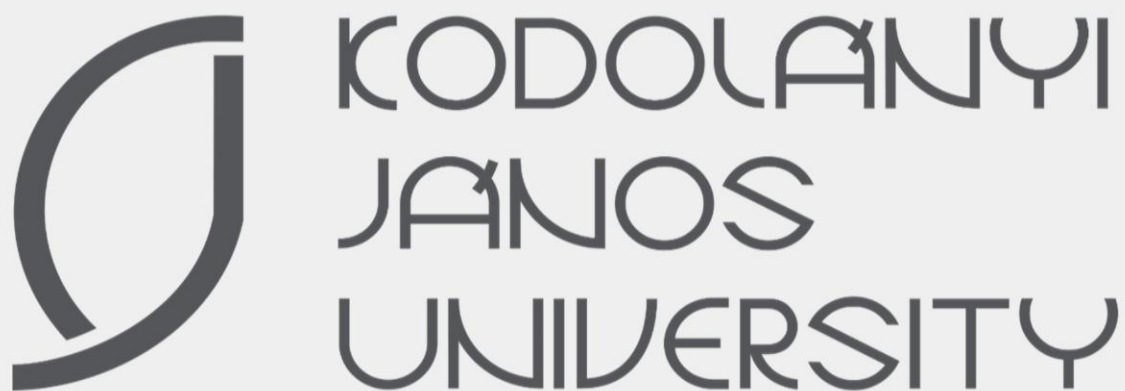




THESIS

Name: Latif Muhammad Khuram

Neptun code: YX1J10

Professor: Dr László Pitlik

Training location (Budapest, Hungary)2025

Kodolanyi János University

Analysing Cybersecurity Risks Among Remote Workers in Operational Technology Environments

Consultant: László Pitlik, Associate Professor

Author: Latif Muhammad Khuram
BPROF in Computer Science Operational Engineering

Training location (Budapest, Hungary)2025

Abstract

This thesis examines the increasing cybersecurity risks that remote workers face in Operational Technology environments. As OT systems are increasingly integrated with IT networks, new vulnerabilities arise that can compromise critical operations, lead to significant financial losses, and even impact public safety. The research focuses on developing an automated cybersecurity solution that detects risks specifically for remote workers. By processing data such as security logs, internet traffic, and response times, the developed software rapidly identifies remote worker with high-risk profiles. It uses an Object-Attribute Matrix and the COCO Y0 model to objectively analyse the risk levels, replacing previous manual and error-prone methods with an efficient, AI-driven approach.

The solution is designed to benefit several sectors including software companies, healthcare, educational institutions, insurance firms, and government agencies that need to protect their important systems and data. It saves time, avoids mistakes, and helps take action before problems happen. I used programming languages like C# to make this tool and tested it with cases base on real life This research highlights the importance of robust cybersecurity measures in modern OT environments, offering practical insights and recommendations to safeguard remote workforces against evolving digital threats.

1 Introduction	4
1.1 Title	4
1.2 Problem	4
1.3 Aims/Goals.....	4
1.4 Target Group and Usefulness	6
1.5 Risk Assessment Tasks Completed	7
1.6 Motivation	8
1.7 About the structure of the Final Thesis	8
2 Literature Review	11
2.1 Relationship to another thesis	11
2.1.1 Comparison of my Thesis and Aadi's Thesis.....	12
2.1.2 Total Number of Attributes from both Publications.....	14
2.2 Remote Access Vulnerabilities	16
2.3 Risk Detection	16
2.4 Multi-Factor Authentication	16
2.4.1 Two-Factor Authentication for Remote Work	17
2.4.2 MFA for Remote Work in OT Environments	17
2.4.3 MFA and Home Network Security in Remote Work	17
2.4.4 Enhancing Cybersecurity in Remote Work.....	17
2.5 System for Risk Assessment in IT Security Surveys	17
2.5.1 Security in Health Care	18
2.5.2 Security in Distance Education	18
2.5.3 Assessing the Effectiveness of Internal IT Controls	18
2.5.4 Endpoint Protection for Remote Work.....	18
2.5.5 Endpoint Protection for Home Network Security	19
2.6 Relationship between subject and thesis	19
2.6.1 Introduction to Mathematics	20
2.6.2 Introduction to Algorithm	20
2.6.3 Introduction to Programming and programming I,II&III.....	20
2.6.4 Networks and Computer Architecture.....	20
2.6.5 Intercultural Communication	21

2.6.6 Introduction to Electronics and Electronic Circuits	21
2.6.7 System Modelling and Planning	21
2.6.8 Data Visualization.....	21
2.6.9 Globalisation & Social Problems	21
2.6.10 Databases I & II	22
2.6.11 System Operation.....	22
2.6.12 ICT Security	22
2.6.13 Understanding Europe: History, Culture, and Economy	22
2.7 Hacking	22
2.7.1 Problem Identification.....	23
2.7.2 Relevance to Pakistan	23
2.7.3 Common Techniques Used in Hacking.....	23
2.7.4 Ethical Hacking.....	24
2.8 Phishing Emails Introduction	25
2.8.1 Problem Identification.....	25
Solutions and Mitigation Strategies	26
2.8.2 Relevance to Pakistan	26
3 Own Development.....	28
3.1 Object-Attribute Matrix for Risk Assessment.....	28
3.1.1 Objects	29
3.1.2 Attributes.....	29
3.1.3 Data Collection	32
3.1.4 Naive Risk Assessment	33
3.1.5 COCO Y0 Analysis.....	35
3.1.6 The Legend of Remote Worker Attributes	35
3.1.7 Results Of COCO Y0 analysis	36
3.1.8 Validation checks for COCO Analysis	36
3.2 Implementation of Automation for Risk Assessment.....	37
3.2.1 Testing the Program	38
3.2.2 Correlation Analysis	40

3.2.3 Ranking Methodology.....	42
3.2.4 Automation Results.....	43
3.2.5 How to involve AI.....	44
4 Discussions.....	45
5 Conclusion.....	47
6 Future	49
7 Summary	50
8 Annexes	52
8.1 Annex I: Raw Data & Ranked Tablee based on ChatGPT-conversations.....	52
8.2 Annex II: Abbreviations	52
8.3 Annex III: Figures	52
8.4 Annex IV: References	52
8.5 Annex V Conversations with LLMs	56
8.6 Annex VI: Test Cases	59
8.7 Annex VII: Correlation Alerts.....	64

1 Introduction

Technology in Operational Technology enhances efficiency in industries but introduces new cybersecurity risks when integrated with IT networks, especially for remote workers. This thesis develops a system to detect threats and providing risk assessments. This first chapter introduces the main topic of the thesis. It explains the problem, the goals of the thesis, who the system is meant to help, and the motivation why this topic is important. It also gives an overview of the software created during the thesis. The last part of the chapter (c.f. chapter.7) explains how the rest of the thesis is organized so the reader can easily follow along.

1.1 Title

Analysing Cybersecurity Risks Among Remote Workers in Operational Technology

1.2 Problem

As digital technologies become more common in Operational Technology environments, cybersecurity risks for remote workers are increasing. These workers face challenges like network vulnerabilities, Internet traffic, and system downtime, which can seriously impact operations. Traditional security systems often fail to detect and prevent these threats, leading to disruptions, financial losses, and risks to public safety.

1.3 Aims/Goals

The main aim of this thesis is to develop a comprehensive cybersecurity solution specifically designed to identify the risks faced by remote workers in Operational Technology environments (see chapter 3), with a particular focus on different attributes (chapter 3.1.2) because: by leveraging a systematic risk assessment, Software (c.f. chapter 3.2.4 Figure 6: Automation Results) will quickly pinpoint which remote workers are at the highest risk by analysing all the attributes contributing to these risks. The software will rank the risk levels of these workers in case of each attribute and analyse the particular attributes contributing to these risks in an objective way based on similarity analyses. It will then offer detailed risk assessments (chapter 3) to help organizations effectively manage and reduce cybersecurity threats. This approach ensures that remote teams can work securely, protecting sensitive data and critical infrastructure from malicious activities.

Real-Life Scenarios

There are three situations given below which shows us how cybersecurity threats impact different sectors and why risk detection is essential. Remote workers manage sensitive data (e.g. system passwords, financial records, patient details), making them targets for cyber threats.

The software helps identify risk potential and their changes. The users as such are responsible for their attributes.

Situation 1:

A software house with remote maintenance teams: They check remote login records to find unusual activity that could mean a hacker is trying to break in. The software helps measure risk levels based on the given data.

Reason: Remote teams need access to company systems. Hackers can try to break in. The team checks login activity and alerts for any unusual access.

Risk and Benefits

- Benefit: Find the risk levels and improves security for the remote workers.
- Risk: Hackers can break into systems by tracking login activity.
- Estimated Loss: \$4 to \$5 million per breach.
- Estimated Benefit: \$4 to \$5 million saved by preventing cyberattacks.

Situation 2:

A healthcare facility allows remote access to patient data for medical staff. The program will analyse attributes about access patterns to identify any anomalies that may suggest a data breach.

Reason: Patient data is private and must be protected. The software looks at user-defined attributes about e.g. login attempts access frequency or device type risk scores. who is accessing the data and spots any unusual behaviour.

Benefits

- Protects sensitive data from cyber threats.
- Risk: Patient data breaches can lead to heavy fines and loss of trust.
- Estimated Loss: \$9 to \$10 million per breach.
- Estimated Benefit: \$9 to \$10 million saved by stopping unauthorized access.

