetrable firewalls will be irrelevant until a simple phishing attack can deceive users. Vigilance is key; users should always take a moment to decide on clicking on suspicious links or downloading files from dubious sources. One of the important conditions for malware distribution is that the user typically initiates the first step of infection. It is very important that the attackers want the user to click on the attachment or the link in the email or on the website, so the subject of the letter

is designed to catch the attention of the users. Deceiving strategies include malwares camouflaged as scanned documents, invoices, package delivery updates or banking information.

As new technologies and applications appear, individuals' proactivity is a deciding factor. Cybersecurity issues are not taught in school, and it gives rise to instability. Shred-it's Data Protection Report (2022) surveyed that 67% of small businesses are afraid that workers do not understand basic security concepts, even with training. Acquiring security knowledge had an incidence of 11 out of 20. By participating in (even free) online awareness training, individuals can maintain relevant knowledge about the constantly evolving threat landscape.

9.11 Reaction plan

Even with best practices, data breaches and cyberattacks might be inevitable. In an article from 2011, Dmitri Alperovitch, a former computer security industry executive, famously said: "There are only two types of companies – those that know they have been compromised, and those that do not know." The same can be said for individuals. Once an attack is identified, it needs an adequate response. The overall goal is risk mitigation, including identification of the issue, eradication, and recovery (e.g., changing compromised credentials and restoring data from back-ups). After an incident is resolved, it is worth a review in order to avoid similar problems in the future. Notifying the potential victims is also required. Having a reaction planned has been mentioned seven times out of 20 in the research.

Information security incidents can be avoided if people are alert to potential dangers, follow established protocols in the event of an incident, and know how to report suspicious activity. In the incident management process, users are extremely valuable to the incident management team. However, they also have a great deal of responsibility on their shoulders. Users are particularly important to the incident management process since they are typically the first to notice any traces of an occurrence. For example, consider the erratic behaviour of a program, the receipt of a strange attachment in one's inbox, a suspicious phone call, the discovery of an abandoned flash drive in the office corridor, or the presence of an unknown individual. Critical to any incident management system's success is its users' capacity to detect risks rapidly, evaluate them accurately in light of their risk tolerance, and immediately report them (Erdősi & Solymos, 2018).

9.12 Public WiFi

Connecting to free public WiFi at a restaurant or cinema can be tempting and seems convenient to our lifestyle. Nevertheless, it is not as harmless as some would imagine. In many cases, these networks are not encrypted, which allows cybercriminals to monitor and potentially steal data from the users. The public network can already be infected by hackers. Pre-installed, hidden back door threats or forced installation of malicious software are all in the hackers' arsenal. By surveilling traffic, credentials become vulnerable. It is advised to avoid activities involving sensitive data, such as banking, online shopping or confidential work-related communication. One known defensive tool is a Virtual Private Network (VPN). A virtual private network is an additional network constructed virtually on top of a computer network. A VPN provides an encrypted server for data transmission– even in the case of public WiFi – so instead of the computer, the data comes from the VPN. It helps to keep data private, and the user can remain anonymous. Encrypted data packets ensure that data going over a VPN is not accessible to the original network, hence its "private" nature. This assures that a person can access the company's resources (file server, business apps, email, etc.) when physically absent from the office, even if they are on the opposite side of the globe. This method is more and more popular, and recommended for organizations to counteract the threats posed by spread of remote work and the changed conditions.

Other ways to increase protection are choosing public networks that require passwords, accessing only secure websites and using firewalls.

9.13 Reduce cyber footprint

Cyber footprint (also called digital footprint) is information or data that the user leaves behind in the online space. Two types can be distinguished: passive and active. A passive cyber footprint is all data that is collected and saved in an online database (often even without the user's knowledge). Since networks have a unique identifier (IP address), the user's online habits become identifiable and accessible as well. The data that the user voluntarily shares about himself on social media or other websites is called an active cyber footprint. This can be anything: personal data, photos, videos, our posts, and even the content we like (Family Lives, 2022).

Unfortunately, due to the default social media settings, data can become public, available to anyone, and even fall into the wrong hands. The potential dangers include online harassment, even sexual exploitation, and the preparation of kidnapping, which can be caused by putting

together all the small pieces of information. This is primarily a danger to younger people, but it can affect anyone. It is equally dangerous to share information about your vacation – while the user is away, they could be the victim of a burglary. In order to limit the occurrence of the above threats, it is absolutely necessary to regulate the data protection settings as strictly as possible and, of course, to seek to limit the personal data shared. Their privacy settings may differ for different platforms, but the main controllable elements are as follows:

- Who can find and see the user's profile?
- From whom can the user receive messages?
- Who can see the user's entries and photos?

By limiting access in this way, we can actually achieve that only our friends and acquaintances can contact us.

It requires special attention if we seek to manage our cyber footprint from a public network (See **Section 9.12**). Users must be very careful not to stay logged in to their accounts and delete their data. Carrying out highly confidential activities such as online banking is strictly unadvised.

9.14 Protect mobile devices

People rely on their mobile phones more than ever before, and it already becomes the number one source for internet usage. The number of smartphones has already surpassed 6.5 billion globally (Zippia, 2022). Phones are used for research, communication and entertainment, and these types of activities are often meant to be private. Since the majority of threats are also valid for mobile devices, security and awareness must be extended to this area as well. While it would be reasonable for smartphone users to take precautions similar to those taken with computer systems, a sizable fraction of the population still does not believe this to be the case. Almost every major maker of antivirus software also offers a mobile-optimized version of their product. Free and premium endpoint protection solutions are also available for smartphones. The most popular platforms for smartphones (Android, IOS, Windows) have all been the target of a large number of malware. Smartphones are connected to the Internet nearly around-the-clock, and vice versa, these devices are also accessible online. If attackers are successful in infecting the smartphone, it can be used as part of a botnet network and susceptible to the same types of malware that target personal computers.

Unlike computers, mobile phones are more likely to be carried around, leaving room for an additional but rather severe issue: device theft. According to research, 113 phones are stolen

every single minute in the world (World Backup Day, 2022). Therefore, similar to computers, security measures should be applied to mobiles.

1. Protect your data by choosing a PIN or password to your phone. Never leave it unlocked or unattended in public.
2. Be careful about suspicious links, email attachments. Downloads should be limited to trusted sites (Google Play, AppStore).
3. Keep your phone and applications updated.
4. Limit personal, confidential data and use strong passwords to protect it.

It goes without saying that the access requirements of mobile applications must be mentioned when discussing dangers to mobile devices. The applications need access to the resources provided by the phone, according to the function and objective of the application. Access may include the camera, microphone, call log, location information, keystrokes and even more. The terms of use for an application specify what data developers may access through the program, what they can do with it, to whom it is given, and why. It is worth reading these documents carefully, and if an app has excessive privileges and wants to access data that is not justified for its function and objective, then look for another application with lower authorization requirements. When upgrading these applications, there is a chance that the privacy settings change automatically, especially when a major update or new features are introduced. It is advised to check from time to time whether the permissions took a step in the wrong direction.

10. STATE OF CYBER SECURITY

10.1 The cost of data breaches and cyberattacks

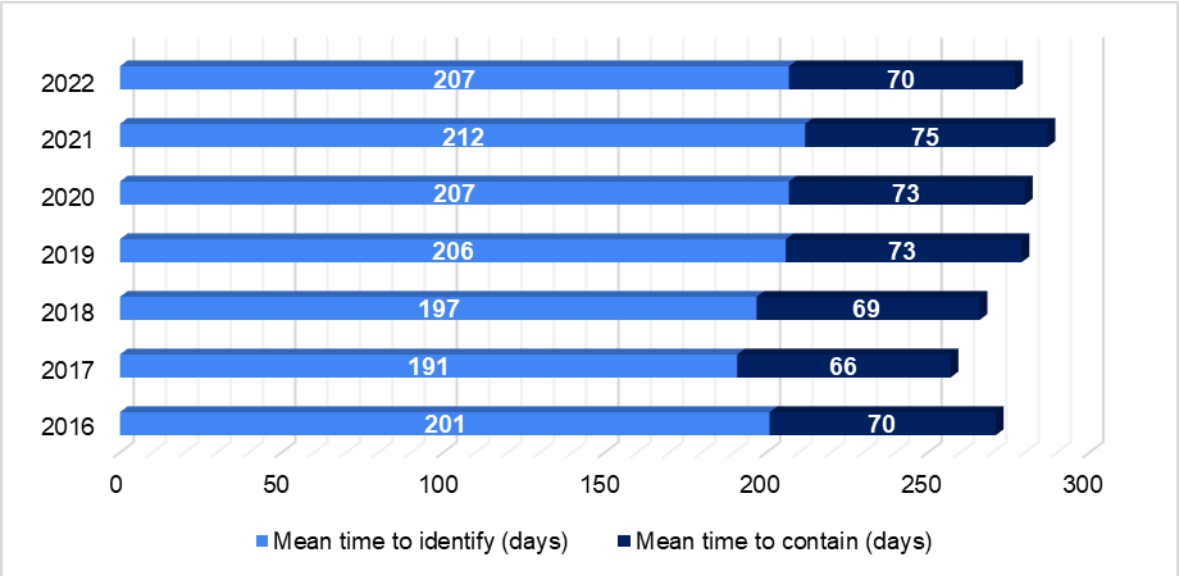
Our world is becoming more and more digital, which cybercriminals are willing to follow. The more confidential data are out there, the more rewarding it is for the hackers to join in the end. Cybersecurity Ventures (2020) estimates that the cost of cybercrime will surpass 10 trillion USD annually by 2025. This is an almost unfathomable number: for comparison, the total GDP of the USA in 2021 is 23 trillion (World Bank, n. d.). The World Economic Forum's Global Risk Report (2020) lists cyberattacks as both a short-term and long-term risk with the expected increase in likelihood and impact in the next years. With such a high potential source of income, cybercrime has become a consciously built, constantly evolving professional industry. Cyber attacks can have extremely serious consequences, paralyzing companies and the critical

infrastructure of whole cities or countries. The recovery costs of such an incident can be huge, so no matter how unprepared companies and governments are in the present, it is worth commencing to spend money on prevention. Determining the average costs of a cyberattack is not straightforward. In the IBM report (2022), the authors took the following main activities as a basis to calculate the expenditures:

