

Aadi Rajesh

Neptun code: SKANN0

Supervisors: László Pitlik & László Pitlik, PhD

Training location (Budapest, Hungary)2025

Kodolányi János University

Kodolányi János University

Risk-evaluation possibilities concerning IT-activities in home-office

Supervisors: László Pitlik & László Pitlik, PhD

Created by: Aadi Rajesh

BPROF in Computer Science Operational Engineering

Training location (Budapest, Hungary) 2025

Acknowledgements

While the learning the IT world is a long, constantly upskilling process, I am deeply grateful to Kodolányi János University for accepting me as part of the bachelor's course in Computer Science Engineer (BPROF) and giving me the opportunity to learn and be part of the Computer Science world.

I would like to sincerely thank all my professors, especially Dr. László Pitlik, Dr. János Rikk, Professor Balázs Erdész, Professor László Pitlik, and Professor Mátyás Pitlik. The professors have been in my learning journey, since my first semester at Kodolányi János University and besides top-quality education, they have taught me the art of seeking excellence and being a constant lifelong learner.

Dear Professors, for your constant guidance, I am forever grateful.

Abstract

Cybersecurity has become a key challenge for companies worldwide and while large and medium sized firms have developed and implemented critical capabilities in cybersecurity prevention and protection, smaller companies are often left vulnerable due to various reasons such as lack of funds, shortage of trained cybersecurity professionals and weak, outdated policies.

The thesis will understand various cybersecurity risks from the past, in the present, and possible risks in the future and explore how smaller companies can not only mitigate the challenges of cybersecurity but also create robust policies and critical capabilities to prevent cyberattacks and its related challenges.

Following the thesis, as part of my Bachelor's project, specializing in cybersecurity, I will propose a risk-parameter matrix and strategies to use AI to create a robust, secure and reliable cybersecurity tool for small companies. The project will also be followed by a software demonstration, using C#, AI tools such as coco-analysis and automated log APIs, to create a working software model for small companies.

Table of Contents:

Chapter 1. Introduction	8
Chapter 1.1 Aims and Objectives	8
Chapter 1.1.1. Hypothesis.....	10
Chapter 1.1.2. Methodology	10
Chapter 1.2. Tasks.....	11
Chapter 1.3. Targeted Groups	11
Chapter 1.4. Utilities.....	11
Chapter 1.5. Motivation	12
Chapter 1.6. About the Structure of the Publication	12
Chapter 2. Literature Review	15
Chapter 2.1. Various types of cyber security threats	15
Chapter 2.2. Theoretical Models for Cyberattacks	17
Chapter 2.2.1. OSI model and TCP/IP Model	17
Chapter 2.2.2. Comparing the OSI and TCP/IP Model	20
Chapter 2.2.3. OSI and TCP/IP Model and my Project	21
Chapter 2.2.4. Other Models	21
Chapter 2.3. Zero Trust Architecture (ZTA)	21
Chapter 2.4. Blue Team and Red Team	22
Chapter 2.5. Cyberattacks on various forms of Technology	23
Chapter 2.5.1. Pre Computer Era	23
Chapter 2.5.2. 2G Technology	23
Chapter 2.5.3. 3G Technology	24
Chapter 2.5.4. Dial-Up Internet.....	24
Chapter 2.5.5. Human Centric.....	24
Chapter 2.5.6. Modern Computers	24
Chapter 2.6. Cybersecurity threats in closed network systems.....	25
Chapter 2.7. Military Grade cybersecurity.....	26
Chapter 2.8. Comparative Cybersecurity Laws worldwide.....	27
Chapter 2.8.1. The United States of America	27
Chapter 2.8.2. The European Union	28
Chapter 2.8.3. The United Kingdom	29
Chapter 2.8.4. India	29
Chapter 2.8.5. Similarities and Comparison.....	30

Chapter 2.9. Future, Quantum-based cybersecurity	30
Chapter 2.10. Cybersecurity in Workspace.....	32
Chapter 2.11. Relationship between Subject and Thesis	33
Chapter 2.11.1. Introduction to Mathematics.....	34
Chapter 2.11.2. Introduction to Algorithms	34
Chapter 2.11.3. Operating Systems	34
Chapter 2.11.4. Introduction to Programming	34
Chapter 2.11.5. Networks and Computer Architecture	35
Chapter 2.11.6. Intercultural Communication.....	35
Chapter 2.11.7. Electronic Circuits.....	35
Chapter 2.11.8. Introduction to Electronics	35
Chapter 2.11.9. System Modelling	36
Chapter 2.11.10. Programming I, II & III.....	36
Chapter 2.11.11. Data Visualisation	36
Chapter 2.11.12. Business Law and Regulation.....	36
Chapter 2.11.13. Globalisation and Social Problems.....	36
Chapter 2.11.14. Databases I and II	37
Chapter 2.11.15. System Operation.....	37
Chapter 2.11.16. ICT Security	37
Chapter 3. Own Developments.....	38
Chapter 3.1. Cybersecurity Project for Small Companies.....	38
Chapter 3.2. COCO Y0 Analysis	44
Chapter 3.3. Practical Use	44
Chapter 3.4. Automation	45
Chapter 3.5. Testing	45
Chapter 3.6. IT Security Aspects	45
Chapter 3.7. Relationship with another Thesis.....	46
Chapter 3.8. Step by Step Elimination	49
Chapter 4. Discussions	51
Chapter 5. Conclusions	52
Chapter 6. Future areas of improvements	54
Chapter 7. Summary	55
Chapter 8. Annexes.....	57
Chapter 8.1. Abbreviation	57
Chapter 8.2. Figures	58
Chapter 8.3. References	59

Chapter 8.4. Conversations with LLMs	67
Chapter 8.5. IKSAD Publication: Aadi Rajesh et. al	73
Chapter 8.6. Software Documentation	86
Chapter 8.7. Screenshots of the Project with My Parameters	91
Chapter 8.8. Coco Analysis and my Excel File	92

Chapter 1. Introduction

“Cybersecurity has become a major pillar of maintaining, safeguarding, upkeeping, and securing the digital, physical and network infrastructure, which has become a crucial aspect of our lives, society and the economy in the 21st century¹.” As the world has become ever more interconnected, the role of securing the cyber space has gained importance for business continuity, education, government administration, human interactions etc.

“Cybersecurity encompasses a wide range of fields, technologies and practices which include securing the physical infrastructure and digital devices, security the networking tools such as wires, care, optic fibres, Wi-Fi router etc. and securing the software’s and human interactions with the digital machines².” This wide spanning world of responsibilities has made the profession highly critical in workplaces and in companies such as mine, cybersecurity professionals hold a key role in not only preventing cyberattacks but also in cost-reputation and business continuity analysis.

“As home offices, e-commerce and digital education has transformed our lives and made the digital world an integral part of our lives, securing the digital world, from malicious actors has become an integral part of cybersecurity and cybersecurity experts, device various defence, offensive and vulnerability testing strategies to mitigate the risks of cyberattacks and prevent cyberattacks from damaging or affecting critical elements of the digital infrastructure³.”

The main goal of cybersecurity experts is to reduce risks and protect systems, networks, and data from cyberattacks, unauthorized access, and other security vulnerabilities. *“Cybersecurity experts achieve this critical goal by implementing and constantly improving security measures, monitoring for threats, responding to incidents, and continuously improving and advancing defences⁴.”*

Chapter 1.1 Aims and Objectives

The Project aims to understand the major cyber security challenges faced by small companies and create a tool, which can help mitigate cybersecurity challenges for small companies.

¹ Vieira, 2017

² Schiliro, 2023

³ Admass et al., 2023

⁴ Cybersecurity Careers of the Future, 2018

“Cybersecurity is a key challenge faced by companies, governments organizations and institutions across the world and has become a key consideration in a company’s security calculations to not only prevent cybersecurity attacks but also preserve market reputation and maintain business continuity⁵.” For smaller companies such as mine, the challenge to mitigate cybersecurity risks is a critical struggle and a constant work in progress.

“While large companies and government organizations are often protected against cybersecurity risks due to high end, often proprietary cybersecurity tools, smaller companies are often more vulnerable to cybersecurity risks. With small companies, the issue is further exacerbated due to various other factors such as lack of funds to develop cutting edge proprietary software, shortage of skills cybersecurity professionals who could dedicate work on security company networks and hardware assets, data scientists and the lack of trainings⁶.”

This major burden, faced by smaller companies is the motivation for my research and project.

“As more and more companies are opting for remote or hybrid work opportunities, workers are enjoying the possibility to work from home or anywhere, which gives them more freedom and a better work-life balance. But this luxury comes at a cost and risk of increased vulnerabilities to cyber-attacks and other challenges⁷.”

“While people are aware of the cyber security risks, a majority of cyber security attacks happen due to human failure⁸.” Therefore, the project focuses on smaller companies, seeking to advance their cybersecurity preparedness and provide a sustainable and scalable tool to early detect cybersecurity vulnerabilities and using targeted trainings and mitigation strategies, close the loopholes and gaps in their cybersecurity infrastructure.

The project focuses on using AI and data analytical tools such as COCO YO analysis to use certain parameters in a risk-attribute matrix and assist the company by finding key security challenges in their digital system. While the project is flexible and scalable to companies of various sizes, as a case study, the project focuses on small firms, with four main assumptions, which are often the four main challenges faced by small client companies, first the client companies have limited funds to procure, deploy and sustain expensive software and

⁵ World Economic Forum et al., 2025

⁶ Small Business Reputation & the Cyber Risk, 2015

⁷ Fenner-Jamieson, 2024

⁸ Kost, 2024

hardware, second, the client companies lack the technical skills to keep the application running, third the client companies lack IT or cyber security professionals as full time employees, and fourth, the client companies have limited knowledge about potential cyber security risks.

Chapter 1.1.1. Hypothesis

My research begins with the following hypothesis, which I would attempt to challenge and verify during the course of my theoretical researcher and practical project.

Using a dedicated risk-attribute matrix and AI-based data analytical modules, we can predict cyber security challenges faced by user.

Chapter 1.1.2. Methodology

The thesis uses qualitative research methodology, and with a literature-based research approach, I studied primary and secondary literature from academic sources, auditing firms, and other sources to establish the grounds of my research and develop a strong methodological and logical framework for the thesis.

Furthermore, under the guidance of professor László Pitlik (Jr.) & professor Dr. László Pitlik, I created a project to assist companies in creating a robust cybersecurity and digital infrastructure. The project has three major approaches, a real life needs analysis approach, a technical approach and a software development approach.

For the real life needs analysis, I focused on challenges faced by small companies due to lack of funds, technical challenges, and inability to hire cybersecurity professionals (See chapter 2.10).

For the technical approach, I focused on selecting the appropriate parameters and attributes, which can be used to quantifiably analyse various aspects of cybersecurity and provide a scientific analysis for observations (See Chapter 3.1).

While Chapter 2 focuses on the literature review on cybersecurity, Chapter 3 focuses on primary research and my project, where using a risk-attribute matrix I identified the key components of cybersecurity and create a working model to identify which attributes affect more, for a particular user and create customized solutions for each worker.

For the software development approach, I used the needs and requirements of a small company, based on the works of Komron Rahmonbek ⁹and the parameters and attributes to develop a scalable software, which could be adapted to personalized needs of small companies and provide regular reports to management for assisting in developing well informed cybersecurity policies (See Annexe 8.5-8.7).

Chapter 1.2. Tasks

The main Task of the thesis and the project is to first understand the theoretical background for cybersecurity risks faced by small companies and then develop an AI based tool and software, which small companies can use to mitigate cybersecurity challenges and maintain a robust, secure and well-functioning cyber infrastructure.

To achieve this, I studied in depth the various scientific and practical approaches to cybersecurity and the special and unique challenges faced by small companies due to limited financial and technological resources and technical expertise.

Chapter 1.3. Targeted Groups

The targeted group for this project is home office workers in small companies. Large and medium sized companies generally have the financial flexibility and resources to buy, create and maintain robust cybersecurity infrastructure and hire professional to upkeep their digital and physical assets. *“Small companies, often work with outdated software without proper updates and trainings, due to which they are often more vulnerable to cybersecurity risks¹⁰.”*

Chapter 1.4. Utilities

The project and the software can help companies to identify major cybersecurity risks in their digital and physical infrastructure and provide targeted trainings and upgrades to mitigate those risks for an overall better cybersecurity infrastructure. While the project is flexible and scalable to companies of various sizes, as a case study, the project focuses on small firms.

“Cybersecurity has a very important role in economics as well. President Obama estimated the economic impact of cyberattacks at over \$1 trillion/year or about 6% of the Gross Domestic Product (GDP) of the United States¹¹.” Furthermore, accordingly the Forbes Technology

⁹ Rahmonbek, 2025

¹⁰ Rahmonbek, 2025

¹¹ AFCEA International Cyber Committee et al., 2013

Council, investing in cybersecurity for firms of all sizes is an overall beneficial return on investment¹². For example, if the fixed cost of running a small business per day is 120 USD for office rent and utilities, 200 USD for employee costs, 50 USD for overheads and 50 USD for rental costs for equipment, the small business will losses this 420 USD per day if a cyberattacks affects business operations. This project can assist companies in not only mitigating cybersecurity risks but also saving costs and protecting business continuity.

Chapter 1.5. Motivation

The motivation for my project for the BPROF thesis, where I create a software, which can assist small companies, in being cybersecurity ready and assist the small companies to take preventive and corrective steps in time, to prevent a major cyber security challenge.

Chapter 1.6. About the Structure of the Publication

The structure of the thesis is as follows.

Chapter 1 includes the introduction and sets the stage for the research, outlining the main goals and objectives. It introduces the hypothesis, methodology, and tasks involved in the project. The targeted groups, including small companies and IT professionals, are identified. The chapter also highlights the motivation for the study and provides an overview of the publication's structure.

Chapter 2 is the Literature Review and discusses various aspects of cybersecurity. It begins with an examination of different types of cyber threats and then moves on to theoretical models such as the OSI and TCP/IP models, comparing and applying them to the project. Zero Trust Architecture (ZTA) is explored as a modern cybersecurity framework. The roles of Blue Teams (defenders) and Red Teams (attackers) in cybersecurity are discussed, as well as how cyberattacks have evolved across different technologies, from the pre-computer era to modern systems.

The chapter continues with a look at cybersecurity in closed networks and military-grade cybersecurity measures. A comparative analysis of global cybersecurity laws in the USA, EU, UK, and India is included. The future of cybersecurity, particularly with quantum-based technologies, is examined, followed by a discussion on cybersecurity in workplace

¹² Return on Investment of Cybersecurity: Making the Business Case, 2024

environments. Finally, the relationship between various academic subjects like mathematics, algorithms, programming, and electronics is connected to the research.

Chapter 3 is about my own developments. This chapter focuses on the author's original work, detailing a cybersecurity project designed specifically for small companies. It includes an analysis of the COCO Y0 model, the practical use of the developed solutions, and the automation of security processes. The testing phase of the project is described, and IT security aspects are discussed. There is also a brief mention of how the author's work ties into other research or theses.

Chapter 4 is about discussions regarding my work. In this chapter, the author reflects on the findings of the research. The results are analysed in the context of the initial hypothesis, and the effectiveness of the developed cybersecurity solutions is evaluated. It includes insights into the successes and limitations of the approach.

Chapter 5 is a concluding chapter. This chapter summarizes the main findings of the research and evaluates whether the initial hypothesis was proven correct. It provides a concise conclusion to the study's objectives and the contributions it makes to the field of cybersecurity.

Chapter 6 is about future improvements and suggestions for further research and potential improvements to the project are made in this chapter. It discusses areas where the current project can be enhanced or expanded upon, including new technologies or approaches that may improve cybersecurity practices.

Chapter 7 includes the summary for my work. This chapter serves as a brief recap of the entire publication, summarizing the research objectives, methodology, findings, and conclusions. It emphasizes the key contributions of the study.

Chapter 8 is for the Annexes. This section includes various supporting materials:

1. 8.1 Abbreviations: A list of acronyms used throughout the publication.
2. 8.2 Figures: Visual elements such as charts, graphs, and diagrams.
3. 8.3 References: A comprehensive list of academic sources and citations.

4. 8.4 Conversations with LLMs: Includes dialogues or interactions with large language models that may have been part of the research process.

This chapter also includes some additional Annexes:

1. 8.5: IKSAD Publication by Aadi Rajesh and others.
2. 8.6: Software documentation related to the project.
3. 8.7: Screenshots of the Project with My Parameters.
4. 8.8: Coco Analysis and my Excel File

To conclude, the thesis is divided in 3 parts, where chapter 2 focuses on the existing literature and the literature review on cybersecurity and in Chapter 3, I present my own risk-attribute matrix, which I created for better cybersecurity protection in small companies as my degree project. Following that, in the Annexes I present a working model for the project, which uses all the theoretical knowledge and base from Chapter 2, the parameters and technical analysis from Chapter 3 of the thesis.

Chapter 2. Literature Review

The chapter deals with major scientific, academic and professional publications focused on cybersecurity and a literature review which helps understand my project better and create the project. By understanding the core of cybersecurity through literature, we can better understand the needs of certain attributes and parameters used in my project, for a better cybersecurity analysis.

Chapter 2.1. Various types of cyber security threats

“As the fourth wave of industrialization brought it a wave of digitalization, it improved human productivity and accelerated societal development through technological innovations. But with this innovation and productivity gain, challenges of cybersecurity also grew¹³.” (See Chapter 3.1). This new and ever-growing cybersecurity threat has challenges not only our assumptions about security in the physical world but also brought in a new dimensions of digital security challenges for companies and individuals across the world.

“Among the first documented cyberattack is the Morris Worm attack in 1988, which was a self-replicating worm and spread across the early internet (ARPANET) and affected thousands of computers¹⁴.” This virus showed the fundamental challenge in the cyberworld, that digital technologies are ever vulnerable to security challenges.

“Since then, as the spread and reach of the cyber domain has grown, cyber-attacks have become more systematic, dangerous, creative and difficult to detect. Cyber security threats can happen at various levels, such as on the hardware level, the software level and the network level¹⁵.” This has become a crucial struggle for companies and individuals across the world and increased the requirements for cybersecurity professionals worldwide.

“While over 1000 types of cyber security threats have been detected and documented in the Common Vulnerabilities and Exposures (CVE) database, some of the most common in small companies include, denial of service attacks, phishing, man in the middle attacks, etc.” Many of the cyber threats, such as Phishing and spams have become a daily occurrence in various offices, especially in my workplace.

¹³ Dahmani, 2024

¹⁴ History of Cyber Attacks From the Morris Worm to Exactis | Mindsight, 2019

¹⁵ The Evolution of Cyber Threats: Past, Present and Future, 2024

At the software level, malware threats, which include viruses, trojans, worms, spyware etc. are used to damage or disrupt a software or steal information from the user. *“Another major attack at the software level includes SQL Injection, where attackers send malicious SQL code to manipulate, delete or copy a database¹⁶.”*

Beyond malware threats and SQL Injection, Phishing and social engineering level attacks are carried out which prey on the victim and use their vulnerabilities to get access to their digital infrastructure.

