BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES

ÚSTAV JAZYKŮ

SOCIAL CONTEXT OF CYBERSECURITY

SPOLEČENSKÉ SOUVISLOSTI KYBERNETICKÉ BEZPEČNOSTI

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR
AUTOR PRÁCE

Ondřej Abraham

SUPERVISOR
VEDOUCÍ PRÁCE

PhDr. Milan Smutný, Ph.D.

BRNO 2023

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Bachelor's Thesis

Bachelor's study field **English in Electrical Engineering and Informatics**

Department of Foreign Languages

Student: Ondřej Abraham ***ID:*** 229989

Year of study: 3 ***Academic year:*** 2022/23

TITLE OF THESIS:

Social context of cybersecurity

INSTRUCTION:

Describe how different security events / incidents (dangers and prevention of these phenomena) may affect functioning the society at different levels (state institutions, business, individuals, legal context).

RECOMMENDED LITERATURE:

BOSSOMAIER, Terry R. J., Steven D'ALESSANDRO a R. H. BRADBURY. Human dimensions of cybersecurity. Boca Raton: CRC Press, Taylor & Francis Group, [2020]. ISBN 978-1-138-59040-3.

GUIORA, Amos N. Cybersecurity: geopolitics, law, and policy. London: Routledge, 2017. ISBN 978-1-138-03329-0.

OSULA, Anna-Maria, Bríd NÍ GHRÁINNE, Dan Jerker B. SVANTESSON, et al. Cybersecurity law casebook. Brno: Masaryk University, 2021. ISBN 978-80-210-9773-5.

Date of project specification: 9.2.2023 ***Deadline for submission:*** 30.5.2023

Supervisor: PhDr. Milan Smutný, Ph.D.

doc. PhDr. Milena Krhutová, Ph.D.
Subject Council chairman

Abstract

This thesis deals with the social context of cybersecurity. The objective was to describe how different security events or incidents may affect the functioning of society at different levels, like state institutions, businesses, individuals, and legal contexts. The thesis is divided into four parts. The first chapter describes what cybersecurity is, the dimensions of cybersecurity, the five functions of cybersecurity, why cybersecurity is important for us, who is the enemy, and also deals with cybersecurity history. The second chapter focuses on social networks, social norms like emergent and agreed norms, social media marketing, and trends. The third chapter classifies different types of computer threats and attacks and explains hacker‘s motivations and objectives and the impact of cyberthreats. The last chapter describes cybersecurity strategy with the example of the current EU strategy.

Keywords

Cybersecurity, information, people, internet, social norms, social networks, government security, computer threats and attacks

Abstrakt

Tato práce se zabývá společenským kontextem kybernetické bezpečnosti. Cílem bylo popsat, jak mohou různé bezpečnostní události nebo incidenty ovlivnit fungování společnosti na různých úrovních, jako jsou státní instituce, podniky, jednotlivci a právní souvislosti. Práce je rozdělena do čtyř částí. První kapitola popisuje, co je to kybernetická bezpečnost, dimenze kybernetické bezpečnosti, pět funkcí kybernetické bezpečnosti, proč je pro nás kybernetická bezpečnost důležitá, kdo je nepřítel, a zabývá se také historií kybernetické bezpečnosti. Druhá kapitola se zaměřuje na sociální sítě, sociální normy, jako jsou normy vznikající a dohodnuté, marketing sociálních médií a trendy. Třetí kapitola klasifikuje různé typy počítačových hrozeb a útoků a vysvětluje motivace a cíle hackerů a dopad kybernetických hrozeb. Poslední kapitola popisuje strategii kybernetické bezpečnosti na příkladu současné strategie EU.

Klíčová slova

Kybernetická bezpečnost, informace, lidé, internet, sociální normy, sociální sítě, vládní bezpečnost, počítačové hrozby a útoky

Rozšířený abstrakt

Kybernetická bezpečnost hraje v dnešní neustále rozvíjející se digitalizované společnosti důležitou roli. Její význam neustále roste s novými technologiemi a rostoucí závislostí lidstva na digitální infrastruktuře. Kybernetické hrozby a útoky mohou významně ovlivnit jednotlivce, organizace i společnost jako celek, proto je důležité porozumět jejich sociálnímu kontextu a důsledkům.

Tato práce se zabývá společenským kontextem kybernetické bezpečnosti. Cílem bylo popsat, jak mohou různé bezpečnostní události nebo incidenty ovlivnit fungování společnosti na různých úrovních, jako jsou státní instituce, podniky, jednotlivci a právní souvislosti. Práce je teoretického charakteru, využívá různé zdroje, jako jsou odborné knihy a časopisy, zprávy a blogy. Práce je rozdělena do čtyř kapitol podpořených rešerší z vybrané literatury.

První kapitola pojednává o předmětu kybernetické bezpečnosti a vysvětluje co přesně kybernetická bezpečnost je. Dále také popisuje síť a hardware, které jsou součástí kybernetické bezpečnosti. Zmiňuje také CIA triádu, která je nezbytná k ochraně informaci. Kapitola dále představuje dimenze a pět funkcí kybernetické bezpečnosti. Charakterizuje důležitost kybernetické bezpečnosti a nepřátelé v kyberprostoru. Kapitola je zakončena stručnou historií kybernetické bezpečnosti. Kapitola představuje důležitý teoretický základ kybernetické bezpečnosti.

Druhá kapitola zkoumá interakci mezi sítěmi, sociálními normami a kybernetickou bezpečností. Text dále vysvětluje strukturu sociálních sítí. Diskutovány jsou dvě hlavní vlastnosti sociálních sítí, shlukování a řazení. Dále jsou v kapitole popsány sociální normy jako nepsané kodexy chování, které se liší ve složitosti a významu. Jsou zmíněny i kybernetické standardy Globální komise pro stabilitu kybernetického prostoru a předmět veřejného projevu a státní suverenita při stanovování těchto norem. Kapitola je zakončena trendy a marketingem na sociálních sítích.

Třetí kapitola popisuje nejběžnější typy hrozeb a útoků v kyberprostoru jako jsou malware, phishing, ransomware, cryptojacking, DOS, SQL injection a MITM. Popisuje nezbytné kroky, které mohou těmto útokům pomoct předejít. Dále je také zmíněna motivace hackerů od finančního zisku přes uznání úspěchu, vnitřní hrozby, politické motivy až po státní aktéry. Každé odvětví čelí nebezpečí kybernetických útoků, proto na závěr charakterizuje dopady kybernetických hrozeb.

Poslední kapitola shrnuje koncept strategie kybernetické bezpečnosti a nastiňuje sedm kroků k vytvoření silné strategie kybernetické bezpečnosti. Strategie kybernetické bezpečnosti je flexibilní a dynamický plán na ochranu majetku organizace a minimalizaci kybernetických rizik. Text také popisuje novou strategii kybernetické bezpečnosti EU představenou v roce 2020. Cílem strategie je zvýšit odolnost vůči kybernetickým hrozbám tím, že zajistí, aby podniky a občané měli prospěch z důvěryhodných digitálních technologií.

Na individuální úrovni hraje kybernetická bezpečnost klíčovou roli při ochraně osobních údajů a soukromí. Kvůli rostoucímu množství osobních informací uložených online a rostoucí závislosti na internetu pro osobní, pracovní a finanční transakce jsou lidé často terčem kybernetických útoků. Kybernetické útoky mohou způsobit značné škody, jako jsou finanční ztráty, ztráta důvěry a porušení soukromí.

Pro organizace je kybernetická bezpečnost zásadní pro udržení provozu a ochranu citlivých informací. Od malých podniků po velké korporace a vládní agentury, každý je potenciálním cílem kybernetických útoků. Je nezbytné, aby organizace investovaly do kybernetické bezpečnosti nejen do technologických řešení, ale také do školení zaměstnanců a vytváření kultury kybernetické bezpečnosti.

Také na společenské úrovni může kybernetická bezpečnost ovlivnit národní bezpečnost, ekonomiku a demokracii. Země jsou často terčem složitých kybernetických útoků, které mohou ohrozit kritickou infrastrukturu, jako je energetika, doprava nebo komunikace.

Kybernetická bezpečnost je tedy komplexní a mnohostranný problém, který se dotýká všech aspektů společnosti. Efektivní řešení vyžaduje rozsáhlou spolupráci mezi jednotlivci, organizacemi a vládami a také informovanost veřejnosti o rizicích a opatřeních k zajištění kybernetické bezpečnosti.

ABRAHAM, Ondřej. *Společenské souvislosti kybernetické bezpečnosti* [online]. Brno, 2023 [cit. 2023-05-08]. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/151508. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků. Vedoucí práce Milan Smutný.

Author's Declaration

Author:	*Ondřej Abraham*
Author's ID:	*229989*
Paper type:	*Bachelor's Thesis*
Academic year:	*2022/23*
Topic:	*Social context of cybersecurity*

I declare that I have written this paper independently, under the guidance of the advisor and using exclusively the technical references and other sources of information cited in the project and listed in the comprehensive bibliography at the end of the project.