Situation 3:

Government offices with remote employees managing confidential information. The government will assess network traffic and communication patterns to detect any signs of cyber-attacks. The software helps to analyse these data in an optimized/anti-discrimination-oriented way – in an other way as naive approaches (c.f. average-oriented calculations) would do it. The software helps analyse risk without making unfair judgments.

Reason: Government agencies store critical information. If hackers get access, it can lead to national security threats.

Benefits

- Provides insights and recommendations to reduce security risks.
- Risk: Sensitive government data leaks can cause security threats.
- Estimated Loss: \$2 to \$5 million per cyberattack.
- Estimated Benefit: \$2 to \$5 million saved by detecting and blocking threats

1.4 Target Group and Usefulness

This software provides essential cybersecurity solutions for industries managing sensitive data and managing remote workforces.

Software Companies

- Why included: These companies work with private client data and remote teams, so strong security is needed.
- Real benefit: The software checks all users through the Object-Attribute Matrix and finds risky activity early.

Added value

- Before: A data breach can cost around €80,000.
- After: The software can stop 60% of the risk.
- Value of improvement: €48,000 saved per year per company

Schools and Universities

- Why Rational: They keep student and teacher records and use online systems for classes.
- Real benefit: The software shows which users may be weak in login or access habits and helps fix it.

Added value

- Before: Problems like data loss or system issues can cost about €20,000 per year.
- After: The software can reduce problems by 70%.
- Value of improvement: €14,000 saved per year per school or university.

Insurance Companies

- Why included: They collect personal and money-related information that needs protection.

- Real benefit: The software checks employee to find out if they have high risk of hacking or other attacks (e.g. phishing email). So, we get to know whose security is weak and stop data leak.

Added value:

- Before: A data leak may cost €100,000 to €150,000.
- After: The software lowers that risk by 50%.
- Value of improvement: €65,000 saved per year per company.

Government Offices

- Why Rational: They handle citizen information and provide public services that must be safe.
- Real benefit: The software checks the risk levels of people in the different cities using system online to find and fix security issues.to keeps systems running safely.

Added value:

- Before: Service failure or data issues may cost up to €200,000.
- After: The software can reduce risks by 60%.
- Value of improvement: €120,000 saved per year per office.

Healthcare Centers

- Why included: They allow remote access to patient records and medical tools, which must be protected.
- Real benefit: The software watches for doctors or medical systems to see if they have high security risk due to unusual access in order to protect patients' data..

Added value

- Before: A data breach may cost about €75,000.
- After: The risk is lowered by 70%.
- Value of improvement: €52,500 saved per year per center.

1.5 Risk Assessment Tasks Completed

Initially, I used AI tools like COCO-Y0 (Component-based Object Comparison for Objectivity antidiscrimination-oriented module) analysis to assess remote workers' risk levels required manual data input of authentication logs, internet usage patterns, and response time reports into spreadsheets. This manually driven Method for example, data such as Authentication Logs, internet traffic, and response time reports etc had to be manually entered into Excel. Once the data was in Excel, we would use formulas and ranking functions to evaluate and compare the risk levels of different remote workers. was inefficient, time-consuming, and prone to errors,

especially as the workforce expanded. To streamline this process, To overcome these limitations, I developed a dedicated risk assessment software. This software automates data extraction from CSV databases, eliminating the need for manual input such as typing data or copy-pasting data. It instantly ranks workers based on risk according to the attribute's direction and quicker identification of high-risk workers This software could perform continuous monitoring and applies AI-driven security measures such as real automatic threat detection, , and risk prediction, enhance protection and can take real data from online sources like Virus Total in the future Additionally, I implemented and analysed a correlation matrix (c.f. chapter 3.1.10) for quality assurance, ensuring consistency in the subjective parameters of users regarding the relationships between risk and each attribute. This reduces human error (e.g. inconsistency) and improves accuracy. By fully automating risk assessment and cybersecurity threat detection, organizations will be able to better protect their digital infrastructure in the future. These improvements will help prevent hacking, and other cyber threats, while making security management easier for remote workers.

1.6 Motivation

Technology has made work in Operational Technology faster and more effective, but it also brings serious security problems. Most of the people now working remotely, and they often face risks that can harm both them and their companies. Hackers can attack their systems, causing money loss, data leaks, and work interruptions. In OT, these attacks can be even worse, like stopping a factory or power plant. A real example is the 2017 cyberattack on Ukraine's power grid, which showed how weak security can lead to big dangers. Many OT systems are old and not well protected, making them easy for hackers to target. My motivation to choose this topic because I want to help remote workers and companies understand which workers are at the most risk and how they can protect themselves. By finding security threats, businesses can take better safety steps. Simple methods like multi-factor authentication and intrusion detection systems can help stop attacks. My goal is to provide useful solutions that improve security for remote workers and protect important OT systems from cyber threats.

1.7 About the structure of the Final Thesis

This chapter explains how the thesis is organized. It follows a clear flow, starting with basic concepts, moving to practical work, and ending with results and future recommendations. Each chapter builds on the previous one to give a complete understanding of cybersecurity risks for remote workers in Operational Technology environments. The comparing ratio is given to help

balance the focus on each chapter based on its importance. It ensures that each chapter has enough space to explain its main points and key concepts properly.

Interesting Chapters and Structure

The structure is designed to ensure smooth reading from basic knowledge to risk assessment and solutions. The chapters are divided based on their importance:

- **Introduction (18.3%) chapter1:** Gives a clear start by explaining the research, goals, and methods. Less percentage would miss details, more would take space from analysis. Explains the research problem, goals, tasks completed and why this topic is important.
- **Literature Review (37.5%) chapter2:** Builds a strong background with past research. Less would weaken the base, more would repeat known facts. Summarizes past research and industry reports on OT cybersecurity, providing a powerful base for the risk assessment method. This is the core of your research, so it needs enough space to explain your methods. Too little would not explain fully, too much would shift focus.
- **Own Development (28.1%) chapter 3:** Explains the COCO Y0-analyses (c.f. chapter 3.1.5 Figure 4: COCO Y0 Analysis) https://miau.my-x.hu/myx-free/coco/beker_y0.php
The Object-Attribute Matrix is used because it helps us check which objects are facing more risk by looking at their different attributes (c.f. chapter 3.1 Object-Attribute Matrix for Risk Assessment). Explains how AI can be used to improve risk assessment and automation in cybersecurity. AI is important but not the main focus. Too much space would take away from the core topic.
- **Discussions (5%) chapter 4:** Talks about the results of the study and compares them with existing research. Compares your results with another research. Too short would miss explanations, too long would repeat points.
- **Conclusion (4.9%) chapter 5:** Summarizes the main findings and stresses the need for ongoing risk evaluation and security measures. Summarizes your research. Too short would miss key points, too much would be repetitive.
- **Future (1%) chapter 6:** Describes possible future improvements using AI and automation to enhance security for remote workers. Needs to be brief since it's just about suggestions for the future.

- **Summary (3.2%) chapter 7:** Gives a brief overview of the research, focusing on cybersecurity risks for remote workers and the solutions proposed. Summarizes key findings. Too little would miss details, too much would overlap with other sections.

The total percentage is 100%. Each percentage is carefully assigned to maintain balance and ensure all topics are covered properly.

- **Annexes and References (4%) chapter 8:** Provides extra material and sources used in the research.

Citations

A “*citation*” is a reference to a source that supports the research. It gives credit to original authors, adds reliability, and helps avoid plagiarism. Readers can also use citations to find more details. Citations are used in this thesis to:

- Support statements with reliable sources.
- Maintain academic honesty and avoid plagiarism.
- Help readers find original research for more details.

Topics Not Included and Why?

Some topics were considered but excluded to keep the research focused:

- **Psychological Impact of Cyber Threats** – The study focuses on technical and strategic aspects, not the mental effects of cyber risks.
- **Economic Impact of Cyber Attacks** – While cybersecurity incidents can cause financial losses, this thesis does not analyse their economic consequences.
- **Social Engineering in Cybersecurity** – Instead of human manipulation tactics, the research focuses on broader cybersecurity risks.
- **Cyber Warfare and Nation-State Attacks** – The study is limited to remote worker security in OT, not geopolitical cyber conflicts.
- **Entire automation of the whole analytical process:** My focus is not the full automation of the whole analytical process, but rather on automating specific tasks (e.g., data collection, ranking, risk calculation).

2 Literature Review

The subchapters (2.1-2.8) are structured and selected logically to explain cybersecurity risks in remote work. It begins with remote access vulnerabilities, highlighting security issues faced by remote employees. Then, risk detection methods are discussed, showing how threats can be identified. Multi-Factor Authentication is presented as a key solution to prevent unauthorized access, risk assessment systems help analyse security threats in IT environments. Endpoint protection ensures secure home and work networks. This structure balances theoretical understanding with practical security measures, making the topic clear and well-organized.

2.1 Relationship to another thesis

I have compared my thesis with one of my benchmarks (Aadi, 2024) AND (Aadi, 2025). Aadi's thesis and my thesis are closely related as both focus on cybersecurity risks in remote work environments. Aadi research evaluates risks in IT activities for home-office setups, while my thesis focuses on security risks among remote workers in Operational Technology. The real difference between home office workers and remote workers is home office workers always work from home, while remote workers can work from anywhere, like cafés, coworking spaces or different cities. Home office workers usually follow company rules for setup and security, but remote workers can manage their own workspace. Home office workers use a private and stable internet connection, while remote workers may use public Wi-Fi, which can be less secure. Remote workers have more flexibility, but they also face higher cybersecurity risks, especially when working in places with busy networks with higher internet traffic (c.f. chapter 3.1.2). Both studies use data analyses (Coco analyses), ranking methods, and the Object-Attribute Matrix for risk assessment. But our parameters of analysis and attributes are different. Detailly explain in the Comparison of My Thesis and Aadi's Thesis (c. f chapter 2.1.1).