At the hardware level, among various possible threats, hardware trojans are a major threat, where a specific code can alter the working of a chip and give backdoor access to the attacker. Another common hardware level includes supply chain attack, where a component of a digital ecosystem is replaced with compromised hardware components.

At the network level, Denial-of-Service (DoS), Man-in-the-Middle (MitM) Attacks, Packet Sniffing & Eavesdropping and DNS Spoofing & Poisoning are some common cybersecurity attacks.

In Denial-of-Service (DoS), the access to the internet or a particular webpage is controlled or denied by the attacker using physical blocks. In Man-in-the-Middle (MitM) Attacks, the attacker, listens and even alters the communication between two parties. In Packet Sniffing & Eavesdropping, the attacker captures the network traffic and steals information from the information packets¹⁷.

In DNS Spoofing & Poisoning, the attacker redirects the user requests to malicious and compromised websites, which could steal, alter or delete the user’s data.

Another common network level cyberattack is the Rogue Access Points (Evil Twin Attacks), where the user is tricked to join a rouge Wi-Fi or access point, which steals, alters or deletes the user’s data¹⁸.

“According to a study, conducted by the McKinsey Global Institute in 2014, over 50% small and medium sized companies (SMEs) have been victims of cyberattacks in the USA and over

¹⁶ Luknar & Jovanović, 2024

¹⁷ Luknar & Jovanović, 2024

¹⁸ LPN-0 · Mobile Threat Catalogue, n.d.

60% went bankrupt because of those cyberattacks¹⁹.” “While large and medium companies have invested large sums on developing proprietary anti-virus software and various other cyber security tools regularly conduct cybersecurity trainings and offer refresher courses to their employees., it is the smaller companies and startups, which face the burden of cybersecurity challenges, without proper infrastructure, software or access to expertise²⁰.” This major burden, faced by smaller companies is the motivation for my research and project. (See Chapter 3.1).

Chapter 2.2. Theoretical Models for Cyberattacks

Cyberattacks can happen at various level. The physical level, the software level and the network level. To understand and theorizes the levels of Cyber Attacks, various models have been proposed. Among those, *“the OSI model and the TCP/IP Model are the most popular models used for theoretical analysis²¹.”*

Chapter 2.2.1. OSI model and TCP/IP Model

While various theoretical models have been proposed to better understand and explore the various aspects of cybersecurity, the OSI model and the TCP/IP Model are the most commonly used models. Both the models divide the threats between two layers, namely the network layer and the application layer²².

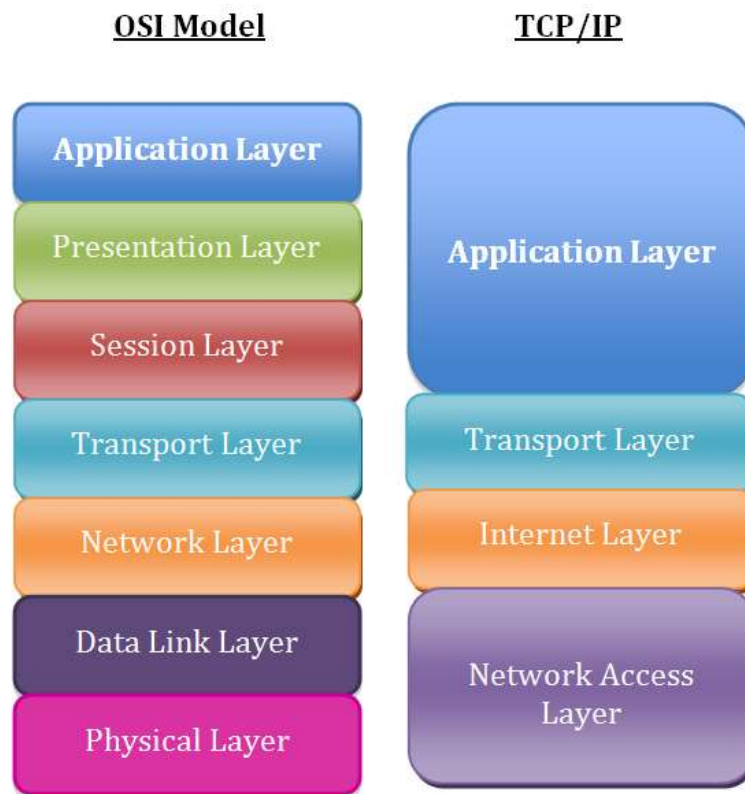
OSI (Open Systems Interconnection) Model and the TCP/IP (Transmission Control Protocol/Internet Protocol) Model, while both are theoretical concepts, they can help better understand the structure and limitations of the cybersecurity infrastructure.

¹⁹ McKinsey Global Institute, 2014

²⁰ Rahmonbek, 2025

²¹ Rao & Nayak, 2014

²² Rao & Nayak, 2014



Source: Chunte7, CC BY-SA 3.0 <<https://creativecommons.org/licenses/by-sa/3.0/>>, via Wikimedia Commons,

https://upload.wikimedia.org/wikipedia/commons/d/d7/Application_Layer.png

Chapter 2.2.1.1. OSI Model

“The OSI model is divided into 7 layers, namely the Physical layer, the Data Link Layer, the Network Layer, the Transport Layer, the Sessions Layer, the Presentation Layer and the Application Layer²³.”

Layer 1 is the Physical layer, which deals with the physical connections between devices, such as wires, cables etc. The layer ensures the transmission of data through electrical, optical or radio signals. The cybersecurity risk in this layer is this layer include physical damage, physical unauthorized access such as tapping etc.

Layer 2 is the Data Link Layer, which assists and manages the communication between adjacent network nodes. The layer uses MAC addresses for device identification. The cybersecurity risk in this layer includes MAC spoofing, where the MAC addresses of the victim

²³ An Overview of the OSI Model and Its Security Threats, 2023

is cloned and used and ARP poisoning, where a malicious ARP package is sent over the Local Area Network (LAN).

Layer 3 is the Network layer, which handles routing and forwarding of data packets between networks. The layer uses IP address for device identification. The cybersecurity risk in this layer includes IP spoofing, where the IP address of the victim is cloned and used, and the Distributed denial-of-service attacks (DDoS attacks), where normal traffic to the internet is disrupted.

Layer 4 is the Transport layer, which ensures reliable data transfer between devices. It uses various protocols such as the TCP, for physical connections and UDP, for wireless connections. The cybersecurity risk in this layer includes SYN flood attacks, where there is an attempt on denial of service for the user, and session hijacking, where the session is cloned and used to gather information and hijack the communication system.

Layer 5 is the Sessions layer, which manages sessions between applications. Its main function to help is session authentication and session restoration. The cybersecurity risk in this layer includes session hijacking, where the entire or part of a session is hijacker and replay attacks, where a part of the session is replayed to gather data maliciously.

Layer 6 is the Presentation layer, which is responsible for translating data from binary to low level or even high-level language and encrypting and decrypting data. The cybersecurity risk in this layer is data corruption or leaks due to weak encryption.

Layer 7 is the Application layer, which provides network service to applications through protocols such as Hypertext Transfer Protocol (HTTP), Secure Hypertext Transfer Protocol, (HTTPS), File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP). The cybersecurity risks in this layer includes phishing, SQL Injection, where a malicious code is passed, which can manipulate or destroy a database, malware transfer and DNS spoofing, where the user is directed to fraudulent and malicious websites.

Chapter 2.2.1.2. TCP/IP Model

“While the OSI model presents a detailed theoretical framework, the TCP/IP model presents a more practical, real-life oriented model²⁴.” The TCP/IP Model is divided into 4 layers, namely

²⁴ Yang, n.d.

the Network Interface (Link) Layer, the Internet Layer, the Transport Layer, the Application Layer.

Layer 1 is the Network Interface (Link) Layer, which is equivalent to OSI Model Physical and Data link layers. The layer manages physical transmissions and connections and MAC addresses. The cybersecurity risk in this layer included, packet sniffing, where the data of a packet is accessed and analysed by unauthorized party and ARP poisoning.

Layer 2 is the Internet Layer, which is equivalent to the Network layer in the OSI model. The layer uses IP address and routes data packages across the network. The cybersecurity risks in this layer include IP spoofing and DDoS attacks.

Layer 3 is the Transport Layer, which is equivalent to the Transport layer in the OSI model. The layer uses various protocols such as TCP and UDP to ensure data delivers to the correct device within a network. The cybersecurity risks in this layer include, Port scanning, which is method to detect which ports in a network are open and could receive or transport data and Denial of service attacks such as SYN flood attacks.

Layer 4 is the Application layer, which merges three layers in the OSI model, namely, the Sessions layer, the Presentation layer and the Application layer.

The cybersecurity risks in this layer include SQL injections, phishing and malware attacks.

Chapter 2.2.2. Comparing the OSI and TCP/IP Model

“While the OSI model provides a more detailed theoretical framework, the TCP/IP model is preferred in real life and has become more popular due to its practical approach by joining the similar layers in the OSI model into single layers, thus reducing the number of layers²⁵.”

Besides the OSI and TCP/IP models, various other models have been developed at the academic, scientific or corporate levels, to develop realistic frameworks and address the complexities of network architecture, communication networks, hardware and software.

²⁵ Rao & Nayak, 2014

Chapter 2.2.3. OSI and TCP/IP Model and my Project

The OSI and TCP/IP Models have a significant application in my own project. (See chapter 3). Various attributes used in my project directly fall in the layers presented by the OSI and TCP/IP Models, which help in targeted cybersecurity analysis in my project.

Attributes such as Layers of the Firewall fall on the TCP/IP Application layer and the OSI model Network Transport and Application layers, while attributes such as Total amount of data downloaded in the last week follow the TCP/IP Transport layers and the OSI Transport layer as well. (See Chapter 3.1).

Chapter 2.2.4. Other Models

"Some popular models besides the OSI and TCP/IP models include, the DoD Model (Department of Defence Model), which is also known as the ARPANET Reference Model. The ARPANET model was developed by the US Department of Defence. The model focused on encryption and strict security protocols and also included protocols for war and other server conditions²⁶."

Chapter 2.3. Zero Trust Architecture (ZTA)

"Another modern model is the Zero Trust Architecture (ZTA). The architecture works on the principles of "Never Trust, Always Verify.". The Zero Trust Architecture assumes that all devices can be a potential attacker, including the ones within a secured network. The model revolves around strict entry principles of verifying a device thoroughly before gaining access to the network and giving least privilege access and divides the network into smaller isolated zones, with strict entry rules and sometimes no entry at all. This also follows continuous monitoring of all the devices witing a network and remove access in real time²⁷."

"Although the model has presented itself as a viable alternative to the TCP/IP and the OSI models, it is very restrictive and costly due to the continuous monitoring and encryption architecture. Using open internet on this architecture would be challenging and bring in integration issues for various users and their devices²⁸."

²⁶ ARPANET, 2014

²⁷ What Is Zero Trust Architecture?, n.d.

²⁸ Sweny, 2024

Understanding the Zero Trust Architecture is crucial for future developments of my project (See Chapter 3) as according to client needs, the project can also offer ultra-secure communications and data storage options.

Chapter 2.4. Blue Team and Red Team

“In Cybersecurity, the domain expertise is divided into two sections, known as the Blue Team and the Red team. While both the teams, perform a different task, within the large cybersecurity domain, their tasks complement each other for improving the overall cybersecurity infrastructure²⁹.”

Understanding the Blue team and Red team concept is crucial for my project (See Chapter 3) as the project works in sync with cyber security professionals and with the help of cybersecurity professionals, the interpretations of the result of the project can be done better.

The red team is responsible to stimulate real life attack scenarios and test the security vulnerabilities of an organization. Among various others, their key objective is to identify vulnerabilities, exploit weaknesses, and assess how well the company can withstand attacks.

Various strategies used by the red team include, ethical hacking & penetration testing social engineering like phishing, exploiting software, hardware, and network vulnerabilities and simulating insider threats.

The blue team is responsible for preventing the cyberattacks by creating various preventive and defensive strategies. Among various others, their key objectives include strengthen security, prevent breaches, and responding effectively to threats.

Various methods used by the blue team include, penetration testing, threat monitoring & intrusion detection, incident response & forensic analysis, implementing firewalls, IDS/IPS, and security policies Security awareness training for employees³⁰.

Beyond the red and blue teams, there are also purple teams, which include aspects of both red and blue teams and provide a holistic approach towards cybersecurity³¹.

²⁹ Murphey, 2024

³⁰ Murphey, 2024

³¹ Murphey, 2024

Both Red team and Blue team together are part of a larger group of ethical hackers. Ethical hackers are professional cybersecurity experts, who exploit the weakness of the digital infrastructure to find issues and propose solutions. *“In the 21st century, the role of ethical hackers has become essential. Companies, government agencies and institutions employ ethical hackers for not only cybersecurity prevention, but also creating a robust, infrastructure and conduct trainings for employees³².”*

Various startups and consultancy firms have also created cybersecurity testing, analysis, training policy advice as a product and have become an essential part of not only the tech ecosystem but also the international economy at large³³.

Chapter 2.5. Cyberattacks on various forms of Technology

While cybersecurity is often associated with modern day computers and digital world, privacy and challenges with information security have been a major concern for every technology throughout the centuries. By understanding the various cybersecurity risks throughout history, a better understanding of cybersecurity could be achieved in my project (See Chapter 3) as companies use various old and new technologies parallel in their operations.

Chapter 2.5.1. Pre Computer Era

In pre-computer era, radio signals and telegraphs were a common form of communication, which were vulnerable to eavesdropping, denial of service and jamming risks. Radio signals and telegraphs could also be intercepted and given unauthorised access to information. In walkie talkies, or two-way radios, vulnerabilities similar to radio signs were present such as eavesdropping, jamming and denial of service. These devices used open analogue frequencies, which also had minimal encryption, making them vulnerable to information leaks and exploitation³⁴.

Chapter 2.5.2. 2G Technology

In 2G Phones, which are GSM based phones, better encryption was offered, but they were highly vulnerable to IMSI catchers (Stingrays attacks), where the victims calls and SMS could

³² SentinelOne, 2024

³³ Global Cyber Security Network, 2025

³⁴ Heinaaro, 2015

easily be intercepted, blocked, or eavesdropped. *“The weak authentication in 2G phones and the SIM cards used also posed the vulnerability of device cloning and spoofing³⁵.”*

Chapter 2.5.3. 3G Technology

In 3G Phones, much stronger encryption techniques were used, but due to design flaws, the devices were highly vulnerable to man in the middle attack and eavesdropping. *“Security flaws in many 3G phones also allowed unauthorized tracking and spying³⁶.”*

Chapter 2.5.4. Dial-Up Internet

Beyond the phones, during the dawn of the modern internet, dial-up internet connections, which made up majority of networks across the world between 1990s and early 2000s also faced various cybersecurity risks. *“Dial-Up Internet Computers didn’t have any firewall by default, which made them highly vulnerable to various cyber-attacks. They were also highly vulnerable to malware, spoofing, tracking and phreaking attacks, which were cyber-attacks over the telephone lines³⁷.”*

Chapter 2.5.5. Human Centric

Also, beyond the technical challenges, human centric cyber security challenges such as fake and spam calls, malware updates in the shadow of software updates, social engineering through manipulative calls, messages, advertisements etc. became a common challenge. *“Furthermore, weak encryption and authentication in Dial-Up Internet Computers led to hacking, data manipulation and spying³⁸.”*

Chapter 2.5.6. Modern Computers

Modern computers, post the era of Dial-Up Internet Computers, improved significantly in cyber security through enhanced encryption, multi-layer authentication and modern cyber security and preventive software. But despite the constant innovations and upgradations, challenges remained and still remain with modern computers and modern networking solutions³⁹.

³⁵ Security, 2024

³⁶ Security, 2024

³⁷ Troy & NATL INST OF STANDARDS & TECH R.I.C., 1986

³⁸ International Modem Dialing Scams, 2020

³⁹ Admass et al., 2023

“Modern computers and networks face cybersecurity risks such as phishing, ransomware, denial of service attacks, cloning of devices etc⁴⁰.” While the advancements in artificial intelligence and machine learning have made defensive software and cyberattack detection faster and more advanced, because of the advancements in AI, with artificial intelligence and machine learning, cyber-attacks have also become highly sophisticated and multi-layered, which have brought in a new set of challenges for cybersecurity experts.

Furthermore, modern technologies such as cloud computing and internet of things have brought in a new era of cybersecurity vulnerabilities, which have caused severe challenges to the cybersecurity infrastructure and challenged the core cybersecurity principles and techniques⁴¹.

Chapter 2.6. Cybersecurity threats in closed network systems

While Cyber security has traditionally been limited to the physical and digital domain of computer connected over open access internet, with new technologies, even closed networks have become target of cyber security attacks⁴².

Understanding the cybersecurity in closed network systems is crucial for future developments of my project (See Chapter 3) as according to client needs, the project can also offer ultra-secure communications and data storage options, in critical areas of operations.

Closed systems, are isolated from external networks such as the internet and external devices and were often considered safer and more secure. They are used in military installations and in critical infrastructure such as nuclear power plants, dams, irrigation networks, electricity generation plants, coal plants etc.

“But with the advancements of technologies, closed systems have also become vulnerable to cyber security attacks. Some forms of cybersecurity threats in closed systems include, Insider threats, Supply chain attacks, Electromagnetic (TEMPEST) Attacks, Removable Media Infections, Physical Security Breaches, Social Engineering, Firmware & Hardware Exploits and Maintenance & Update Risks⁴³.”

⁴⁰ Perwej et al., 2021

⁴¹ Admass et al., 2023

⁴² Makrakis et al., 2021

⁴³ What Is a Supply Chain Attack? | CrowdStrike, n.d.

Insider threats happen when negligent or malicious employees, use their position and access to inject malware into the closed system. This malware could edit, delete, copy or manipulate information or commands in the closed system. *“Edward Snowden’s case is a classic example of Insider threats, where he used his position to leak classified data from closed systems⁴⁴.”*

Supply chain attacks happen, when the software or hardware procured already had malware or backdoor access by design. *“The SolarWinds attack of 2020 in the United States is an example of such cyberattack, where hackers, installed backdoors, into a software update, and gained access to closed systems⁴⁵.”*

Electromagnetic (TEMPEST) Attacks is a highly sophistic cyber-attack strategy, where valuable data and information can be extracted by analysing the electromagnetic emission from a hardware, even if it’s in a closed system. *“In the 1980s, Dutch scientist Wim van Eck demonstrated that by analysis electromagnetic emissions of the computer hardware, even from a distance, actual screen data could be regenerated⁴⁶.”*

Removable Media Infections happen when an infected USB stick or CD is inserted in a closed system⁴⁷. *“An example of such type of cyber-attack is when in 2010 in Iran, the nuclear program was affected by the Stuxnet worm, injected through a USB stick⁴⁸.”*

Chapter 2.7. Military Grade cybersecurity

Military grade cybersecurity works on the following principles, it uses quantum encryption for ultra secure communications. The Military grade infrastructure employs a Zero trust architecture (ZTA) which ensures verification and re-verifications at every level. It employs air gapped, closed system networks, to prevent any outside access or communication. It uses AI to predict and test vulnerabilities in the system and gaps in logic. *“Military level cybersecurity also involves highly trained cybersecurity experts and well tested and reliable software, hardware and supply chains⁴⁹.”*

⁴⁴ Cisomag, 2020

⁴⁵ Kerner, 2023

⁴⁶ Grey Dynamics, 2025

⁴⁷ USB Attacks: The Threat Putting Critical Infrastructure at Risk, n.d.