As the author, I furthermore declare that, with respect to the creation of this paper, I have not infringed any copyright or violated anyone's personal and/or ownership rights. In this context, I am fully aware of the consequences of breaking Regulation S 11 of the Copyright Act No. 121/2000 Coll. of the Czech Republic, as amended, and of any breach of rights related to intellectual property or introduced within amendments to relevant Acts such as the Intellectual Property Act or the Criminal Code, Act No. 40/2009 Coll., Section 2, Head VI, Part 4.

Brno, May 30, 2022 Ondřej Abraham

Acknowledgement

I would like to thank my supervisor PhDr. Milan Smutný, Ph.D., for great guidance, advice, and encouragement throughout the work on this thesis.

Table of Contents

List of Figures

List of Abbreviations

CCNA - Cisco Certified Network Associate

CEO – Chief Executive Officer

CISA - Cybersecurity and Infrastructure Security Agency

CIA - The Central Intelligence Agency

CPU - Central Processing Unit

EU – European Union

IEEE - The Institute of Electrical and Electronics Engineers

IT - Information Technology

KGB – Committee for State Security

NSA - The National Security Agency

NIST - The National Institute of Standards and Technology

URL – Uniform Resource Locator

US – The United States

Wifi – Wireless Fidelity

1.Introduction

The enterprise security in the world is constantly changing, as also how networks and organizations are attacked. These threats and cyber criminals using them are the experts that are hidden from traditional security using their intelligence, resiliency, and patience, which are constantly improving. To control these threats, we need to multiply security disciplines working together with their context. Next-generation security provides the unique visibility and control of, and the true integration of, threat-prevention disciplines needed to find and stop these threats when there is no single solution to the problem of advanced threats on its own.

The aim of this thesis was to describe how different security events or incidents can affect the functioning of society at different levels such as government institutions, businesses, individuals and legal contexts. The thesis was written using different sources such as professional books and journals, news and blogs. The thesis is divided into four chapters supported by a search of selected literature.

2. What is Cybersecurity

The news on the internet or television usually talks about hackers, data leaks, and common things like stolen credit cards, which are all connected to cyber security. Cybersecurity is every technique or tool used to prevent unauthorized activity or illegal use of electronic data. Everyone wants to protect their computer resources from fraudless activity. Nowadays, our daily lives depend on the use of the internet, and that is the reason why cybersecurity is more and more important. The information transferred over the networks and devices has to be secured. There has to be some kind of protection to prevent fraudless activity. The physical infrastructure like electricity or fiber optic cables and the physical security of hardware is also the object of cyber security.

CISA defines cybersecurity in the following way: “Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or illegal use and the practice of ensuring confidentiality, integrity, and availability of information“ [1]. Cybersecurity protects all the data that technology systems like computers and mobile devices collect, store, manipulate or transfer, so all the networks, software, hardware and other devices must be secured and protected.

Kinza and Gillis describe a network as a group of electronic devices like computers and others that are connected and can communicate [2]. Nowadays, many networks are wireless. They allow people to work from home or for children to study at home. Computer networks are also providing services to their customers. The internet is rapidly growing, and it is the largest computer network in the world, with billions of devices connected to it.

Vijay claims that the hardware is the physical connection that creates networks like computers, tablets, routers, and more [3]. The devices such as printers, video cameras, smoke alarms or monitoring systems are also part of the hardware. Fitzgibbons gives a description of the Data as the information stored in information technology systems, and they are communicated over networks. We can divide them into three types: 1) at rest or in storage, 2) in transit, and 3) in use [4]. They have to be protected in each state. Examples of the data can be financial records, budgets, personally identifiable information like names, addresses, driver‘s licenses, or ID numbers, and records of various kinds.

The important part is also maintaining the organization‘s information and its protection from illegal use. Fruhlinger points out that the words confidentiality, integrity, and availability create the CIA triad, and they have served as one of the bedrock principles of the field since the early 1970s [5]. Maintaining the triad should help with the protection from criminal use. Fruhlinger explains the confidentiality as the information only accessible to groups with the proper authorization, while the integrity verifies that the information was not changed improperly, and users can trust it [5]. Availability makes information accessible when people need them. The confidentiality and integrity of information can reinforce each other, but there has to be a balance to ensure that the information will be available as planned.

Confidentiality of data and information is achieved by emphasizing the concepts of authentication and authorization when obtaining the local government‘s information resources. Shacklett describes the authentication as the process that determines whom the users depend on and what they say [6]. It can be executed with strong passwords or new forms of authentication like biometrics, facial recognition, or the nowadays popular multi-factor authentication, which can be downloaded into a mobile phone or laptop. Authorization creates the authority for authenticated users to access information relevant to their job duties, and they do not have access to information outside of their responsibilities. There is also a possibility of encrypting the information to make it confidential or by physical security controls limiting who can access it. Confidentiality means that the users who were properly authenticated can access a local government‘s systems and information.

Fruhlinger definitions of the integrity claim that the information is protected against unwanted changes and ensures users can trust it [5]. It also includes human mistakes and errors, malfunctions, or physical corruption caused by software or hardware problems. Fruhlinger points out that the integrity makes the information accurate and complete in its original form. The data can be corrupted when they are in the process of writing, reading, storing, or transmitting the information, but it is also caused by ignorance and negligence[5]. Physical corruption of hardware can be caused by too much heat or through the prolonged use of a hard drive.

Fruhlinger further explains that the availability makes the information accessible to users when they need it, and to ensure availability, so in order to do that, the information systems

must be working correctly [5]. For example, when the data are stored on the cloud, they need the necessary internet bandwidth to access the information. When there is high traffic, they might not be available. The task may need to be completed more efficiently.

2.1. Dimensions of Cybersecurity

Organizational cybersecurity needs more than the specific technologies utilized by a local government. We can consider it like a cube, where one dimension is the three principles of security (protecting the confidentiality, integrity, and availability of information); the second dimension is the three states of data (at rest, in transit, and in use): and the third dimension involves the three ways of ensuring the CIA of information in its three states through technology, policies and practices, and people.

John McCumber, a retired Air force officer, and former Cryptologic Fellow at NSA, developed the cube of information security for a paper he presented at a conference in 1991. According to McCumber the intent of cube is to establish a comprehensive model for understanding the threat to our automated information systems. This model not only addresses the threat, it functions as an assessment, systems development, and evaluation tool [8].

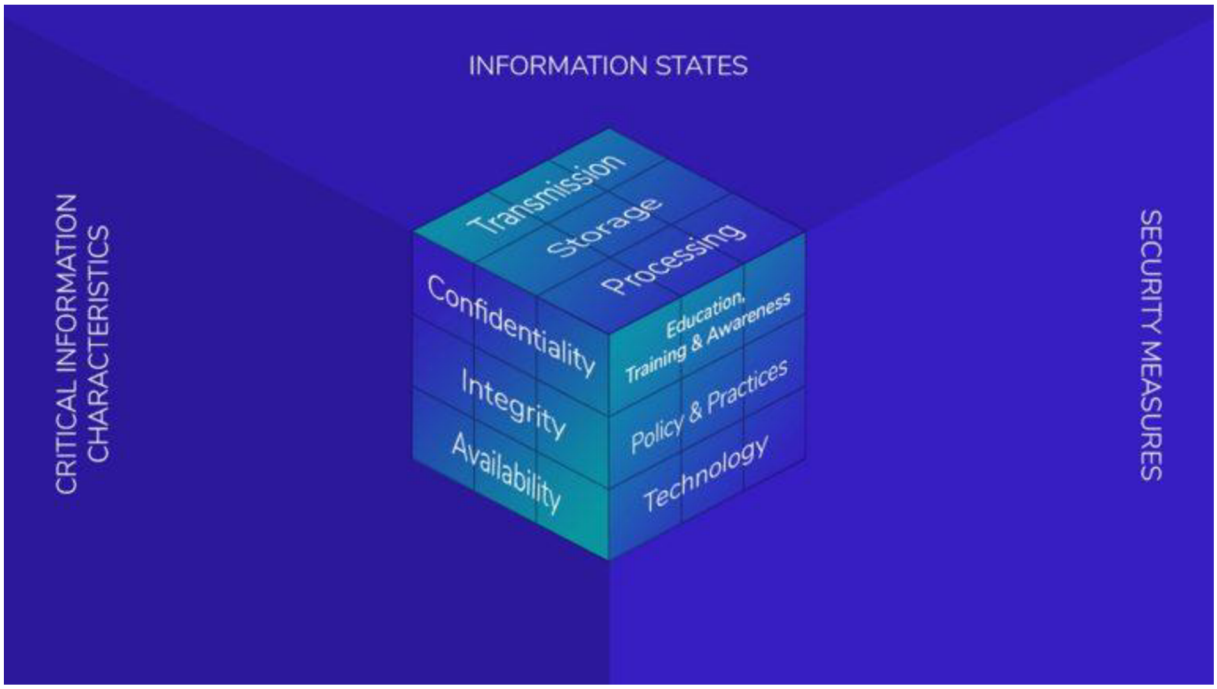

Figure 2.1 Cybersecurity cube (McCumber cube).[7]

The remaining aspects of cybersecurity safeguards that should be mentioned include policies, practices, and people. McCumber explains that these policies, procedures, and practices allow local governments to use information technologies to protect the CIA's information in its three

states. Policies are also written measures that local governments implement through various practices and procedures, which can or can not be specifically established by policy [8]. People develop policies, procedures, and practices and use technologies. According to McCumber, the third cybersecurity safeguard is education, training and awareness [8]. Without cybersecurity education, training, and awareness among staff and officials, local governments can not protect the security of their information resources. All local government employees and officials must be trained in essential cybersecurity awareness. Each aspect of the three dimensions of the cybersecurity cube must be considered when developing and implementing a comprehensive cybersecurity policy. The five functions of cybersecurity address how people are involved in successful cybersecurity operations.