1. Detection and escalation – In order to begin troubleshooting the problem, you must first realize that you have really been the victim of an attack. This can take much time. Based on IBM's survey, it took an average of 207 days in 2022 to identify a breach. This means that malicious software could operate undisturbed for an average of more than half a year, constantly getting deeper and deeper into the systems. Escalating problems to a higher level, accurately determining legal backgrounds and damages, and involving external experts can be extremely costly and time-consuming. There were no significant fluctuations in the statistical indicators in the last four years; however, a small decrease of 5 days can be observed compared to 2021.

Figure 5.

Average time to identify and contain a data breach (in days)



Source: IBM Corporation, 2022

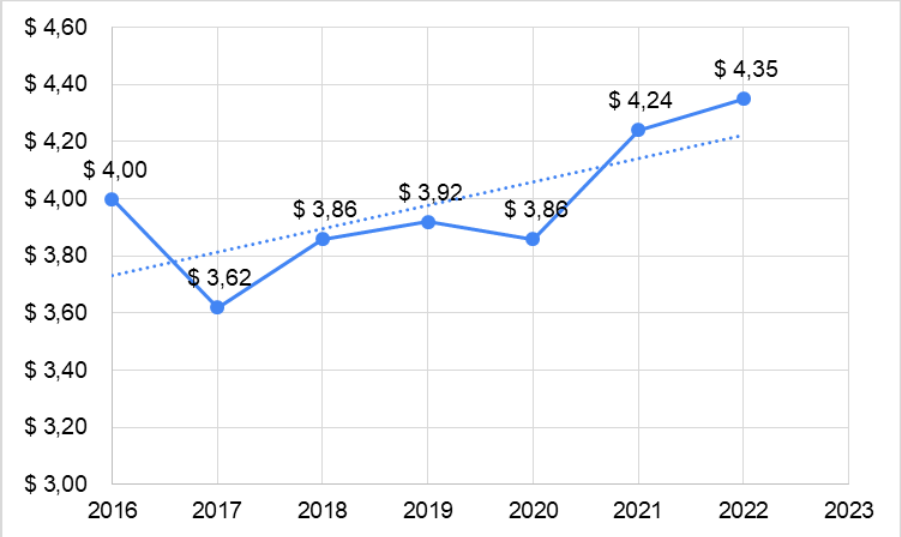
2. Notification – As soon as the infection has been confirmed, the affected parties must be notified: authorities, internal and external partners, and customers. It is possible that the involvement of additional outside experts will be necessary.

3. Post-breach response – Activities that can help victims. Creation and maintenance of a line for injured parties, crediting of balances, provision of discounts and payment of possible penalties may also be included.
4. Lost business – All costs that serve the purpose of ensuring that customers, business processes and cash flow do not feel the breach taking place in the background. But this also includes the costs of a possible actual shutdown. This can result in a decrease in customer satisfaction. Losing a significant amount of customers can bring serious reputational damage along, turning investors away and influencing stock value.

According to IBM's 2022 Cost of Data Breach Report, the average cost of a data breach is $4.35 million USD. (By their methodology, this does not include "mega breaches", where more than 1 million records are compromised.) The 2022 data is a record, compared to the year 2020 it is more than 12 percent higher.

Figure 6.

Average total cost of data breach (in million USD)



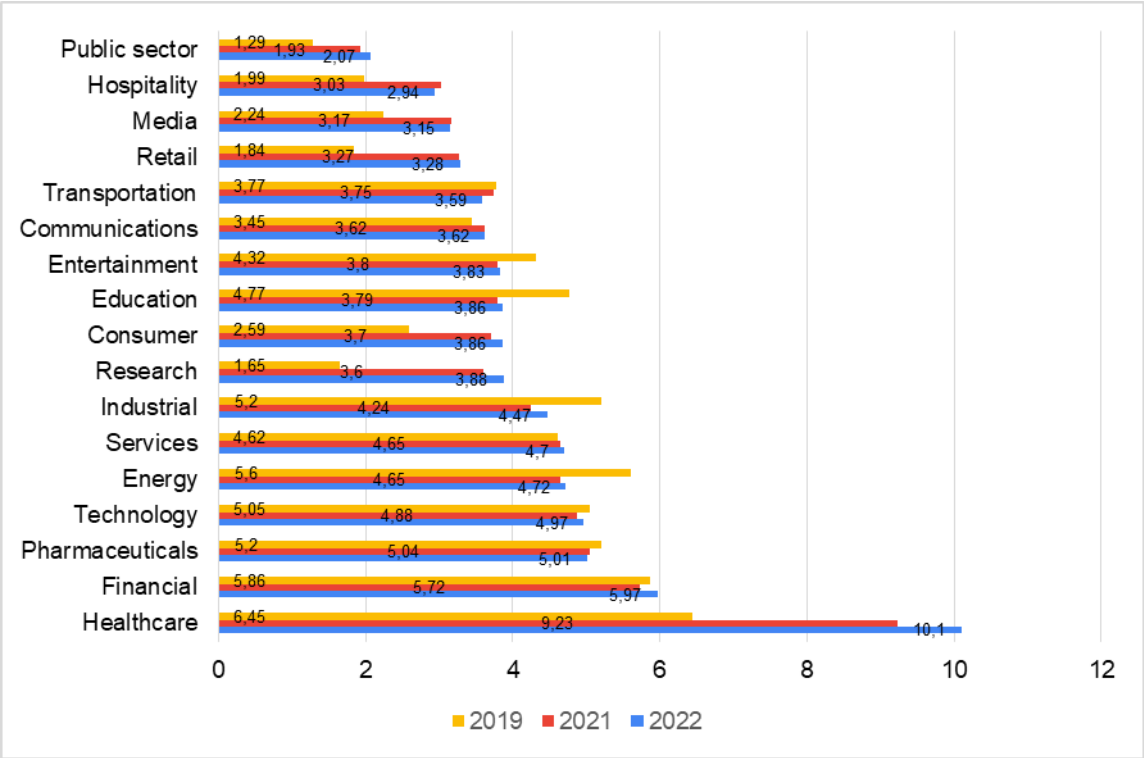
Source: IBM Corporation, 2022

When broken down into different sectors, it can be seen that Healthcare stands out in particular. It can be observed that the sectors performing above the average are all those that are subject to strict regulation and are considered critical infrastructure. Healthcare ranks first with an average cost of $10.10 million. This is an increase of almost 10% compared to the previous year and almost twice as much as the Finance sector that followed. The skyrocketing costs of the sector are spectacular; in 2019, it had an edge of only a 10% compared to Finance, which

will increase to 70% by 2022. Among the top 10 industries, only the Pharma sector experienced a minimal decline in average spending. Compared to 2019, there is no significant change between the leading averages; Healthcare, Financial, Pharma and Energy sectors have been in the top 5 for four years in a row. At the same time, the less regulated public sectors (Hospitality, Retail) are constantly below average, given that in those areas, a data breach would less likely result in the loss of customers.

Figure 7.

Average cost of data breach by industry 2019 – 2022 (in million USD)



Source: IBM Corporation, 2022

10.2 The impact of Covid-19

Covid-19 caught the whole world by surprise and presented unknown challenges to everyone, including those fighting against cyberattacks. Starting from the beginning of 2020, the number of fake news, spam messages and malicious links also jumped enormously, all of which can be linked to Covid. As a result of the widespread remote working caused by the coronavirus, IT departments play a crucial role in ensuring the business continuity of their organization. The exceptional circumstance necessitates new processes and policies affecting authorization levels and access. In exceptional circumstances, an internal communication plan that guarantees

colleagues working remotely receive pertinent information from a reliable and trustworthy source is crucial. In such a scenario, employee training is also a topic of discussion. Data management, data security and cyber hygiene are primary concerns. The requirement to comply with information and data protection regulations extends to teleworking (Deloitte, n.d).

On the part of cybercriminals two major trends were noticeable. In the hope of maximizing profits, they focused on areas that were known to be burdened by the virus, often affecting critical infrastructure. Attacks against individuals have changed; now, they are trying to take advantage of the security weaknesses created by the transition to remote work. The development of remotely controlled systems and applications placed a massive burden on IT personnel. The multiplication of tasks caused a shortage in the labour market. Vacant positions provided hackers with an even greater attack surface.