⁴⁸ Kushner, 2024

⁴⁹ U.S. Department of Defense, n.d.

But despite, the well calibrated strategies of military grade cybersecurity, there are always vulnerabilities, which are actively exploited by attackers and often exploited.

Understanding military grade cybersecurity is crucial for future developments of my project (See Chapter 3) as by following certain protocols from military grade protocols, such as “Never trust, always verify” even companies can create a more robust cybersecurity infrastructure.

“The NSA Data Breach (2016) is an example of such an attack, when despite having military grade cybersecurity measures, the attackers could exploit the system and steal information on top-secret cyber weapons. The hackers used various forms of cybersecurity attacks in closed systems and breached NSA’s systems and leaked the details of top-secret cyber weapons⁵⁰.”

Till date, the NSA has not been able to understand how and which vulnerabilities the attackers exploited, and an investigation is still ongoing since 2016⁵¹.

Chapter 2.8. Comparative Cybersecurity Laws worldwide

All major nations across the world have created their own versions of cybersecurity laws, to match their security needs and requirements. The section will discuss and compare the cybersecurity laws in some major countries. Understanding the various cybersecurity laws is crucial for future developments of my project (See Chapter 3) as it is critical to follow all protocols and cyber laws in the country of operations and adapt best practices from various parts of the world.

Chapter 2.8.1. The United States of America

In the United States, various laws such as the Cybersecurity Information Sharing Act (CISA) (2015), focuses on sharing cyber threat information and data between the government and private companies. Health Insurance Portability and Accountability Act (HIPAA) focuses on securing healthcare data and patient’s records. Gramm-Leach-Bliley Act (GLBA) focuses on consumer data held by private companies, Federal Information Security Modernization Act (FISMA), this law deals with the storage and use of data of federal agents and various state level laws, such as the California Consumer Privacy Act (CCPA), which focuses on the data privacy of all residents of California⁵².

⁵⁰ Schneier, 2016

⁵¹ Biggest Data Breaches in US History (Updated 2025) | UpGuard, n.d.

⁵² Cybersecurity Laws Every Business in the US Should Know About, 2025

Being the centre of global geopolitics and the largest economy of the world, the United States is a major centre of cyber security attacks. Some major cyber security incidents include JPMorgan Chase Data Breach (2014)⁵³, Equifax Data Breach (2017)⁵⁴, Colonial Pipeline Ransomware Attack (2021)⁵⁵ and SolarWinds Cyberattack (2020-2021)⁵⁶.

Chapter 2.8.2. The European Union

In the European Union, laws such as the General Data Protection Regulation (GDPR) have become the backbone of data privacy for all residents of the European Union. GDPR follows strict data protection with laws on data protection, sharing and consent.

According to the GDPR, organizations must implement security measures from the outset of any system development, ensuring data protection is a built-in feature rather than an afterthought.

A major success of the law is that GDPR needs to be observed even beyond the borders of the European Union. Furthermore, GDPR mandates the reporting on any cyber-attack within 72 hours and has strict noncompliance penalties which range from Up to €20 million or 4% of global annual turnover, whichever is higher⁵⁷.

Besides the General Data Protection Regulation (GDPR), various national governments have implemented some more laws, such as the Federal Data Protection Act, in German Bundesdatenschutzgesetz (BDSG)⁵⁸ and the French Data Protection Act (Loi Informatique et Libertés)⁵⁹ go beyond the GDPR with stricter compliance and penalties.

Beyond the GDPR, in the EU, the NIS 2 (Network and Information Security Directive) is a strong unified legal framework which is developed and implemented to uphold cybersecurity in 18 critical sectors across the EU. Sectors such as Energy generation, transmission and distribution, Transportation sector including air, rails, road and waterways, health sector,

⁵³ Rushe, 2017

⁵⁴ Center, n.d.

⁵⁵ The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA, 2023

⁵⁶ Kerner, 2023

⁵⁷ Regulation - 2016/679 - EN - Gdpr - EUR-Lex, n.d.

⁵⁸ Federal Data Protection Act (BDSG), n.d.

⁵⁹ La Loi Informatique Et Libertés, n.d.

public administration etc. are covered under the NIS 2 directives⁶⁰. While GDPR focuses on general data privacy rules, NIS 2 focuses on cybersecurity.

Both the laws, are backed with strong enforcement directives and are implemented with strict provisions to protect the citizens, social fabric and the economy within the European Union.

But similar to the United States, the EU has been a victim of various cyber security attacks. Some major attacks include France TV5Monde Cyberattack (2015) - France⁶¹, European Medicines Agency (EMA) Cyberattack (2020) - EU⁶² and San Carlo Cyberattack (2023) – Italy⁶³.

Chapter 2.8.3. The United Kingdom

Similarly to the EU, in the United Kingdom, UK GDPR is the key law which protects residents of the United Kingdom. The UK adopted GDPR while it was part of the European Union and kept the law post Brexit.

While various aspects of the UK GDPR overlap with EU's GDPR, the UK version is more localized and newer laws in pipeline such as the Data Protection and Digital Information Bill in the UK could include various new provisions in UK's cyber security laws.

Similar to the EU GDPR, the scope of the law extends beyond the borders of the United Kingdom for and includes strict financial penalties for noncompliance⁶⁴.

Major cyberattacks in the UK include Tesco Bank Cyberattack (2016)⁶⁵, British Airways Data Breach (2018)⁶⁶ and the UK Electoral Commission Hack (2021-2022, revealed in 2023)⁶⁷.

Chapter 2.8.4. India

In India, Information Technology Act, 2000 (IT Act)⁶⁸ is the backbone of cybersecurity and privacy laws in the country. The law is comprehensive in its approach and reach and involves various aspects of data privacy, cybersecurity prevention and enforcement. Beyond the Information Technology Act, 2000, CERT-In Guidelines (2022)⁶⁹ focus on the active reporting

⁶⁰ NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems, n.d.

⁶¹ Corera, 2016

⁶² (Cyberattack on EMA - Update 5 | European Medicines Agency (EMA), 2021)

⁶³ La Rocca, 2025

⁶⁴ ICO, n.d.

⁶⁵ Treanor, 2017

⁶⁶ BBC News, 2020

⁶⁷ Seddon, 2023

⁶⁸ IT Act 2000, Information Technology Act 2000, Bare Act, Information Technology Law, 2019

⁶⁹ BreachRx, 2022

of cyberattacks within 6 hours and the Digital Personal Data Protection Act (DPDP Act), 2023⁷⁰ focuses on personal data protection of all Indian residents.

In India, the major challenge is in implementation of laws. Being a developing nation, India's law enforcing agencies often struggle to uphold the law due to the large size of the nation and its population and the weakness of its institutional networks including the policing system, the public administration and the justice system⁷¹.

Despite the challenges, India has made considerable progress in improving its IT and Digital infrastructure and created a strong network of laws and regulations to secure the digital infrastructure and protect its citizens.

Major cybersecurity attacks in India include UIDAI Aadhaar Data Leak (2018)⁷², Cosmos Bank Cyber Heist (2018)⁷³, AIIMS Hospital Delhi Cyberattack (2022)⁷⁴.

Chapter 2.8.5. Similarities and Comparison

The cyber security and privacy laws in the United States, European Union, the United Kingdom and India overlap in various cases such as data encryption and secure access controls, individuals right to digital privacy, incident reporting guidelines for private and public companies, employee trainings etc.

The difference between the laws includes that while European Union's GDPR has extra territory implications, Indian law is limited to Indian territory and cannot be applied abroad.

Chapter 2.9. Future, Quantum-based cybersecurity

"As cybersecurity attacks are getting more complex, advanced, and sophisticated due to the advancements in AI and various other technologies, various governments, institutions and private firms are working on finding solutions to deter cybersecurity attacks in a world of advance AI⁷⁵."

Understanding the future technologies such as quantum technology is crucial for future developments of my project (See Chapter 3) because to keep my product inline with market

⁷⁰ Data Protection Laws in India - Data Protection Laws of the World, n.d.

⁷¹ Agrawal, 2025

⁷² BBC News, 2018

⁷³ Purkayastha, 2020

⁷⁴ Uberoi, n.d.

⁷⁵ History of Cyber Attacks From the Morris Worm to Exactis | Mindsight, 2019

needs, I have to keep up with the latest developments in technologies, which can help in keeping the competitive advantage and make my product worthwhile.

Various theories and technologies are being researched and studied and quantum-based cybersecurity is becoming a viable option for future cybersecurity growth and advancements. While AI based cybersecurity has shown great potential, in creating next generation cybersecurity tools, quantum computing might also present a new era, in the cybersecurity domain⁷⁶.

Quantum computers, work in a unique way from computers used till date and instead of binary bits, where either a function is 0 or 1, quantum qubits, can be either 0 or 1 or both 0 and 1 at the same time. This layer of complexity makes quantum based technology ideal for encryption methods and various researchers are trying to use quantum based encryption methods, to not only enhance cyber security infrastructures, but also create a layer of complex systems of quantum encryptions, which could make critical networking, such as in military and highly critical networks even more secure.

Another reason for further research in quantum-based encryption is to prevent attackers from using quantum-based technologies, to crack and decrypt encryption codes in highly vulnerable industries.

“Encryption methods, such as the RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are used in banking and military operations and it is practically impossible for a regular computer or even a supercomputer to break these encryption methods, with the technology available today⁷⁷.”

With the help of quantum-based decryption technology, it has been proven that even the most relatively secure encryption methods are highly vulnerable. Hence, the quantum research has moved ahead with Post-Quantum Cryptography (PQC). Post-Quantum Cryptography (PQC) is the method of developing encryptions, which can restrict and withstand quantum-based decryption. A relatively successful application of quantum

⁷⁶ Edwards, 2025

⁷⁷ Edwards, 2025

computing is the Quantum Key Distribution (QKD). In Quantum Key Distribution, quantum mechanics is used to enable ultra secure encryption and communication⁷⁸.

The United States is actively adapting quantum-based technology in their cybersecurity infrastructure and have created protocols, and procedures for quantum-based research, planning, execution and implementation⁷⁹.

While quantum-based computing and its cyber security applications are showing some successes in their applications for the future, the long term, and industry wide application is still challenged due to the high cost, challenges with scalability of creating and doing quantum research and the barrier to our knowledge about quantum physics and its limitations⁸⁰.

Various new areas of research are also being explored, newer areas, focused on more niche market are also being explored and developed. Some of the areas include Deepfake and Digital Identity Security, Bio-Cybersecurity & Neurosecretion, Space Cybersecurity.

To conclude, as hackers and attackers are getting more sophisticated, better equipped and technological advanced, newer technologies are paving the way for smarter, better, and more secure cybersecurity methods to protect against any unauthorized intrusion at the software, hardware or the network level⁸¹.

Chapter 2.10. Cybersecurity in Workspace

“Cybersecurity in the workplace is the practice of security the entire digital infrastructure of the company, the data of its business, employees etc. and or security the physical, networking and software infrastructure from cyber threats⁸².”

While various companies have used various strategies to implement cybersecurity in workplace environments, some common practices include, Network Security using Firewalls, Intrusion detection systems (IDS) and Virtual Private Network (VPN), Data Protection & Encryption and backup strategies, Access Control & Authentication such as Multi-factor authentication (MFA), Incident Response & Monitoring, Cloud security, Database security,

⁷⁸ Edwards, 2025

⁷⁹ National Quantum Initiative, n.d.

⁸⁰ Edwards, 2025

⁸¹ History of Cyber Attacks From the Morris Worm to Exactis | Mindsight, 2019

⁸² Workspace Security: Challenges, Threats, and Security Solutions, 2024

Government policy and best practices management and trainings. These strategies can help an organization mitigate the challenges of cybersecurity and avoid major cyber incidents.

Among all the common measures adopted by various companies, it is reported that a majority of cybersecurity incidents occur due to human error, which brings to light the role of trainings and cybersecurity awareness programs in the overall cybersecurity planning. *While various methods used by the blue teams and red teams might offset the flaws in the digital infrastructure, human error remains the key cause of cyberattacks. Therefore, the role of cybersecurity trainings in workplace is essential*⁸³.

*According to a research, published by the IBM's Cyber Security Intelligence Index in 2014, more than 95% percent of cyber security incidents occurred due to human error. Most of those incidents were preventable and could be avoided with proper trainings*⁸⁴.

Large companies in all major sectors have created proprietary software and training material for their employees to training on, which help mitigate the human error and prevent cybersecurity risks. These trainings are also regularly conduct and updated by professionals.

Smaller companies, on the other hand, due to limited funds are unable to hire and consult blue and red teams to detect cybersecurity vulnerabilities and fail to conduct regularly updated cybersecurity trainings for their employees, due to a which, they remain highly vulnerable to cybersecurity attacks.

Chapter 3, which is my own project tackles this critical issue by proposing a self-developed project, under the supervision of Professor László Pitlik (Jr.) & Professor Dr. László Pitlik.

Chapter 2.11. Relationship between Subject and Thesis

During my studies at Kodolányi János University, I completed several subjects that directly supported the development of my thesis, which focuses on cybersecurity risks for remote workers in Operational Technology (OT) environments. Each subject contributed valuable knowledge and practical skills that helped me understand and analyse cybersecurity issues more effectively.

⁸³ Workspace Security: Challenges, Threats, and Security Solutions, 2024

⁸⁴ The Importance of Mitigating Human Error in Cybersecurity, 2022

Chapter 2.11.1. Introduction to Mathematics

“Mathematics is essential in assessing cybersecurity risks as similar to Mathematics, cybersecurity also requires the ability to understand, communicate, and create logic using symbols and numbers⁸⁵.” For example, tools like correlation matrices help in identifying relationships between different variables such as internet traffic and packet error rates⁸⁶. This understanding supports better prediction of risk and allows stronger security measures to be planned during high-risk periods.

Chapter 2.11.2. Introduction to Algorithms

“Algorithms such as Deep learning algorithms are a fundamental aspect of modern cybersecurity study and analysis.⁸⁷” This subject helped me understand how algorithms work and how their efficiency can be measured in terms of time and memory usage. In cybersecurity, especially in OT environments, it is important to use fast and resource-efficient algorithms to detect and respond to threats quickly.

Chapter 2.11.3. Operating Systems

“An operating system is a software program that manages computer hardware and software resources and provides common services for computer programs. In an increasingly complex digital era, operating system security is a very important issue and critical for cybersecurity analysis and protection.⁸⁸” Knowledge of operating systems is crucial for recognising system-level vulnerabilities. This subject enabled me to understand how systems operate, how processes are managed, and how weaknesses in system design can be exploited by attackers.

Chapter 2.11.4. Introduction to Programming

“Coding is a critical skill for cybersecurity professionals, as it prepares the professionals for better offensive and defensive strategies.⁸⁹” Basic programming knowledge is the foundation of all cybersecurity tools and applications. This subject taught me how to write structured code and build small-scale applications, which is useful for creating secure software solutions.

⁸⁵ Bowcut, 2025

⁸⁶ Exisor. (n.d.).

⁸⁷ Dixit & Silakari, 2020

⁸⁸ Mintenajah, 2023

⁸⁹ Webb, 2024

Chapter 2.11.5. Networks and Computer Architecture

“Cybersecurity architecture, also known as network security architecture, is the practice of designing computer systems to assure the security of your underlying data. Generally speaking, cybersecurity architecture is at the foundation of your organization’s defence against security threats.”⁹⁰ “This subject provided insights into network protocols and hardware structure. It helped me understand how data travels across networks, how devices communicate, and how security can be implemented to protect these systems.

Chapter 2.11.6. Intercultural Communication

“Globalization has taken the tech world into a global village and brought in experts from all across the world.”⁹¹ Cybersecurity is often a team effort involving professionals from different cultural backgrounds. This subject improved my communication skills and taught me how to collaborate effectively with international teams, especially when working on global cybersecurity projects.

Chapter 2.11.7. Electronic Circuits

“Any piece of electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities. The risks increase if the device is connected to the internet or a network that an attacker may be able to access.”⁹²

Understanding electronic circuits is important for identifying hardware-level risks in OT systems. This subject introduced me to various components and helped me learn how they interact within larger systems.

Chapter 2.11.8. Introduction to Electronics

“Understand electronics and its modern upgradations is crucial for cybersecurity experts. Attackers may be able to take advantage of technological advancements to target devices previously considered “safe.”⁹³ This subject gave me an essential understanding of electronic devices and systems. This knowledge is essential for protecting electronic components used in operational technologies.

⁹⁰ ZenGRC Team, 2024

⁹¹ Globalization and Technology - a Twin Phenomena, n.d.

⁹² Cybersecurity for Electronic Devices | CISA, 2021

⁹³ Cybersecurity for Electronic Devices | CISA, 2021

Chapter 2.11.9. System Modelling

“As cyberattacks are becoming more frequent and dangerous, system modelling can help with understanding flaws in the system through simulation and correct them for better cybersecurity.”⁹⁴ System modelling allows the analysis and simulation of complex systems. It helps in identifying risks, testing responses, and planning system improvements. This is especially useful in the design of secure OT networks.

Chapter 2.11.10. Programming I, II & III

“A deep knowledge of computer programming is essential for cybersecurity as it can assist the expert in Reverse Engineering and Malware Analysis.”⁹⁵ These subjects provided in-depth knowledge of programming and software development. They enhanced my ability to write secure, efficient, and scalable applications which are required in cybersecurity environments.

Chapter 2.11.11. Data Visualisation

“Effective data visualization plays a crucial role in enhancing understanding and facilitating informed decision-making. While simply presenting raw data can be confusing, a well-designed visualization makes it easier for users to interpret complex information.”⁹⁶ Presenting data in a clear and understandable way is very important in cybersecurity. This subject helped me learn how to use visual tools to communicate threats, trends, and solutions effectively to both technical and non-technical stakeholders.

Chapter 2.11.12. Business Law and Regulation

“As globalisation and digital revolutions has connected businesses and people across the world, the need for understanding regulatory requirements and business law has also become more critical.”⁹⁷ Understanding the legal framework surrounding cybersecurity is vital for ensuring compliance and managing risks responsibly. This subject taught me the basics of business law and how regulations affect data protection and cybersecurity policies.

Chapter 2.11.13. Globalisation and Social Problems

“Globalization has brought about far-reaching changes in our lives. This has been driven primarily by the momentous economic progress made by the countries. Technology has played

⁹⁴ Navas et al., 2019

⁹⁵ Webb, 2024

⁹⁶ Elgart, 2025

⁹⁷ Globalization and Technology - a Twin Phenomena, n.d.

a pivotal role in speeding up globalization, while globalization itself has been a constant driving force for the newer technologies to surface.⁹⁸ This subject offered a broader view of how globalisation and social issues are linked to cybersecurity challenges. It showed how interconnected societies and technologies lead to new vulnerabilities that need to be managed at both local and global levels.