“Cyber security threats can happen at various levels, such as on the hardware level, the software level and the network level” (Aadi, 2025a). Aadi explains that cybersecurity threats can occur at the hardware, software, and network levels. Similarly, in my thesis, I analyse threats across these same levels by examining internet traffic, system logs and intrusion attempts etc.

2.1.1 Comparison of my Thesis and Aadi's Thesis

ID	Phenomenon	My Thesis	Aadi Thesis
1	Objects	16 Objects: Remote Workers created by Chat GPT (c.f. chapter 3.1.4)	16 Objects: Real Test Subjects (Mr. K, Mr. L, etc.)
2	Number of Attributes	12 Attributes (c.f. chapter 3.1.1)	17 Attributes (16 unique, 1 repeated) (see Annex B with 2 attribute-columns + with all the necessary attribute-types, incl. direction)
3	Common Attributes (5) form both Theses	Internet Traffic, Key Length Intrusion Attempts Malware Infections System Downtime	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
4	Attribute with Different Direction	E.g., the more System Availability Percentage the lower the risk (the directions can be set by users freely)	The more days beyond 12 hours worked last week the less the risk.

		correlation-matrix-based alerts are integrated to avoid arbitrary misunderstandings of the users)	(the directions can be set by users freely correlation-matrix-based alerts are integrated to avoid arbitrary misunderstandings of the users)
5	Focus Area	Cybersecurity risks in remote work environments (OT) with different numbers, kinds, and directions of attributes. (c.f. chapter 2.1.2)	General cybersecurity in home-office environments with different numbers, kinds, and directions of attributes.
6	Data Collection	Kind of Realistic values obtained using ChatGPT (c.f. Figure#2)	Initially, Data was generated using Excel random number function Later Test Subjects Data was collected from real people
7	Ranking Method	Ranking applied based on behavior such as risk direction (0 or 1)	Same methodology applied
8	Ranking Method for automation (Using a Correlation matrix as a supportive	Used for automation, In Chapter 3.2.2 I gave alert-generating rules for the analysis of the correlation values compared to a given direction-vector	Similar, and there is no need for Excel's correlation matrix. Because software can perform the correlation matrix but to ensure the

	forcefield for direction-alerts)		quality, we can also do excel correlation and compare the results.
9	AI Analysis	Used COCO AI content free engine to predict risk	Used COCO AI for risk predictions
10	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
11	Results	Identifies high-risk remote workers	Same outcome: higher-risk test subjects identified to enhance cybersecurity practices and provide mitigation solutions
12	Automation	Programming languages C#, Functionalities (e.g., correlation matrix and alerts for assigning attributes direction for ranking of data, COCO Y0 analysis for risk assessment tested by 5 test cases with different attributes (c.f. chapter 3.2.1).	Programming languages C#, Functionalities (e.g., correlation matrix and alerts for assigning attributes direction for ranking of data, COCO Y0 analysis for risk assessment tested by 5 test cases.

2.1.2 Total Number of Attributes from both Publications

The total number of attributes is based on both theses. My thesis has 12 attributes, while Aadi's thesis has 16 attributes.

Total Number of Attributes from my Thesis

1. Internet Traffic source:(own publication)
2. Packet Error Rate source:(own publication)
3. Security Logs source:(own publication)

4. Authentication Logs source:(own publication)
5. Key Length source:(own publication)
6. Response Time source:(own publication)
7. Malware Infections source:(own publication)
8. Average Time to Respond source:(own publication)
9. Unauthorized Access Events source:(own publication)
10. System Availability Percentage source:(own publication)
11. Intrusion Attempts source:(own publication)
12. System Downtime source:(own publication)

Total Number of Attributes from Aadi Thesis

1. Layers of the Firewall (Aadi, 2024)
2. No. of Devices connected to the Wi-Fi network (Aadi, 2024)
3. How many times is the Wi-Fi password changed in a month (Aadi, 2024)
4. Year of the Router (Aadi, 2024)
5. Year of the User Device (Aadi, 2024)
6. Number of Days since the last Software Update (Aadi, 2024)
7. How many Threats Detected by the Antivirus software in the last month (Aadi, 2024)
8. Total Number of Files Downloaded in Last Week (Aadi, 2024)
9. Percent of total Logins hours when VPN was used (Aadi, 2024)
10. How many times user visited Blacklisted websites by company Last week (Aadi, 2024)
11. How many times Personal Accounts were used to Login in the last week (Aadi, 2024)
12. How many times the user downloaded company Unauthorized Software (Aadi, 2024)
13. Total Amount of Downloaded Data in Last Week (Aadi, 2024)
14. Length of Wi-Fi Encryption Key (Aadi, 2024)
15. Intrusion Detection System (Aadi, 2024)
16. How Many Threats Detected by Antivirus in Last Month (Aadi, 2024)
17. How Many Days Beyond 12 Hours Worked Last Week (Aadi, 2024)

Different Attributes from my Thesis

1. Packet Error Rate
2. Security Logs
3. Authentication Logs
4. Response Time
5. Average Time to Respond
6. Unauthorized Access Events
7. System Availability Percentage

Different Attributes from Aadi Thesis

1. Number of Days since the last Software Update
2. How many Threats Detected by the Antivirus software in the last month
3. Total Number of Files Downloaded in Last Week
4. How many times user visited Blacklisted websites by company Last week
5. How many times Personal Accounts were used to Login in the last week

6. How many times the user downloaded company Unauthorized Software

2.2 Remote Access Vulnerabilities

"Having to move employees to working from home in such a short space of time opened up new vulnerabilities that cybercriminals were quick to target. The volume of corporate traffic grew, and users swiftly moved to using third-party services to exchange data, and work via potentially insecure Wi-Fi networks" (Kaspersky, 2020). Remote work quickly introduced new security weaknesses that cybercriminals exploited, as corporate internet traffic increased, and employees used third-party services and potentially unsafe Wi-Fi networks.

2.3 Risk Detection

"A kockázat észlelése kontextuális szinteken és/vagy kontextusmentes naplókban történhet. A kontextuális módon észlelés vezethet gyanús válaszlehetőségekhez, kérdésekhez, személyekhez – a becsült válaszok alapján. Minden személy-kérdés-válasz egységben a személyek száma és/vagy a kérdések száma optimalizált terhelési mód szerint legyen maximalizálva. A kockázat meghatározható válaszopcióként, mint a tényleges és a becsült válaszok közötti különbség." (Pitlik, L., Pitlik, M., & Pitlik, M, 2018). Risk perception can occur at contextual levels and/or in context-free logs. Contextual perception may lead to suspicious responses, questions, or individuals based on the estimated answers. In each person-question-answer unit, the number of individuals and/or questions should be maximized according to an optimized load mode. Risk can be defined as a response option, represented by the difference between actual and estimated responses.

" Die Risiken der IT-Nutzung werden einschätzbar durch die nähere Betrachtung und detaillierte Analyse der auf ihrer Grundlage umgesetzten Geschäftsprozesse und Geschäftsvorfälle der jeweiligen Organisation."(Pohlmann, German language.N, 2019, p.41.). The risks associated with using IT can be better understood by closely examining and analysing the business processes and transactions that are conducted within the organization using IT. This helps identify and assess the potential risks in a more detailed and reliable way.

2.4 Multi-Factor Authentication

"Ensuring that strict policies and measures are in place and creating the highest level of security possible now that employees work from home. He continues by stating that one of the topic strategies to achieve this is enforcing employees to use MFA for the login process to access company portals." (Chapman, 2022, p.8.). When employees work remotely, it is crucial to require MFA for secure login, which helps prevent unauthorized access. This step is an

important precaution to protect sensitive information and improve overall security, especially for remote workers.

2.4.1 Two-Factor Authentication for Remote Work

"Core Cybersecurity Practices for Remote Work: A Focus on Two-Factor Authentication." Journal of Information Security. (Furnell & Shah, 2020, p.6-12.) Highlights the role of Two-Factor Authentication (2FA) as a fundamental cybersecurity practice for securing remote work systems and data.

2.4.2 MFA for Remote Work in OT Environments

"Enhancing Cybersecurity for Remote Work through MFA in Operational Technology Environments." KJU Cybersecurity Journal. (Alawida et al., 2022) Focuses on the importance of Multi-Factor Authentication (MFA) for securing Operational Technology (OT) in remote work environments.

2.4.3 MFA and Home Network Security in Remote Work

"Top strategies of such enforcement include requiring MFA to be able to log into company portals, that each personal device be equipped with security software provided by the employer, as well as not permitting access to remote systems unless the latest software updates have been installed." (Chapman, 2020). Organizations strengthen security by mandating MFA, employer-provided security software on personal devices, and up-to-date software before accessing company systems.

"Password Hygiene for Remote Workers: Best Practices from WHO and Kaspersky." (Saleous et al, 2023). Password hygiene for remote workers focuses on using strong, unique passwords, enabling two-factor authentication, and regularly updating credentials to protect sensitive information from cyber threats.