Serial phishing attacks, malicious links and cloned websites were developed to scam people searching for Covid information. Due to the novelty of the phenomenon, only some people knew which sources they could really trust and which sites were safe to click on. Misinformation has reached enormous proportions. Fake news, conspiracy theories, vaccination and treatment information flooded the Internet, and many of these sources were infected with malware. On social media platforms, these contents were suitable for creating panic.

Even with the easing of the Covid pandemic, remote work remained optional in many places, so vulnerabilities will continue to be present in the future. Even if Covid disappears completely over time, the methods and strategies developed and mastered in recent years can still serve as potential weapons in the future. The epidemic showed that there is room for improvement in the field of global cooperation because the attacks affected all areas of the world in a similar way. Ensuring the global flow of cybercrime information and providing cooperation could help in threat mitigation (Interpol, 2020).

10.3 Cybercrime-as-a-service

The enormous profit and "economic potential" that lies behind cyber-attacks can trigger conscious aspirations. Cyberattacks are more profitable annually than the global illegal drug trade (Cybersecurity Ventures, 2020). In order for someone to become a professional cybercriminal, high skills and dedication are necessary, but for curious and enthusiastic young people, it can be a quick and easy way to make money. The most talented and sophisticated

ones already market their knowledge as a service. Cybercrime-as-a-Service (CaaS) is available on the dark web – i.e., a portion of the Internet that cannot be found with search engines, only available via specific software and provides anonymity to their users – a perfect place to conduct illegal business. Amateur hackers and vindictive individuals or organizations can call for the help of professional, organized service providers. The global revenues coming from CaaS are estimated to be at least 1.6 billion USD annually (McGuire, 2018). The most common services include unauthorized access, website hacking and stealing credentials. The list of sellers is also diverse. Notorious, international hacker groups and semi-professionals can be found at the same time. There is no skill barrier; an insider or malicious software written by others (and an instruction manual) can be enough to carry out an attack (Graphus 2022).

In research, Digital Shadows (2020) observed that the number of credentials up for sale on the dark web could be more than 15 billion. The price of these credentials depends on the quality. Some of them are given away or shared for free on hacking forums. These are usually music or video streaming services, which can be a cheap, leftover asset that the seller does not need. The sharing of these accounts can be considered a gesture of camaraderie among the hacker community. More expensive assets include accounts for e-commerce, social media, streaming services and banking, with the latter being the most valuable, selling for an average of 71 dollars per piece. Sellers also provide hacking tools for those who are interested in do-it-yourself methods for an average price of 4 dollars.

Table 3.

Average cost of one account on dark web (in USD)

Bank/financial	≈71
Antivirus programs	≈22
Cable	≈10
Social media	≈10
VPN	≈10
Streaming	>10
Adult content	>10
Music	≈5
Education	>5
Video games	>5

Source: Digital Shadows Photon Research Team, 2020

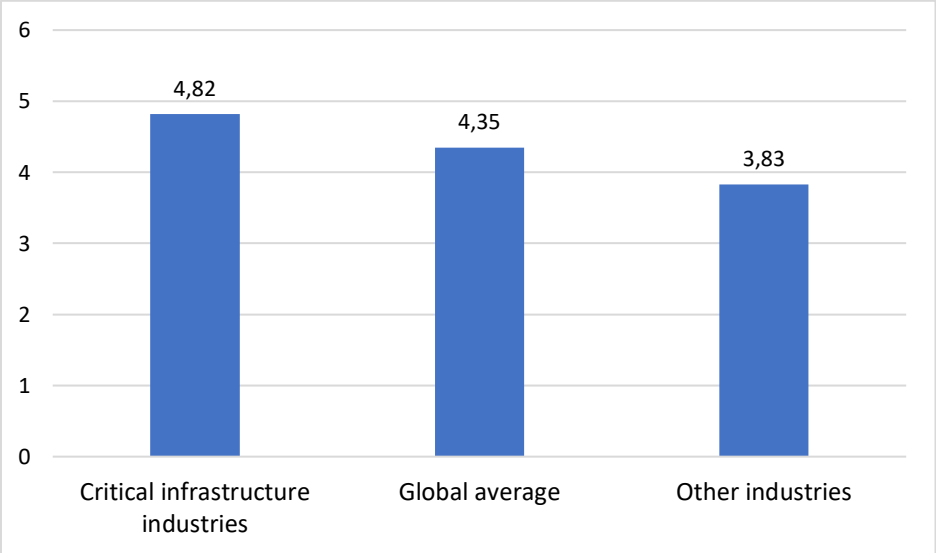
10.4 Critical infrastructure

Critical infrastructure is defined as networks, resources, services, products, physical or information technology systems, and equipment which may directly or indirectly, temporarily or in the long term, have a serious impact on citizens' economic, social welfare, public health, public safety, national security, the functioning of the national economy and government in case of the failure, disruption, loss or destruction of these elements (Békés Megyei Katasztrófavédelmi Igazgatóság, n.d.). Healthcare, financial services, energy, industrial, technology, transportation, communications, education, and the public sector were among the industries with critical infrastructure organizations.

The impact of these attacks is more powerful, and it requires urgent containment. Of course, these infrastructures are also subject to much stricter regulations. Many countries, including the United States, started to implement new frameworks in order to make the system more transparent and prevent prolonged and costly downtimes. These include increased budget and technological support, but also mandatory reporting requirements towards the government in case of incidents and heavy fines issued to those who do not comply. According to IBM data (2022), the average cost of a data breach against critical infrastructure is 4.82 million USD, almost 0.5 million higher than the overall average (Thales, 2022).

Figure 8.

Average cost of data breaches in critical and non-critical industries (in million USD)



Source: IBM Corporation, 2022

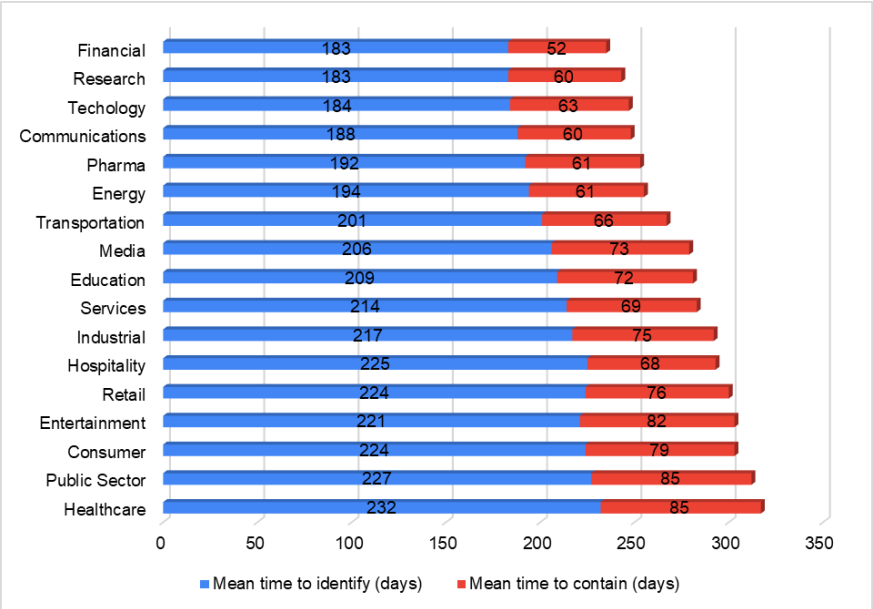
The number one threat to critical infrastructure is a ransomware attack. Hackers have realized that if they successfully carry out large-scale attacks against such institutions, they can make large sums of money in a short period of time. Governments have also realized that such attacks must be dealt with much more severely. As a result, the perception of ransomware attacks has changed. Such action against critical institutions is no longer considered a simple criminal but rather a terrorist act. In 2017, the NotPetya ransomware was categorized as an "act of war" by NATO. Strict action is likely to deter amateur, minor attacks; however, on an international level, between opposing countries, such an incident could even result in a casus belli that can easily spread from the virtual front to the "real world" (Paganini, 2017).

10.5 Healthcare industry

As explained in **Section 10.1**, Healthcare is the leading sector in terms of financial damages, with average damage of $10.1 million per data breach. With this, it has been the most expensive sector for 12 years in a row. The situation is particularly complicated by the fact that hospitals are still feeling the burden caused by Covid, which diverted attention from routine checks and processes, delaying the identification of the data breach for weeks. Unfortunately, Healthcare also stands out in this regard. The identification and treatment of a data breach take an average of 317 days, which is 40 days longer than the overall average. This gives attackers plenty of time to dig deep and get the most out of their actions (IBM, 2022).

Figure 9.

Average time to identify and contain a data breach by industry (in days)



Source: IBM Corporation, 2022

Since Healthcare is a critical infrastructure, it is essential to plan for attack scenarios that will not disrupt services and recovery times that will not be excessively lengthy. A potential interruption in hospital operations might result in massive financial losses and put patients' lives in peril. Having to seek medical care in a facility with a poor reputation is one of the worst possible outcomes. Hackers, however, are well aware of this, and they frequently attempt to take advantage of it through means such as ransomware attacks. As a result, the pressure on hospitals is significantly higher, as not only data but human lives may be at stake if the ransom is not paid. The healthcare industry was the most inclined of all industries to pay a ransom, with 61% of respondents to a Sophos study in 2022 admitting to doing so. Attackers also know how stringent the laws are in this area. In the event of a breach, the relevant authorities have the ability to apply severe fines, thereby raising the cost of the attack even further (Kessem, 2022).