Chapter 2.11.14. Databases I and II

“Database security includes a variety of measures used to secure database management systems from malicious cyber-attacks and illegitimate use. Database security programs are designed to protect not only the data within the database, but also the data management system itself, and every application that accesses it, from misuse, damage, and intrusion.⁹⁹”

This subject focused on the structure and security of databases. It provided essential knowledge about how to store, retrieve, and protect sensitive information, which is a major part of modern cybersecurity.

Chapter 2.11.15. System Operation

“The understanding of system operations is a crucial skill for cybersecurity professionals, and it can help the professional in better and thorough cybersecurity analysis.¹⁰⁰” Practical knowledge of how systems are operated and maintained is important in preventing and responding to cyber threats. This subject taught me how to manage systems securely on a day-to-day basis.

Chapter 2.11.16. ICT Security

“Information and communication technology (ICT) security measures are necessary to protect confidential information from unauthorised use, modification, loss or release. The three key elements of an effective ICT security system include: Monitoring and controlling access to confidential information Safe transmission of data Secure storage and disposal of data.¹⁰¹”

This subject focused directly on securing information and communication technologies. It covered topics such as threat identification, risk assessment, and security controls—all of which are central to my thesis work.

⁹⁸ Globalization and Technology - a Twin Phenomena, n.d.

⁹⁹ Robertson, 2023

¹⁰⁰ ZenGRC Team, 2024

¹⁰¹ Information and Communication Technology Security, n.d.

Chapter 3. Own Developments

Following the literature review in Chapter 2, Chapter 3 will focus on my own project, developed during the IT Engineering course.

The project is inspired by my own challenges working for a small company and how cybersecurity risks affected our operations and business activities.

The project uses simple and easily available parameters, without the need for sophisticated and expensive software and hardware equipment. The project also assumes that the managers using the software have basic or no IT or cybersecurity training, and hence the project is highly practical and user friendly.

Chapter 3.1. Cybersecurity Project for Small Companies

After building the theoretical background and literature review in Chapter 2, Chapter 3 focuses on a real-life project, which can help mitigate cybersecurity risks in small companies and provide a more robust and sustainable operating environment and cybersecurity infrastructure.

Step 1

To mitigate the challenges of cybersecurity in small companies, I first created a set of major attributes which affect cybersecurity. Following that, *I divided the set into human vs machine scores, which helps in assessing if there is a human error involved or a technical flaw in the architecture.*¹⁰²

Type	Attributes
Machine Scores	Public vs Private Wi-Fi
Machine Scores	Devices in the LAN
Machine Scores	Quality of hardware
Machine Scores	Number of Firewalls

¹⁰² Rajesh: et al., 2024

Machine Scores	Settings on Firewall
Machine Scores	VPN
Machine Scores	Antivirus Results
Machine Scores	Software Updates
	Intrusion Detection System (IDS)
Machine Scores	Alerts
Machine Scores	Network Traffic Analysis
Human Scores	Using unauthorized websites
Human Scores	Compliance with accounts
Human Scores	Stress
Human Scores	Phishing Email Testing
Human Scores	Trainings score
Human Scores	Questionnaire
Human Scores	Authorized Software

Source: Rajesh: et al., 2024: 5th International Congress on Scientific Research April 21-22, 2024, Türkiye by IKSAD Institute

Then I assigned an attribute ID to all major attributes.

Attribute ID	Name	Function
A1	Layers of the Firewall	<ul style="list-style-type: none"> More layers improve security by filtering threats at multiple points. Prevents unauthorized access and network intrusions. Helps in detecting and blocking malicious traffic.
A2	No. of Devices connected to the Wi-Fi network.	<ul style="list-style-type: none"> More devices increase potential attack surfaces.

		<ul style="list-style-type: none"> ○ Infected devices can spread malware across the network. ○ Unauthorized devices may indicate a security breach.
A3	How many times is the Wi-Fi password changed in a month.	<ul style="list-style-type: none"> ○ Frequent changes reduce the risk of password leaks. ○ Prevents unauthorized access from old devices. ○ Helps in mitigating brute-force attacks.
A4	Length of Wi-Fi encryption Key	<ul style="list-style-type: none"> ○ Longer keys make it harder to crack encryption. ○ Ensures strong protection against eavesdropping. ○ Reduces the chances of unauthorized decryption.
A5	Year of the Router.	<ul style="list-style-type: none"> ○ Older routers may have unpatched vulnerabilities. ○ Newer models have better security features. ○ Ensures compatibility with the latest security standards.
A6	Year of the User Device.	<ul style="list-style-type: none"> ○ Older devices may not support the latest security updates. ○ Increased risk of software and hardware vulnerabilities. ○ Lack of support for modern encryption protocols.
A7	Number of Days since the last Software Update.	<ul style="list-style-type: none"> ○ Outdated software contains known security vulnerabilities. ○ Updates patch critical security flaws.

		<ul style="list-style-type: none"> ○ Reduces the risk of malware exploiting old software.
A8	How many Threats Detected by the Antivirus software in the last month.	<ul style="list-style-type: none"> ○ Indicates the level of exposure to cyber threats. ○ Helps in assessing the effectiveness of security measures. ○ High threat detection may signal a compromised system.
A9	How many Threats Detected by the Antivirus software in the last month.	<ul style="list-style-type: none"> ○ Monitors network traffic for suspicious activity. ○ Helps in detecting cyberattacks before they escalate. ○ Can prevent unauthorized access attempts.
A11	Intrusion Detection System.	<ul style="list-style-type: none"> ○ Monitor network traffic for suspicious activity. ○ Helps in detecting cyberattacks before they escalate. ○ Can prevent unauthorized access attempts.
A11	Total Amount of downloaded Data in Last week	<ul style="list-style-type: none"> • Large downloads may indicate data exfiltration. • Helps in identifying unusual network activity. • Can indicate unauthorized software downloads.
A12	Total Number of Files Downloaded in Last Week	<ul style="list-style-type: none"> • A high number of downloads may include malicious files. • Helps in tracking unauthorized data transfers. • Can indicate potential insider threats.

A13	Percent of total Logins hours when VPN was used	<ul style="list-style-type: none"> • VPN encrypts traffic, ensuring secure remote access. • Reduces the risk of data interception on public networks. • Helps in maintaining privacy and security.
A14	How many times user visited Blacklisted websites by company Last week	<ul style="list-style-type: none"> • Accessing blacklisted sites can introduce malware. • Can indicate policy violations or insider threats. • Helps in enforcing company cybersecurity policies.
A15	How many times Personal Accounts were used to Login in the last week	<ul style="list-style-type: none"> • Personal accounts may lack corporate security controls. • Increases the risk of credential leaks. • Can lead to data breaches if mixed with work credentials.
A16	How many days beyond 12 hours per day were worked in the last week	<ul style="list-style-type: none"> • Fatigue leads to human errors and security lapses. • Increases risk of phishing and social engineering attacks. • Can result in improper handling of sensitive data.
A17	How many times the user downloaded company Unauthorized Software	<ul style="list-style-type: none"> • Unauthorized software can contain malware. • Can lead to compliance and licensing issues. • Increases the risk of security vulnerabilities.

Step 2

Following this initial analysis, a more complex analysis is done. Here, we further add directions to the attributes. The directions mean that if improving the attributes affects the cybersecurity positively or negatively. For example: *It is generally agreed that by updating software in time, the network becomes more secure. (See The Advice of the European Cyber resilience Act <https://www.european-cyber-resilience-act.com/>).* This means that timely software updates have a positive effect on the cybersecurity, hence the direction of the attribute is 1.

On the other hand, increasing visiting blocked websites or working more hours, which causes stress can increase risks, hence the direction of the attribute is 0.

“But some attributes might be like the Schrödinger cat or an electron with dual personalities. For example, firewall threat detection: If a firewall is showing us a lot of threats, that could mean both things, either our network is very unsafe, or the firewall works too well, or both. On the other hand, if the firewall detects too less or 0 cases, either our network is military grade secure, or our firewall doesn't work at all, or both¹⁰³.”

Similar dilemmas could be in intrusion detection systems, malware analysis or antivirus analysis. In these cases, we could set some generic rules, to create a balance of power and make some checks and balances. We could use the classic If-Else. If pyramid. For example: if firewall detects less threats, and the intrusion system detects less threats and antivirus analysis detects less threats than we can use this case as true. But, if either of the cases is not true, we can assume false. We could also add to the if-else clause more predictable measures such as percentage of time VPN was used etc.

Going ahead with the attribute selection and their direction, I populated the matrix (see Figure 1) with possible real-life values for various attributes and test subjects.

Data collection

All the data used in the risk-attribute matrix is randomised and anonymized real-life data, which can be used to simulate a real-life test case. The data was collected based on inputs from my classmates at the university and colleagues at my office.

¹⁰³ Rajesh: et al., 2024

Chapter 3.2. COCO Y0 Analysis

In coco analysis, the staircase function is used, which assigns and allows variable weight to different variables, in contrast to traditional regression analysis, which gives equal weight to each variable.

	Layers of the Firewall	No. of Devices connected to the wifi network	How many times is the Wifi password changed in a month	Length of Wifi encryption Key	Year of the Router	Year of the User Device	Number of Days since the last Software Update	How many Threats Detected by the Antivirus software in the last month	How many Threats Detected by the Antivirus software in the last month	Intrusion Detection System	Total Amount of download ed Data in Last week	Total Number of Files Downloaded in Last Week	Percent of total Logins hours when VPN was used	How many times user visited Blacklisted websites by company Last week	How many times Personal Accounts were used to Login in the last week	How many days beyond 12 hours per day were worked in the last week	How many times the user downloaded company Unauthorise d Softwares
Attribute ID	Count	Count	count/month	Bits	Year	Year	Days	count/week	count/week	Integer	GB	count/week	Percentage	count/week	count/week	Hours	count/week
Attribute Unit	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1	1	1
Attribute Direction	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1	1	1
Test Subject : Mr. K	5	9	0	128	2014	2018	78	45	45	50	15	59	76	5	12	3	4
Mr. L	9	8	0	192	2015	2019	76	99	99	31	158	454	27	123	10	25	5
Mr. J	7	2	5	256	2024	2015	68	24	24	5	59	209	10	151	10	5	8
Mr. P	4	6	1	192	2021	2016	59	50	50	61	603	150	29	53	9	30	10
Mr. T	6	2	5	128	2014	2016	69	16	16	78	34	61	48	144	2	1	0
Mr. W	4	7	5	128	2022	2018	86	74	74	22	837	480	50	112	5	7	7
Mr. Z	8	5	3	128	2022	2024	80	23	23	1	985	296	70	58	8	14	8
Mr. I	6	3	4	128	2023	2020	42	12	12	38	121	286	73	117	2	14	0
Mr. Q	8	5	5	256	2022	2019	81	32	32	25	939	138	75	186	3	5	1
Mr. U	4	9	5	128	2019	2019	35	72	72	49	204	417	86	35	5	20	5
Mr. A	9	7	1	192	2019	2018	64	82	82	40	409	231	97	39	4	20	5
Mr. D	9	5	3	128	2019	2017	10	2	2	19	309	67	24	168	0	6	3
Mr. Y	3	2	2	128	2021	2016	33	83	83	8	447	151	97	134	0	12	4
Mr. H	9	5	1	128	2022	2019	50	54	54	72	463	2	31	91	4	20	3
Mr. C	8	9	3	128	2021	2014	14	25	25	62	264	66	100	4	5	19	0

Figure 1: Various Attributes (OAM) used for the Risk Analysis

Source: Author's own work: <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>: Sheet title COCO, V5:V22, AM5:AM22.

Units: Attribute ID: Please see Annex 8.5. My IKSAD Conference

Figure 1 in a base data set which was used for the analysis. All data was collected from real individuals namely Kodolányi University students and from my workplaces. All names were anonymized. For more information, please check Author's own work, excel sheet title COCO.

Chapter 3.3. Practical Use

Using this software, small companies can gain the following benefits.

1. They can find the weak points in their cyber security infrastructure and dedicate resources in improving the weaknesses for an overall stronger architecture.
2. The companies can use targeted trainings for employees who are at a higher risk of cyberattacks and using this approach, the companies can save costs and improve the overall efficiency of their digital services.
3. Companies can add or delete attributes based on their needs, making the software a highly customizable.

4. The data from the software is based on real time information and provides constant feedback to managers and employees.
5. The companies don't need to invest their limited resources in hiring specialized consultants fulltime, with this software, the company leadership can hire cybersecurity consultants and training for targeted seminars, which will reduce costs and save company's reputation and market.
6. The software is open source, and the source code is shared with the companies, and they can customize it and scale it as per requirements.
7. For any company, financial interests are the key driving factor. By mitigating possible cyber security challenges, the company can save cost, protect reputation, provide continuous delivery of goods and services and save itself from the psychological challenges faced by victims of cyber security attacks.

Chapter 3.4. Automation

The use of automation in the project can improve the real-time efficiency and scalability of the project. With AI based tools such as COCO analysis and specialized scripts, which can get log data from users in real time basis, an efficient and sustainable software can be built. As part of my final semester IT engineering project, a working model was created, which uses AI to efficiently use my risk-attribute matrix and find possible cybersecurity risks for a company. (Please find the project in Annex 8.6)

Chapter 3.5. Testing

The risk-attribute matrix and the software were tested using various real and randomized data sets. Real data was collected from real life users and randomized data was collected used various internet sources and AI tools.

In all tests, the risk-attribute matrix and the coco-analysis gave similar results, which confirmed the validity and reliability of the model. See my Excel File for more information.

<https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>:

Chapter 3.6. IT Security Aspects

The risk-attribute matrix covers various major areas of cybersecurity digital and physical security and provides a comprehensive tool for early warnings and threat detections.

With the help of AI and advanced data analytical tools, the project can be further expanded to encompass modern and upcoming cybersecurity challenges.

Chapter 3.7. Relationship with another Thesis

Various students at the university have worked diligently on interesting and thought-provoking topics for their portfolio but for comparison, my thesis can be compared to my colleague, Mr. Latif Muhammad Khuram whose thesis is about Analysing Cybersecurity Risks Among Remote Workers in Operational Technology Environments¹⁰⁴. (

After reading Mr. Latif's thesis, I could learn so much more about his ideas and how I could improve my ideas and project as well. His thesis, similar to mine focuses on cybersecurity and there are many similarities and differences between his and my approach.

In similarities, both Mr. Latif's and my project focuses on cybersecurity aspects in the corporate world. We both also used a comprehensive set of parameters and AI tools such as COCO Y0 analysis for analysis. Furthermore, we developed a joint working software (See Annexe 2-4), where we worked together to create a working software, which can use the attributes from both our projects and beyond to provide cybersecurity analysis of various workers in a company.

In differences, especially in the literature review, while I have focused on the scientific and academic literature on cybersecurity, its past, present and future, Mr. Latif uses as novel strategy and focused on the learning outcomes of the various courses done at the university and related the learning outcomes and experiences from the courses for this thesis. This approach is highly relevant and a great build-up for readers as the readers can better understand the relationship between teaching, knowledge acquisition at the university and how the course prepares students to become independent creators.

Comparison of My Thesis and Latif's Thesis

ID	Phenomenon	My Thesis	Latif's Thesis
----	------------	-----------	----------------

¹⁰⁴ Latif, 2025

1	Objects	16 Objects: Real Test Subjects (Anonymized names to Mr. K, Mr. L, etc.)	16 Objects: Remote Workers created by Chat GPT (See chapter 3.1.4)
2	Number of Attributes	17 Attributes (16 unique, 1 repeated) (see Annex B with 2 attribute-columns + with all the necessary attribute-types, incl. direction)	12 Attributes (See chapter 3.1.1)
3	Common Attributes (5) form both Theses	Same attributes but named differently. Total Amount of Downloaded Data in Last Week Length of Wi-Fi Encryption Key Intrusion Detection System How Many Threats Detected by Antivirus in Last Month How Many Days Beyond 12 Hours Worked Last Week	Internet Traffic, Key Length Intrusion Attempts Malware Infections System Downtime
4	Attribute with Different Direction	The more days beyond 12 hours worked last week the less the risk. (the directions can be set by users freely correlation-matrix-based alerts are integrated to avoid arbitrary misunderstandings of the users)	E.g., the more System Downtime the more the risk (the directions can be set by users freely correlation-matrix- based alerts are integrated to avoid arbitrary misunderstandings of the users)

5	Total Combined Attributes (24) from both Theses	24 (same calculation method) $(17-5) + (12-5) + 5 = 24$	24 (based on a combination of different and common attributes)
6	Focus Area	General cybersecurity in home-office environments with different numbers, kinds, and directions of attributes.	Cybersecurity risks in remote work environments (OT) with different numbers, kinds, and directions of attributes. (c.f. chapter 2.1.2)
7	Data Collection	Initially, Data was generated using Excel random number function Later Test Subjects Data was collected from real people	Kind of Realistic values obtained using ChatGPT (c.f. chapter 3.1.4)
8	Ranking Method	Same methodology applied	Ranking applied based on behavior such as risk direction (0 or 1)
9	Ranking Method for automation (Using a Correlation matrix as a supportive forcefield for direction-alerts)	Similar, and there is no need for Excel's correlation matrix. Because software can perform the correlation matrix but to ensure the quality, we can also do excel correlation and compare the results.	Used for automation, In Chapter 3.1.10 I gave alert-generating rules for the analysis of the correlation values compared to a given direction-vector
10	AI Analysis	Used COCO AI for risk predictions	Used COCO AI content free engine to predict risk

11	Steps of COCO AI Analysis	Three-step process: Auxiliary table, score computation, final risk assessment	Three-step process: Auxiliary table, score computation, final risk assessment
12	Results	Same outcome: higher-risk test subjects identified to enhance cybersecurity practices and provide mitigation solutions	Identifies high-risk remote workers

Chapter 3.8. Step by Step Elimination

After gathering the raw data, COCO Y0 analysis was used to first understand the relationship between each attribute and the final risk score. By analysing, it was confirmed that some attributes have a specific influence on the final risk score . It means a set of attributes can lead to an anti-discriminative constellation. This set should however always be eliminated from the OAM in order to see the impact of all other attributes.