2.1.1 The five functions of Cybersecurity

The five functions of Cybersecurity found in the NIST Cybersecurity Framework form a cycle through which local governments can help protect the confidentiality, integrity, and availability of their information resources by organizing how to accomplish these goals through technology, policies, practices, and people. NIST [9] describe these functions as: Identity, Protect, Detect, Respond, and Recover. They work together in a continuous cycle, with each function reinforcing the other [9].

Figure 2.2 Cybersecurity Framework Functions [9]

When the local government moves through the framework, it can assess its current cybersecurity posture and identify how to improve its cybersecurity and reach its desired level of performance. NIST maintains that the framework puts forth flexible standards and guidelines that can be applied differently depending on the critical infrastructure sector in

which the organization operates. Depending on their local geography, the functions they perform, and the services they provide, local governments will likely be in the cybersecurity issues facing several sectors [10]. Usually, these governments share common concerns with sectors like emergency services, government facilities, healthcare, power, and water/wastewater systems.

NIST points out that the *identify function* involves developing an organizational understanding of the particular cybersecurity risks facing the local government [9]. Assessing a local government cybersecurity posture involves identifying which systems, people, assets, data, and capabilities are involved in supporting critical functions and services. A local government must know the hardware and software it uses before its systems can be protected. It must also develop risk assessment and management plans, as presented in the NIST Risk Management Framework. The Identify functions proceed beyond identifying how the local government currently governs cybersecurity and involves identifying all the stakeholders and the objectives specific to the local government's overall operations. Local governments must first identify risks in order to protect against them.

NIST describes the second *Protect function* as the developing and implementing appropriate safeguards to ensure the delivery of critical services [9]. Local governments must aim to protect their information resources' confidentiality, integrity, and accessibility. This function involves protecting the local government's assets identified in the previous function to prevent adverse cybersecurity events and limit the effects of successful cybersecurity attacks. Examples of basic protocols under the Protect function can be either access management or regular maintenance. Maintenance should occur regularly and accordingly to policy. Cybersecurity awareness training for all system users is also important. Protect requires more technical functions such as system changes, system back-ups, or logs of audits. NIST explains if the local government information systems are under protection with high levels of cybersecurity, they are also under constant attack, which can result in cybersecurity incidents and breaches [9]. Because of this, these systems must be properly staffed, equipped, and managed to perform the Detect function.

NIST points out that the *detect function* means developing and implementing appropriate activities to identify the occurrence of a cybersecurity event [9]. The time to discover a breach

can exponentially increase the amount of damage inflicted. Identifying a cybersecurity breach can take a long time, for example, about 300 days. Anomalous activity on a local government's information systems should usually be detected through continuous monitoring of the network, the physical environment, and employee activity. NIST demonstrates that when the baseline of network activity is understood, then incident alert thresholds can be established, and events can be analyzed for attack targets and methods [9]. Regular testing of these detection methods can improve them.

According to NIST, the *respond function* involves instituting appropriate activities to take action regarding a detected cybersecurity incident [9]. This function includes response planning, external and internal communications, analysis, mitigation, and improvement. When a cybersecurity incident is detected, the response plan must be executed, and procedures must be followed. NIST suggests that the local governments should develop and implement clear personnel roles and responsibilities to ensure quick and effective responses[10] [9]. Event analysis can help to understand the incident's full impact. This includes performing digital forensics, addressing the vulnerabilities found and properly collecting and preparing evidence for possible legal action.

NIST describes that the *recover function* entails utilizing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident [9]. Local governments should maintain resiliency plans for when events occur and update them with lessons learned. The goal is to return to normal operations as quickly as possible and improve the systems

2.1.2 Why do we need Cybersecurity?

One of the main reasons would be that the Internet is fundamentally insecure. ITU states that in Samoa a wide variety of cybersecurity incidents are being reported, ranging from distributed denial of service attack to Internet Fraud [11]. The Internet was originally designed with the thought that only large computers would connect to it. Mainframes were only affordable to large universities, governments, and private sector companies because they were expensive. The Internet was built to allow them to connect with each other.

The identity of the Internet changed mainly during the 1980s and early 1990s because the number of connected computers has grown extremely fast. Firstly there were only computers

connected to the Internet but later, other devices such as mobile devices, elevators, trains, and cameras connected to it. Evans states that the size of the internet is doubling every 5.3 years [12]. There is currently about 91.8% population using the internet in 2023. According to Brown, it is estimated that there will be 75 billion connected devices to the internet by 2025 [13].

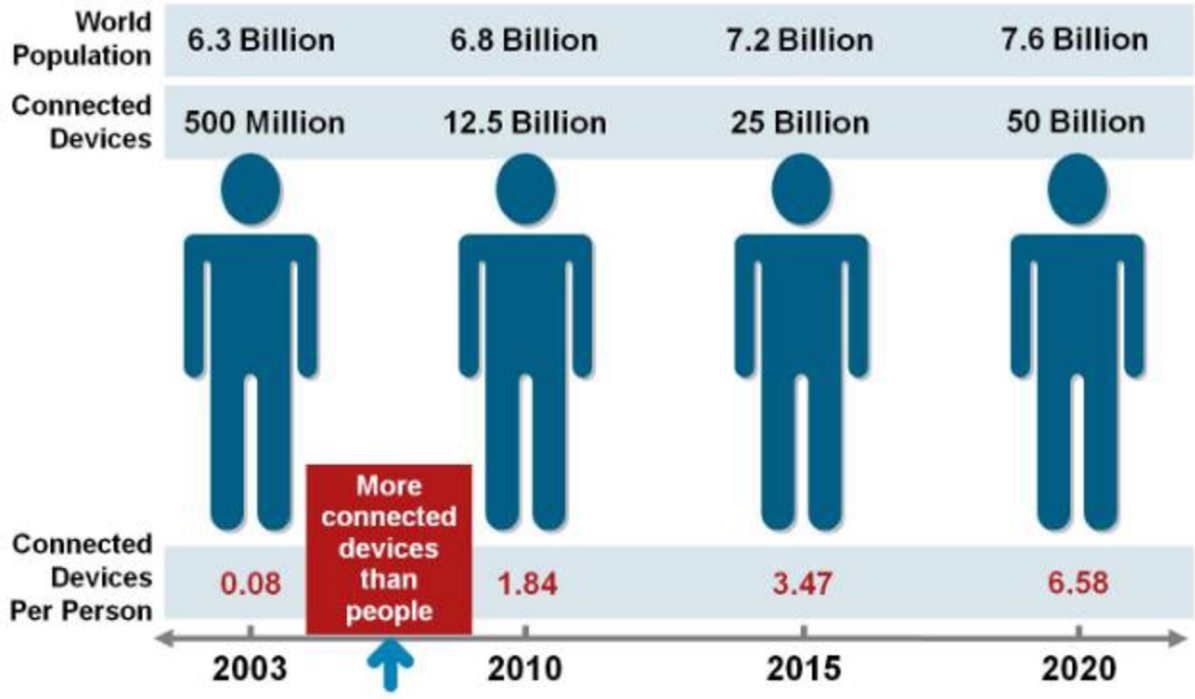

Figure 2.3 Number of connected devices to the Internet [12]

The Internet is nowadays a part of interactions between people and machines. By enabling us to instantaneously send messages, hold phone or video chats, and share documents with individuals around the world, it has completely changed the way we communicate. By offering a vast amount of information, it has also transformed education. Additionally, the Internet offers immediate access to news and information from around the world, enabling users to keep current on events, comprehend many viewpoints, and come to wise conclusions. It is a part of modern society, and many people cannot live without it these days.

Security is one of the essential things on the Internet. Criminals on the Internet are nowadays stealing billions of dollars, and they are also stealing the identities of people. ISBS states that 81% of large companies that took part in the survey in the UK had been breached with the costs of between £600,000 and £1.5 million for each breach [14]. Breaches can damage the

companies but also their users or their money. According to Pascual, Marchini and Miller [15], 16.7 million instances of identity fraud took place in 2017 in the US alone.

Communication via email, voice calls, banking, gaming, shopping, government services, industrial control systems for manufacturing, infrastructure monitoring, border control, and warfare, all of these are happening through cyberspace, and they are vulnerable.

Cybersecurity was designed to prevent interruption and to protect such interactions and services in ways such as maximizing the return on the investments made, preventing financial or damage to the reputation of citizens, businesses, and governments, and enabling compliance with laws and regulations.

2.1.3 Who is the enemy?

There are many enemies in cyberspace. Cyberspace attackers constantly evolve, adjusting to new security measures, and developing new ways to exploit systems. The danger scenario is made more complex by the difficulty of identification and retribution due to the anonymous and open nature of cyberspace.