Credentials that are exposed or stolen are also a crucial component of healthcare data breaches. According to data from the US Department of Health and Human Services (HHS), 45 million individuals were affected in 2021. Thus, hackers can acquire access to the extremely valuable protected health information of patients (PHI). Two significant variables contribute significantly to their value. The first factor is data density. Numerous patient-related details (date of birth, residence, state of health, diagnoses, prescribed medications, and Social Security numbers) are contained in hospital records. Secondly, these facts are difficult to alter. The same cannot be said for our residency and identity card information, which can therefore remain relevant in the hands of hackers for many years.

The biggest Healthcare-related data breach to date can be linked to Anthem Inc. Anthem, one of the largest Health Insurance companies in the United States, who was the victim of a cyberattack in February 2015. The number of people affected was almost 80 million, whose personal data, including names, dates of birth, email addresses, and Social Security Numbers, were stolen. The attack did not affect medical and financial information. A whole month had passed after the actual data theft occurred before it was uncovered. Identity theft, the most severe risk posed by the theft of such information, will need the victims to remain vigilant for the rest of their life. A record $16 million in damages were assessed against Anthem by HHS after an investigation revealed insufficient measures were in place to prevent hacking attacks. The corporation also shelled out an additional $115 million in settlements for other civil actions. The scandal rocked public confidence and sparked a discussion about the need to tighten regulations around the theft of sensitive medical information (Freeman, n.d.).

10.6 Energy industry

As the energy sector became increasingly network-connected and smart devices are brought to board every day, its exposure to cyberspace has been growing as well. Since this phenomenon is new, the companies in the sector need to be fully aware of the extent of the danger they may be exposed to. In its infancy, the energy sector is particularly attractive to cybercriminals. Their arrival is much less expected than, for example, in the financial areas, which have been facing cyber threats for many years. According to the experts interviewed by the DNV (2021), organizations are aware of the potential dangers. Sixty per cent of them believe that they have never been as vulnerable as they are now, but their mindset is reactive: 35 per cent answered that a major incident would be necessary to devote time and money to cyber defence. The explanation also lies in the innocence of the sector. Only 22% of respondents answered that they had experienced a significant breach in the last five years.

The complexity of the energy sector worsens the situation. The lack of IT professionals is particularly noticeable, and only a very few people understand both cyber security and the operation of wind turbines, gas pipelines or other machinery. The joint knowledge about the two different worlds ensures only the appropriate efficiency. Only 31 per cent of those questioned in the survey answered that they would confidently react in the event of a potential cyberattack. The sector experiences the same kinds of attacks as other sectors, including those that target credentials and use ransomware, but it also has a large volume of social engineering attempts like phishing.

In recent years, the energy sector has been the target of one of the biggest cyberattacks. In May 2021, a ransomware attack affected Colonial Pipeline, which is in charge of providing roughly 50% of the East Coast with its 9,000 km oil pipeline network. In order to stop the attack, the company shut down its whole network, and in an effort to restart fuel deliveries as soon as possible, it even paid the $4.4 million ransom in a matter of hours. Even so, the restoration procedures took close to a week. A state of emergency was declared in the country, which led to massive panic buying. Due to supply problems, shortages developed in several places, as a result of which even the price of diesel began to rise. The fact that the attackers only had to crack a single password points to extreme weaknesses in critical infrastructure. It was an inactive account of an employee with a weak password and no two-factor authentication in place. The national-scale disaster resulted from the sheer negligence of the protection of critical infrastructure, which could have been easily prevented by following the basic security rules. The incident caused serious repercussions; the US president signed an executive order to

strengthen federal cyber defence capabilities. Law enforcement later managed to recover $2.3 million of the ransom paid (Geller, Gonzalez & Lefebvre, 2021).

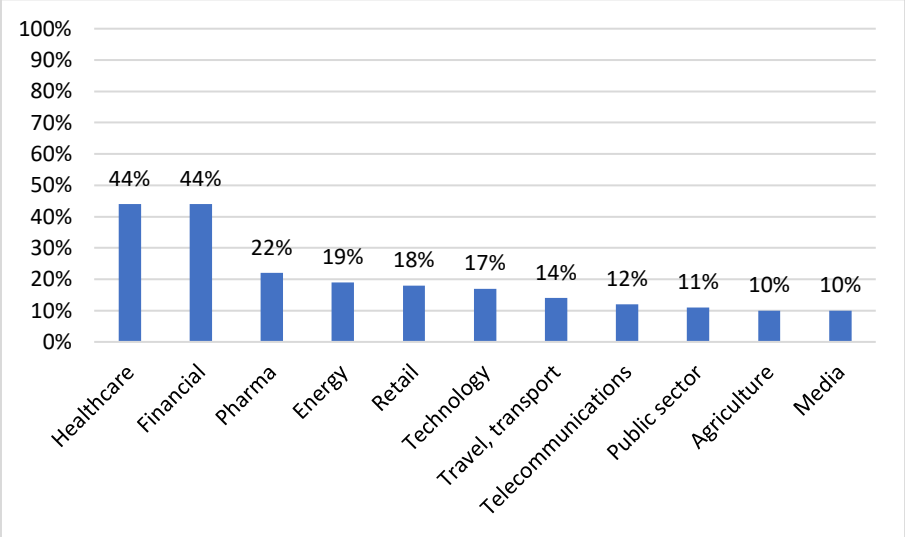
10.7 Finance and banking

The digital revolution and technological innovations have also appeared in the financial sector. In order to meet the ever-increasing customer needs, more and more new services and applications are becoming available in the digital space. At the same time, unfortunately, the attack surface also increases as a result. The financial sector is subject to extremely strict data protection rules. Money is not a game for either the banks or the bank customers, and vigilance is in the interest of both parties.

Data from IBM (2022) showed that after Healthcare, the costs of a data breach are the highest in the Financial sector, with an average of 5.97 million dollars. Report by Varonis on financial data (2021) found, that the main problems in the sector were remote work-related issues, poor access management policies and never expiring passwords. According to Varonis, almost 60% of financial organizations have more than five hundred passwords that never expires, and employees have access to 11 million files on average, including sensitive data. The danger in both sectors is enormous: medical and financial data are extremely valuable, the loss of which can result in massive customer exodus, as these are areas where trust is crucially important. In McKinsey's data security survey, 87% of respondents said they would cut ties with a company if they felt that they could not trust them. In the same survey, only 44 per cent of the respondents trust that their data can be safe in the healthcare sector, and also 44% in the financial sector. Moreover, that is not even the astounding statistic. The two sectors are also towering ahead of the others (Anant et al., 2020).

Figure 10.

Most trusted industries in protecting data and privacy



Source: McKinsey Survey on North American Consumers on Data Privacy and Protection, 2019

In 2019, a vast data breach shook the financial sector. Eight hundred eighty-five million documents related to the insurance giant First American Financial got exposed. This unfathomable amount of data was available on the company's website without barely any security involved. The data went back to 2003 and included bank account numbers, tax documents, photographs, and Social Security Numbers. The data was not protected by a password either, and someone just had to look for it in the right place. It is difficult to assess the severity of the case because it was not a malicious attack but rather a human error. The link containing sensitive data was hidden but completely accessible in case of manual editing and consequent guessing. The case is a perfect example of when a data breach happens without a proper cyberattack – there is no need for a back door attack if someone leaves the front door open. Regarding the incident, it could not be ruled out with absolute certainty that the data was not collected by bots. In the worst case, it could have even happened to all the 885 million files that were compromised.

After an investigation by the government, the company only had to pay 500 thousand dollars as punishment, which is incredibly low given the possible severity of the case. The settlement involved no admission of guilt by First American Financial (Dellinger, 2019).

10.8 Data protection

We can talk about the security of personal data when all of the data is safe against unauthorized use and possession, i.e. data protection is achieved. People frequently share their photos and thoughts on social media without regard to who can see them, control them, or have access to them. Other times, they voluntarily share their personal data with certain organizations for a variety of reasons. Undoubtedly, all of this could be harmful. Data protection is primarily a concept used in legislation, and it primarily means the proper handling of personal data as required by law (Erdősi & Solymos, 2018).

As consumers adopt digital technology at a faster rate, the data they produce give businesses the opportunity to engage with their customers but also the duty to protect their personal data safely. Managing the data that businesses collect is their responsibility. McKinsey's survey about the collection and protection of data was conducted in 2020. The results showed that consumers are becoming more intentional about the data they shared with organizations. They are much more likely to disclose private information when it is required for them to interact with businesses, although no sector reached a trust rate of more than 44% (See **Section 10.7** and **Figure 10**.). Given the recent, serious history of consumer data breaches, the lack of trust is completely reasonable. The surveyed were aware of these breaches, even if they were not affected by them directly. It is understandable that people are willing to restrict data that is less important or given to low-trust companies. Governments from all around the world are introducing regulations concerning data protection. This is a massive help for those who are concerned about data collection but do not know well enough how to secure that data themselves. Violating regulatory compliance can result in costly fines; therefore, companies do not hesitate to invest considerable amounts in remaining compliant (Anant et al., 2020).