2.4.4 Enhancing Cybersecurity in Remote Work

"Top strategies of such enforcement include requiring MFA to be able to log into company portals, that each personal device be equipped with security software provided by the employer, as well as not permitting access to remote systems unless the latest software updates have been installed." (Chapman, 2020) He emphasizes security strategies like requiring MFA for portal logins, ensuring personal devices have employer-provided security software, and restricting access until software updates are installed, reducing vulnerabilities.

2.5 System for Risk Assessment in IT Security Surveys

“A tanulmány célja annak az általános érvényű robot-alkotási lépéssornak a bemutatása, mely próbaképpen az IT-biztonság területén, ezen belül is a biometrikus azonosítási eljárásokkal (pl. ujjlenyomat, kézgeometria, arc, gépelési dinamika, hang, aláírás, retina, írisz, DNS).” (Pitlik, L., Pitlik, M., & Pitlik, M, 2018). This study aims to develop a robot system that automatically checks and analyses risks in IT security attitude surveys, using biometrics like fingerprints, face recognition, and voice for improved accuracy.

2.5.1 Security in Health Care

“using VR and AR technologies in defence and health care, as these tools can help all those involved in solving the indicated problems. = The safety of students and patients” (Fejes, Z. D., Pitlik, L., Rikk, J., Szűcs, D., & Túri, P, 2021). Virtual Reality (VR) and Augmented Reality (AR) can help solve problems in Défense and healthcare by offering safe and realistic training. These technologies make sure students and patients stay safe while improving practices.

2.5.2 Security in Distance Education

The IT layer must focus on security to protect personal data and privacy in online learning. Using secure platforms and tools helps keep student information and academic work safe. It's important to set up access controls, encryption, and regular checks to stop unauthorized access. These security measures make the learning environment safe and trustworthy for both students and teachers. *“The IT layer means how should we use the technology in an effective, efficient way as part of the planned didactical effects.”* (Pitlik, L., Rikk, J., Gángó, V., & Tóth, C, 2020) the upper/lower cases must be always used consequently!!!

2.5.3 Assessing the Effectiveness of Internal IT Controls

This process involves reviewing how well the internal controls protect the organization's data and IT systems from threats. It ensures that security measures are in place to prevent unauthorized access, data breaches, and other cyber risks. *“A belső informatikai kontrollok hatékonyságának feltárására szolgáló funkcionális terület megnevezése az informatikai audit-csoport.”* (Barta & Göröcsi, 2021)The functional area responsible for evaluating the effectiveness of internal IT controls is called the IT audit group.

2.5.4 Endpoint Protection for Remote Work

“Endpoint protection is crucial for securing home networks in remote work environments, ensuring that remote workers' devices are not compromised.” (Sabin, 2021, p.18.). This article provides key information on endpoint protection, which is central to your thesis on protecting

remote OT environments. It stresses the importance of securing devices that connect remotely to OT systems.

2.5.5 Endpoint Protection for Home Network Security

"Endpoint Protection in Remote Work: Best Practices for Home Network Security." Published in Cybersecurity Tech Review. (Sabin, 2021) Focuses on best practices for endpoint protection and home network security, essential for maintaining cybersecurity in remote work environments.

"It must be ensured that all work-from-home devices are protected, and patch management (acquisition, testing, and installation of multiple patches, code changes, etc. should be implemented on any computers used for work tasks." (Graham, 2021). He emphasizes the need for securing all work-from-home devices through patch management, including acquiring, assessing, and installing updates to protect computers used for work tasks.

"In order to protect home networks and mitigate attackers reaching the company network through home networks due to lacking home network security, cloud-based patch and endpoint management should be used and is the strongest approach to safeguard against home network attacks." (Sabin, 2021). He is recommending cloud-based patch and endpoint management to protect home networks and prevent attackers from accessing company networks through vulnerable home network security.

"Successful security professionals have had to modify the process of responding to new threats in the high-profile, ultra-connected business environment. But just because a threat exists does not mean that your organization is at risk. This is what risk assessment is all about." (Peltier, T.R, 2010). He points out that while new threats are always emerging, they do not always pose a real risk to an organization. Risk assessment is about identifying which threats are most likely to impact an organization's security and focusing on those. This helps security professionals prioritize their efforts and resources effectively.

"Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten Risikomanagements verstehen: Die Unternehmensleitung muss Cyber-Sicherheit nicht nur als IT-Risiko, sondern als strategisches Unternehmensrisiko verstehen und angehen." (HS Anhalt, German Language, 2015, p. 9.) Understand cybersecurity not only as an IT issue but as a component of the company-wide risk management. The management must view cybersecurity not only as an IT risk but as a strategic business risk and address it accordingly.

2.6 Relationship between subject and thesis

During my program at Kodolányi János University, I completed the following courses which have directly contributed to my thesis on cybersecurity risks for remote workers in Operational Technology environments:

2.6.1 Introduction to Mathematics

Mathematics is important in cybersecurity risk assessment. One useful tool is the correlation matrix, which shows how different attributes like internet traffic and packet error rate are related. A real-life example is checking if more internet traffic leads to more packet error. Then two attributes are strong positively correlated, it may mean stronger security is needed during high traffic times.

“Passage of correlation into causal relationship” (Aldrich, J, 1995) It means moving from just observing a relationship (correlation) to proving that one thing actually causes the other (causation) using scientific methods.

2.6.2 Introduction to Algorithm

Algorithm efficiency is important to make sure cybersecurity systems work fast and don't waste resources. We check how fast an algorithm works (called time complexity) and how much memory it uses (called space complexity). For example, if an algorithm checks security logs for threats but takes too long ($O(n^2)$), it won't be helpful in real-time situations. A faster algorithm ($O(\log n)$) can help quickly find problems, especially in large logs.

“THE NOTION of an algorithm is basic to all of computer programming, so we should begin with a careful analysis of this concept.” (Knuth, D. E, 1997). Understanding algorithms is fundamental to programming, so analysing them carefully ensures efficient and effective problem-solving. A good algorithm is important for good and valuable risk assessment.

2.6.3 Introduction to Programming and programming I,II&III

Help me to understand advance programming skills and need of software development. It helps me to perform desire steps number of times *“repetition of events became the baseline of computer programming”* (Goutam, R. K, 2021a).

2.6.4 Networks and Computer Architecture

Essential for implementing secure network protocols and understanding hardware vulnerabilities, *“Computer Architecture is concerned with the structure and behaviour of the computer seen by user.”* (Mano, M. M, 2006, p.3.).

2.6.5 Intercultural Communication

Improved my teamwork and communication across cultures, religions and different people during my thesis. *“get some assistance on how to understand people’s emotions and respond appropriately”* (Corbet, Jonathan, 2018a) It helps us work more efficiently.

2.6.6 Introduction to Electronics and Electronic Circuits

Helped understand how to secure devices used in OT environments and gives general awareness of electronic safety and crimes. *“In order to counter the threats, Pakistan passed Prevention of Electronic Crimes Act, 2016, amended in 2022.”* (Pakistan Parliament, 2016). It explains how to secure OT devices and highlights Pakistan's Prevention of Electronic Crimes Act, 2016, amended in 2022, to counter electronic threats.

2.6.7 System Modelling and Planning

System Planning and Modelling helps me in understanding importance of designing secure and efficient computer systems by deciding in advance how components will work to make process fast same as we created OAM to decide how risk analysis will take place efficiently (c.f. chapter 3.1). *“The architectural design of a computer system is concerned with the specifications of the various functional modules, such as processors and memories, and structuring them together into a computer system.”* (Mano, M. M, 2006, p.4.). The architectural design of a computer system deals with how different parts, like processors and memories, are specified and connected to form a complete system.

2.6.8 Data Visualization

Important for presenting cybersecurity data clearly and effectively in various forms such as. *“After the introduction of multimedia, the term data has expanded its boundaries and incorporated audio, images, graphics and video in itself.”* (Goutam, R. K, 2021b). With the introduction of multimedia, the term 'data' now includes audio, images as in thesis, graphics, and video.

2.6.9 Globalisation & Social Problems

Provided awareness abouts connection among countries global effects and their social problems. Such as during the time of covid *“Individuals were a more vulnerable and easily exploitable target, with fears around the pandemic itself leading them to be concerned, and therefore keen to seek or receive new information about it”* (Furnell, S., Shah, J. N, 2020, p.9.). It introduced the idea of remote working for safety of individuals.

2.6.10 Databases I & II

Focused on secure database management. *“Data is used as input for computer system to generate information.”* (Goutam, R. K, 2021c). It helps me to understand how we can use and manage raw data to make information about attributes in my thesis c.f. chapter 3.1.4

2.6.11 System Operation

It tells me importance secure running of computer systems by monitoring, backups, and security measures. Otherwise *“computer-to-computer and computer-to-network attack that breaches confidentiality, integrity and availability of a computers and disrupting information passing through them.”* (Goutam, R. K, 2021d). Attacks between computers or networks that steal or change information or process (e.g. risk analysis) and stop it from being perform safely.

“The programs included in a systems software package are referred to as the operating system.” (Mano, M. M, 2006, p.2.). The programs inside system software are called the operating system.

2.6.12 ICT Security

ICT security protects digital systems and data from unauthorized access. *“Informational security concerned to protecting digital information from destruction, stealing and unauthorized access.”* (Goutam, R. K, 2021e). Information security means protecting digital data from being destroyed, stolen, or accessed without permission.