ITU explains that the cybercriminals are motivated by financial gain when creating and using fraudulent information or selling off valuable information, and industrial competitors can be motivated to gain a commercial or economic advantage for their company or country [16]. Hackers are usually motivated by the intellectual challenge to crack open a system and earn money from their people for doing so. ITU states that activist hackers can be motivated by political or ideological reasons and attack companies to make their point [16]. The other people who got legitimate access to the information and system resources can intentionally or accidentally damage or misuse resources.

Organized crime groups, such as criminal gangs, carry out their operations on a wider scale, carrying out cyberattacks including ransomware attacks, operating illegal online markets, and conducting cyber fraud. These organizations frequently have substantial resources, are organized, and have strong hacking skills that they use to gain access to systems and networks.

2.1.4 History of Cybersecurity

The history of cybersecurity started with a research project in the early 1970s. Bob Thomas working at Bolt, realized that a computer program could move across a network, leaving a small trail [17]. He named the program Creeper, travelling between telex terminals on the early Arpanet printing the message: “The Creeper: Catch me if you can“. The creation of this virus led to the Discovery of the first antivirus. Kopriva describes that Bob’s colleague Ray made the first computer worm with this idea, and then he also wrote another program called Reaper, which was the first antivirus software to chase the virus Creeper and delete him [18].

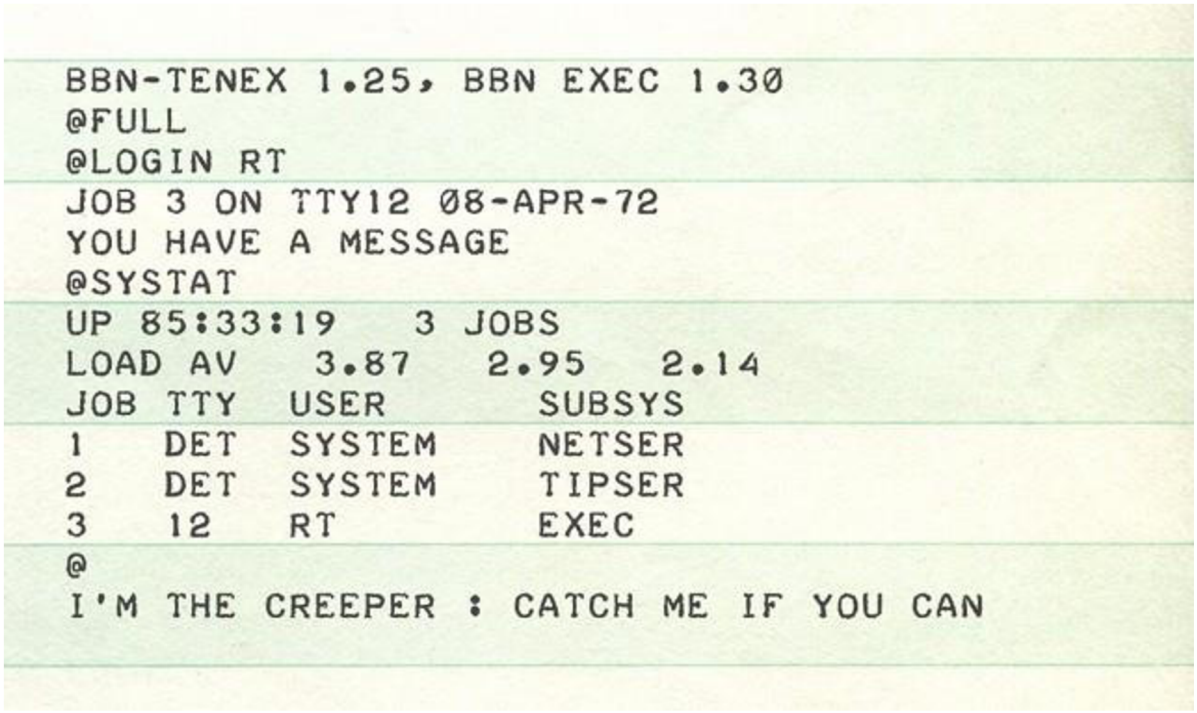

Figure 2.4 Message from the computer virus Creeper [19]

The following major cybersecurity incident between 1976 and 2006 was an Insider attack. Kopriva states that Greg Chung stole over 30 years some US 2 billion dollars of aerospace documents and gave them to China, and 225,000 items of trade secret information were found in his house [18]. This cyberattack included stealing secrets of national importance about aerospace and space technology.

Kopriva claims that in 1986, the German computer hacker Marcus Hess hacked an internet gateway in Berkeley and used that connection to piggyback on the Arpanet [18]. He hacked about 400 military computers, including the Pentagon’s mainframes, to sell their secrets to

the KGB. He was caught by astronomer Clifford Stoll, who deployed a honeypot technique. After this incident, the computer viruses were considered more like a threat.

According to SentionelOne, Late in 1988, Robert Morris wrote a program designed to propagate across networks, infiltrate Unix terminals using a known bug, and then copy itself [19]. His worm replicated such extensive damage that he became the first person charged under the computer fraud and abuse act. After this, viruses started getting more lethal and deadlier, so they were affecting more systems.

In 1994, the first significant financial cybercrime was reported. Hayat [20] states that a Russian hacker group led by Vladimir Levin carried out the attack when they accessed the accounts of several large corporate customers of Citibank via their wire transfer service. They transferred funds to accounts set up by his accomplices in Finland, the United States, The Netherlands, Germany, and Israel. $10 million was fraudulently transferred from the bank into a bank account in Switzerland. Levin was later arrested at Heathrow Airport on his way to Switzerland. Hayat explains that after this attack, Citibank updated its system and started using a Dynamic encryption card using a physical authentication token [20].

Later, in 2012, there was the largest data breach in history to date. Stempel and Finkle [21] describe that Yahoo reported over 3 billion records stolen by the hackers, including names, addresses, passwords, and security questions. The company claimed that the results of the inquiry showed that no clear-text passwords, credit card information, or bank account details were among the stolen data. The data was shielded by outdated, understandable encryption. Additionally, it had backup email addresses and security questions, which might make it simpler to access the users' other accounts. Yahoo failed to report this breach and was fined 35 million dollars by the Security and Equity Exchange in the United States. This breach was the main issue for government legislation in privacy and reporting data breaches in the EU, the United Kingdom, and Australia.

2.2 Summary

Considering how dependent we are on the internet and other linked gadgets daily, cybersecurity is a crucial component of modern civilization. Cybersecurity is preventing unwanted access to and illegal use of electronic data, networks, devices, and systems while

maintaining the confidentiality, integrity, and accessibility of information. The McCumber cube highlights the significance of people, technology, policy, and procedures in sustaining a strong defence by highlighting all aspects of cybersecurity. The five functions of the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover—help local governments and enterprises create successful plans to combat cyberthreats. The internet's explosive growth and inherent vulnerabilities highlight the importance of cybersecurity for shielding people, organizations, and governments from the possible financial, reputational, and legal repercussions of cyberattacks and data breaches. The field of cybersecurity is wide and complex, and it has many adversaries driven by various goals, including financial gain, intellectual challenge, and political or ideological motivations. With the invention of the Creeper virus and the subsequent creation of the first antivirus software, the history of cybersecurity can be traced back to the 1970s. Since then, hackers have grown in size and sophistication, focusing on crucial systems and stealing private data while causing enormous financial harm.

3. Networks and Norms

The social behaviour on the network is essential to our understanding of how viruses and malware spread, and these changes in the social network can respond to this. The information can be spread extremely fast on social networks, which can be used to reduce the impact of a large-scale cyberattack. On the other hand, providing so much information can lead to designing and launching attacks. Social norms can be either ubiquitous or resilient. The problem can occur when they change faster than technology changes, leading to increased vulnerability to cyberattacks.

Even though there is much news about the leaking of passwords and multiple data breaches, some people are still ignoring these messages and not even using strong passwords. It is easy to set up strong passwords nowadays, but many people still prefer to use their favourite food or pet name as a password. Social norms often transcend legal or other imperatives. Social influence mediated by social networks is one of the key factors in forming and maintaining norms.

When browsing the internet, one of the main issues can be the mindset. When they receive an email and are reading it, they can proofread it and miss the essential details, which can negatively impact cybersecurity. For example, a client receives an email from his bank with the logo, and the email looks like the original one. Still, when client clicked on the link inside it, he lost $5 thousand from his bank, and the only difference was that the website had double I at the URL (ceskasporitelna. cz – ceskasporiitelna.-cz) (original website – fake website). For example, this risk can be reduced by information messages from the bank, where they mention the fake website and warn their clients. This can also happen to people with the highest levels of expertise and not only to low-knowledge people.

In 2018 Levary and his colleague published a study in the prestigious journal Science that got potential implications for cybersecurity mindsets. Levary and his colleagues proposed a concept creep across various concepts: dot colour, hostile human faces, and research ethics [22]. This concept says that if we believe that hostile human faces occur about 15% of the time, then if the occurrence drops to 10% after, something surprising happens. People now reclassify some faces as hostile to keep the percentage at 15. Our mindset can consider that unsolicited emails are safe, but some of them can also contain malware. Nowadays, people trust emails and text messages, although some famous people and celebrities have suffered multiple hacker attacks.