10.9 GDPR and other regulations

Of all the evolving privacy regulations, the GDPR was the first. It is often considered the archetype or the flagship among all. The European Union recognized the importance of managing personal data early on. In 1995 the Data Protection Directive was enacted. The goal of the directive was to define the principles of the free movements and processing of data. This was later annulled and replaced by the General Data Protection Regulation (GDPR). It became enforced in 2018. The regulation states that "the protection of natural persons in relation to the processing of personal data is a fundamental right" (Official Journal of the European Union, 2016). Regulations have already appeared in other countries as well recently, such as General Data Protection Law (Brazil, 2020); California Consumer Privacy Act (US, 2020); Personal

Information Protection Law (China, 2021). Similar to the GDPR, non-compliance results in penalties in all cases; however, the severity of the fines can differ notably. It is worth noting that many of these acts and laws came into effect in the last five years, proving that urgent intervention is necessary because of obsolete legislation and the difficulties of keeping up with technological development.

By that, greater protection and more options are given to the consumers, providing them with better access to the data firms collect from them and making it simpler to request that their data be deleted. Achieving compliance with the regulations requires precision and transparency from organizations that might have to change the former methods of data confidentiality. In the absence of this, companies could face expensive fines of millions of euros. According to the McKinsey survey, GDPR 6 out of ten people are aware that their data is regulated, which is an increase of 50 per cent compared to 2015.

We can differentiate between data collectors and data processors. The data controller decides how and why personal data is processed. On the other hand, the data processor processes the data on behalf of the collector. The exchange is regulated by contracts in which the means of process and authorization rights are clearly indicated (European Commission, n.d.). Collectors and processors are both required to provide an adequate technical background, including:

- data encryption
- service-level agreements on availability and breach containment
- regular back-ups
- process monitoring and efficiency testing.

Even in the presence of regulations, it happens that companies handle user data carelessly, as seen in the previous examples (See **Section 10.5, 10.6 and 10.7**). The most significant danger of these is that even a user who has followed and applied all possible security advice can become a victim of identity theft. Data protection rules primarily serve to prevent this. By limiting the sharing of personal data, we can do a lot to avert dangerous circumstances, but we can also improve the situation by consciously choosing data controllers. It is worth striving to share only the most necessary data and only with those service providers whom we absolutely trust. (Anant et al., 2020; Erdősi & Solymos, 2018).

11. PRIMARY RESEARCH ON IT SECURITY AND SECURITY AWARENESS

11.1 Aim of the research

The secondary sources used and analyzed in the thesis primarily focus on IT security and the development of security awareness in the corporate culture. There is little data from secondary research on the individual's knowledge and skills, despite several studies highlighting the importance of the "human factor" and "human error" in IT security. The shortcomings are located on the individual side, but the damages are suffered mainly by the companies. The purpose of the primary research is to gain a greater insight into the quality of personal, user-level knowledge outside of the work environment. The assessment of individual knowledge level and cyberculture can help in determining the appropriate starting point, direction and gaps in order to achieve stronger and more effective security awareness and IT security.

11.2 Hypothesis and research questions

The literary history of the hypothesis to be established:

Secondary research analyzed in this paper (Verizon, 2022, see also IBM, 2022; Varonis, 2022) showed the extensive involvement of human elements in data breaches, making human error the leading factor of incidents.

Hypothesis:

The prominent role of human error concerning data breaches can be traced back to individuals' incomplete knowledge of IT security and security awareness. Despite digital technology, access to knowledge is limited, and its value is underestimated.

The main research questions to be addressed are:

1. What are the most prevalent habits of individuals related to IT security?
2. How familiar are individuals with cyber threats and preventive tools?
3. How do the level of IT security knowledge and security awareness influence individual behaviour in cyberspace?

11.3 Research methodology

This research is primary, quantitative research. The data was gathered by the author between October 2022 and December 2022. The data collection method was an online survey. It was shared in various online channels, including social media, messaging apps and emails.

The questionnaire contained close-ended questions to gain quantifiable insight into the subject. The research follows a positivist philosophy, as it concentrates on measurement and numeric data, and the author is limited to interpreting the findings in an objective, quantifiable way.

11.4 Results

The sample size of the results was 161. Among the respondents, 75 were women and 86 were men. The average age of the participants was 26.

Passwords:

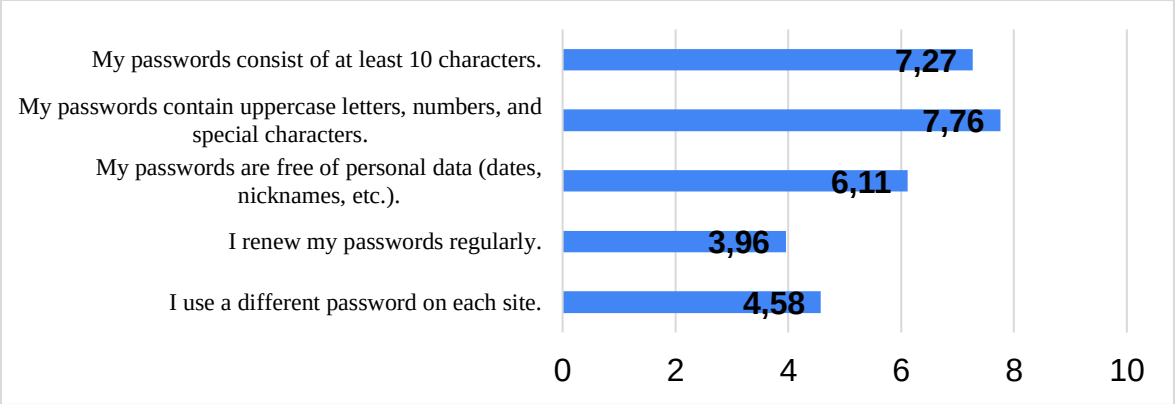
For the first section of the questionnaire, participants were asked about their security practices related to credentials. The respondents were asked to rate the following statements on a scale from 1 to 10 (1= never, 10 = always).

- My passwords consist of at least ten characters.
- My passwords contain uppercase letters, numbers, and special characters.
- My passwords are free of personal data (dates, nicknames, etc.).
- I renew my passwords regularly.
- I use a different password on each site.

On a modern and secure website, choosing long passwords with numbers and special characters are mandatory by default during registration. These two scored the highest in the survey, with 7.27 and 7.76 out of 10, respectively. Unfortunately, further, more sophisticated password security practices would be needed to be adapted. Password renewal and differentiation reached the lowest scores among the participants, 3.96 and 4.58 out of 10. Respondents tended to include personal data in their credentials; the result was 6.11 out of 10.

Figure 11.

Password practices of individuals (on a scale of 1 to 10, 1=never, 10=always)



Source: self-edited, 2022

Regarding mobile phones and laptops, only 57 per cent of the surveyed answered that every device in their possession was protected by passwords. Combining these ratings, a "password awareness" rating was created, which can be calculated by taking the average of the five statements. The average password awareness rating was 5.94 out of 10, with a standard deviation of 1.46. The minimum score was 2.4, and the maximum was 9.2.

Table 4.

Password awareness rating statistics (on a scale of 1 to 10, 10 being the strongest)

Average	5.94
Standard deviation:	1.46
Minimum:	2.4
Maximum:	9.2
Median:	6

Source: self-edited, 2022

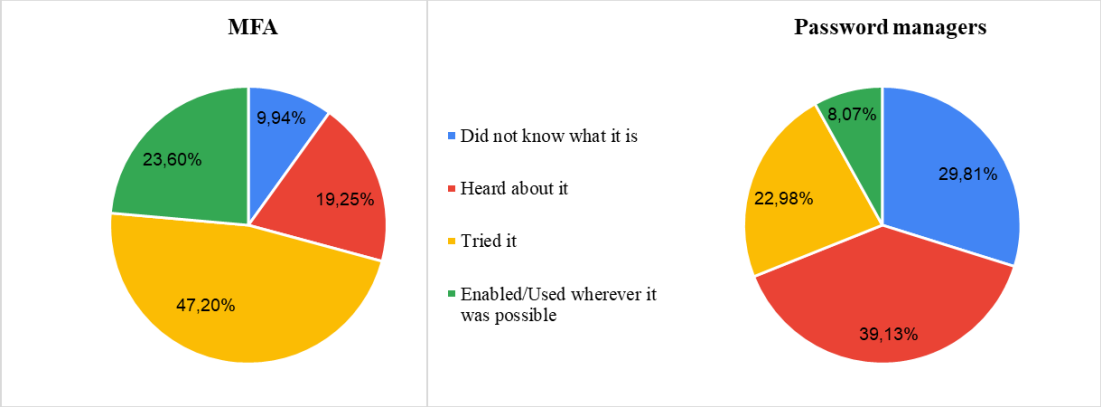
MFA and password managers:

Layered security approaches, such as multi-factor authentication (MFA) and password management, were also observed. 9.9 per cent of the respondents did not know what MFA was. 19.3 per cent of the people heard that such a method exists but have yet to try it. 47.2 per cent of the participants said that they only use MFA in places where it is mandatory by default (e.g., banking apps), and only 23.6 per cent made an effort to enable MFA at every possible place.

Password managers were unknown for 29.8 per cent of the surveyed, and 39.1 per cent heard about this solution. Twenty-three per cent of the participants tried applications like that, and only 8.1 per cent replied that they used this technology actively.

Figure 12.