	Layers of the Firewall	No. of Devices connected to the self network	How many times is the WiFi password changed in a month	Length of WiFi encryption Key	Year of the Router	Year of the User Device	Number of Days since the last software updates	How many Threats Detected by the Antivirus software in the last month	How many Threats Detected by the Antivirus software in the last month	Intrusion Detection System	Total Amount of Data in Last week	Total Number of Files Downloaded in Last Week	Percent of total Logins hours when VPN was used	How many times user visited Blacklisted websites by company Last week	How many times Personal Accounts were used to Login in the last week	How many days beyond 12 hours per day were worked in the last week	How many times the user downloaded company sensitive Software	Norm value
Units	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Ranking number	Risk Point
01	11	14	15	7	15	7	12	8	9	11	1	2	4	2	16	3	7	1000
02	1	13	13	4	14	8	11	16	1	7	5	15	14	11	14	13	9	1000
03	8	1	1	1	1	18	8	5	12	2	2	16	16	14	24	3	14	1000
04	12	9	12	4	7	11	7	9	8	12	12	7	13	5	12	16	16	1000
05	9	1	1	7	15	11	10	3	14	16	2	3	11	13	4	1	1	1000
06	13	10	1	7	3	7	16	13	4	5	13	16	10	9	9	6	12	1000
07	5	5	1	7	3	1	14	4	12	1	14	12	8	7	12	8	14	1000
08	9	4	4	7	2	2	3	2	15	8	4	12	8	10	4	8	1	1000
09	5	5	1	1	3	3	13	7	10	6	15	6	7	16	6	3	4	1000
010	13	14	1	7	10	3	4	12	3	10	6	14	4	3	9	13	9	1000
011	1	10	12	4	10	7	8	14	3	9	9	11	2	4	7	12	9	1000
012	1	5	7	7	10	10	1	1	16	4	8	2	13	12	1	2	5	1000
013	16	1	11	7	7	11	2	15	2	3	10	8	2	12	1	7	7	1000
014	1	5	12	7	3	3	6	10	7	13	11	1	12	6	7	12	5	1000
015	5	14	7	7	7	16	2	6	11	14	7	4	1	1	9	11	1	1000
016	11	10	7	1	13	11	12	11	6	12	14	9	5	6	1	10	12	1000

Figure 2: COCO Analysis

Source: Author's own work: <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>: Excel sheet title COCO, A5:V22, S4:S22

In Figure 2, using COCO Analysis, we see that some attributes have a specific relationship with the ranked scores. For more information, please check Author's own work, excel sheet title COCO.

After filtering the specific set of the attributes, COCO Y0 analysis was used again to rank our test subjects in order of their risk profiles.

Data type Raw unit	Integer Count	Integer Count	Integer Count/month	Integer Bits	Integer Days	Integer Days	Integer Count/week	Integer Risk Point
RAW DATA	Layers of the Firewall	No. of Devices connected to the wifi network	How many times is the Wifi password changed in a month	Year of the Router	Number of Days since the last Software Update	Number of Days since the last Software Update	How many times the user downloaded company Unauthorised Softwares	Norm Value
Test Subject Mr. K	5	9	0	2014	78	76	4	1000
Test Subject Mr. L	9	8	0	2015	76	27	5	1000
Test Subject Mr. M	7	2	5	2024	68	10	8	1000
Test Subject Mr. N	4	6	1	2021	59	29	10	1000
Test Subject Mr. O	6	2	5	2014	69	48	0	1000
Test Subject Mr. P	4	7	5	2022	86	50	7	1000
Test Subject Mr. Q	8	5	3	2022	80	70	8	1000
Test Subject Mr. R	6	3	4	2023	42	73	0	1000
Test Subject Mr. S	8	5	5	2022	81	75	1	1000
Test Subject Mr. T	4	9	5	2019	35	86	5	1000
Test Subject Mr. U	9	7	1	2019	64	97	5	1000
Test Subject Mr. V	9	5	3	2019	10	24	3	1000
Test Subject Mr. W	3	2	2	2021	33	97	4	1000
Test Subject Mr. X	9	5	1	2022	50	31	3	1000
Test Subject Mr. Y	8	9	3	2021	14	100	0	1000
Test Subject Mr. Z	5	7	3	2018	78	82	7	1000

Figure 3: COCO Analysis Part 2

Source: Author's own work: <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>: Excel sheet title COCO Colored, B2:B21, J2:J21

In Figure 3, we see after filtering out and using the most import module, COCO Analysis gives us a ranked module and ranks all test subjects according to their individual attribute score.

For more information, please check Author's own work, excel sheet title COCO Colored.

Chapter 4. Discussions

The project opens various opportunities for small companies, to not only upgrade their cybersecurity infrastructure but also help develop a robust system or systems to maintain business continuity while conducting constant risk-analysis of their employees and IT infrastructure.

The main discussions, following the literature review and the project are as follows.

1. How can AI be used to train employees for better cyber-risk compliance?
2. In cases of internet breakdown due to weather, war or human mal intentions, how can business continuity be maintained and how can the project cope up with that.
3. What new kinds of cyber risks can emerge from developing countries, due to challenges with maintain infrastructure and keeping up with software updates.
4. As the internet and cybersecurity has gotten globalized, will there be a wave of data localization, as already seen in European countries and in the US.

Chapter 5. Conclusions

The results of the risk-attribute matrix can be used for two observations. The first being the risk scores of various employees and the second being the relative importance of some attributes over others.

For the first observation, by analysing the results of the risk-attribute matrix, cyber risk scores were calculated for each employee based on the data from various attributes. Employees which have a higher risk score are at a higher risk and vulnerability for cybersecurity threats and employees with a lower risk score are at a relatively lower risk and vulnerability for cybersecurity threats.

This information can be key knowledge source for managers to use targeted methods of training, software and hardware upgradation and cyber risk management to reduce the overall cyber security risks for the company. This can help save costs, protect business interests and reputation and avoid any unauthorized access, manipulation and loss of data.

For smaller companies, which have budget issues and lack of technical expertise, the results of this risk-attribute matrix can be highly relevant as they can dedicate their limited resources towards finding solutions, instead of organizing general trainings, or upgrading the entire hardware, software and network infrastructure.

For the second observation, various attributes have a different impact with varying degrees on the cybersecurity risk of them employees. By using coco-analysis, it could be determined that some attributes have a stronger influence on the cyber-risk scores of the employees and some attributes have limited influence on the cyber-risk scores.

By studying the relationship between relatively more important and relatively less important attributes, the project and the software can be customized according to client needs and budget. Based on the clients, needs, infrastructure and software availability, budgets, technical expertise and requirements, a tailor-made solution can be offered, which would make this product, adaptable, flexible and fit for the requirements of various kinds of business.

For example, the requirement of a small law firm, would include more focus on data access and privacy, due to attorney-client privilege laws and requirements, while a small marketing

firm, focused on digital marketing, branding and advertising services would need to secure its physical infrastructure and networking infrastructure to ensure it can continuous and round-the-clock provide its digital marketing services.

Therefore, considering the two major observations from the risk-attribute matrix, the project can be used as a project for real life corporate, industrial and business needs¹⁰⁵.

¹⁰⁵ For further steps and analysis on how the, please refer to Annex 8.5, 5th International Congress on Scientific Research April 21-22, 2024, Türkiye by IKSAD Institute Risk-evaluation possibilities concerning IT-activities in home-office Presenter: Aadi Rajesh: Kodolányi János University Supervisors: László Pitlik (Jr.) & Dr. László Pitlik

Chapter 6. Future areas of improvements

The primary challenge on the software is data collection and the regulations governing data collection such as GDPR.

In case a company decides to use this software, they will need to strictly monitor compliance with data safety and security and also constantly inform and upskill their employees about their digital rights and responsibilities.

In terms of the future areas of improvement, the software in its current form provides real time information about cybersecurity vulnerabilities for small companies but has the potential to further improve.

The future improvements can be done on 3 levels, client feedback level, market need levels and changes in cybersecurity threats and vulnerability.

At the client feedback level, after gaining valuable user inputs from their experiences, the software can be fine-tuned to improve functionality and accessibility.

At the market needs level, as the software will enter newer markets, we can study the specific opportunities, risks and challenges a new market presents and improve our product to match market needs.

At the changes in cybersecurity level, as hackers are getting more proficient and cyberattacks are become more sophisticated due to AI and various other technological advancements, the software can use big data analysis, stronger cryptography tools and AI to improve security¹⁰⁶. Furthermore, the risk-attribute matrix, can be upgraded to a working software model, which can automatically gather information without manual data entry.

¹⁰⁶ Rikk et al., 2023

Chapter 7. Summary

The literature review and the cybersecurity risk-attribute matrix provide a comprehensive overview of cybersecurity risks and their mitigation. In the 21st century, as societies have evolved and adapted to the digital age, the role of cybersecurity professionals has increased over time and become critical.

While malicious groups and hackers such as Anonymous, Lazarus Group, Carbanak (Anunak), The Dark Overlord, etc.¹⁰⁷ are finding newer ways to exploit vulnerabilities in the systems¹⁰⁸, cybersecurity professionals are developing new systems, protocols and technologies to prevent and mitigate cybersecurity risks¹⁰⁹.

With the help of various theoretical models, such as OSI model and the TCP/IP model (See chapter 2.2.1), hiring cybersecurity professionals (See chapter 2.4) and conducting trainings for employees (See chapter 2.10), companies across the world are trying to de-risk their cybersecurity risk exposure.

For larger companies and government institutions, cybersecurity risks are professionally managed due to the availability of funds, technical expertise, manpower and the possibility to invest and create proprietary and custom-built technology for individual needs. But the smaller companies, due to lack of funds and expertise often face the burden and remain highly vulnerable to cybersecurity risks (See chapter 2.10).

In Chapter 2 of my Thesis, I explored the academic, scientific and theoretical aspects of Cybersecurity and in Chapter 3, I used the knowledge build from Chapter 2 and practical experiences for a project, which is designed for small companies with limited resources and cybersecurity expertise. The project uses various attributes and datapoints and using AI and data analytics to provide guidance and suggestions for managers to prevent and mitigate cybersecurity risks.

¹⁰⁷ Fox, 2024

¹⁰⁸ The Evolution of Cyber Threats: Past, Present and Future, 2024

¹⁰⁹ Murphey, 2024

For larger companies and government institutions, the tasks are mitigated due to the availability of funds, technical expertise, manpower and the possibility to invest and create proprietary and custom-built technology for individual needs.

For my hypothesis, *"Using a dedicated risk-attribute matrix and AI-based data analytical modules, we can predict cybersecurity challenges faced by users (See Chapter 1.1.1),"* I can conclude using the literature review in chapter 2 and the practical project in chapter 3 that cybersecurity risks and challenges can be mitigated for users by following the risk-attribute matrix, collecting the essential real time data points and using AI analysis such as COCO-Y0 analysis. (See Chapter 3.2 and Chapter 3.3)

In conclusion, "The best defence is a good offense" in cybersecurity planning and execution strategy and companies, government organizations, institutions and individuals must be well prepared for all outcomes in cybersecurity.

Chapter 8. Annexes

Chapter 8.1. Abbreviation

Abbreviation	Full Form
--------------	-----------

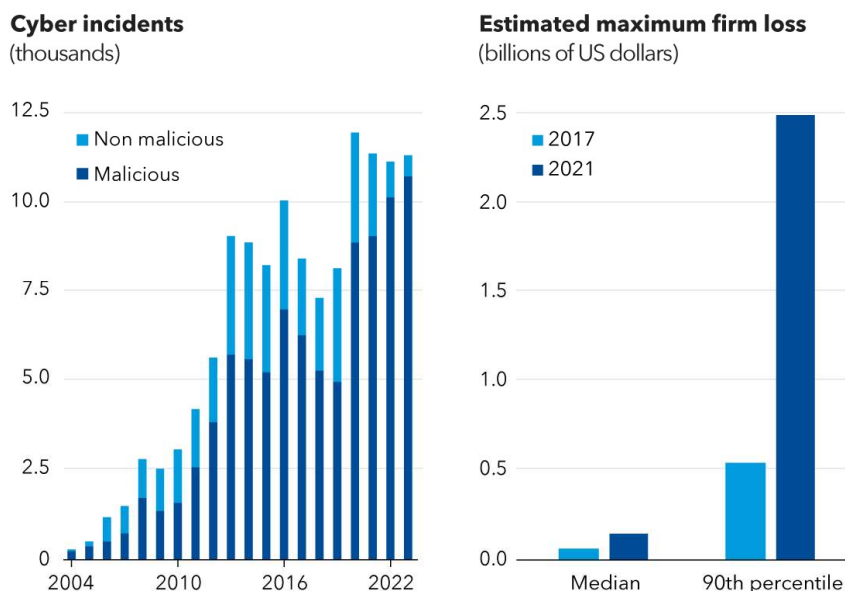
APT	Advanced Persistent Threat
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
DNS	Domain Name System
EDR	Endpoint Detection and Response
FIM	File Integrity Monitoring
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IoC	Indicator of Compromise
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
NAC	Network Access Control
NIST	National Institute of Standards and Technology
PAM	Privileged Access Management
RAT	Remote Access Trojan
SIEM	Security Information and Event Management

SOC	Security Operations Center
SSL/TLS	Secure Sockets Layer / Transport Layer Security
Zero Trust	Zero Trust Security Model

Chapter 8.2. Figures

Greater threat

The risk of suffering a cyberattack and extreme losses from it has increased.



Sources: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.
Note: Panel 1 cyber events are classified according to Advisen. Delayed reporting may lead to the underestimation of cyber events in more recent periods. Panel 2 is based on the estimated posterior density function of the highest loss of all firms within a year.

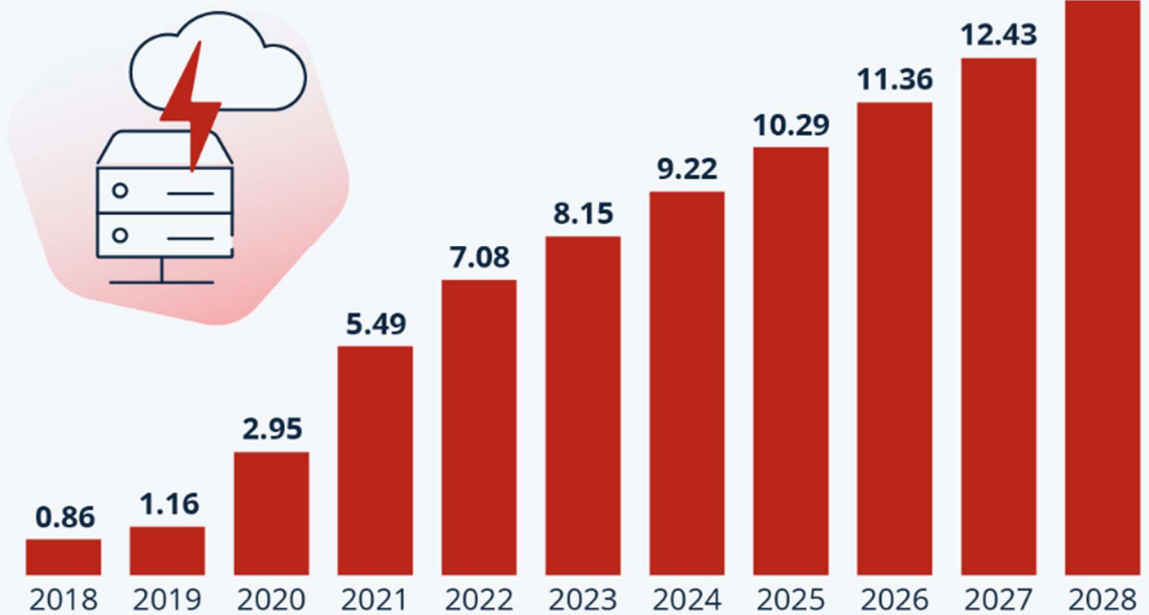
IMF

Figure F1: Increasing risks of suffering a cyberattack. Source: IMF:

<https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability>

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide
(in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights



statista

Figure F2: Cost impact analysis of cybercrimes. Source: Statista

<https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>

Chapter 8.3. References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023a). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031. <https://doi.org/10.1016/j.csa.2023.100031>

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023b). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031. <https://doi.org/10.1016/j.csa.2023.100031>

AFCEA International Cyber Committee, Gilligan, J., Dix, R., Palmer, C., Sorenson, J., Conway, T., Varley, W., Gagnon, G., Heitkamp, K., Lentz, R., Venables, P., Paller, A., Lute, J. H., & Reeder, F. (2013). *THE ECONOMICS OF CYBERSECURITY: A PRACTICAL FRAMEWORK FOR CYBERSECURITY INVESTMENT*.

<https://www.afcea.org/committees/cyber/documents/cybereconfinal.pdf>

Agrawal, A. (2025, March 22). Contemporary legal issues in India. LawBhoomi.
<https://lawbhoomi.com/contemporary-legal-issues-in-india/>

An overview of the OSI model and its security threats. (2023). Tripwire.
<https://www.tripwire.com/state-of-security/overview-osi-model-and-its-security-threats>

ARPANET. (2014). Science Direct. <https://www.sciencedirect.com/topics/computer-science/arpabet>

Author's own work <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>

BBC News. (2018, January 5). Aadhaar: "Leak" in world's biggest database worries Indians.
<https://www.bbc.com/news/world-asia-india-42575443>

BBC News. (2020, October 16). British Airways fined £20m over data breach.
<https://www.bbc.com/news/technology-54568784>

Biggest data breaches in US history (Updated 2025) | UpGuard. (n.d.).
<https://www.upguard.com/blog/biggest-data-breaches-us>

Bowcut, S. (2025, April 7). *Why math matters in cybersecurity*. Cybersecurity Guide.
<https://cybersecurityguide.org/resources/math-in-cybersecurity/>

BreachRx. (2022, December 15). India's CERT-In directive - BreachRX.
<https://www.breachrx.com/global-regulations-data-privacy-laws/india-cert-in-directive/>

Center, E. P. I. (n.d.). EPIC - Equifax Data breach. <https://archive.epic.org/privacy/data-breach/equifax/>

Cisomag. (2020, December 19). What Edward Snowden taught us about insider threats. CISO MAG | Cyber Security Magazine. <https://cisomag.com/snowden-insider-threats/>

Corera, G. (2016, October 10). How France's TV5 was almost destroyed by "Russian hackers." BBC News. <https://www.bbc.com/news/technology-37590375>

Cyberattack on EMA - update 5 | European Medicines Agency (EMA). (2021, January 15). European Medicines Agency (EMA). <https://www.ema.europa.eu/en/news/cyberattack-ema-update-5#:~:text=The%20ongoing%20investigation%20of%20the,processes%20for%20COVID%2D19%20vaccines.>

Cybersecurity careers of the future. (2018). [https://insights.sei.cmu.edu/documents/6078/Cybersecurity Careers of the Future.pdf](https://insights.sei.cmu.edu/documents/6078/Cybersecurity_Careers_of_the_Future.pdf)

Cybersecurity for Electronic Devices | CISA. (2021, February 1). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/news/cybersecurity-electronic-devices>

Dahmani, M. (2024). The Impact of the Fourth Industrial Revolution on Business Performance and Sustainability: A literature review. *Theoretical Economics Letters*, 14(01), 94–106. <https://doi.org/10.4236/tel.2024.141006>

Data protection laws in India - Data Protection Laws of the World. (n.d.). <https://www.dlapiperdataprotection.com/?t=law&c=IN>