3.1 Social Networks

Social networks are a part of everyday life. The most popular Social networks are Facebook, Twitter, Tik Tok, Youtube, and Instagram. People share their lives with others through pictures or videos there, and they can express their own opinion through comments. All theories have three important concepts: small worlds, scale-free networks, and network motifs. Watts and Strogatz [23] proposed a graph theory parlance where are the nodes and the edges that connect them. A node can be anything, from a house in a village to a person in a social network. An edge can be anything that connects nodes together, such as a road between houses. Watts says that there are also degrees, the number of connections a node got with its neighbours [23]. These connections can be directed, called digraphs, or without a direction.

In 1998 Watts and Strogratz [23] introduced the idea of miniature worlds. According to Strogatz and Watts, the nodes have local connections, but some have a local connection

replaced by a long-range connection, which jumps across the network [23]. It can be explained with the example of a country village where everybody knows each other, but some people will know people in other villages. Therefore, everybody is close to everybody else in a small-world network. Watts demonstrates that in a small-world network, most nodes have roughly the same degree and number of connections since the long-range behaviour is created by the small number of distant links [23].

A year after Watts introduced his theory, another theory was introduced by Barabási [24]. Barabási introduced another network with short distances between nodes, but the structure was different, more like an airline network. Barabási points out that the scale-free network has the same property as a hub and spoke network of some nodes with a lot of connections and others with few [24]. In a scale-free network, there is a range of all possible node degrees, but the frequency of occurrence goes down as the degree goes up. It can be explained with the example of followers on the social network Twitter. When the number of followers goes down, the number of people with that number of followers goes up.

The last important thing in characterizing networks is the network motifs. Alon suggests that we should start from small network fragments and build up the network therefrom [25]. He took networks from very diverse systems, from biological cells to society, that particular network fragments were more common than others.

3.1.1 Measure on Networks

A range of methods for inferring structures was developed with social network analysis. Small-world and scale-free networks were mainly concentrated on the degree and the number of connections in and out of each node, but two graphs can have the same degree of distribution and can be different in other ways that require other metrics.

Two critical properties in social networking are clustering and assortativity. Strogatz and Watts claim that the clustering is used to define small-world networks [23]. The small-world network can be a road, map, foodchain or the electric power grid. Gera describes the assortavity, also known as homophily, as the measure of the extent to which nodes that are connected are alike, it is the tendency of individuals to choose friends with similar characteristics [26]. With the knowledge of social network structure, we can communicate with people and modify the network. Networks can have effects on various health conditions. Christakis demonstrates

that if your friends are obese, or if they smoke, you too are more likely than average to be obese or to smoke [27]. This influence extends not just to your friends but their friends and friends of friends

3.1.2 Social Norms

Social norms are usually codes of practice. They are not written down anywhere and do not have legal force. The social norm, according to Burke and Peyton, is a conventional, traditional, or ideal style of behavior that members of a social group attempt to conform to. [28]. There is a constellation of internal and external mechanisms that hold norms in place, and the salience of these factors varies from one situation to another. Social norms can be simple, like taking a gift for someone‘s birthday, to more complex ones as social protocols. Their importance depends on, for example, the society of a country.

Social norms are compelling, even with their uncertain origin. Young and Burke point out that the medical practice may be nonoptimal as a result of local norms [28]. One thinks of medicine as objective or evidence-based, but he disagrees with it because such choices may entail welfare losses for patients due to conformity warp.

It's essential to remember that these norms are constantly changing to keep up with the constantly evolving internet. They are influenced by social, cultural, and technological changes and depend on user behavior as a whole. Understanding and upholding these social standards becomes even more crucial for maintaining a polite, secure, welcoming cyberspace since we are becoming more interconnected through the digital world.

3.1.3 Emergent and Agreed Norms

The Global Commission for the Stability of Cyberspace presented the following set of cyber norms [29]:

- Norm on the Non-interference with the Public Core
- Norm to Protect the Electoral Infrastructure
- Norm to Avoid Tampering
- Norm Against Commandeering of ICT Devices into Botnets
- Norm for States to Create a Vulnerabilities Equities Process
- Norm to Reduce and Mitigate Significant Vulnerabilities

- Norm on Basic Cyber Hygiene as Foundational Defence
- Norm Against Offensive Cyber Operations by Non-State Actors

Mueller argues that there is too much public posturing, and more interest in running out in front of a parade as leaders and getting publicity than in doing the actual work to achieve effective global governance in cyberspace [30]. People should not position themselves to further their status and goals and should create a common institutional infrastructure that can generate effectively, shared rules and procedures. Mueller states that another cause of uneasiness is how national governments are gradually edging aside the multistakeholder community [30]. The state increasingly drives the high-level panels, commissions, and norm proclamations, which are aligned with the state. People from these groups are preferably invited to participate in the meetings of these entities. Norms emerge rather than being developed top-down.

3.1.4 Trends and Social Media Marketing

An important feature on social media is trending. Social media are allowing fashions and fads to spread rapidly and quickly. Some people can use it to share a corporate message rapidly. Famous people can usually help with marketing through their profiles on social media when they are offered sponsorship from big companies offering them free products for advertising. When we say this phone is a trend, we usually mean that most people are buying this phone because it was advertised by famous people and recommended by them to buy it.

However, with the popularity of social media marketing, there are also critical social norms such as terms and conditions, personal cyber hygiene, and distributed trust. If they download an app for their mobile phone or laptop, there is usually a long list of terms and conditions. People usually need to pay more attention to them because it is the only app and blindly agree with them. However, they would read them carefully if they were buying a house or a car. If they download these apps, there can be hidden unpleasant terms, and they blindly agree. For example, most apps contact their maker or vendor when they download them and upload the information about the user. It can be blocked, but only a few people do it. Many applications like Tinder, Facebook, or Instagram can see their location on the map because they are usually sharing it with them via WiFi.

Many corporations ask them for a lot of personal data in order to sign up. People should pay attention to two rules here, the first is to assume if the company needs this information, and the second is if this data will be safe. For example, Uber had problems because of uploading users' contact lists from their mobile phones, and they were in trouble for a massive data breach. Wong states that two hackers obtained login credentials to access data stored on Uber's Amazon Web Services account [31]. Paul Lipman, CEO of cybersecurity firm BullGuard, said that the data were stored unencrypted, which is unforgivable [31].

Bossomaier, D'Alessandro and Bradbury [32] demonstrates that cyber hygiene is connected to the authentication of a computer system with two assumptions connected to this norm: if something goes wrong, somebody else will pay and that you, as the individual, will be the only victim. With weak passwords, hackers can gain entry and compromise an entire system. Bossomaier claims that the password safes are a simple and very effective solution to good password hygiene [32]. Another important thing is trust. Can we trust the analyses and recommendations of other computer professionals? Password safes are rarely used.

The last thing is distributed trust. Botsman points out that the trust in organizations has been declining, such as loss of faith in banks after the Global Financial Crisis but a new phenomenon emerged, distributed trust [33]. A decade ago, it would be impossible for us to trust a stranger to give us a lift like Uber right now or invite a stranger to their home through Airbnb like nowadays. People's reviews also hardly influence us when choosing service providers or goods on the internet. The reviews can be easily faked, but people still believe them when there are many reviews. The emergence of distributed trust has enabled many valuable services to develop.

Distributed trust involves changing societal and economic systems as well as technology. To enable equal involvement and collaboration, it entails shifting the balance of power away from centralized institutions and toward individuals and communities. Distributed trust may offer an appealing approach for creating more reliable and resilient systems in the future in a world where trust, security, and transparency issues are becoming more and more important.

The Bitcoin network is the most well-known example of distributed trust in practice. Bitcoin is a decentralized digital currency that doesn't require a central bank or government to create and control it since trust is built into the system.

3.2 Summary

To understand how cyber dangers, such as viruses and malware, spread, it is essential to appreciate social behaviour on networks and the impact of social norms. Social networks can help prevent cyberattacks but can also be used to start ones. Despite multiple password leaks and data breaches, many people still use insecure passwords and disregard cybersecurity-recommended practices. Their mentality significantly influences the way internet users react to potential cyber dangers. Social networks have assimilated into daily life, but understanding their organizational structure and impact on social norms is important to address cyberthreats successfully. Network motifs, small-world networks, and scale-free networks are all important concepts in network characterization. Social norms, which may be permanent or emerging, greatly influence how people approach cybersecurity. Individuals and organizations must uphold good cyber hygiene and prioritize certain online activities as social media marketing and dispersed trust become more standard.

4. Threats and attacks

Because of the nowadays connectivity and advancements in technology available in our world, threats are evolving to exploit different aspects of these technologies. The applications and services based on the network can create security risks to individuals and to the information of companies and governments. Governments and local governments are constantly under attack. Local governments often lack the funds and skills to defend against such attacks. Hugh states that cyber-attacks can create failures in government, business, and military equipment; they are very dangerous to a nation's security [33]. Cyber threats can change people‘s mindsets regarding their political views. The cyber attacks can be performed with social engineering, bots, malware, computer viruses, spyware, adware, trojan, or drive-by attacks.
CCNA points out that Individuals, governments, and companies are completely dependent on the Internet, and should be protected for this reason [35]. Money and the need for sensitive information is usually the main reason for cyber attacks. The threats can occur because of poor network design, technology weaknesses, misconfigured hardware and software, or the carelessness of the users.