2.6.13 Understanding Europe: History, Culture, and Economy

Enhanced my understanding of the European history, culture and economy. *“Every such town has some eccentric and difficult personalities; people learn how to cope with them.”* (Corbet, Jonathan, 2018b). Every remote team has some difficult members, and others learn to handle them to keep things secure and smooth.

2.7 Hacking

Hacking means gaining access to computer systems, networks, or devices without permission. Some hackers use it for harmful reasons, such as stealing data, while others, known as ethical hackers, use their skills to find security weaknesses and fix them. Hackers use different techniques to break security systems, which can lead to both positive and negative outcomes.

“Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.” (János Rikk, 2017a, p.5.). Hacking means finding weaknesses in computer systems or networks and using them to get access without permission.

Example:

A hacker steals sensitive data from a company, while an ethical hacker identifies security flaws to help improve the system.

2.7.1 Problem Identification

Cyberattacks have become a major global issue, affecting individuals, businesses, and governments. Hackers use phishing, malware, and brute-force attacks to steal data, disrupt systems, and cause financial losses. Most organizations in Pakistan and globally suffer from cyber threats due to weak cybersecurity policies, outdated infrastructure, and a lack of awareness. *“Hacker is one of the most misunderstood and overused terms in the security industry.”* (János Rikk, 2017a, p.5.). Hackers using various methods to steal data and cause harm, while the term "hacker" is often misunderstood and overused in the security industry.

2.7.2 Relevance to Pakistan

There has been growth in Cybersecurity awareness in Pakistan, banks, e-commerce platforms, and government institutions have all also been attacked. NADRA, the banks and themselves high profile attacks and high need for stronger cybersecurity measures. This chapter helps in understanding hacking techniques and ethical hacking solutions that can be applied to protect critical systems in Pakistan.

“A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.” (János Rikk, 2017b). A hacker is a person who finds weaknesses in computer systems or networks and uses them to gain access. Hackers are mostly skilled in programming and know a lot about computer security.

2.7.3 Common Techniques Used in Hacking

There are some common techniques which use in hacking such as

- **Phishing:** A technique where attackers send fake emails, messages, or websites designed to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details.
- **Malware Deployment:** Malicious software, such as viruses, ransomware, and worms, is used to take control of systems, steal data, or damage files.
- **Brute-Force Attacks:** A technique where hackers try different password combinations until they find the right one. This method depends on time and computing power.

Example:

“Kaspersky detected a smaller number of high severities incidents but observed a simultaneous increase in the number of medium and low severity ones. The detection of malware without visible traces of active human participation in attacks, which can be explained by the 'commoditization of tools’” (Kaspersky, 2024). He found fewer high-severity incidents but noticed more medium and low-severity ones. These incidents were linked to malware that did not need human involvement, which is due to the easy access to such tools.

2.7.4 Ethical Hacking

Ethical hacking involves testing systems for security weaknesses to protect them from real cyberattacks. Ethical hackers legally perform security assessments to help companies identify and fix risks before they can be exploited by criminals. This includes penetration testing and vulnerability assessments.

Example:

An ethical hacker finds a flaw in an e-commerce platform’s payment gateway, allowing unauthorized transactions. The company fixes the issue before malicious hackers can exploit it.

Example:

"A company hires an ethical hacker to test its e-commerce platform. The hacker discovers a vulnerability that allows users to manipulate payment details, preventing potential losses." (IBM, 2023). A company asks an ethical hacker to check its online store, and the hacker finds a weakness that could let users change payment info, helping the company avoid future losses. To improve cybersecurity, the following recommendations are strongly suggested by me.

- **Cybersecurity Awareness Campaigns:** Companies and individuals in Pakistan must be educated about hacking risks through training programs, awareness sessions, and digital literacy initiatives.
- **Strong Cybersecurity Policies:** Organizations should implement strict password policies, multi-factor authentication, and security audits to prevent hacking attempts.
- **Encouraging Ethical Hacking:** The government and private sector should promote ethical hacking programs by hiring certified ethical hackers to improve cybersecurity infrastructure.
- **Investment in Cybersecurity Technologies:** Pakistani organizations must adopt AI-based threat detection, advanced firewalls, and encryption methods to secure sensitive data.
- **Legislation & Enforcement:** Strengthening cybercrime laws and ensuring strict penalties for cybercriminals will help reduce hacking incidents.

2.8 Phishing Emails Introduction

Phishing emails are a type of online scam where hackers try to trick people into sharing personal information like passwords, bank details, or ID numbers. These emails look like they are coming from any real companies, such as banks or social media websites, which makes them hard to find out, so people believe them. Because they look so real, many people get tricked, making phishing a big problem.

“It is identified that employees pose the most prominent threats to businesses due to the commonness of human errors, meaning that even if not much is needed for a human error to occur, such as missing a single character when specifying the recipient's email address, the consequences could be severe. Even if this is then something that can very easily happen.” (Babbs, 2020) This means that human mistakes, like typing an incorrect email address, can lead to serious security issues, even though such errors are easy to make. Employees are often the biggest security risk due to their vulnerability to making simple but costly mistakes.

2.8.1 Problem Identification

- The primary problem associated with phishing emails is human error. Employees, often due to lack of awareness or training, can fall victim to cleverly disguised emails, inadvertently compromising sensitive data. In OT environments, such breaches can disrupt essential services, leading to severe operational and financial consequences. The case study of a financial institution falling victim to phishing attacks underlines the critical nature of this issue. The characteristics of phishing emails include:
 - **Spoofted Emails:** Phishing uses fake addresses resembling legitimate ones (e.g., "support@paypal.com" vs. "support@paypal.com").
 - **Urgent Language:** Emails create panic with phrases like "Your account is compromised" to prompt quick action.
 - **Suspicious Links/Attachments:** Includes links to fake websites or attachments that steal credentials or install malware.
 - **Requests for Sensitive Info:** Legitimate companies rarely ask for personal details via email; treat such requests cautiously.

Example Scenario

You are receiving an email from your bank saying that your account needs to be verify your bank account right now. The email has a link to a website that looks like your bank's login page. If you enter your , the attacking person will steal them and reach your real account.

“FIA further notes that the ratio of cybercrimes has increased by eighty-three percent in over three years, with the financial frauds holding the top category.”(Mirza, M. N, & Akram, M. S, 2022). FIA says cybercrimes have gone up by 83% in 3 years, and most of them are about financial fraud.

Solutions and Mitigation Strategies

- **Train Employees:** Teaching employees about phishing emails can help them spot scams. Awareness is the best way to stay safe because trained employees are less likely to fall for these tricks.
- **Use Email Filters:** Advanced email filters can stop phishing emails before they reach employees. These filters check emails for strange content or patterns that may indicate a scam.
- **Turn On Multi-Factor Authentication (MFA):** Even if hackers steal a password, MFA can stop them from getting in. MFA adds an extra step, like sending a code to the user's phone, which hackers usually don't have.
- **Keep Software Updated:** Updating software is very important because updates fix security weaknesses that hackers could use. Regular updates help keep systems safe.
- **Check Before Clicking:** Always confirm where an email is coming from before clicking on links or opening files. It is safer to contact the company using official contact details instead of the ones given in the email.

2.8.2 Relevance to Pakistan

Phishing attacks are increasing in Pakistan, especially in banks, government offices, and important industries like electricity and manufacturing.

“Resecurity identified a surge in smishing (SMS phishing) attacks from a cybercrime group known as the smishing Triad. This group targets Pakistan by sending fake messages on behalf of Pakistan Post, tricking recipients into clicking malicious links and entering sensitive personal information,” (Qadri Zara, 2023)

One big reason for this is that many employees do not know much about cybersecurity. Also, many companies do not have strong security systems because they lack resources. Many businesses in Pakistan still use old systems that are not safe from modern cyberattacks.

“The upsurge in remote working demands more attention regarding cybersecurity because of the larger exposure to cyber-attacks, threats, and risks, with 47% of employees and individuals

experiencing an attempted phishing scam whilst working at home.”(Hijji, M., & Alam, G, 2022)

To solve this problem, companies should train their employees to recognize phishing emails. Also, using smart email security tools with artificial intelligence can help detect and stop phishing emails before they reach people. Improving cybersecurity in Pakistan is very important. It will not only protect private data but also keep important services like electricity and water running smoothly.

To reduce phishing attacks, I recommend the following:

- Simple cybersecurity training for all employees so they can understand and avoid phishing scams.
- AI-powered email filters to check emails and block dangerous ones before they reach people.
- Multi-Factor Authentication in all companies to add extra security. Even if a hacker steals a password, they still cannot access the system without a second step of verification.
- Regular software updates and security checks to fix weaknesses and keep cybersecurity strong.

Organizations to conduct regular software updates and security audits. Regular updates help in fixing security vulnerabilities, while frequent audits ensure that the cybersecurity measures are effective and up to date. By following these steps, organizations in Pakistan can reduce phishing risks and protect their important data.

3 Own Development

A system was developed to analyse cybersecurity risks for remote workers. The process starts with identifying key security related attributes by the author because it is important step for the risk assessment that affect security in remote work. followed by data collection and ranking, and risk analysis using COCO Y0 analysis. Initially, this was done manually with Microsoft Excel because Excel is easy to use manual experiment and helps in organizing and analysing data without needing programming skills. but a C# console-based program was later developed to automate the analysis, calculate risk scores, and suggest mitigation strategies. because automation makes the process faster, reduces mistakes and provide appropriate results The system was tested using sample data from ChatGPT and self-created data sets to ensure quality and test the software behaviour with different real-like problem and the results were compared with manual COCO Y0 analysis for accuracy in order to check the software results similarity and accuracy.