Edwards, J. (2025, January 6). Quantum computing and the future of cybersecurity. The National CIO Review. <https://nationalcioreview.com/articles-insights/information-security/quantum-computing-and-the-future-of-cybersecurity/#:~:text=The%20quantum%20era%20is%20approaching,can%20facilitate%20theoretically%20unhackable%20communication.>

Elgart, A. (2025, April 7). *The Significant Role of Data Visualization in Cybersecurity*. Radware. <https://www.radware.com/blog/public-cloud-protection/the-significant-role-of-data-visualization-in-cybersecurity/>

Fenner-Jamieson, M. (2024, December 10). *How working from home has increased cyber threats* - INTASO. Intaso. <https://intaso.co/news/how-working-from-home-has-created-more-cyber-threats/>

Fox, J. (2024, July 31). Top 10 most notorious hacker groups in History | Cobalt. *Cobalt*.
<https://www.cobalt.io/blog/top-10-most-notorious-hacker-groups>

Global Cyber Security Network. (2025, February 14). A smarter approach to building a profitable cybersecurity startup | GCS Network.
<https://globalcybersecuritynetwork.com/blog/a-smarter-approach-to-building-a-profitable-cybersecurity-startup/>

Globalization and technology - A Twin Phenomena. (n.d.). IndiaAI.
<https://indiaai.gov.in/article/globalization-and-technology-a-twin-phenomena>

Grey Dynamics. (2025, March 25). TEMPEST: Electronic spying and countermeasures.
<https://greynamics.com/tempest-electronic-spying-and-countermeasures/>

Heinaaro, K. (2015). Cyber attacking tactical radio networks. 2015 International Conference on Military Communications and Information Systems (ICMCIS), 1–6.
<https://doi.org/10.1109/icmcis.2015.7158684>

History of cyber attacks From the Morris Worm to Exactis | Mindsight. (2019, March 21). Mindsight. <https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/>

ICO. (n.d.). The UK GDPR. <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/>

International modem dialing scams. (2020, March 11). Federal Communications Commission.
<https://www.fcc.gov/consumers/guides/international-modem-dialing-scams>

Information and communication technology security. (n.d.).
<https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security>

IT Act 2000, Information Technology Act 2000, Bare Act, Information Technology Law. (2019, October 7). Info. Technology Law. <https://www.itlaw.in/>

Kerner, S. O. S. M. (2023, November 3). SolarWinds hack explained: Everything you need to know. WhatIs. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>

Kost, E. (2024, December 30). *Human factors in Cybersecurity in 2025*. UpGuard. <https://www.upguard.com/blog/human-factors-in-cybersecurity>

Kushner, D. (2024, May 24). The real story of Stuxnet. IEEE Spectrum. <https://spectrum.ieee.org/the-real-story-of-stuxnet>

La loi Informatique et Libertés. (n.d.). CNIL. <https://www.cnil.fr/fr/le-cadre-national/la-loi-informatique-et-libertes>

La Rocca, M. (2025, February 18). Italy under attack again: Russian hackers target Ministries and Guardia di Finanza sites. Eunews. <https://www.eunews.it/en/2025/02/18/italy-under-attack-again-russian-hackers-target-ministries-and-guardia-di-finanza-sites/>

Latif, 2025, Khuram Muhamad Latif. https://miau.my-x.hu/temp/2025tavasz/en_1u.docx

LPN-0 · Mobile Threat Catalogue. (n.d.). <https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-0.html>

Luknar, I., & Jovanović, F. (2024). Various types of cyber threats. *Srpska Politička Misao*, 83(1), 161–177. <https://doi.org/10.5937/spm83-46059>

Makrakis, G. M., Koliass, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and critical infrastructure Security: Technical analysis of Real-Life Security Incidents. *IEEE Access*, 9, 165295–165325. <https://doi.org/10.1109/access.2021.3133348>

McKinsey Global Institute. (2014). THE IMPACT OF CYBERSECURITY ON SMALL BUSINESS. In P O W E R E D B Y S B A. <https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial1.pdf>

Murphey, D. (2024, February 14). The differences between red, blue and purple team engagements. *Security Magazine*. <https://www.securitymagazine.com/articles/100373-the-differences-between-red-blue-and-purple-team-engagements>

National Quantum Initiative. (n.d.). <https://www.quantum.gov/>

Navas, J., Thales Corporate Engineering, Voirin, J.-L., Thales Airborne Systems, Thales Technical Directorate, Paul, S., Thales Research & Technologies, Bonnet, S., & Thales Corporate Engineering. (2019). *Towards a Model-Based approach to Systems and Cyber*

Security co-engineering. https://mbse-capella.org/resources/pdf/Towards-a-model-based-approach-to-Systems-and-Cybersecurity-co-engineering_v2.pdf

NIS2 Directive: new rules on cybersecurity of network and information systems. (n.d.). Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

Bánkuti, Gy., Pitlik, L.(2010). About the method of Component-based Object Comparison for Objectivity (COCO). Magyar Internetes Alkalmazott/Agrárinformatikai Újság (MIAÚ). 13. https://www.researchgate.net/publication/270576061_About_the_method_of_Component-based_Object_Comparison_for_Objectivity_COCO

Own Project: <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=aadi%20rajesh>

Perwej, D., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A Systematic Literature review on the Cyber Security. *International Journal of Scientific Research and Management (IJSRM)*, 9(12), 669–710. <https://doi.org/10.18535/ijssrm/v9i12.ec04>

Purkayastha, R. (2020, October 6). Lessons learnt from cosmos bank attack. Tata Communications New World. <https://www.tatacommunications.com/blog/2018/09/lessons-learnt-from-cosmos-bank-attack/>

Rahmonbek, K. (2025, January 2). 35 Alarming small business cybersecurity statistics for 2025. *StrongDM*. <https://www.strongdm.com/blog/small-business-cyber-security-statistics#:~:text=Small%20businesses%20are%20generally%20not,tar%20just%20like%20larger%20companies>.

Rao, U. H., & Nayak, U. (2014). Understanding networks and network security. In *Apress eBooks* (pp. 187–204). https://doi.org/10.1007/978-1-4302-6383-8_9

Rajesh, A., Pitlik, L., & Pitlik, L. (2024). Risk-evaluation possibilities concerning IT-activities in home-office. 5th International Congress on Scientific Research April 21-22, 2024, Türkiye by IKSAD Institute. https://miau.my-x.hu/miau/311/home_office_risks/full_home_office_risks.pdf

Regulation - 2016/679 - EN - gdpr - EUR-Lex. (n.d.). <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

Return on Investment of Cybersecurity: Making the Business Case. (2024, May 15). *Forbes Technology Council*. <https://councils.forbes.com/blog/roi-of-cybersecurity>

Rikk, J., Pitlik, L., & Gyula, B. (2023). AI-based derivation of the importance of attributes in case of evaluation models. 17th International Congress on Artificial Intelligence - August 21-22, 2024 – Türkiye by IKSAD Institute. https://miau.myx.hu/miau/314/full_importance_of_attributes_in_evaluation_models.docx

Robertson, B. (2023, December 20). *What is Database Security | Threats & Best Practices | Imperva*. Learning Center. <https://www.imperva.com/learn/data-security/database-security/>

Rushe, D. (2017, September 20). JP Morgan Chase reveals massive data breach affecting 76m households. *The Guardian*. <https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach>

Schneier, B. (2016, August 24). New leaks prove it: the NSA is putting us all at risk to be hacked. *Vox*. <https://www.vox.com/2016/8/24/12615258/nsa-security-breach-hoax>

Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.2302.02274>

Security, P. (2024, December 24). The Phasing Out of 2G and 3G Networks: What It Means for Telecom Security. P1 Security. <https://www.p1sec.com/blog/the-phasing-out-of-2g-and-3g-networks-what-it-means-for-telecom-security#:~:text=Vulnerabilities%20in%20Legacy%20Systems,communications%20and%20steal%20sensitive%20data>.

Seddon, B. P. (2023, August 8). Cyber-attack on UK's electoral registers revealed. <https://www.bbc.com/news/uk-politics-66441010>

SentinelOne. (2024, April 12). The realm of ethical hacking | Red, blue & purple Teaming explained. SentinelOne. <https://www.sentinelone.com/blog/the-realm-of-ethical-hacking-red-blue-purple-teaming-explained/#:~:text=The%20red%20team%20provides%20insights,improve%20their%20overall%20cyber%20resilience>.

Small Business Reputation & The Cyber Risk. (2015).
<https://assets.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf>

Sweny, G. (2024, May 1). Zero-Trust architecture: implementation and challenges. AgileBlue.
<https://agileblue.com/zero-trust-architecture-implementation-and-challenges/>

The attack on Colonial Pipeline: what we've learned & what we've done over the past two years | CISA. (2023, May 7). Cybersecurity and Infrastructure Security Agency CISA.
<https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

The evolution of cyber threats: past, present and future. (2024, July 3). Katz.
<https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats>

The importance of mitigating human error in cybersecurity. (2022).
<https://www.cetrom.net/resources/blog/importance-of-mitigating-human-error-in-cybersecurity#:~:text=A%20global%20study%2C%20the%20IBM,cybersecurity%20breaches%20would%20not%20have>

Treanor, J. (2017, November 28). Tesco Bank cyber-thieves stole £2.5m from 9,000 people. The Guardian. <https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m>

Troy, E. F. & NATL INST OF STANDARDS & TECH R.I.C. (1986). Security for Dial-Up lines. In NBS Special Publication 500-137 [Report]. U.S. DEPARTMENT OF COMMERCE.
<https://www.exampleurl.com>

Uberoi, A. (n.d.). AIIMS ransomware attack. <https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack>

U.S. Department of Defense. (n.d.). "Zero trust" architecture could prevent adversary data theft, protect. <https://www.defense.gov/News/News-Stories/Article/Article/4078717/zero-trust-architecture-could-prevent-adversary-data-theft-protect-warfighters/#:~:text=The%20Defense%20Department%20Zero%20Trust%20architecture%2C%20which%20is%20scheduled%20to,protect%20military%20networks%20from%20>

adversaries.&text=A%20Zero%20Trust%20architecture%20is,the%20network%20can%20be%20trusted.

USB attacks: the threat putting critical infrastructure at risk. (n.d.). <https://www.cybersecurityintelligence.com/blog/usb-attacks-the-threat-putting-critical-infrastructure-at-risk-8066.html>

Vieira, H. (2017, September 24). Cybersecurity is the defining business challenge of the 21st century - LSE Business Review. LSE Business Review - Social Sciences for Business, Markets, and Enterprises. <https://blogs.lse.ac.uk/businessreview/2017/03/28/cybersecurity-is-the-defining-business-challenge-of-the-21st-century/>

World Economic Forum, Accenture, Jurgens, J., & Dal Cin, P. (2025). *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Webb, H. (2024). *The Connection Between Coding and Cybersecurity*. <https://www.cyberdegrees.org/resources/coding-and-cybersecurity/>

What is a supply chain attack? | CrowdStrike. (n.d.). <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/supply-chain-attack/>

What is Zero Trust Architecture? (n.d.). Palo Alto Networks. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>

Workspace Security: challenges, threats, and security solutions. (2024, September 24). Perception Point. <https://perception-point.io/guides/cybersecurity/workspace-security-challenges-threats-and-security-solutions/>

Yang, G. (n.d.). Introduction to TCP/IP network attacks. <http://seclab.cs.sunysb.edu/sekar/papers/netattacks.pdf>

ZenGRC Team. (2024, September 25). *What is Cybersecurity Architecture and Why is it Important?* ZenGRC. <https://www.zengrc.com/blog/what-is-cybersecurity-architecture-and-why-is-it-important/>

Chapter 8.4. Conversations with LLMs

LLM 1: ChatGPT

Critical Review of the Project

Title: *Risk-evaluation possibilities concerning IT-activities in home-office*

Author: Aadi Rajesh

Overview

This project offers a well-organized and insightful approach to evaluating the **risks associated with IT activities in home-office environments**. It reflects a clear understanding of the challenges businesses face when shifting to or maintaining remote work models. The author builds a logical flow from risk identification to evaluation and offers thoughtful suggestions for how to mitigate them using practical tools and parameters.

Strengths of the Project

1. Clear Logic and Structure





The project follows a logical progression:

- Identification of risk areas
- Selection of relevant parameters
- Proposal of evaluation steps
- Consideration of mitigation strategies

This makes the work accessible and easy to apply to real-world scenarios.

2. Use of Realistic and Practical Parameters

The project outlines several important parameters that help in identifying and evaluating risk, including:

-  **Security aspects** (e.g. unauthorized access, data leakage)
-  **Compliance** (legal and regulatory risk)
-  **Business continuity** (handling disruptions and outages)
-  **Reputation management** (trust, branding)

- 💰 **Cost-efficiency** (balancing safety and expenditure)

These dimensions are well chosen and form a balanced evaluation framework.

3. Integration of AI and Modern Tools

A standout feature is the mention of **online AI tools** for assisting with risk evaluation and **anti-discriminative optimization**. This shows a forward-thinking mindset and aligns with current trends in intelligent automation and digital risk monitoring.

📝 Suggestions for Enhancement

1. Include Real-World Examples

While the structure is solid, the project would benefit from adding practical scenarios or simulated case studies to demonstrate how the parameters and steps can be applied in a business context.

2. Expand on Evaluation Methodology

A more detailed explanation of how the risk parameters are weighted or prioritized (e.g. scoring models, decision matrices) would make the framework even more usable in real settings.

3. Address Emerging Threats

The project could be even more current by including modern home-office risks like:

- AI misuse
- Cloud misconfigurations
- Collaboration tool vulnerabilities
- Employee mental health and burnout

🌟 Final Thoughts

This project is a strong and timely contribution to discussions around IT risk management in remote work environments. Its logical structure, practical parameters, and openness to AI-based solutions make it both relevant and forward-looking.

With the addition of applied examples and deeper methodological detail, it could serve as a **valuable framework for businesses and IT managers** developing home-office strategies.

LLM 2: Copilot

Critical Review of the Project

Title: Risk-evaluation possibilities concerning IT activities in home-office

Author: Aadi Rajesh

Overview

The project offers a structured framework for addressing risks in IT activities within home-office settings. It acknowledges the challenges remote work poses, especially in terms of technological vulnerabilities and organizational resilience. While the overall approach is commendable, combining clear logical steps with practical recommendations, there is room to refine certain aspects to maximize its impact.

Strengths of the Project

1. Comprehensive Structural Framework

The project clearly outlines key stages of risk assessment:

- Identifying potential risk zones.
- Employing parameters for evaluation.
- Outlining mitigation strategies.

This layered approach demonstrates a well-thought-out structure that can be easily adapted by professionals looking for actionable insights.

2. Selection of Practical and Relevant Parameters

The inclusion of parameters such as security, compliance, business continuity, cost efficiency, and reputation management provides a comprehensive lens through which risks can be evaluated. These parameters are well-targeted and address both immediate and long-term considerations for organizations.

3. Modern and Forward-Looking Approach

By integrating AI-driven tools and anti-discriminative optimization into the discussion, the project reflects a forward-thinking perspective. This is particularly valuable in a world where automation and ethical considerations are increasingly central to IT operations.

4. Ethical Considerations

The project's acknowledgment of the social responsibilities tied to remote work, such as preventing discrimination and promoting inclusivity, adds depth to its recommendations. This signals an awareness of the human element in technological risk management.

Suggestions for Improvement and Critique

1. Insufficient Depth in Evaluation Processes

While the project identifies critical parameters, the methodology for evaluating and prioritizing risks is somewhat underexplored. For instance:

- How are parameters weighted or scored in practical scenarios?
- Are there quantitative models, like scoring systems, to rank risks effectively?

Adding such details would greatly enhance the utility and replicability of the framework.

2. Limited Practical Application

A notable gap is the lack of real-world examples or case studies. These would help translate theoretical ideas into actionable strategies, making the framework more relatable and robust.

3. Overlooked Emerging Threats

Although the project effectively addresses traditional risks, it could have explored modern challenges in greater detail, such as:

- Cybersecurity vulnerabilities in collaboration tools (e.g., video conferencing).

- Employee well-being, particularly mental health and productivity in remote settings.
- AI misuse and cloud service misconfigurations.

Including these would ensure the framework remains relevant in the fast-evolving landscape of IT risk management.

4. Balance Between Theoretical and Practical Aspects

The project leans heavily on a theoretical foundation. While the structure is solid, the lack of specific actionable guidelines or tools for implementation makes it less practical for immediate adoption by businesses.

5. Room for Innovation

While the integration of AI tools is a strong point, the project could delve deeper into how AI technologies can proactively predict and prevent risks, rather than merely assist with evaluation.

Final Thoughts

This project lays a strong foundation for addressing IT risks in home-office environments, combining logical structure with an emphasis on technological and ethical considerations. Its strengths lie in its comprehensiveness and adaptability. However, to truly stand out, it needs to bridge the gap between theory and application by incorporating more actionable insights, real-world examples, and a detailed evaluation methodology. Additionally, addressing modern and emerging threats would bolster its relevance in an ever-changing digital landscape.

Overall, it's a promising and commendable initiative, but refining these areas would elevate its impact significantly.

Legend: Attribute ID

A1: Layers of the Firewall

A2: No. of Devices connected to the Wi-Fi network

A3: How many times is the Wi-Fi password changed in a month

A4: Length of Wi-Fi encryption Key

A5: Year of the Router

A6: Year of the User Device

A7: Number of Days since the last Software Update

A8: How many Threats Detected by the Antivirus software in the last month

A9: How many Threats Detected by the Antivirus software in the last month

A10: Intrusion Detection System

A11: Total Amount of downloaded Data in Last week

A12: Total Number of Files Downloaded in Last Week

A13: Percent of total Logins hours when VPN was used

A14: How many times user visited Blacklisted websites by company Last week

A15: How many times Personal Accounts were used to Login in the last week

A16: How many days beyond 12 hours per day were worked in the last week

A17: How many times the user downloaded company Unauthorized Software

Chapter 8.5. IKSAD Publication: Aadi Rajesh et. al

https://miau.my-x.hu/miau/311/home_office_risks/full_home_office_risks.pdf

5th International Congress on Scientific Research April 21-22, 2024, Türkiye by IKSAD Institute

Risk-evaluation possibilities concerning IT-activities in home-office

Presenter: Aadi Rajesh: Kodolányi János University

Supervisors: László Pitlik (Jr.) & Dr. László Pitlik

Full Text

Introduction

As more and more companies are opting for remote or hybrid work opportunities, workers are enjoying the possibility to work from home or anywhere, which gives me more freedom and a better work-life balance.

But this luxury comes at a cost and risk of increased vulnerabilities to cyber-attacks and other challenges. Therefore, companies need to invest in advanced cyber-security tools and strategies to mitigate these risks and challenges and continue operational stability, data protection and focus on business related activities.

Evaluating risks associated with IT activities in a home-office environment involves identifying potential threats and vulnerabilities, assessing their likelihood and impact, and implementing measures to mitigate or manage these risks¹.