The goals of network security should be to protect confidentiality, maintain integrity and ensure availability [37]. Developing an understanding of what threats can be faced and the vulnerabilities should be looked out for is very important to develop effective defences. The vulnerabilities can also be the main reason for an attacker‘s opportunity why the organizations are targeted.

4.1 Classification of Computer Threats and Attacks

Computer threats and attacks can be classified into several categories. Fruhlinger classifies cyber threats into physical and nonphysical ones [38]. Physical cyber threats can damage the targetted computer or knock it offline, while the nonphysical has the goal of getting access to the target computer’s data and gaining admin privileges on it.

There are several types of attacks, but the most common are the following, as presented in [42] [43] [44]:

- Malware – It is any program or code that is created with the intention to harm a computer, network, or server. It is the most common type of cyber attack, and malware can have many forms like trojan, spyware, virus, worm, or keylogger. Malware breaches a network through its vulnerability when a user clicks on a dangerous link or opens an email attachment that installs software. The prevention from malware attacks can be the newest installed protection software on the computer, having a strong password policy, using a multi-factor authentication or monitoring network for malicious activity.
- Phishing – It is a technique where the attacker uses emails, SMS, phone, or social media to fool a target into doing harmful actions. The targetted user usually downloads malware containing important data or clicks on a fake website pretending to urgently enter his information, where he has to fill in sensitive information like bank information or credit card. Phishing is becoming increasingly popular these days on the internet. The most common phishing attacks are Spear phishing, whaling, SMiShing and Vishing. Preventing phishing attacks is the same as preventing malware attacks, but negligence and awareness are the most important factors here.
- Ransomware – Ransomware is one of the types of malware where the attack encrypts a user‘s data and offers him to provide a decryption key in exchange for money, usually

as cryptocurrency – Bitcoin. Ransomware is usually started through malicious links delivered through phishing emails.

- Denial of service (DoS) – A DoS attack is a malicious attack where the targetted network, system or server is unavailable to the users because of a large number of ping requests. The system is usually unstable for basic tasks like accessing email, websites, and accounts. There is also a second type known as Distributed Denial of Service(DDoS) attack that is launched from multiple systems, while the DoS attack is performed through just one system. DDoS attacks are much faster and harder to block because multiple systems must be neutralized.
- Man in the middle – A MITM attack is a method where the attacker interposes himself between the user and a web service they are accessing. The goal is usually to spy on a target, steal his personal information, data, and banking details or conversate with him and convince the target to complete a transaction or initiate a transfer of funds. A MITM attack can be performed, for example, through public Wi-FI, but it is less common these days because most emails and systems for chat use end-to-end encryption that prevents the third party from joining.
- Cryptojacking – A cryptojacking attack involves forcing the targetted computer to generate cryptocurrency like a Bitcoin for the hacker. The attacker usually installs malware on the computer to perform the tasks or run the code in JavaScript that executes through the browser. The hacker can use network resources to mine a cryptocurrency without the victim knowing about it, so this attack should not be underestimated. The prevention from cryptojacking can be monitoring the CPU Usage of all network devices or training employees to look out for suspicious emails containing Cryptojacking malware.
- Structured Query Language injection (SQL) – A SQL injection attack is specific to SQL databases. The attacker inserts malicious code into a server that is using SQL statements to query the data and forces the server to show information that is not normally visible. The hacker usually extracts the information from a database or can change and erase it. The only prevention from SQL attacks is caution from the side of web developers and care of all inputs.
- Spoofing - Spoofing is a method used by cybercriminals to pretend as a reputable or well-known source. By doing this, the attacker can interact with the target and get

access to their systems or devices to steal data, demand money, or infect the device with malware or other malicious software.

- Supply chain Attack - A supply chain attack is a particular cyberattack that targets a trustworthy third-party provider of goods or services on which the supply chain depends. While hardware supply chain attacks affect physical components for the same reason, software supply chain attacks insert malicious code into an application to infect all users. Software supply chains are particularly vulnerable since modern software often uses pre-made components like third-party APIs, open-source code, and proprietary code from software vendors rather than being created from scratch.
- Zero-day Exploit - A zero-day exploit occurs when cybercriminals identify a vulnerability in popular software programs and operating systems, target the companies that use those programs, and use the weakness to their advantage before the fix gets available. The installation of unknown software onto a victim's computer by attackers can be stopped with the use of Next-Generation Antivirus technologies. Naturally, updating all software will help remove vulnerabilities, and having a tried-and-true incident response plan will help speedy recovery in the case of an infection.
- DNS Tunnelling - A sophisticated attack method, DNS Tunnelling, has been developed to offer attackers continued access to a specific target. Attackers can insert malware into DNS queries, which are DNS requests sent from the client to the server because many businesses ignore to monitor DNS traffic for suspicious activity. Most firewalls cannot identify the persistent communication channel the malware uses to construct. The techniques used automatically to prevent the execution of malware in malicious DNS requests can be assisted by avoiding DNS tunnelling. Additionally, it should enable real-time analysis of all DNS queries to look for suspicious trends and ban locations known for data exfiltration.

Figure 4.1 The example of Ransomware [36]

Computer threats and attacks continue to evolve as technology advances. Individuals and organizations must know these threats and implement robust security measures to mitigate their risks. Essential steps include updating software and operating systems regularly, creating strong and distinct passwords, implementing multi-factor authentication, and raising awareness among users regarding potential threats and the importance of adhering to best practices for maintaining a secure digital landscape.

4.1.2 Hacker's Motivations and Objectives

Fruhlinger states that hackers have their own purposes and objectives [38]. Cyber exploitation capitalizes on existing flaws in a system to circumvent its security defences. The main goal is to penetrate the protective mechanisms of the targeted system. Mottl describes that the most common motivations of the hackers are financial gain, recognition and achievement, Insider threats, political motivation and state actors.

The main driving force behind a hacker's actions is financial gain. Mottl states that this can be achieved through various methods [39]. Hackers might directly access a bank or investment account, steal passwords to financial websites and subsequently transfer funds to their accounts, deceive employees into executing money transfers using sophisticated spear phishing tactics, or launch a ransomware attack against an entire organization.

Adlam claims that hackers like the sense of power and achievement from defacing hundreds of websites [40]. The hackers seek recognition and notoriety, instilling fear and ensuring they are taken seriously. Whether working individually or in groups, these hackers desire acknowledgement for their achievements in breaching major systems. Additionally, cybercriminals are competitive, thriving on the challenges their activities present.

Mottl describes that cybercriminal groups can use their hacking skills to target large organizations [39]. Typically, these hackers are driven by a specific cause, such as raising awareness about human rights issues or exposing vulnerabilities in a large corporation's systems. Alternatively, they may target groups with opposing ideologies to their own. Certain companies engage hackers to acquire confidential data from competitor firms. In such cases, hackers are tasked with identifying vulnerable databases or initiating attacks on the target organization's servers or websites.

According to Adlam, two significant motivations for hackers are human curiosity and the drive to learn [40]. Some of these individuals are novices with no prior experience, seeking to broaden their knowledge and hone their skills. It's important to recognize that not all cybercriminals harbour malicious intentions. Security professionals responsible for safeguarding our data and systems are also referred to as hackers, but they are hackers with benevolent objectives.

Lastly, some cyberthreats have their roots in terrorism, where radicals employ hacking to spread propaganda, gather supporters, plan attacks, or harm their targets. In order to successfully fight the variety of threats in cyberspace, cybersecurity measures must be comprehensive and include technology advancements, education, legal frameworks, and international cooperation.

4.1.3 The impact of cyberthreats

Keshiv describes that a data breach may cause a financial, regulatory, reputational or operational loss [44]. A single, well-coordinated attack has the potential to inflict widespread harm on individuals, including identity theft, financial losses, and emotional distress. Businesses may suffer from diminished confidence, tarnished reputation, loss of customers, financial difficulties, market share erosion, and even the company's collapse. When the scope of such an attack expands to a national level, the consequences can be severe, encompassing threats to national security, significant financial losses, international reputation damage, investment and export declines, political setbacks, and psychological trauma.

Cyberthreats represent the most prevalent category faced by various industries. These industries become vulnerable due to open access channels and networking, which store vast financial and personal information. Connella states that the global economy lost $600 billion due to cybercrime in 2017 [45]. With the increasing profitability of cybercrime, the likelihood of cyber attacks also rises. It is crucial to comprehend the potential short-term and long-term consequences of such incidents on business. As a business leader, the most vital step the leader can take is to both prevent cyber attacks and establish policies and procedures that enable the organization to recover effectively in case of an attack. Connella advises conducting a risk assessment to analyze the present security posture, identify weaknesses that may allow attacks in, and develop a strong incident response strategy to lessen the significant impact of a cyberattack in order to achieve this [45].

Subhani states that every industry is in danger of cyberattacks nowadays [46]. Cyberthreat‘s impact spans various industries, affecting businesses of all sizes and causing significant security costs. Hackers target servers to steal valuable information, gain control over physical machines, compromise software used in employee recruitment, and access employees' personal data. Law enforcement agencies employ similar techniques as hackers to identify and prevent incidents, but hackers continually adapt their methods, making apprehension and protection an ongoing struggle.