MFA and password managers usage of respondents



Source: self-edited, 2022

6.8 per cent of the surveyed used both MFA and password managers actively, while 7.5 per cent did not know about either security tool. The result showed that those who were not aware of the existence of the two security methods did underscore the password-related question. On the other hand, those who relied actively on MFA and password manager tools had a significant increase in average ratings. The password awareness ratings were 4.78, and 7.37, respectively.

Table 5.

Password practices and awareness ratings (on a scale of 1 to 10, 10 being the strongest)

	Did not know about MFA and password	Total average	Used MFA and password manager wherever it was
My passwords consist of at least 10 characters.	**5.58**	**7.27**	**8.73**
My passwords contain uppercase letters, numbers, and special characters.	**6.25**	**7.76**	**8.36**
My passwords are free of personal data (dates, nicknames, etc.).	**5.83**	**6.11**	**6.64**
I renew my passwords regularly.	**3.25**	**3.96**	**6.64**
I use a different password on each site.	**3**	**4.58**	**6.47**
Password awareness rating:	**4.78**	**5.94**	**7.37**

Source: self-edited, 2022

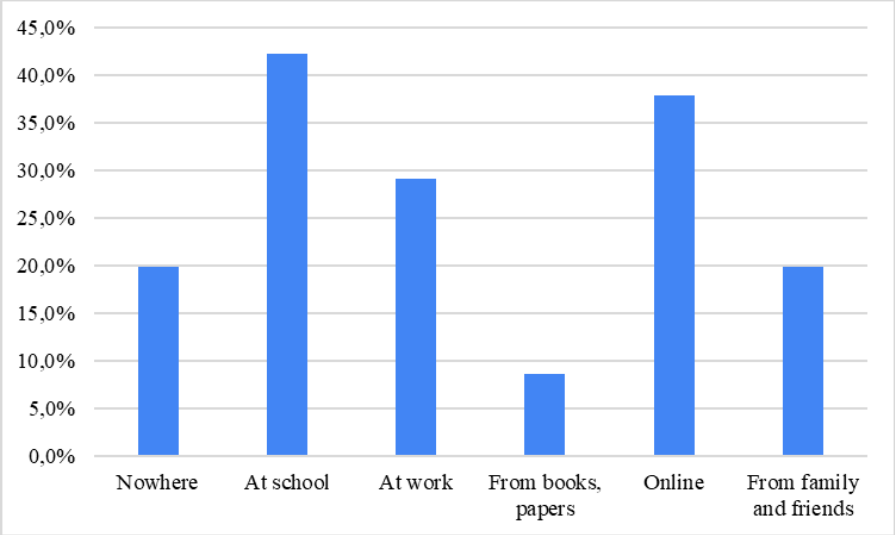
Security awareness and cyber threats:

The second section of the questionnaire was designed to gain insight into the participants' knowledge about cyber threats, prevention and awareness.

When asked about the source of their knowledge about dangers and security knowledge, respondents' results painted a mixed picture. The most common sources were school (42.2%), the Internet (37.9%) and work (29.8%). 1 out of 5 respondents said that they did not learn about the issues at all. It is worth noting that the result regarding the work does not reflect that younger people are less likely to have work experience. When all participants aged under 20 were excluded, the ratio of work as a source went up to 43.1 per cent.

Figure 13.

Source of IT security knowledge of individuals



Source: self-edited, 2022

To the question, "On a scale from 1 to 10, how afraid are you that you and your data may get attacked online?" the average score given by the participants was 4.74. However, according to the findings, there is a direct link between education and fear. The higher the level of education, the more aware people are of the dangers.

Table 6.

Fear of online attacks among individuals by level of education (on a scale of 1 to 10, 10 being the most serious)

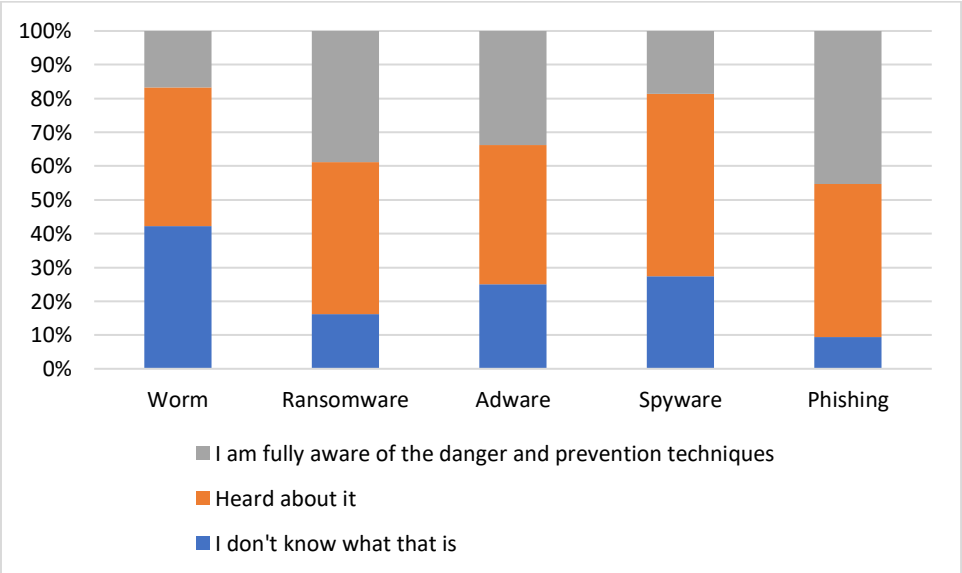
Level of education	Average score of "fear"
College/university	5.42
Secondary school	4.84
Primary school	4.19

Source: self-edited, 2022

The respondents were also asked about participation in security awareness lectures and training. 31.7 per cent were not interested at all, and 54 per cent said that they would only take part in training free of charge. Only 14.3% of the respondents were interested in paid training. Concerning the threats, the surveyed people had to categorize the following definitions: worm, ransomware, adware, spyware and phishing. Ransomware and phishing were the most recognized, but neither of the examples reached an "awareness rate" of more than 50 per cent. On the other end, 42.2 per cent of the surveyed had no information about worms.

Figure 14.

Threat awareness of individuals



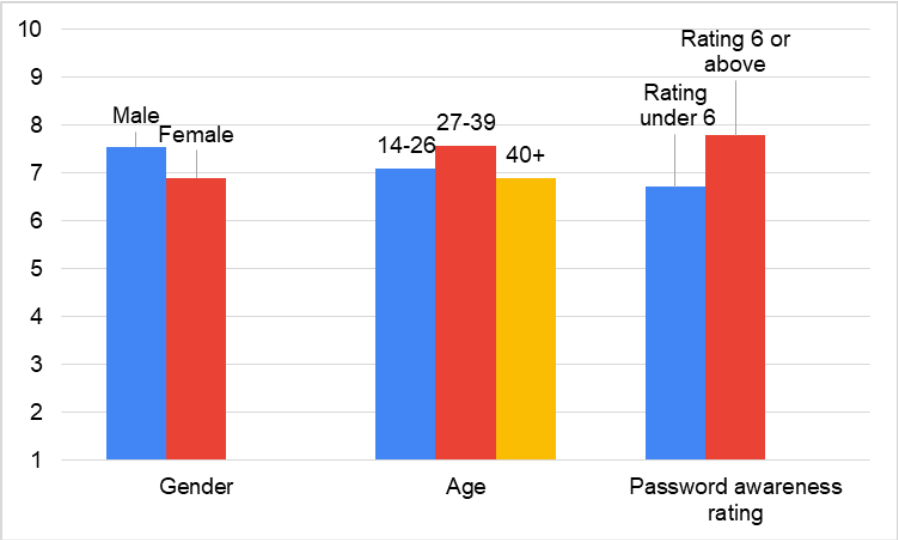
Source: self-edited, 2022

Updates, back-ups, public Wifi

The last section of the survey contained general questions related to the cyber habits of individuals. The main aspects were update regularity, backup methods and regularity and usage of public WiFi. In the survey, the following question was asked: "On a scale of 1 to 10, how often do you update your devices and applications?" The average rating given by the participants was 7.25. Further subdivided for particular groups, men, people aged between 27 and 39, and respondents with password awareness ratings higher than 6 had a slightly better score.

Figure 15.

On a scale of 1 to 10 how often do you update your devices and applications?

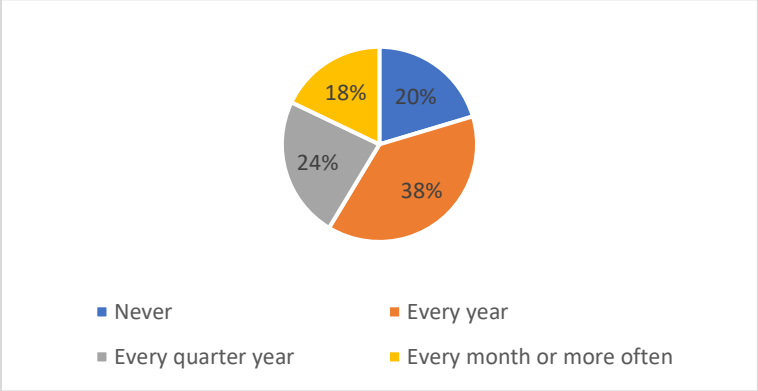


Source: self-edited, 2022

Regarding data back-ups, questions were posed about frequency and methods. When asked about frequency, 20.4 per cent of participants replied that they never backed up data. 38.3 per cent save important documents every year, 23.5 per cent every quarter year and 17.9 per cent every month or even more often. Cloud services were used by 63 per cent, hard drives by 40.6 per cent, smaller removable media (CDs, DVDs, pen drives) by 47.1 per cent and 7.2 per cent chose non-digital format.