Literature

Performing risk evaluations for IT activities in a home-office environment is crucial for several reasons:

1. Security: It helps ensure the security of sensitive data and information. With the increasing prevalence of cyber threats such as malware, phishing, and ransomware, understanding and mitigating risks is essential to protect personal and business data.²
2. Compliance: Many industries and jurisdictions have regulations and compliance standards related to data protection and security. Conducting risk evaluations helps ensure compliance with these regulations, avoiding potential legal consequences and penalties.³
3. Business Continuity: Identifying and mitigating risks helps minimize the potential for disruptions to home-office activities. By proactively addressing vulnerabilities, individuals can reduce the likelihood and impact of incidents that could interrupt work or compromise productivity⁴.
4. Protecting Assets: Home-office setups often include valuable assets such as computers, networking equipment, and intellectual property. Assessing risks helps safeguard these assets from theft, damage, or unauthorized access⁵.
5. Reputation Management: A security breach or data loss can damage an individual's or business's reputation. By understanding and mitigating risks, individuals can demonstrate

their commitment to security and protect their reputation among clients, customers, and stakeholders⁶

6. Cost Savings: Addressing risks proactively can help avoid the financial costs associated with security incidents, such as data recovery, legal fees, regulatory fines, and loss of business opportunities. Investing in security measures upfront can save money in the long run.⁷

7. Peace of Mind: Knowing that risks have been identified and mitigated provides peace of mind for individuals working from home. It allows them to focus on their work without constantly worrying about potential security threats or disruptions.⁸

8. Compliance, trust and reliability: For a company, being able to be compliant, trusted and reliable is of utmost importance for its business continuity, customer satisfaction and future growth potential. Companies which invest in better cyber security can gain trust and confidence of their vendors and customers, which is crucial for a sustainable long-term business growth and continuity strategy⁹.

In summary, conducting risk evaluations for IT activities in a home-office environment is essential for protecting data, ensuring compliance, maintaining business continuity, safeguarding assets, managing reputation, saving costs, and providing peace of mind.

Own analyses

The risk potential concerning the IT activities in the home office can be described with a lot of abstraction/attributes (c.f. Compliance Violations, Remote Access Vulnerabilities, Cyber Attacks, Data Breaches, Third-party Software Risks etc.) By creating a system of most important objects and attributes, we can create parameters based on which we could analyse the risk based on an online AI-tool where anti-discriminative optimizations can be run using stair-case functions concerning the hypothesis whether each object can have the same risk index or not? Some of the attributes include Number of firewalls in the network, Scores from Intrusion detection and antivirus systems, no of users who access the device, number of non-authorized user logins, Password change frequency, etc. While creating an analytical model brought it its own challenges and issues, the most challenging task is the collection of real or realistic raw data. As most antivirus and threat detection software use proprietary access, and getting data from offices can be challenging due to various legal issues

such as GDPR, company policies, data sharing rules etc. This task has been circumvented by first creating quasi-randomized data using real life research on the likelihood of various parameters and their minimum, maximum, average, mean, median and mode values and gain real life data, without names or any personalized information of the user.

Rational and OAM

The first step for this project was to understand which attributes can affect cyber security at home office situations and if they are human factors or machine factors. Figure 0 summarizes the progress.

Type	ID + Attributes
Machine Scores	Public vs Private Wi-Fi
Machine Scores	Devices in the LAN
Machine Scores	Quality of hardware
Machine Scores	Number of Firewalls
Machine Scores	Settings on Firewall
Machine Scores	VPN
Machine Scores	Antivirus Results
Machine Scores	Software Updates
Machine Scores	Intrusion Detection System (IDS)
Machine Scores	Alerts
Machine Scores	Network Traffic Analysis
Human Scores	Using unauthorized websites
Human Scores	Compliance with accounts
Human Scores	Stress
Human Scores	Phishing Email Testing

Human Scores	Trainings score
Human Scores	Questionnaire
Human Scores	Authorized Software

Figure#0: Various Machine and Human Scores and Attributes, source: Own Presentation

After analyzing this Machine-Human Attribute matrix, I could select some appropriate attributes for the Object-Attribute Matrix (OAM)

Attribute ID

1. A1: Layers of the Firewall
2. A2: No. of Devices connected to the Wi-Fi network
3. A3: How many times is the Wi-Fi password changed in a month
4. A4: Length of Wi-Fi encryption Key
5. A5: Year of the Router
6. A6: Year of the User Device
7. A7: Number of Days since the last Software Update
8. A8: How many Threats Detected by the Antivirus software in the last month
9. A9: How many Threats Detected by the Antivirus software in the last month
10. A10: Intrusion Detection System
11. A11: Total Amount of downloaded Data in Last week
12. A12: Total Number of Files Downloaded in Last Week
13. A13: Percent of total Logins hours when VPN was used
14. A14: How many times user visited Blacklisted websites by company Last week
15. A15: How many times Personal Accounts were used to Login in the last week
16. A16: How many days beyond 12 hours per day were worked in the last week
17. A17: How many times the user downloaded company Unauthorized Software

Moving forward from the attribute selection, it was important to understand the direction vector of the attribute. In short, 0 was assigned to attributes whose higher value is directly proportional to more security and 1 was assigned to attributes, whose higher value meant less security.

But some attributes might be like the Schrödinger Cat or an Electron with dual personalities. For example: Firewall threat detection: If a firewall is showing us a lot of threats, that could mean both things:

- Either our network is very unsafe
- Or the Firewall works too well
- Or Both

On the other Hand, if the Firewall detects too less or 0 cases

- Either our network is military grade secure
- Or our firewall doesn't work at all
- Or both

Similar dilemmas could be in Intrusion detection systems, Malware analysis or Antivirus analysis.

In these cases, we could set some generic rules, to create a balance of power and make some checks and balances. We could use the class If-Else. If pyramid. For example: if firewall detects less threats, and Intrusion System Detects less threats and Antivirus analysis detects less threats than we can use this case as TRUE. But, if either of the cases is not true, we can assume false. We could also add to the if-else clause more predictable measures such as percentage of time VPN was used etc.

Going ahead with the attribute selection and their direction, I populated the matrix (see Figure#1) with possible real-life values for various attributes and test subjects.

Attribute ID	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17
Attribute Unit	Integer Number	Integer number	Integer Number	Bits	Year	Year	Days	Integer	Integer	Integer	GB	Integer	Percentage	Integer	Integer	Hours	Integer
Attribute Direction	0	1	0	0	0	0	0	1	1	0	1	1	1	0	1	1	1
Test Subject : Mr. K	5	9	0	128	2014	2018	78	45	45	50	15	59	76	5	12	3	4
Mr. L	9	8	0	192	2015	2019	76	99	99	31	158	454	27	123	10	25	5
Mr. J	7	2	5	256	2024	2015	68	24	24	5	59	209	10	151	10	5	8
Mr. P	4	6	1	192	2021	2016	59	50	50	61	603	150	29	53	9	30	10
Mr. T	6	2	5	128	2014	2016	69	16	16	78	34	61	48	144	2	1	0
Mr. W	4	7	5	128	2022	2018	86	74	74	22	837	480	50	112	5	7	7
Mr. Z	8	5	3	128	2022	2024	80	23	23	1	985	296	70	58	8	14	8
Mr. I	6	3	4	128	2023	2020	42	12	12	38	121	286	73	117	2	14	0
Mr. Q	8	5	5	256	2022	2019	81	32	32	25	939	138	75	186	3	5	1
Mr. U	4	9	5	128	2019	2019	35	72	72	49	204	417	86	35	5	20	5
Mr. A	9	7	1	192	2019	2018	64	82	82	40	409	231	97	39	4	20	5
Mr. D	9	5	3	128	2019	2017	10	2	2	19	309	67	24	168	0	6	3
Mr. Y	3	2	2	128	2021	2016	33	83	83	8	447	151	97	134	0	12	4
Mr. H	9	5	1	128	2022	2019	50	54	54	72	463	2	31	91	4	20	3
Mr. C	8	9	3	128	2021	2014	14	25	25	62	264	66	100	4	5	19	0
Mr. N	5	7	3	256	2018	2016	78	62	62	51	912	201	82	54	0	15	7
Max	9	10	5	256	2024	2024	90	100	100	100	1000	500	100	200	10	30	10
Min	3	0	0	128	2014	2014	1	1	1	1	1	0	0	0	0	0	0

Figure 1: Various Attributes (OAM) used for the Risk Analysis

(Source: Own presentation)

Legend: for Attribute IDs see above

With the working model, attributes, objectives and data at hand the next step is to analyze this data using specialized tools, such as AI and advanced data analytics. For this, first a rank analysis was done using EXCEL features and then COCO (Component-based Object Comparison for Objectivity: <https://miau.my-x.hu/myx-free/>) AI Analysis was used.

The rank (see Figure#2) feature arranged the test subjects in order of their direction and for every attribute, calculated which test subjects are at higher risks for a cyber-attack and show more vulnerability. This helped us bring out real and useful information from our raw data, but we needed a better tool, which could analyze the entire data sets, with all the rankings per attributes and then predict from all the subjects, and attributes, which test subjects are at the higher risk.

For this task, a three-step process was used.

Step 1: Creating an auxiliary table, using a Y (0) constant module

Step 2: Getting the scores and differences of the Auxiliary Table

Step 3: Using online COCO analysis

COCO Analysis is an AI based analytical tool which can help in predicting pointers and key data directions in large data sets. The AI program can be used as a ranking module and helps predict which attributes are more important than others and use ai to predict outcomes¹⁰.

With this data from the COCO AI analysis, the data analytics team and the company managers can have real life use for this project as a power strategy for data analytics and data summarization.

The tool can be used by the IT monitoring team for threat analysis and Management team to provide targeted training and preventive measures against cyber security threats.

Ranking	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	Y
Attribute ID																		
Test Subject : Mr. K	11	14	15	7	15	7	12	8	9	11	1	2	6	2	16	2	7	1000
Mr. L	1	13	15	4	14	3	11	16	1	7	5	15	14	11	14	15	9	1000
Mr. J	8	1	1	1	1	15	9	5	12	2	3	10	16	14	14	3	14	1000
Mr. P	13	9	12	4	7	11	7	9	8	13	12	7	13	5	13	16	16	1000
Mr. T	9	1	1	7	15	11	10	3	14	16	2	3	11	13	4	1	1	1000
Mr. W	13	10	1	7	3	7	16	13	4	5	13	16	10	9	9	6	12	1000
Mr. Z	5	5	7	7	3	1	14	4	13	1	16	13	9	7	12	8	14	1000
Mr. I	9	4	6	7	2	2	5	2	15	8	4	12	8	10	4	8	1	1000
Mr. Q	5	5	1	1	3	3	15	7	10	6	15	6	7	16	6	3	4	1000
Mr. U	13	14	1	7	10	3	4	12	5	10	6	14	4	3	9	12	9	1000
Mr. A	1	10	12	4	10	7	8	14	3	9	9	11	2	4	7	12	9	1000
Mr. D	1	5	7	7	10	10	1	1	16	4	8	5	15	15	1	5	5	1000
Mr. Y	16	1	11	7	7	11	3	15	2	3	10	8	2	12	1	7	7	1000
Mr. H	1	5	12	7	3	3	6	10	7	15	11	1	12	8	7	12	5	1000
Mr. C	5	14	7	7	7	16	2	6	11	14	7	4	1	1	9	11	1	1000
Mr. N	11	10	7	1	13	11	12	11	6	12	14	9	5	6	1	10	12	1000

Figure 2: Ranking Based on Excel Solver Module (source: Own presentation)

Unit Ranking 1- 16, 1= Least risky, 16: Highest risk, Unit for Y0: risk index/score

Figure #3 shows the results from the excel solver analysis, which helped us understand the work model of the OAM matrix and helped in understanding the rank function and analysis.

Auxiliary Tables	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17
1	75	67	14	50	99	72	43	84	54	66	64	85	61	92	85	77	88
2	59	77	93	70	22	46	49	54	24	72	16	64	61	68	31	72	86
3	78	31	62	31	78	90	97	76	96	77	98	71	44	99	28	82	12
4	15	38	36	74	19	83	97	53	16	87	29	42	32	56	96	58	96
5	37	88	39	36	25	63	34	18	84	88	11	81	13	97	94	52	71
6	87	37	92	95	38	25	26	27	88	68	69	90	11	82	13	15	94
7	28	100	57	69	28	76	17	15	20	96	78	99	72	75	51	11	58
8	53	19	40	28	23	88	100	23	23	53	31	95	30	21	84	88	12
9	83	16	66	55	52	42	56	26	80	92	76	38	92	54	59	70	62
10	19	21	94	89	76	47	84	98	60	76	65	56	28	90	39	57	67
11	54	60	46	58	33	60	75	52	20	37	38	57	99	67	22	17	78
12	56	57	54	86	14	66	51	38	51	82	92	100	55	82	51	22	76
13	55	44	69	69	10	30	52	29	98	62	92	95	40	89	48	81	68
14	64	93	31	10	26	46	65	95	32	42	27	36	46	42	54	71	84
15	12	92	29	74	47	69	96	14	38	50	61	57	32	14	18	71	67
16	91	53	90	17	54	32	21	13	90	31	42	53	90	83	18	85	91

Figure 3: Excel Solver (Source: Own presentation)

Unit 0-100, 0: Low Likelihood of Cyber Threat, 100: High Likelihood

But due to the complexities of the data and the need to analyze the entire data sets, with all the rankings per attributes and then predict from all the subjects, and attributes, which test subjects are at the higher risk. Coco AI analysis (online) was used Figure #4 and in Figure #5,

The analysis not only predicted which test subjects are at higher cyber security risks but also predicted which attributes had a higher impact on the score and which ones lesser. This analysis using AI tools provides invaluable power of information to the human users and helps understand vulnerabilities and points of improvements in our own systems.

Figure 4: Coco Analysis (online) (Source: Own presentation)

Unit for Y0: risk index/score

Figure 5: Score Calculation Chart (based on two parallel calculation processes)

Unit for Y0 and for all its aggregated component: risk index/score

stairs(2)	X(A1)	X(A2)	X(A3)	X(A4)	X(A5)	X(A6)	X(A7)	X(A8)	X(A9)	X(A10)	X(A11)	X(A12)	X(A13)	X(A14)	X(A15)	X(A16)	X(A17)
S1	15	15	15	35	15	423	15	33	540	426	424	397	15	434	16	394	15
S2	14	14	14	14	14	422	14	32	88	425	423	58	14	433	15	14	14
S3	13	13	13	13	13	14	13	31	87	424	422	57	13	432	14	13	13
S4	12	12	12	12	12	13	12	30	86	423	421	56	12	431	13	12	12
S5	11	11	11	11	11	12	11	29	85	422	381	55	11	430	12	11	11
S6	10	10	10	10	10	11	10	28	84	421	380	54	10	429	10	10	10
S7	9	9	9	9	9	10	9	9	83	9	379	53	9	40	9	9	9
S8	8	8	8	8	8	9	8	8	82	8	378	8	8	39	8	8	8
S9	7	7	7	7	7	8	7	7	7	7	373	7	7	38	7	7	7
S10	6	6	6	6	6	7	6	6	6	6	372	6	6	6	6	6	6
S11	5	5	5	5	5	5	5	5	5	5	371	5	5	5	5	5	5
S12	4	4	4	4	4	4	4	4	4	4	370	4	4	4	4	4	4
S13	3	3	3	3	3	3	3	3	3	3	369	3	3	3	3	3	3
S14	2	2	2	2	2	2	2	2	2	2	368	2	2	2	2	2	2
S15	1	1	1	1	1	1	1	1	1	1	367	1	1	1	1	1	1
S16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 6: Score Chart (staircase functions) (Source: own presentation)

Unit for Y0 and for all of its aggregated component (especially for all stair-levels):

risk index/score

COCO: Y0	X(A1)	X(A2)	X(A3)	X(A4)	X(A5)	X(A6)	X(A7)	X(A8)	X(A9)	X(A10)	X(A11)	X(A12)	X(A13)	X(A14)	X(A15)	X(A16)	X(A17)	Estimation	Fact+0	Delta	Delta/Fact
O1	5	2	1	9	1	10	4	8	7	5	424	58	10	433	0	14	9	1000	1000	0	0
O2	15	3	1	12	2	14	5	0	540	9	381	1	2	5	2	1	7	1000	1000	0	0
O3	8	15	15	35	15	1	7	29	4	425	422	6	0	2	2	13	2	1001	1000	-1	-0.1
O4	3	7	4	12	9	5	9	7	82	3	370	53	3	430	3	0	0	1000	1000	0	0
O5	7	15	15	9	1	5	6	31	2	0	423	57	5	3	13	394	15	1001	1000	-1	-0.1
O6	3	6	15	9	13	10	0	3	86	422	369	0	6	38	7	10	4	1001	1000	-1	-0.1
O7	11	11	9	9	13	423	2	30	3	426	0	3	7	40	4	8	2	1001	1000	-1	-0.1
O8	7	12	10	9	14	422	11	32	1	8	421	4	8	6	13	8	15	1001	1000	-1	-0.1
O9	11	11	15	35	13	14	1	9	6	421	367	54	9	0	10	13	12	1001	1000	-1	-0.1
O10	3	2	15	9	6	14	12	4	85	6	380	2	12	432	7	4	7	1000	1000	0	0
O11	15	6	4	12	6	10	8	2	87	7	373	5	14	431	9	4	7	1000	1000	0	0
O12	15	11	9	9	6	7	15	33	0	423	378	55	1	1	16	11	11	1001	1000	-1	-0.1
O13	0	15	5	9	9	5	13	1	88	424	372	8	14	4	16	9	9	1001	1000	-1	-0.1
O14	15	11	4	9	13	14	10	6	83	1	371	397	4	39	9	4	11	1001	1000	-1	-0.1
O15	11	2	9	9	9	0	14	28	5	2	379	56	15	434	7	5	15	1000	1000	0	0
O16	5	6	9	35	3	5	4	5	84	4	368	7	11	429	16	6	4	1001	1000	-1	-0.1

Figure 7 Estimation of the risks (multidimensional optimized aggregation)

(Source: Own presentation)

Unit for Y0 and for all its aggregated component: risk index/score

Legend: Attribute ID

1. A1: Layers of the Firewall
2. A2: No. of Devices connected to the Wi-Fi network
3. A3: How many times is the Wi-Fi password changed in a month
4. A4: Length of Wi-Fi encryption Key
5. A5: Year of the Router
6. A6: Year of the User Device

7. A7: Number of Days since the last Software Update
8. A8: How many Threats Detected by the Antivirus software in the last month
9. A9: How many Threats Detected by the Antivirus software in the last month
10. A10: Intrusion Detection System
11. A11: Total Amount of downloaded Data in Last week
12. A12: Total Number of Files Downloaded in Last Week
13. A13: Percent of total Logins hours when VPN was used
14. A14: How many times user visited Blacklisted websites by company Last week
15. A15: How many times Personal Accounts were used to Login in the last week
16. A16: How many days beyond 12 hours per day were worked in the last week
17. A17: How many times the user downloaded company Unauthorized Software

Results

The result of the project was that using the OAM, Data Analysis and COCO analysis, I could predict which users are at a higher risk and vulnerability than others.