According to Safranski, fighting digital piracy is crucial at all levels to safeguard entire industries and the rights and interests of individual content creators and company employees [47]. Piracy in the entertainment industry is particularly damaging, as leaked and stolen music,

movies, and TV series are challenging to recover, and the extent of the damage is difficult to assess. Modern societys reliance on the internet and social media further exacerbates the issue, as these platforms can be exploited for malicious purposes. Individuals often store sensitive documents and personal information on devices that can be hacked, exposing them to significant risks. As cyber threats continue to evolve, industries must adapt and improve their security measures to protect their assets and their users' privacy.

4.2 Summary

Numerous cyber risks and attacks have emerged due to the rapid development of technology and our growing reliance on the internet. To safeguard their assets and maintain their confidentiality, integrity, and availability, people, organizations, and governments must be vigilant in assessing these dangers and putting in place strong security measures. Organizations can create effective defences against various cyberattacks, including malware, phishing, ransomware, and others, by remaining current with the latest threats and vulnerabilities. To lessen the effects of cyberattacks, firms must conduct risk assessments, establish policies and processes for recovery, and develop an incident response strategy. Cyber threats will also continue to develop as technology does. Thus, all parties involved must adjust and enhance their security measures.

5. Cybersecurity strategy

Stone describes a cybersecurity strategy as a plan for protecting an organization's assets and minimizing cyber risk [48]. The cybersecurity plan should be a flexible, dynamic document that can adapt to the shifting business environment and the constantly changing cyber threat landscape. These strategies should be altered and examined as often as necessary, even though they are normally intended to last three to five years. The organization's cybersecurity strategy act as a wide road map, directing important stakeholders as the company and industry change.

Unni claims that seven essential steps can be used to create a strong cybersecurity strategy [49]:

- Performing a security risk assessment – RiskOptics states that cybersecurity risk assessment is a process to evaluate organization's capabilities of safeguarding its IT

systems and data against cyberattacks as well as potential risks to those systems and data [50]. Although the impact of threats can differ significantly between companies, doing a thorough risk evaluation is a crucial first step in identifying the gaps and weaknesses in the company‘s current policies and procedures. Unni points out that risk assessments can assist with identifying risks connected to third – and fourth-party entities, which is essential to establishing complete security in addition to helping to understand the specific risk profile [49]. A security risk evaluation helps companies identify, classify, and arrange their data and information assets according to their importance, in addition to helping them understand the overall risk.

- Defining and establishing security goals – Ellis states that the best way to approach it is to assess current technology capabilities, cybersecurity maturity, and business needs [51]. The cybersecurity goals should be specific, measurable and relevant. Unni describes that setting security objectives might be difficult, but the following questions can make the process easier [49]: What is the organization’s maturity level; What is the organisation’s risk appetite; Are these goals realistic and achievable?
- Assessing the level of technology against Industry best practices - Each company needs to audit its present technology thoroughly. An organization's technology needs to keep up to date with the most recent security patches and updates due to the rapid growth of the tactics, strategies, and procedures used by attackers. Unni explains that a company is more vulnerable to cyberattacks if its technology is out-of-date [49]. An example can be compromised networks because attackers may easily access them due to outdated systems that no longer receive upgrades.
- Choosing a cybersecurity framework – A cybersecurity framework is simply a set of standards, recommendations, and best practices for controlling risks in the virtual world. Ellis explains that NIST’s identify, protect, detect, respond, and recover is an example of a cybersecurity framework, and it is a common security framework that is widely used and is one of the very best [51].
- Reviewing existing security policies and creating new ones - Every business must have a clear and legally binding security policy. Swanagan states that addressing security risks and implementing cybersecurity strategies into practice are the objectives of security policies [52]. Any changes in technology, vulnerabilities, and security needs should be reflected in these policies. Unni explains that addressing appropriate

passwords and privileging identity access management is essential to informing and upholding employees to a high information security standard [49]. Every employee in an organization must be considered responsible for information security, and these security policies must be enforced.

- Creating a risk management plan - The risk management strategy is used by the company's security team to identify potential threats and calculate their probability of occurring. This plan helps the company deal with their potential negative effects on the business.
- Implementation and Evaluation - After the project management or information security team has implemented the cybersecurity strategy, it is critical to recognize the need for ongoing support and evaluation. Unni states that its cybersecurity strategy should be continuously analyzed and examined to verify that it stays in accordance with the current threat landscape as threat actors develop new attack strategies [49].

Creating cybersecurity strategies is crucial for defending an organization against online threats. Organizations can make sure they have the proper controls in place to reduce cybersecurity risks by taking the time to design a cybersecurity strategy. Organizations can further guarantee that their cybersecurity plan is current and successful by routinely examining and upgrading it.

5.1 EU cybersecurity strategy

At the end of 2020 [53], The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy introduced a new EU cybersecurity strategy. The EU Cybersecurity Strategy aims to increase cyber threat resistance while ensuring that enterprises and citizens equally benefit from reliable digital technologies. StandICT describes that the European Union is given more authority by the revised Cybersecurity Strategy to strengthen its influence over global norms and standards for the online environment [54]. Additionally, it improves cooperation with international partners to promote an open, stable, and secure global cyberspace. This digital environment is based on the values of democracy and human rights.

StandICT explains that the Commission will put forth two directives, one on measures for a high common level of cybersecurity across the Union and one on the resilience of critical

entities to address both the cyber and physical resilience of critical entities and networks [54]. They control current and potential online and offline threats, such as cyberattacks, criminality, and natural catastrophes, in a coordinated and complementary way.

Figure 5.1 EU cybersecurity strategy [55]

StandICT explains that the main goal of the new cybersecurity strategy aims to maintain an open, global Internet while simultaneously providing protections that preserve not only security but also European values and everyone's fundamental rights [54]. It offers specific recommendations for using three key instruments, building on the improvements made under the prior strategy. European Union states that these three tools include investment, policy, and regulatory activities, and three areas of EU action will be covered: resilience, technological sovereignty and leadership; operational capacity to prevent, deter and respond; cooperation to advance a global and open cyberspace [53]. Over the next seven years, the EU is committed

to investing an unprecedented amount in the digital development of the EU in order to implement the new cybersecurity strategy.

5.2 Summary

A well-defined cybersecurity strategy is a dynamic roadmap that helps to protect an organization's digital assets and reduce cybersecurity risks. This plan needs to be adjusted on a regular basis to the shifting business environment and threat landscape. A strong cybersecurity strategy is built using a seven-step process that includes assessing security risks, setting security goals, assessing technology against industry standards, choosing a cybersecurity framework, creating and updating security policies, creating a risk management plan, and implementing and evaluating the strategy. This technique has been demonstrated by the European Union (EU) through the introduction of its recently published cybersecurity plan in 2020. The revised plan aims to increase the EU's resistance to cyberthreats while also guaranteeing fair access to safe digital technologies for both citizens and companies. Along with boosting cooperation with international partners to promote a more open, safe, and stable cyberspace, it also enables the EU to establish more control over global norms and standards in the digital world. The plan promotes the ideals of democracy, respect for human rights, and an open internet. Additionally, it offers detailed instructions for the use of three important tools, including investment, policy, and regulatory activities, in three major domains: operational capacity, technical sovereignty and leadership, and resilience. The flexibility of a cybersecurity plan to adapt and change, along with the always-shifting cyber threat landscape, is what makes it effective. This plan must be regularly reviewed and updated if it is to be effective in securing an organization's information assets and reducing risks.

6. Conclusion

The Internet is fundamentally insecure, and the number of devices connected to it has grown extremely fast. Many people cannot live without it, and security is one of the most important things there. Every communication via email, shopping, and voice calls is vulnerable because it is happening through cyberspace. Cybersecurity is protecting such services and interactions and is an essential part of it. Everyone can be an enemy because of high motivation for financial gain or valuable information. Hackers are also paid for cracking a system and earning a lot of money for it.

Cyberattacks and other security-related events can significantly impact various societal aspects, including state institutions, corporations, people, and the legal system. Security events can have a significant impact on state institutions since they may disrupt essential services, cause financial loss, or even threaten national security. Attacks against critical infrastructure, such as power grids or transportation networks, as well as data breaches involving private information held by the government, are examples of these risks. For the purpose of avoiding these possible threats, effective cybersecurity procedures, frequent security audits, and ongoing employee education are essential.

Security incidents can cause significant financial consequences for businesses as well. Long-term consequences like losing customer trust or reputational harm can compound the immediate effects, such as operational disruption or asset theft. Intellectual property may occasionally also be stolen, providing rivals with an unfair edge. Businesses may prevent attacks by implementing comprehensive cybersecurity strategies, keeping their hardware and software up to date, and enforcing strict access control policies.

Security events can personally result in identity theft, financial loss, and serious invasions of privacy for people. This can be extremely upsetting and undermine trust in digital systems. People should keep secure, unique passwords, be on the watch for phishing efforts, keep their electronic devices up to date, and be cautious when sharing information online in order to avoid similar events.