I have also compared my development with Aadi's development, which also looks at cybersecurity risks for remote workers by comparing 2 approaches helps us to see what the similarity, uniqueness and difference is in both Thesis. The key difference between the two theses (c.f. chapter 2.1) is the set of attributes used to analyse the risks in remote working environment. Aadi's aims to find solutions for enhancing safety in home-office environments, While my focuses are on determining which specific remote worker is at the greatest risk. The relationship and differences between the two theses are clarified in detail (c.f. Chapter 2.1).

3.1 Object-Attribute Matrix for Risk Assessment

This research focuses on analysing cybersecurity risks for remote workers in OT environments. Various attributes are considered, including Internet Traffic, Packet Error Rate, Security Logs, Authentication Logs, Key Length, Response Time, Malware Infections, Average Response Time, Unauthorized Access Events, System Availability, Intrusion Attempts, and System Downtime. because these attributes directly impact the security and performance of remote work environments.

This section explains the Object-Attribute Matrix framework, which helps assess cybersecurity risks by mapping attributes to remote workers (c.f. chapter 3.1 Figure1).

- Objects: (Remote workers)
- Attributes (phenomenon with direction for comparison)



Figure 1: Steps Flow Chart

(Source: Author's own work, 2025, based on Microsoft word SmartArt graphic).

3.1.1 Objects

The dataset includes 16 fictional objects such as remote workers generated by ChatGPT (c.f. Figure 2). They work outside traditional offices, using technology for tasks and communication.

- **Application:** Analyse security risks and performance.
- **Minimum Workers:** At least one.
- **Maximum Workers:** No limit.
- **Defined Range:** Helps manage teams effectively.

3.1.2 Attributes

The analysis covers 12 attributes based on definition, unit, type, and direction:

1. Internet Traffic

- **Description:** Measures the amount of data transferred over the network by the remote worker.
- **Definition:** Reflects the volume of network activity and potential exposure to security risks.

- **Unit:** GB (Gigabytes)
 - **Direction:** MORE=0 (Higher values indicate potentially higher risk)
2. **Packet Error Rate**
- **Description:** Measures the rate at which data packets are lost or corrupted during transmission.
 - **Definition:** Indicates the quality of network connectivity and potential disruptions in data transmission.
 - **Unit:** Percentage
 - **Direction:** MORE=0 (Higher values indicate potentially higher risk)
3. **Security Logs**
- **Description:** Represents the number of security-related events or incidents recorded.
 - **Definition:** Reflects the frequency of security incidents and potential vulnerabilities in the network.
 - **Unit:** Count
 - **Direction:** MORE=0 (Higher values indicate potentially higher risk)
4. **Authentication Logs**
- **Description:** Represents the number of authentication attempts or events recorded.
 - **Definition:** Reflects the activity related to user authentication and potential unauthorized access attempts.
 - **Unit:** Count
 - **Direction:** MORE=0 (Higher values indicate potentially higher risk)
5. **Key Length**
- **Description:** Represents the length of the cryptographic key used for data encryption.
 - **Definition:** Indicates the strength of encryption applied to protect data and communications.
 - **Unit:** Bits
 - **Direction:** LESS=1 (Higher values indicate potentially lower risk)
6. **Response Time**
- **Description:** Represents the time taken to respond to requests or events.
 - **Definition:** Indicates the efficiency of response mechanisms and potential delays in addressing security incidents.
 - **Unit:** Seconds
 - **Direction:** MORE=0 (Higher values indicate potentially higher risk)
7. **Malware Infections** source:(own publication)
- **Description:** Represents the number of malware infections detected.
 - **Definition:** Reflects the presence of malicious software and potential security breaches.

- **Unit:** Count
- **Direction:** MORE=0 (Higher values indicate potentially higher risk)

8. **Average Time to Respond**

- **Description:** Represents the average time taken to respond to incidents or alerts.
- **Definition:** Indicates the efficiency of incident response processes and potential delays in mitigating security threats.
- **Unit:** Minutes
- **Direction:** MORE=0 (Higher values indicate potentially higher risk)

9. **Unauthorized Access Events** source:(own publication)

- **Description:** Represents the number of unauthorized access attempts or breaches.
- **Definition:** Reflects the frequency of security incidents related to unauthorized access and potential vulnerabilities in access controls.
- **Unit:** Count
- **Direction:** MORE=0 (Higher values indicate potentially higher risk)

10. **System Availability Percentage** source:(own publication)

- **Description:** Represents the percentage of time the system is available and operational.
- **Definition:** Reflects the reliability of the system's availability and potential disruptions in service.
- **Unit:** Percentage
- **Direction:** LESS=1 (Higher values indicate potentially lower risk)

11. **Intrusion Attempts** source:(own publication)

- **Description:** Represents the number of attempts to gain unauthorized access or compromise the system.
- **Definition:** Reflects the frequency of security incidents related to intrusion attempts and potential vulnerabilities in access controls.
- **Unit:** Count
- **Direction:** MORE=0 (Higher values indicate potentially higher risk)

12. **System Downtime**

- **Description:** Represents the total time the system is non-operational or unavailable.
- **Definition:** Reflects the reliability of the system's uptime and potential disruptions in service.
- **Unit:** Hours
- **Direction:** MORE=0 (Higher values indicate potentially higher risk)

- **What Users Can Do:** Users can assess risk levels, monitor performance, identify training needs, implement mitigation, and analyse correlation matrix among attributes.

- **Attribute Rules:** I have taken 12 attributes (Minimally start with one). Numeric values must be clearly defined (c.f. Chapter 2.1.2 Attributes Collected from both publications). Risk direction: 0 = lower is better, 1 = higher is better. Users set directions during data entry. “Better” means less/more aggregated risk!
- **Help & Guidance:** Built-in help explains risk directions. The program ensures valid inputs and provides a summary of key features.

3.1.3 Data Collection

	A	B	C	D	E	F	G	H	I	J	K	L	M
	comparable Remote Worker (below) / attributes for comparing-->	Internet Traffic (GB/month)	Packet Error Rate (%)	Security Logs (per day)	Authentication Logs (per day)	Key Length (bits)	Response Time (ms)	Malware Infections (per month)	Avg Time to Respond (hours)	Unauthorized Access Events (per month)	System Availability Percentage (%)	Intrusion Attempts (per month)	System Downtime (hours/month)
6	Remote Worker 1	500	0.05	3,125	625	256	150	2	3	2	99.9	25	2
7	Remote Worker 2	520	0.07	3,200	640	2048	140	1	2.5	2	99.8	20	2
8	Remote Worker 3	480	0.04	3,000	600	2048	160	3	3	1	99.7	30	2.5
9	Remote Worker 4	510	0.06	3,100	620	256	155	1	2.5	1	99.6	25	2.5
10	Remote Worker 5	530	0.05	3,250	650	2048	145	2	3	2	99.9	28	2
11	Remote Worker 6	490	0.08	3,050	610	2048	150	1	2.5	1	99.7	22	2
12	Remote Worker 7	515	0.06	3,200	640	256	145	2	3	2	99.8	27	2.5
13	Remote Worker 8	495	0.05	3,100	620	256	155	1	2.5	1	99.9	26	2
14	Remote Worker 9	520	0.07	3,200	640	2048	140	1	3	2	99.7	24	2.5
15	Remote Worker 10	510	0.06	3,150	630	2048	150	2	2.5	1	99.8	25	2
16	Remote Worker 11	530	0.05	3,250	650	256	145	1	3	2	99.9	29	2.5
17	Remote Worker 12	500	0.07	3,125	625	2048	160	2	2.5	1	99.6	23	2.5
18	Remote Worker 13	490	0.08	3,050	610	2048	155	3	3	2	99.8	28	2
19	Remote Worker 14	515	0.06	3,200	640	256	145	1	2.5	1	99.9	26	2.5
20	Remote Worker 15	480	0.04	3,000	600	2048	160	1	3	2	99.7	22	2
21	Remote Worker 16	500	0.05	3,125	625	256	150	2	2.5	1	99.9	25	2.5

Figure 2: Raw Data Table

(Source: Author's own work <https://miau.my-x.hu/miau/323/rw2/rw2.xlsx>, COCO Y0 Sheet, Range=A6-M22, 2025, based on ChatGPT-generated data. Validated against manual Excel calculations, unit c.f. 3.1.2 Attributes).

The raw data (see Figure#2) for different security attributes of remote workers was generated with the help of ChatGPT. Each row represents a different remote worker, and each column represents a specific security attribute, such as:

- **Request:** ChatGPT was asked to create raw data for 16 remote workers based on security-related attributes.
- **Criteria:** The values had to be numbers. The data was designed to reflect real-world situations, where high internet traffic may indicate a busy network, high error rates could signal security problems, and so on.

- **Response:** Certainly! Here's a table presenting realistic, numerical data for 16 remote workers based on security-related attributes. These values are informed by industry reports and studies to reflect real-world scenarios (c.f. chapter 8.5 Annex V).

- **Why I Used ChatGPT for getting Raw Data**

I used ChatGPT to generate fictional raw data because it is trained on many topics, including current events and general knowledge. ChatGPT can quickly provide relevant information based on the instructions given, making it a useful tool for creating sample datasets. Its fast responses help me get the data I need without any delay (c.f. chapter 8.1 Annex 1).