Figure 16.

Frequency of data back-ups among respondents



Source: self-edited, 2022

When asked about public Wifi usage, only sixteen per cent of the participants answered, that they never connect to open networks available in public areas, such as restaurants or cinemas. Almost one third of the respondents, however, always looks for these opportunities, mainly to reduce their data usage. More than 50 per cent of the surveyed said they connect to public networks occasionally. Consequently, the majority of the surveyed people are not afraid of public networks.

11.5 Summary and conclusion

The survey questions helped to learn about the cyber habits of the respondents. Without complete knowledge regarding the analyzed practices, the creation and maintenance of a secure environment are somewhat tricky. The results of the questionnaire showed that individual knowledge is incomplete. Fundamental knowledge is missing for many, and the proportion of respondents who are aware of all aspects needs to be higher. MFA and password safes are regularly used by only a tiny percentage of those who completed the survey. Less than 50% of them learned about IT security at school, and the subjective sense of danger of the respondents is low. Awareness as a concept can be filtered out of the results: those who pay more attention to IT security got proportionally higher values.

To reduce human error and mitigate risk, the establishment of conscious, consistent and comprehensive security practices are essential. Missing single components (whether it is caused by negligence or the lack of knowledge) is dangerous. In order to increase motivation and change the perspective, IT security needs educational and state reforms. The right mentality requires a collective change of attitude.

12. CONCLUSION

This chapter will offer an overview of every key area covered in the thesis. Moreover, it will conclude with recommendations.

12.1 Main challenges and dangers

The amount of data in the world continues to increase. As a result of digitalization, data has become an integral part of daily life, and its value has increased accordingly. The growing volume and significance of data presented storage and security challenges. Data attacks threaten the operations of businesses and governments, and cybercriminals generate enormous profits. In addition to the expanding attack surface, a modern arsenal, sophisticated methods, and technological advancements guarantee a continuous step advantage to the cybercriminals. The ransomware and phishing attacks presented deserve special attention. Exposure can be significantly reduced by consciously adhering to the outlined defence mechanisms and cyber hygiene based on the principle of uniformity.

12.2 IT security trainings

Individuals can acquire adequate protection with the aid of online Security Training materials available for free. Self-taught acquisition of easily-understood fundamental knowledge has the potential to significantly enhance social awareness. The most common recommendations from Security Training include using strong passwords, multifactor authentication, regular software updates, backups, and security tools. It is essential to acquire security knowledge, safeguard mobile devices, and take precautions. Achieving the required level of security necessitates implementing uniform protection to close all potential entry points for attackers.

12.3 Current state of IT Security and Security Awareness

Both the frequency and severity of data breaches have increased considerably over the past several years. Typically, human mistake is responsible for the attacks. The cybercrime market is currently so huge that it can compete with the GDP of the world's major nations. "Cybercrime as-a-service" refers to the growing tendency of hackers offering their skills as a service. In recent years, global protection has slowed significantly because of the rise of Covid-19 and the following rise of remote working. The healthcare and energy industries are especially susceptible to cyberattacks, which can devastate businesses, entire communities, and even nations, putting lives in danger. Cybercrime is a relatively new phenomena; hence, its legal

framework and rules are currently in the process of development. According to the offered case studies, even the largest companies aren't immune to fundamental flaws and have difficulties related to compliance. Due to the severe shortage of IT specialists, employee awareness-raising programs are also badly impacted. In their infancy, the GDPR and other regulations show potential for future development.

12.4 The weakest link

The weakest link in the workplace is often the employees themselves. The individual's ignorance impacts not only the personal life and the security of personal information and possessions (such as one’s credit card and bank account) but also the professional life (e.g. managing e-mails, online interfaces, recognizing and responding to IT security threats). The likelihood of mishaps and damages may rise if businesses cannot raise workers' level of awareness and their knowledge of security procedures. Secondary sources demonstrate that individuals often perform poorly even in well-organized workplaces with IT departments, training, and considerable budget. Those who lack access to educational resources on security awareness are among the most susceptible. The primary research findings provide a bleak picture of the current state of society. Very few individuals possess collective knowledge and are competent in all sub-topics. Individuals typically do not perceive themselves at risk and do not view fundamental security measures such as regular software updates, data backups, and password security solutions as essential.

12.5 Final thoughts

The results indicate that the gap between users and attackers is widening. If the trend does not change in the near future, it could have global repercussions. Cyber threats will persist in the near and distant future. To reduce vulnerability, reactive steps should be taken to mitigate risk and then, after consolidation proactive measures should be implemented to stay ahead of hackers. To improve the area, it is worth considering the following.

- Mandating IT security training for businesses and increasing supervision by external bodies. Regular risk assessment and training repetition.
- Modernization and rapid growth of the legal framework and rule systems. Aggressive measures and severe punishments for both individual and organized attacks. Detection and disconnection of malicious hackers in advance.
- State action for social sensitization. It can be achieved through social advertising and free or subsidized training. Introducing social awareness to the education system

or setting conditions for filling positions in critical infrastructure can be considered. The government should distribute IT-related grants to small and medium-sized businesses.

Everyone has a vested interest in IT security. Long-term development of our digital world requires well-coordinated collaboration. And the key to efficiency is none other than awareness.

13. REFERENCES

J. Vaughan, 2019. *Definition data*. [Online]
Available at: https://www.techtarget.com/searchdatamanagement/definition/data
[Accessed November 21, 2022].

Statista, 2022a. *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025*. [Online]
Available at: https://www.statista.com/statistics/871513/worldwide-data-created
[Accessed November 21, 2022].

S. Morgan, 2020. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. [Online]
Available at: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[Accessed November 21, 2022].

US Department of Health and Human Services, 2015. *Information Memorandum ACYF-CB-IM-15-04*. [Online]
Available at: https://www.acf.hhs.gov/sites/default/files/documents/cb/im1504.pdf
[Accessed November 21, 2022].

Merriam-Webster, (n.d.). Cyberattack. In *Merriam-Webster.com dictionary*. [Online]
Available at: https://www.merriam-webster.com/dictionary/cyberattack
[Accessed November 07, 2022].

J. Frankenfield, 2022. *Data Breach*. [Online]
Available at: https://www.investopedia.com/terms/d/data-breach.asp
[Accessed November 12, 2022].

R. Sobers, 2022. *89 Must-Know Data Breach Statistics 2022*. [Online]
Available at: https://www.varonis.com/blog/data-breach-statistics
[Accessed November 12, 2022].

Cisco, (n.d.). *What is a cyberattack?* [Online]
Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
[Accessed November 12, 2022].

IBM, (n.d.). *What is a cyberattack?* [Online]
Available at: https://www.ibm.com/topics/cyber-attack
[Accessed November 12, 2022].

Merriam-Webster, (n.d.). Cybercrime. In *Merriam-Webster.com dictionary*. [Online]
Available at: https://www.merriam-webster.com/dictionary/cybercrime
[Accessed November 12, 2022].

Erdősi, P. & Solymos, Á. (2018). *IT biztonság közérthetően*. Neumann János Számítógép-tudományi Társaság (NJSZT)
Available at: https://nki.gov.hu/wp-content/uploads/2019/03/NJSZT_IT_Biztonsag_kozerthetoen_v3.pdf
[Accessed November 07, 2022].

A. Khagram, 2017. *The motivations of a hacker* [Online]
Available at: https://www.swcomms.co.uk/blog/article/the-motivations-of-a-hacker
[Accessed November 16, 2022].

N. Latto, 2020. *Worm vs. Virus: What's the Difference and Does It Matter?* [Online]
Available at: https://www.avast.com/c-worm-vs-virus
[Accessed November 16, 2022].

IBM, (2022a). *What is ransomware?* [Online]
Available at: https://www.ibm.com/topics/ransomware
[Accessed November 13, 2022].

P. Baltazar, 2022. *What is a Botnet and How it Works?* [Online]
Available at: https://www.malwarefox.com/botnet/
[Accessed November 13, 2022].

A. Efimenko, 2018. *Phishing, Vishing, Smishing, Pharming – What Is the Difference?* [Online]
Available at: https://www.protectimus.com/blog/phishing-vishing-smishing-pharming/
[Accessed November 18, 2022].

Statista, 2022b. *Annual number of data compromises and individuals impacted in the United States from 2005 to first half 2022* [Online]
Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-

the-united-states-by-number-of-breaches-and-records-exposed/
[Accessed November 30, 2022].

Privacy Rights, n.d. *Data Breaches* [Online]
Available at: https://privacyrights.org/data-breaches
[Accessed November 13, 2022].

Sellers, E. (2010). T*he Professional Protection Officer: Security Strategies, Tactics and Trends, Second Edition. Butterworth-Heinemann*
Available at: https://www.sciencedirect.com/topics/computer-science/security-awareness
[Accessed November 15, 2022].

Verizon, (2022). *DBIR Data Breach Investigation Report 2022* [Online]
Available at: https://www.verizon.com/business/resources/Te8d/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
[Accessed November 07, 2022].

CyberEdge Group, (2021). *2021 Cyberthreat Defense Report (CDR)* [Online]
Available at: https://www.herjavecgroup.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1.pdf
[Accessed November 18, 2022].