There are better options than providing much information on the Internet because it can lead to launching attacks. Social behaviour on the Internet is essential to understand how viruses

and malware spread. People do not usually pay attention to news about data breaches and use simple passwords, so they are an easy target for hackers. Mindset is crucial on the Internet, and people should pay attention to every email and read it correctly because proofreading can lead to losing a lot of money.

It is important to remember that security incidents can have an impact on society. For example, an incident that initially affects businesses may later affect state institutions, people, and the judicial system. If a company commits a serious offence, new rules may be imposed, which other companies would then have to comply with and which might have an impact on how they operate. If someone's data was compromised in the incident, that person may also be impacted. Therefore, cybersecurity requires a comprehensive strategy.

List of References

[1] Cybersecurity Infrastructure and Security Agency (CISA), US Department of Homeland Security (2019, November 14). Security Tip (ST04-001) What is cybersecurity? Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-001

[2] Kinza, Yasar and Gillis Alexander. (2023). Computer Network. Retrieved from https://www.techtarget.com/searchnetworking/definition/network

[3] Vijay, Kanade. (2022). What Is Network Hardware? Definition, Architecture, Challenges, and Best Practices. Retrieved from https://www.spiceworks.com/tech/networking/articles/what-is-network-hardware/

[4] Fitzgibbons, Laura. (2019). States of digital data. Retrieved from https://www.techtarget.com/searchdatamanagement/reference/states-of-digital-data

[5] Fruhlinger, Josh. (2020, February 10). The CIA triad: Definition, components and examples. CSO Magazine. Retrieved from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

[6] Shacklett, Mary. (2021). Authentication. Retrieved from https://www.techtarget.com/searchsecurity/definition/authentication

[7] Golovatenko, Illya. (2018). The Three Dimensions of the Cybersecurity Cube Golovatenko. Retrieved from https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/

[8] McCumber, J. (1991). Information systems security: A comprehensive model. 14th National Computer Security Conference (pp. 328–337). National Institute of Standards and Technology/National Computer Security Center.

[9] National Institue of Standards of Technology (NIST). (2018). The Five Functions. Retrieved from https://www.nist.gov/cyberframework/online-learning/five-functions

[10] U.S. National Institute of Standards and Technology. (2018, April 16). Framework for improving critical infrastructure cybersecurity: Version 1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[11] ITU. (May 2018). Readiness Assessment Report To Establish A National CIRT For Samoa. International Telecommunications Union.

[12] Evans, Dave. (2011). The Internet of Things - How the Next Evolution of the Internet Is ChangingEverything. Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[13] Brown, Peter. (2016). 75.4 Billion Devices Connected to the Internet of Things by 2025. Retrieved from https://electronics360.globalspec.com/article/6551/75-4-billiondevices-connected-to-the-internet-of-things-by-2025

[14] Information Security Breaches Survey (ISBS) 2014. Retrieved from https://www.focus-on-training.co.uk/blog/gchq-advises-businesses-to-invest-in-information-security-training/

[15] Pascual Al, Marchini Kyle and Miller Sarah. (2018). 2018 Identity Fraud: Fraud enters a New Era of Complexity. Retrieved from https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

[16] ITU. (2018). Readiness Assessment Report To Establish A National CIRT For Samoa. InternationalTelecommunications Union

[17] Buckbee, Michael. (2021). 8 Events That Changed Cybersecurity Forever. Retrieved from https://www.crayondata.com/8-breakthrough-events-in-the-history-of-cybersecurity-infographic/

[18] Kopriva, Jan. (2021). 50 years of malware? Not really. 50 years of computer worms? That's a different story. Retrieved from https://isc.sans.edu/diary/rss/27208

[19] SentionelOne blog, (2019). The History of Cyber Security — Everything You Ever Wanted to Know. Retrieved from https://www.sentinelone.com/blog/history-of-cyber-security/

[20] Hayat, Zia. (2019). 25 Years Later: Looking Back at the First Great (Cyber) Bank Heist. Retrieved from https://www.darkreading.com/perimeter/25-years-later-looking-back-at-the-first-great-cyber-bank-heist

[21] Stempel Jonathan and Finkle Jim. (2017). Yahoo says all three billion accounts hacked in 2013 data theft. Retrieved from https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1

[22] David E Levari, Daniel T Gilbert, Timothy D Wilson, Beau Sievers, David M Amodio, and Thalia Wheatley. (2018). Prevalence-induced concept change in human judgment. Science, 360(6396):1465–1467.

[23] Duncan J. Watts and Steven H. Strogatz. (1998). Collective dynamics of 'smallworld' networks. Nature, 393(6684):440–442

[24] Barabasi, Albert- László. (2003). Linked: The New Science of Networks.

[25] Ron Milo, Shai S. Shen-Orr, Shalev Itzkovitz, N. Kashtan, Dmitri B Chklovskii, and Uri Alon. (2002). Network motifs: Simple building blocks of complex networks. Science, 298(5594):824–827

[26] Gera, Ralucca. (2018). Homophily (or Assortativity). Naval PostGraduate School (NPS). Retrieved from https://faculty.nps.edu/rgera/MA4404/Winter2018/16-Homophily.pdf

[27] Christakis, Nicholas. (2010). Connected: The Amazing Power of Social Networks and How They Shape Our Lives.

[28] Mary A Burke and H Peyton Young. (2010). Social norms. Handbook of Social Economics, 1:311–338,

[29] The Global Commision on the Stability of Cyberspace. (2021). Norms: The Rules of The Road. Retrieved from https://hcss.nl/gcsc-norms/#toggle-id-8-closed

[30] Milton, Mueller. (2018). The Paris IGF: Convergence on norms, or grand illusion? Retrieved from https://www.internetgovernance.org/2018/11/09/the-paris-igf-convergence-on-norms-or-grand-illusion/

[31] Wong, Julia. (2017). Uber concealed massive hack that exposed data of 57m users and drivers. Retrieved from https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

[32] Bossomaier, Terry & D'Alessandro, Steven & Bradbury, Roger. (2019). Human Dimensions of Cybersecurity. 10.1201/9780429490989.

[33] Rachel Botsman. (2017). Who Can You Trust?: How Technology Brought Us Together – and Why It Could Drive Us Apart.

[34] Hugh, Taylor. (2023). What are cyber threats and what to do about them. Retrieved from https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

[35] CISCO Networking Academy. (2008). Cyber security threats, vulnerabilities, and attacks.

[36] Winkler, Ira. (2017). WannaCry: Sometimes you can blame the victims. Retrieved from https://www.computerworld.com/article/3197048/wannacry-sometimes-you-can-blame-the-victims.html

[37] Vulnerabilities, threats, and attacks, chapter 1. Retrieved from http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf

[38] Fruhlinger, Josh. (2020). What is a cyber attack? Recent examples show disrupting trends. Retrieved from www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

[39] Mottl, Camryn. (2022). 6 Motivations of Cyber Criminals. Retrieved from https://www.coretech.us/blog/6-motivations-of-cyber-criminals

[40] Adlam, Stephanie. (2022). All About Hacker Motivation: Why Do Hackers Hack? Retrieved from https://gridinsoft.com/blogs/hacker-motivation-why-do-hackers-hack/

[41] Cisco. (2023). What Is a Cyberattack? Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[42] Baker, Kurt. (2023). 10 Most Common Types of Cyber Attacks. Retrieved from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

[43] Jefferson, Brian. (2023). 15 Common Types of Cyber Attacks and How to Mitigate Them. Retrieved from https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

[44] Kashiv, Mukul. (2019). What is the effect of cyber crime? Retrieved from https://www.quora.com/What-is-the-effect-of-cyber-crime

[45] Connella, Kimberly. (2019). Effects of Cyber Attacks on Business. Retrieved from https://www.anetworks.com/effects-of-cyber-attacks-on-business/

[46] Subhani, Abdul. (2023). Industries At Risk Of Cyberattacks. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2023/02/28/industries-at-risk-of-cyberattacks/

[47] Safranski, Jordan. (n.d). What is the impact of piracy on businesses. Retrieved from https://www.redpoints.com/blog/impact-of-piracy/

[48] Stone, Mark. (2021). What is a cybersecurity strategy and how can your business develop one? Retrieved from https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

[49] Unni, Ajay. (2022). How To Develop A Strong Cybersecurity Strategy. Retrieved from https://www.stickmancyber.com/cybersecurity-blog/how-to-develop-a-strong-cybersecurity-strategy

[50] RiskOptics. (2022). 5 Steps to Performing a Cybersecurity Risk Assessment. Retrieved from https://reciprocity.com/blog/5-steps-to-performing-a-cybersecurity-risk-assessment/

[51] Ellis, Steve. (2023). How to Develop a Cybersecurity Strategy. Retrieved from https://www.office1.com/blog/how-to-develop-a-cybersecurity-strategy

[52] Swanagan, Michael. (2022). How To Plan & Develop An Effective Cyber Security Strategy. Retrieved from https://purplesec.us/learn/cyber-security-strategy/#Review

[53] European Union. (n.d). Cybersecurity Policies. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[54] StandICT. (2020). New EU Cybersecurity Strategy. Retrieved from https://www.standict.eu/index.php/news/new-eu-cybersecurity-strategy

[55] Quointelligence. (2021). EU Council Adopts New Cybersecurity Strategy. Retrieved from https://quointelligence.eu/2021/03/eu-cybersecurity-strategy/