This real-life information can be invaluable as managers and company cost accountants can dedicate resources and training to help those individuals with higher risk analysis scores and help improve the overall risk management and vulnerability of the company.

This will in turn improve the company's performance, efficiency, reliability and can lead to better compliance and profit margins.

Discussions

In cyber security, change is the only constant and regular upgradation of ideas, skills sets and approaches is needed to stay on top of cyber security threats and prevent cyber-attacks and mitigate any risk associated with it.

In a realist world view scenario, being actively prepared for threats and constant vulnerability testing is needed and for that I would appreciate constructive feedback and criticism of my

structure, OAM approach, analysis and results. This feedback will help me improve this project and assist in my personal and professional development as an aspirational cyber security expert.

I encourage you to reach out to my email address, nayyaraadi@gmail.com for your feedback and suggestions for this project.

Conclusions and Summary

In conclusion, the OAM matrix gives us a great springboard for analyzing the threat analysis and use this information for further analysis using AI. AI tools such as COCO analysis can help analyze complex datasets and help predict outcomes which can be used to resolve real-world problems.

The key take away is the use of Human-AI integration as by using AI, humans can solve much complex problems in shorter times and improve the overall efficiency, quality and reliability of the project.

In this project as well, I, a Human creator thought of a real-world problem and created an analysis for this problem, and curated the structures, by which I could solve this issue. The AI helped me in the next step by analyzing points from these architectural structures and gave me real life information and analysis, which could be used to resolve my problem.

Future Directions

To summarize, the project: Risk-evaluation possibilities concerning IT-activities in home-office has reached a critical stage where I could resolve the first part of the real-life problem and implement a computer-based model, with the help of AI analysis, where i could use an OAM and create a working structure for threat analysis and prevention.

This project can be scaled further in various directions and the direction of my choosing is improving the attributes list by adding better and more relevant attributes and removing the attributes which have limited impact of the study and second is to automate the data collection process.

An automated working model, with appropriate attributes, would have a functional real-life application as it could be scaled up or down as per the needs of the company.

Another addition to this project could be the assimilation of the project as a true AI human integration project as human inputs are augmented by AI, and AI gets its logical direction and needs analysis from humans. This integration has begun in most industries of the world, and this project would focus on this direction too.

References

Nwankpa, J. K., & Datta, P. (2023, July 1). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*. <https://doi.org/10.1016/j.cose.2023.103266>

Hewitt, N. (2023, July 28). Cybersecurity Planning for Business Continuity. TrueFort. <https://truefort.com/cybersecurity-business-continuity/>

Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events | NCCoE. (n.d.). NCCoE. <https://www.nccoe.nist.gov/data-integrity-identifying-and-protecting-assets-against-ransomware-and-other-destructive-events>

How to Manage Reputational Damage in Cyber Security | Institute of Data. (2023, October 17). Institute of Data. <https://www.institutedata.com/blog/reputational-damage-in-cyber-security/#:~:text=Managing%20reputational%20damage%20in%20cyber%20security%20requires%20a%20long%2Dterm,the%20risk%20of%20future%20incidents.>

Eeckman, S. (2020, April 27). Peace of mind when it comes to privacy and security. Microsoft Pulse. <https://pulse.microsoft.com/en/work-productivity-en/na/fa2-peace-of-mind-when-it-comes-to-privacy-and-security/>

Pitlik, László. (2010). About the method of Component-based Object Comparison for Objectivity (COCO). *Magyar Internetes Alkalmazott/Agrárinformatikai Újság (MIAÚ)*. 13. https://www.researchgate.net/publication/270576061_About_the_method_of_Component-based_Object_Comparison_for_Objectivity_COCO

Own abstract and presentation: Aadi Rajesh, László Pitlik (Jr.), Dr. László Pitlik. : Risk-evaluation possibilities concerning IT-activities in home-office, 5th International Congress on Scientific Research April 21-22, 2024, Türkiye by IKSAD Institute

Chapter 8.6. Software Documentation

The software was made in collaboration with Latif Muhammad Khuram under the constant support and supervision of Dr László Pitlik, Professor László Pitlik Jr. and Professor Mátyás Pitlik.

Risk Assessment for Remote Workers

Introduction

As more companies embrace remote work, they face an increasing number of cybersecurity challenges. These risks stem from factors such as unsecured network connections, unauthorized access, and potential data breaches. To help mitigate these risks, this system evaluates security threats by analysing key indicators, identifying patterns, ranking individuals based on risk levels, and generating reports for further assessment. This approach enables organizations to take proactive measures to protect sensitive information and maintain a secure remote working environment.

Data Handling and Preprocessing

Importing Data from a CSV File

The system starts by retrieving cybersecurity-related data from a CSV file, which contains various security metrics for remote employees. These metrics may include unsuccessful login attempts, the frequency of software updates, network activity, and other factors that could indicate potential security vulnerabilities.

To maintain data accuracy, the system checks whether the file has a valid header row. If the first row consists of non-numeric values, it is skipped to ensure proper data processing. The system then extracts and processes numerical values, as they are essential for performing risk assessments and ranking employees accordingly.

Removing Unnecessary Data

Some columns in the dataset may not contribute meaningfully to the analysis. If a column contains the same value across all rows, it does not add any variability and is therefore removed. This step helps streamline the assessment process by focusing only on relevant and dynamic data points.

Organizing workers Data

Each employee's cybersecurity information is stored using a structured format. A RemoteWorker class is used to manage individual records, including the employee's name and corresponding numerical security metrics. After preprocessing the data, the system proceeds to correlation analysis to identify risk-related patterns.

Correlation Analysis

Understanding Relationships Between Correlation Metrics

Correlation analysis helps determine how different security attributes are related. This relationship is measured using a correlation coefficient, which falls within the range of -1 to +1:

- +1: Strong positive correlation (when one factor increases, the other also increases).
- -1: Strong negative correlation (when one factor increases, the other decreases).
- 0: No correlation (no clear relationship between the two variables).

For example, if failed login attempts and unauthorized access alerts show a strong positive correlation, it may indicate a security threat requiring further investigation. Similarly, if frequent software updates show a negative correlation with malware infections, it suggests that regular updates help prevent security risks.

Creating a Correlation Matrix

To make these relationships more understandable, the system generates a correlation matrix. This matrix visually represents the strength of connections between different security factors, helping cybersecurity analysts identify potential risk patterns and take appropriate action.

Defining Risk Indicators

How Different Security Attributes Affect Risk Levels

Not all security metrics impact risk assessment in the same way. Some indicate a higher risk when their values increase, while others signal greater risk when their values decrease. To accommodate these differences, the system allows users to classify attributes accordingly:

- Higher Value = Higher Risk (Marked as 0)

- Example: A higher number of failed login attempts may indicate an increased risk of security breaches.
- Example: Frequent unauthorized network access attempts may suggest a potential cyberattack.
- Lower Value = Higher Risk (Marked as 1)
 - Example: Low disk space could indicate poor system maintenance, potentially affecting security.
 - Example: Infrequent software updates may leave a system vulnerable to cyber threats.

Ensuring Logical Consistency in Risk Indicators

To maintain consistency, the system verifies that attribute classifications align logically with the correlation matrix. If two attributes show a strong correlation (absolute value greater than 0.3), the system prompts the user to review their classifications to ensure accuracy.

Process Overview:

1. The system checks correlations between each attribute pair.
2. If a strong correlation is detected, users are asked to confirm or adjust attribute classifications.
3. Adjustments are made to ensure that positively correlated attributes share the same classification, while negatively correlated attributes have opposite classifications.

Key	Benefits:					
✓	Helps	maintain	consistency	in	risk	evaluation.
✓	Improves	the	accuracy	of	cybersecurity	assessments.
✓	Reduces potential errors in risk classification.					

Ranking Methodology

Determining Employee Risk Rankings

The system ranks remote employees based on security-related attributes. It considers whether a higher or lower value corresponds to greater security risk and assigns rankings accordingly:

- If an attribute is set to ascending (1), higher values are considered better and lead to a lower risk ranking.
- If an attribute is set to descending (0), lower values are considered better and result in a lower risk ranking.

Process Overview:

1. Employees are sorted based on their attribute values.
2. Rankings are assigned, with a rank of 1 indicating the least risky value according to the attribute classification.
3. If multiple employees have the same value, they are assigned the same rank to maintain fairness.

Structuring and Storing Rankings

The system organizes rankings using the PrepareRankedValues method, ensuring that they are stored efficiently for further analysis.

Key	Benefits:
✓ Simplifies the interpretation of security risks.	
✓ Facilitates seamless integration with cybersecurity monitoring tools.	

Saving and Submitting Rankings

Storing Risk Rankings Locally

To keep records up to date, the system saves ranked data to a designated file location. Previous files are overwritten to ensure the latest security assessments are always available.

Key	Benefits:
✓ Provides historical records for risk trend analysis.	
✓ Allows offline access for security reviews.	

Submitting Risk Data to a Coco engine

For broader security monitoring, ranked data can be transmitted to a Coco engine using an HTTP POST request through CURL. The Coco engine processes the data and gives an output, which is saved locally for review.

Process Overview:

1. The system reads ranking data from the saved file.
2. The data is securely transmitted to a Coco engine.
3. The Coco engine processes the data and returns an output.

Key

- ✓ Supports integration with enterprise cybersecurity solutions.
- ✓ Enhances scalability by leveraging remote security infrastructure.

Benefits:

Identifying High-Risk Employees

Highlighting Employees with the Highest Risk Scores

Using the `DisplayHighestRiskObjects` method, the system identifies employees with the highest risk levels.

Process Overview:

1. Risk values are analyzed to determine the highest recorded risk.
2. Employees matching this risk level are identified.
3. Their names and associated risk factors are displayed.

Key

- ✓ Helps security teams prioritize threats.
- ✓ Enables targeted security measures for high-risk employees.

Benefits:

User Support and Assistance

Providing Help and Guidance

To ensure ease of use, the system includes a help feature that provides step-by-step instructions on how to input security attributes, interpret rankings, and troubleshoot common issues.

Key

- ✓ Enhances user experience by providing clear guidance.
- ✓ Helps prevent input errors, improving assessment accuracy.

Benefits:

Conclusion

This risk assessment system is designed to help organizations strengthen cybersecurity for remote employees. By integrating data preprocessing, correlation analysis, and ranking methodologies, it provides a structured approach to identifying potential security vulnerabilities. With its modular and adaptable design, the system can be easily maintained and integrated into existing cybersecurity frameworks, making it a valuable tool for organizations seeking to enhance their security posture.

Chapter 8.7. Screenshots of the Project with My Parameters

Test Case: 6 Attributes, 6 Objects

1	oam	Layers of the Firewall	Length of Wi-Fi Encryption Key	Number of Times User Downloaded Unauthorized Software	Total Number of Files Downloaded in the Last	Number of Days Worked Beyond 12 Hours per	Percentage of Total Login Hours When VPN Was	Norm Value
2	o1	324	99	453	523	907	420	1000
3	o2	897	607	272	981	882	231	1000
4	o3	73	945	855	955	942	304	1000
5	o4	588	635	934	931	453	523	1000
6	o5	56	159	510	902	272	981	1000
7	o6	250	916	164	349	855	955	1000
8								
9								

Figure A1: Chosen attributes and values Source: url, sheet-name, range-parameters

Source: Own Software Developed with Latif Muhammad

Correlation Matrix (Lower Triangular):						
Attr\Attr	A1	A2	A3	A4	A5	A6
A1	1.00					
A2	0.05	1.00				
A3	-0.18	0.10	1.00			
A4	0.26	0.01	0.58	1.00		
A5	0.17	0.42	-0.30	-0.34	1.00	
A6	-0.53	-0.14	-0.31	-0.46	-0.57	1.00

Attribute Directions alerts:

1. A high positive correlation (+1.0) means both attributes move in the same direction.
2. A high negative correlation (-1.0) means one attribute increases when the other decreases.
3. For positively correlated attributes, you may want to set similar directions.
4. For negatively correlated attributes, consider setting opposite directions and direction can be 0 and 1.

Figure A2: Ranking file Figure in a Corelation Matrix Source: Own Software Developed with Latif Muhammad

```

Validating user input directions...
negative correlation detected between Attributes 1 and 6 (-0.53).
Directions for Attributes 1 and 6 are already consistent.
positive correlation detected between Attributes 3 and 4 (0.58).
Inconsistent directions detected for Attributes 3 and 4. Adjusting input required.
Re-enter direction for Attribute 3 (current: 1): 0
Re-enter direction for Attribute 4 (current: 0): 0
Do you want to recheck the consistency for Attributes 3 and 4? (yes/no): no
Skipping consistency recheck for Attributes 3 and 4.
negative correlation detected between Attributes 5 and 6 (-0.57).
Directions for Attributes 5 and 6 are already consistent.
Validation complete.
Ranked values saved to: E:\New folder\Curl\tempRankedValues.txt
Sending request to server...

```

Figure A3: Input Directions Source: Own Software Developed with Latif Muhammad

```

Response from server:
997
999
1014
1005
991
993

Object 3 facing the highest risk: 1014

```

Figure A4: Results of Analysis Source: Own Software Developed with Latif Muhammad

Using this analysis, we can see that based on the attributes and the objects, Object 3 faces the highest risks, and the company can use targeted training to assist the employees in improving the cybersecurity score, to improve the overall cybersecurity preparedness of the company.

Chapter 8.8. Coco Analysis and my Excel File

Source: Author's own work <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>

Unit	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	%
COO0-10													
Layer 2 of the Firewall	No. of Devices connected to the self network	How many times is the WiFi password changed in a month	Year of the Router	Number of Days since the last software update	Number of Days since the last software update	How many times the user downloaded company (unauthorized) software	Estimation	PassID	Salary	Debit/Paid			
Test Subject No. 1	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 2	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 3	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 4	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 5	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 6	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 7	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 8	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 9	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 10	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 11	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 12	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 13	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 14	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 15	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 16	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 17	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 18	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 19	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 20	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 21	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 22	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 23	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 24	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 25	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 26	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 27	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 28	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 29	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000
Test Subject No. 30	1000	1	1	1	1000	1000	1000	1000	1000	1000	1000	1000	1000

Figure A5: Risk Point Scores for various Subjects per Attribute: Source: Author's own work <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx> : Excel sheet title COCO , B90:B107, M90:M107

By using COCO Y0 analysis, I got the risk point scores of various subjects per attribute. This information is crucial in my project as it can help identify which subjects are more vulnerable in certain parameters than others, and by using directed, focused trainings and inputs, the cybersecurity risks of the subject can be mitigated.

	Risk Point	Risk Point	Risk Point	Risk Point	Risk Point	Code	Text-template
Validation	Direct Estimation	Direct Delta	NORM	Inverse Estimation	Inverse Delta	VALIDATION	Interpretations
Test Subject Mr. K	974.9	25.1	1000	1023.8	-23.8	1	Symmetry-ok
Test Subject Mr. L	993.9	6.1	1000	1005.3	-5.3	1	Symmetry-OK
Test Subject Mr. M	1018.5	-18.5	1000	981.4	18.6	1	Symmetry-OK
Test Subject Mr. N	979.4	20.6	1000	1019.8	-19.8	1	Symmetry-OK
Test Subject Mr. O	1023	-23	1000	977.9	22.1	1	Symmetry-ok
Test Subject Mr. P	992.4	7.6	1000	1007.8	-7.8	1	Symmetry-ok
Test Subject Mr. Q	985.4	14.6	1000	1015.3	-15.3	1	Symmetry-ok
Test Subject Mr. R	1026.5	-26.5	1000	970.9	29.1	1	Symmetry-ok
Test Subject Mr. S	1011.5	-11.5	1000	984.4	15.6	1	Symmetry-ok
Test Subject Mr. T	991.4	8.6	1000	1009.3	-9.3	1	Symmetry-ok
Test Subject Mr. U	985.4	14.6	1000	1014.3	-14.3	1	Symmetry-ok
Test Subject Mr. V	1029	-29	1000	972.9	27.1	1	Symmetry-ok
Test Subject Mr. W	990.4	9.6	1000	1010.3	-10.3	1	Symmetry-ok
Test Subject Mr. X	1025.5	-25.5	1000	978.9	21.1	1	Symmetry-ok
Test Subject Mr. Y	993.9	6.1	1000	1007.8	-7.8	1	Symmetry-ok
Test Subject Mr. Z	978.9	21.1	1000	1020.3	-20.3	1	Symmetry-ok

Figure A6: Validation for Risk Scores: Source: Author's own work <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>: Excel sheet title COCO, B123:B140, I123:I40

Using validation, I could verify the Consistency of input values via Data Validation to confirm the validity of the project and analysis.

Using	Risk points		Risk points		Risk points		Risk points		Risk points		Risk points		Risk points		Risk points	
	VLOOKUP	Layers of the Firewall	No. of Devices connected to the wifi network	How many times is the Wifi password changed in a month	Year of the Router	Number of Days since the last Software Update	Number of Days since the last Software Update	How many times the user downloaded company Unauthorised Softwares	TOTAL	ESTIMATION						
Test Subject Mr. K	458.9	15	1	1	1	474.4	26.5	22	999	975						
Test Subject Mr. L	468.9	12	1	2	2	472.4	8	25	989	984						
Test Subject Mr. M	461.9	2	21	17.5	470.4	0	23.1	0	1002	1019						
Test Subject Mr. N	456.9	0	4	11.5	468.4	9	30.1	2	988	979						
Test Subject Mr. O	469.9	2	21	1	471.4	21.5	27.1	2	990	1023						
Test Subject Mr. P	456.9	11	21	15.5	477.4	22.5	27.1	2	1031	992						
Test Subject Mr. Q	464.9	7	9	15.5	475.4	22.5	29.1	2	1024	995						
Test Subject Mr. R	460.9	3	10	15.5	466.4	24.5	2	2	983	1027						
Test Subject Mr. S	464.9	7	21	15.5	476.4	25.5	9.5	9.5	1020	1012						
Test Subject Mr. T	456.9	15	21	5	465.4	28.5	25	25	1006	991						
Test Subject Mr. U	468.9	11	4	6	463.4	30.5	25	25	1005	995						
Test Subject Mr. V	468.9	7	9	5	468.4	7	20	20	966	1029						
Test Subject Mr. W	470.4	2	5	11.5	469.4	30.5	22	22	981	990						
Test Subject Mr. X	468.9	7	4	15.5	467.4	16.5	20	20	999	1026						
Test Subject Mr. Y	464.9	15	9	11.5	469.4	31.5	2	2	983	994						
Test Subject Mr. Z	468.9	11	9	3	474.4	27.5	27.1	27.1	1011	979						

Figure A7: VLOOKUP Function: Source: Author's own work <https://miau.my-x.hu/miau/323/rw1/rw1.xlsx>: Excel sheet title COCO, B145:B162, K145:K162

By using VLOOKUP, I could accurately do the cross-referencing of variable for a better analysis in my project. Overall, by correctly targeting and verifying the risk scores of various subjects(workers) in various attributes, the project can help companies in improving their overall cybersecurity capabilities and create a more robust and agile cybersecurity ecosystem.