ForgeRock, 2022. *2022 Consumer Identity Breach Report* [Online]
Available at: https://www.forgerock.com/resource/view/15781
[Accessed November 18, 2022].

Hive Systems, 2022. *2022 Password Table* [Online]
Available at: https://www.hivesystems.io/password-table
[Accessed November 11, 2022].

S. Williams, 2020. *Average person has 100 passwords – study.* [Online]
Available at: https://securitybrief.co.nz/story/average-person-has-100-passwords-study
[Accessed November 20, 2022].

D. Rountree, 2011. *Introduction to General Security Concepts*.
Available at: https://doi.org/10.1016/B978-1-59749-594-3.00001-6.
[Accessed November 20, 2022]

S. Salamun, 2018. *Security Patching is Hard - Survey Results 2017.* [Online]
Available at: https://blog.0patch.com/2018/03/security-patching-is-hard-survey.html
[Accessed November 17, 2022].

BackBlaze, 2021. *The State of Backups: Who's Most at Risk* [Online]
Available at: https://www.backblaze.com/blog/the-state-of-backups-whos-most-at-risk/
[Accessed November 18, 2022].

C. Stouffer, 2022. *Data backups 101: A complete guide for 2023.* [Online]
Available at: https://us.norton.com/blog/how-to/data-backup
[Accessed November 17, 2022]

D. St-Hilaire, 2018. *4 Types of Security Tools that Everyone Should be Using.* [Online]
Available at: https://blog.devolutions.net/2018/02/4-types-of-security-tools-that-everyone-should-be-using/
[Accessed November 26, 2022]

Shred-it, 2022. *Data Protection Report 2022* [Online]
Available at: https://www.shredit.com/content/dam/shred-it/global/documents/Shredit_Data-Protection-Report_2022.pdf.coredownload.pdf
[Accessed November 21, 2022].

Family Lives, 2021. *Digital Footprints* [Online]
Available at: https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints
[Accessed November 22, 2022].

J. Flynn, 2022. *20 Vital Smartphone Usage Statistics [2022]* [Online]
Available at: https://www.zippia.com/advice/smartphone-usage-statistics/
[Accessed November 22, 2022].

World Backup Day, 2022. *Protect Your Data* [Online]
Available at: https://www.worldbackupday.com/en/
[Accessed November 22, 2022].

World Bank, 2022. *United States* [Online]
Available at: https://data.worldbank.org/country/US
[Accessed November 22, 2022].

IBM, 2022. *Cost of Data Breach Report* [Online]
Available at: https://www.ibm.com/downloads/cas/3R8N1DZJ
[Accessed November 6, 2022].

Deloitte, (n.d.). *A vállalati IT kihívásai COVID19 kapcsán {The challenges of corporate IT in relation to COVID19}* [Online]
Available at: https://www2.deloitte.com/hu/hu/pages/technologia/articles/a-vallalati-it-szerepe-az-uzletmenet-folytonossag-fenntartasaban.html
[Accessed December 2, 2022].

Interpol, 2020. *Cybercrime: Covid-19 impact* [Online]
Available at: www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf
[Accessed November 27, 2022].

Graphus, 2022. *The Rise of Cybercrime-as-a-Service Has Major Consequences for Businesses* [Online]
Available at: https://www.graphus.ai/blog/the-rise-of-cybercrime-as-a-service-has-major-consequences-for-businesses-heres-why/
[Accessed November 30, 2022].

M. McGuire, 2018. *Into the Web of Profit – Understanding the Growth of the Cybercrime Economy* [Online]
Available at: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf
[Accessed November 30, 2022].

Digital Shadows, 2020. *From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover* [Online]
Available at: https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover
[Accessed November 30, 2022].

Békés Megyei Katasztrófavédelmi Igazgatóság, (n.d.). *Kritikus Infrastruktúra bemutatása {Presentation of critical infrastructure} [Online]*
Available at: https://bekes.katasztrofavedelem.hu/34105/kritikus-infrastruktura-bemutatasa
[Accessed November 28, 2022].

Thales, 2022. *2022 Thales Data Threat Report Critical Infrastructure Edition* [Online]
Available at:
https://cpl.thalesgroup.com/sites/default/files/content/research_reports_white_papers/field_document/2022-07/2022-Thales-Data-Threat-Report-Critical-Infrastructure-Edition.pdf
[Accessed November 30, 2022].

P. Paganini, 2017. *NATO CCD COE attributed the massive NotPetya attack to a 'state actor' and call for a joint investigation* [Online]
Available at: https://securityaffairs.co/wordpress/60603/cyber-warfare-2/nato-notpetya-state-actor.html
[Accessed November 30, 2022].

L. Kessem, 2022. *Healthcare Breaches Costliest for 12 Years Running, Hit New $10.1M Record High* [Online]
Available at: https://securityintelligence.com/posts/healthcare-data-breaches-costliest/
[Accessed November 30, 2022].

Sophos, 2022. *The State of Ransomware in Healthcare 2022* [Online]
Available at: https://securityintelligence.com/posts/healthcare-data-breaches-costliest/
[Accessed November 30, 2022].

L. Freeman, n.d. *Anthem settles a security breach lawsuit affecting 80M* [Online]
Available at: https://eu.usatoday.com/story/money/business/2017/06/26/anthem-settles-security-breach-lawsuit-affecting-80m/103217152/
[Accessed November 30, 2022].

DNV, 2021. *The Cyber Priority – The state of cyber security in the energy sector* [Online]
Available at: https://brandcentral.dnv.com/fr/gallery/10651/files/original/e45ef6c8-fb14-4b0c-98f3-caa889584cd9.pdf?_ga=2.25929595.716908117.1670357025-64327105.1669586135
[Accessed December 1, 2022].

G. Geller, E. Gonzalez & B. Lefebvre, 2021. *'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack* [Online]
Available at: https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984
[Accessed December 02, 2022].

Varonis, 2021. *2021 Data Risk Report – Financial Services* [Online]
Available at: https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?hsLang=en
[Accessed November 8, 2022].

A. Dellinger, 2019. *Understanding The First American Financial Data Leak* [Online]
Available at: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean
[Accessed November 30, 2022]

V. Anant, L. Donchak, J. Kaplan, H. Soller, 2020. *The consumer-data opportunity and the privacy imperative* [Online]
Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
[Accessed November 27, 2022].

Official Journal of the European Union, 2016. *Document L:2016:119:TOC* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2016:119:TOC
[Accessed December 02, 2022].

European Commission, n.d. *What is a data controller or a data processor?* [Online]
Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en
[Accessed December 02, 2022].

M. Huszár, 2022. *IT-biztonság és biztonságtudatosság* {IT security and security awareness}Google survey [Online]
Available at: https://docs.google.com/forms/d/1I1qi91K7pU5LGrhY86gtDCd7iX0neAbcr9NDQz8oUuA/edit
[Accessed November 20, 2022].

Dmitri Alperovitch, 2011. As cited in *Enter the Cyber Dragon* (M. Gross, 2011). [Online]
Available at: https://www.vanityfair.com/news/2011/09/chinese-hacking-201109
[Accessed November 10, 2022].

14. APPENDIX

Table A1.

Handpicked websites for security tips

www.forbes.com/sites/forbes-personal-shopper/2022/09/27/best-tips-for-cybersecurity-awareness-month/
https://www.btbsecurity.com/blog/top-5-helpful-tips-for-cybersecurity-awareness-month
https://itegriti.com/2022/cybersecurity/tips-to-stay-safe-during-national-cybersecurity-awareness-month/
https://allconnected.com/security-awareness-training-zero-trust/
https://www.trendmicro.com/en_us/ciso/22/i/cybersecurity-awareness-month-3-actionable-tips.html
https://www.securitymetrics.com/blog/5-tips-implement-security-awareness-your-company
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-top-10-cyber-tips.pdf
https://www.ibm.com/ibm/ideasfromibm/zz/en/securesocialsmart/pdf/ibm_cyberattacks_infographic_050112.pdf
https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online
https://www.cybintsolutions.com/10-important-cyber-security-tips-users/
https://www.software.broadcom.com/hubfs/SED/SED%20PDF%20Reports/The_Threat_Landscape_2021_12.pdf
https://www.jpmorgan.com/commercial-banking/insights/12-tips-for-mitigating-cyber-risk
https://www.aon.com/insights/articles/2022/ransomware-epidemic-8-strategies-to-mitigate-risk
https://www.snbsd.com/about/online-safety-guide
https://cybermagazine.com/cyber-security/top-7-security-tips-keep-you-safe-cyber-threats
https://www.align.com/blog/6-ways-to-reduce-the-risk-of-cyber-attacks
https://www.herzing.edu/blog/5-cybersecurity-tips-everyone-should-know
https://dod.hawaii.gov/ohs/sans-security-awareness-top-cybersecurity-risks
https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips

Source: self-edited, 2022

DECLARATION

I, the undersigned MÁRK HUSZÁR aware of my criminal responsibility, I declare that the facts and figures contained in my dissertation correspond to reality and that it describes the results of my own independent work.

The data used in the dissertation were applied taking into account the copyright protection.

No part of this dissertation has previously been used in other training at an educational institution during graduation.

I accept that my dissertation is subject to plagiarism control by the institution.

Budapest, 2022 year 12 month 10 day

student's signature