3.1.4 Naive Risk Assessment

Code	MORE=0				LESS=1				LESS=1				LESS=1				LESS=1			
DIRECTION	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0		
Direction rule	The more is the traffic, the more is the risk	The higher is the error rate, the more is the risk	The more security logs, the higher is the risk	The more authentication logs, the higher is the risk	The shorter key length, the higher is the risk	The longer response time, the higher is the risk	The more malware infections, the higher is the risk	The longer time to respond, the higher is the risk	The more unauthorized access events, the higher is the risk	The lower system availability, the higher is the risk	The more intrusion attempts, the higher is the risk	The longer system downtime, the higher is the risk	Norm value	The less the average ranking value, the less is the risk						
unit	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	RANKING VALUE	Risk points							
type(Numeric&Integer)	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12								
id	attribute1	attribute2	attribute3	attribute4	attribute5	attribute6	attribute7	attribute8	attribute9	attribute10	attribute11	attribute12								
comparable Remote Worker (below) / attributes for comparing->	Internet Traffic	Packet Error Rate	Security Logs	Authentication Logs	Key Length	Response Time	Malware Infections	Avg Time to Respond	Unauthorized Access Events	System Availability Percentage	Intrusion Attempts	System Downtime	Expected Risk Level	HYPOTHESIS	Naiv risk assessment					
Remote Worker 1	9	10	8	8	1	7	3	1	1	11	8	9	1000	each	6.3					
Remote Worker 2	3	3	3	3	8	15	9	9	1	7	16	9	1000	each	7.2					
Remote Worker 3	15	15	15	15	8	1	1	1	9	3	1	1	1000	each	7.1					
Remote Worker 4	7	6	11	11	1	4	9	9	9	1	8	1	1000	each	6.4					
Remote Worker 5	1	10	1	1	8	11	3	1	1	11	3	9	1000	each	5.0					
Remote Worker 6	13	1	13	13	8	7	9	9	9	3	14	9	1000	each	9.0					
Remote Worker 7	5	6	3	3	1	11	3	1	1	7	5	1	1000	each	3.9					
Remote Worker 8	12	10	11	11	1	4	9	9	9	11	6	9	1000	each	8.5					
Remote Worker 9	3	3	3	3	8	15	9	1	1	3	12	1	1000	each	5.2					
Remote Worker 10	7	6	7	7	8	7	3	9	9	7	8	9	1000	each	7.3					
Remote Worker 11	1	10	1	1	1	11	9	1	1	11	2	1	1000	each	4.2					
Remote Worker 12	9	3	8	8	8	1	3	9	9	1	13	1	1000	each	6.1					
Remote Worker 13	13	1	13	13	8	4	1	1	1	7	3	9	1000	each	6.2					
Remote Worker 14	5	6	3	3	1	11	9	9	9	11	6	1	1000	each	6.2					
Remote Worker 15	15	15	15	15	8	1	9	1	1	3	14	9	1000	each	8.8					
Remote Worker 16	9	10	8	8	1	7	3	9	9	11	8	1	1000	each	7.0					

Figure 3: Ranked and Naive Risk Assessment Table

(Source: Author's own work <https://miau.my-x.hu/miau/323/rw2/rw2.xlsx>, COCO Y0 Sheet, Range=A32-P54, 2025, based on ChatGPT-generated data. Validated against manual Excel calculations, Units Ranking values).

The naive risk assessment is the simple average of all attributes for each remote worker, treating every attribute equally. This method does not consider which attributes have a higher impact on security risks. A more advanced optimum approach is needed for further analysis.

Norm Values

A norm-value is a fixed standard used for consistent and fair comparison. The Expected Risk Level for each remote worker is set to 1000 as norm value. This helps avoid very high or low numbers and keep the risk values balanced and makes it easier to measure the risk of each remote worker in the same way.

Direction Vector

A direction vector shows whether increasing an attribute increases or decreases risk,. 0 means higher values increase risk (e.g., internet traffic). 1 means lower values increase risk (e.g. Key length). This keeps rankings accurate.

All attributes have a direction of 0, except for Attribute 5 (Key Length) and Attribute 10 (System Availability), which have a direction of 1. Higher value of Key Length means stronger security, and higher System Availability means better performance, reducing risk. Other attributes increase risk with higher values, so they have 0 direction. e.g. The raw value of remote worker #5 = remote worker #11 = 530 = rank = 1, direction = 0 (c.f. chapter 3.1.3 Figure 2).

Legend: colours in the figure 3

The colours in the figure (cf. Chapter 3.1.4, Figure 3), with higher values marked in red and lower values marked in green, represent different risk levels for remote workers:

- **Red** – Low Risk
- **Yellow** – Medium Risk
- **Green** – High Risk

Why We Need to Rank the Data

We ranked the raw values of attributes by using excel rank formula because they use different measurement units. This means we cannot directly add or average them to determine which remote worker has the highest risk. For example, we cannot add bit or hour to a percentage.

The Figure 3 ranks the raw data from Figure 1 based on different attributes. The ranking follows specific directions:

- **MORE = 0** Higher values mean higher risk.
- **LESS = 1** Lower value mean higher risk.

By ranking the attributes, we standardize them, making it easier to compare risk levels across different workers. This ranking helps identify remote workers with higher or lower risks, allowing organizations to focus on improving security where needed.

How We Ranked the Data

The ranking for each attribute is calculated using Excel's ranking function. The formula used is =RANK(number, reference, order)

- **Order 0** Ranks values in descending order (higher values = higher rank).
- **Order 1** Ranks values in ascending order (lower values = higher rank).

Estimating Risk Values

The estimated risk values for each remote worker come from ranking and averaging the raw data. These values provide an overview of each worker's security status, helping organizations make informed decisions about risk management.

3.1.5 COCO Y0 Analysis

UNITS	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	Risk points	percentage
COCO:Y0	Internet Traffic	Packet Error Rate	Security Logs	Authentication Logs	Key Length	Response Time	Malware Infections	Avg Time to Respond	Unauthorized Access Events	System Availability	Intrusion Attempts	System Downtime	Estimation	Fact+0	Delta	Delta/Fact
Remote Worker 1	7	6	8	8	18	38.4	13	15	15	5	861.5	7	1001.8	1000	-1.7	-0.17
Remote Worker 2	16	26	18	13	8	1	7	7	15	9	853	7	979.8	1000	20.2	2.02
Remote Worker 3	1	1	1	1	8	57.9	15	15	7	13	874	15	1008.7	1000	-8.7	-0.87
Remote Worker 4	10.5	14.5	5	5	18	50.4	7	7	7	15	861.5	15	1015.7	1000	-15.7	-1.57
Remote Worker 5	18	6	20	15	8	5	13	15	15	5	866.5	7	993.3	1000	6.7	0.67
Remote Worker 6	3	29.9	3	3	8	38.4	7	7	7	13	855	7	981.3	1000	18.7	1.87
Remote Worker 7	12.5	14.5	18	13	18	5	13	15	15	9	864.5	15	1012.2	1000	-12.2	-1.22
Remote Worker 8	4	6	5	5	18	50.4	7	7	7	5	863.5	7	984.8	1000	15.2	1.52
Remote Worker 9	16	26	18	13	8	1	7	15	15	13	857.5	15	1004.2	1000	-4.2	-0.42
Remote Worker 10	10.5	14.5	14	9	8	38.4	13	7	7	9	861.5	7	998.8	1000	1.2	0.12
Remote Worker 11	18	6	20	15	18	5	7	15	15	5	867.5	15	1006.2	1000	-6.2	-0.62
Remote Worker 12	7	26	8	8	8	57.9	13	7	7	15	856	15	1027.7	1000	-27.7	-2.77
Remote Worker 13	3	29.9	3	3	8	50.4	15	15	15	9	866.5	7	1024.7	1000	-24.7	-2.47
Remote Worker 14	12.5	14.5	18	13	18	5	7	7	7	5	863.5	15	985.3	1000	14.7	1.47
Remote Worker 15	1	1	1	1	8	57.9	7	15	15	13	855	7	981.8	1000	18.2	1.82
Remote Worker 16	7	6	8	8	18	38.4	13	7	7	5	861.5	15	993.8	1000	6.2	0.62

Figure 4: COCO Y0 Analysis Results

(Source: Author's own work <https://miau.my-x.hu/miau/323/rw2/rw2.xlsx>, COCO Y0 Sheet, Range=A116-Q132, 2025, based on ChatGPT-generated data. Validated against manual Excel calculations, Units Risk points).

Unit for Y0 and for all its aggregated component: Risk Points.

3.1.6 The Legend of Remote Worker Attributes

The legends show us important details about remote workers and whole process.

- Row Headers**

Each row represents a remote worker identified by an ID. Such as Remote Worker 1, Remote Worker 2 and Remote Worker etc.

- Column Headers**

Each column represents a specific attribute (c.f. chapter 3.1.3) related to the remote workers.

- Direction of Risk**

The table provides directional information indicating whether higher values of each attribute increase or decrease the risk level. For example, higher Internet Traffic, Packet Error Rate, Security Logs, etc., correspond to higher risk levels.

- Ranking-wise Table**

The table shows the ranking of each attribute for each remote worker based on the provided direction of risk.

- COCO (Continuous or Categorical Outcome):**

This section seems to provide additional calculations and comparisons based on the given data, including estimations, actual values, deltas, and errors.

- **Summary Statistics:**

Summary statistics are provided, including the sum of attribute values for each remote worker and the discrepancy between estimated and actual values.

3.1.7 Results Of COCO Y0 analysis

In the original experiment, which used ranked risk data from the ranked table, we found that Remote Worker 12 had the highest risk score of 1028 (c.f. 3.1.5 Figure 4: COCO Y0 Analysis). By using the Object Attribute Matrix, Data Analysis, and COCO Y0 Analysis, we identified remote workers with higher security risks in Operational Technology environments. These findings are very useful as they help organizations use their resources wisely by focusing on training and support for workers with high-risk scores. This approach strengthens cybersecurity by reducing threats and making the system more secure. Applying these targeted strategies is expected to improve worker performance, increase efficiency, boost system reliability, and ensure better compliance with security standards. In the long run, these efforts will help the company grow and improve profitability by reducing security risks and making operations smoother.

3.1.8 Validation checks for COCO Analysis

#	S	T	U	V	W	X	Y	Z	AA
136	units		Risk points	Risk points	Risk points	Risk points	Risk points		
137	Validation		Direct Estimation	Direct Delta	NORM	Inverse Estimation	Inverse Delta	VALIDATION	Interpretations
138	Remote Worker 1		1001.8	-1.7	1000	1004.4	-4.4	0	Symmetry-error
139	Remote Worker 2		979.8	20.2	1000	1021.4	-21.4	1	Symmetry-OK
140	Remote Worker 3		1008.7	-8.7	1000	986.9	13.1	1	Symmetry-OK
141	Remote Worker 4		1015.7	-15.7	1000	987.4	12.6	1	Symmetry-OK
142	Remote Worker 5		993.3	6.7	1000	999.4	0.6	0	Symmetry-error
143	Remote Worker 6		981.3	18.7	1000	1019.4	-19.4	1	Symmetry-ok
144	Remote Worker 7		1012.2	-12.2	1000	984.9	15.1	1	Symmetry-ok
145	Remote Worker 8		984.8	15.2	1000	1018.9	-18.9	1	Symmetry-ok
146	Remote Worker 9		1004.2	-4.2	1000	990.4	9.6	1	Symmetry-ok
147	Remote Worker 10		998.8	1.2	1000	1000.9	-0.9	1	Symmetry-ok
148	Remote Worker 11		1006.2	-6.2	1000	986.9	13.1	1	Symmetry-ok
149	Remote Worker 12		1027.7	-27.7	1000	978.4	21.6	1	Symmetry-ok
150	Remote Worker 13		1024.7	-24.7	1000	973.9	26.1	1	Symmetry-ok
151	Remote Worker 14		985.3	14.7	1000	1016.9	-16.9	1	Symmetry-ok
152	Remote Worker 15		981.8	18.2	1000	1017.9	-17.9	1	Symmetry-ok
153	Remote Worker 16		993.8	6.2	1000	1012.4	-12.4	1	Symmetry-ok

Figure 5: COCO Y0 Analysis Validation

(Source: Author's own work <https://miau.my-x.hu/miau/323/rw2/rw2.xlsx>, COCO Y0 Sheet, Range=T136-A153, 2025, based on ChatGPT-generated data. Validated against manual Excel calculations, Units Risk points).

To check, if the COCO Y0 analysis results were correct for each object, we performed a validation test based on function symmetry which is possible for stair-case functions. First, we reversed the direction of all attributes in the ranking table by changing 0 to 1 and 1 to 0 (see direct and invers ranking numbers). Then, we ran the analysis again using the inverse rankings as input, where the Y0 must be the same constant norm-value. For each object, we compared the direct and inverse estimation values by calculating how much they were different from the norm (1000) value. These differences are called delta values. We multiplied the direct delta value and inverse delta value, and if the result was less than or equal to zero, we marked the validation true as 1, which means the result is Symmetry OK. If the result was greater than zero, we marked it as 0, meaning the result might Symmetry-error. It means: the mirrored input has to lead to mirrored sign of the delta values in ideal case. This method helped us confirm whether the analysis gives balanced and logical estimated value (c.f. chapter 3.1.8 Figure 5).

3.2 Implementation of Automation for Risk Assessment

In today's digital world, remote work is growing rapidly, especially in Operational Technology environments like power grids and manufacturing plants. With remote access to these critical systems, cybersecurity risks have increased. My project addresses this by developing an automated risk ranking system for remote workers using C# in Visual Studio Code.

Manual risk assessments are time-consuming and prone to errors, especially as remote workforces grow. My system automates this process by collecting data from Excel and ranking workers based on cybersecurity attributes such as response times and error rates. This automated approach ensures real-time monitoring, improves accuracy, and provides tailored mitigation strategies like multi-factor authentication and security training.

C# was chosen for its efficiency, powerful libraries (like LINQ for data handling), and built-in security features, essential for managing sensitive OT data. My familiarity with C# from my computer science studies also made development smoother. Visual Studio Code was selected as the IDE for its extensibility, cross-platform support, integrated tools, and lightweight design, enhancing the development workflow.

The project benefits from C#'s scalability, efficient data handling, and support for ranking algorithms and automation, ensuring quick and accurate risk analysis. This system not only highlights potential risks but also offers proactive solutions to safeguard OT systems from cyber threats.

3.2.1 Testing the Program

Testing was essential to confirm that the program functioned as expected with data:

AI-Generated Data Transparency

Five Sample datasets were generated using ChatGPT to simulate realistic scenarios. While AI-assisted, all data underwent manual review for consistency with OT cybersecurity parameters. Each dataset contains different problems, remote workers and attributes to mimic real-world scenarios, problems and assess the program's ability to process various types of information accurately. This approach provided a thorough testing ground to confirm the robustness and versatility of the program.(c.f. Chapter 8.6 Annex VI)

Difference between free content COCO Y0 and automated program

COCO Y0 is "context-free," as it only works with data that has already been ranked. It does not handle raw data or make decisions based on inputs. It simply analyses these pre-ranked values with the norm values to determine risks. On the other hand, my program can perform several different tasks such as:

Extracts Raw Data: It pulls data directly from CSV files,(c.f. Figure 2: Raw Data Table)

making it flexible for different datasets and mention attributes and remote worker's number.

Analyses Relationships: It looks at how different worker attributes relate to each other using a correlation matrix.

Ranks the Data: It automatically ranks remote workers based on their directions.

Importance of Risk Assessment in Remote Work:

Remote workers do not always use the company's secure network, which makes them more open to cyber threats. These threats include phishing emails, hackers trying to access their accounts, and sudden system failures. The program checks important things like internet use, login records, and system health. This helps companies find security problems early and fix them before they become serious.

The program also finds workers who need more training, better security, or extra monitoring. This helps companies focus on the biggest risks and use their resources wisely. By doing this, they can keep important information safe and make remote work more secure.

Error Handling in Automation

To mitigate AI limitations, the program includes validation checks for:

- Missing/excessive data (e.g., null values trigger alerts and indicate user in which line value is missing).
- Attribute direction conflicts (e.g., correlation matrix flags inconsistencies).
- Rank equality for identical values (e.g., tied raw scores receive identical ranks).

Validation checks for Missing and Excessive data

Files can have many kinds of different data set of CSV files.

Example: If a CSV file omits "Packet Error Rate" values for 3 remote workers, the program:

- Shows an alert: [WARNING] Missing values detected in "Packet Error Rate" for Workers 5, 9, 14. Defaulting to median (0.12%).
- Substitutes missing values with the attribute's median to avoid skewing rankings.
- Technical Implementation: Uses C# Stream Reader to validate column completeness before processing.

These things help find security risks for objects e.g. remote workers. To make sure the data is correct, the system first checks the file. If the first row has words instead of numbers, it skips that row to avoid mistakes. The system then picks out the numbers because they are needed to check risks and rank workers based on their security level.

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. After preprocessing the data, the system proceeds to correlation analysis.

3.2.2 Correlation Analysis

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

- **0.3 to 1:** positive correlation (when one factor increases, the other also increases).
- **-0.3 to -1:** negative correlation (when one factor increases, the other decreases).
- **0.3 to -0.3:** No correlation (no clear relationship between the two variables)

Validation checks for attribute Direction Conflicts

Example: If "Key Length" is set to MORE=1 (longer = safer) but the correlation matrix detects a strong positive relationship with "Intrusion Attempts" (higher = riskier), the program:

- Shows inconsistency: [CONFLICT] "Key Length" and "Intrusion Attempts" show $\rho=+0.82$. Verify direction assignments..
- Pause ranking until the user confirms or corrects directions.

Technical Note: Pearson correlation (MathNet.Numerics) range limits set at $|\rho|>0.3$ for alerts.

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 attributes.

How Different Security Attributes Affect Risk Levels

Not all security attributes 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.

Excel Validation check for Correlation Alert

I validated the correlation between attributes using Excel by applying a simple direction vector approach, based on binary values. In this method, we assigned 0 to show a positive relationship this means that if two attributes increase or decrease together, they are positively related. We assigned 1 to represent a negative relationship, which means when one attribute increases and the other decreases, they are moving in opposite directions.

Since each attribute could only be either 0 or 1, we calculated all possible rows for an attribute using the formula 2 raised to the power of the number of attributes. To find out how many different combination pairs could be formed among the attributes, we used the standard combination formula:

$$nC_r = n! / [r!(n - r)!]$$

When comparing two attributes, like x1 and x2, if both have same binary values (either 0,0 or 1,1), it indicated a direct correlation. then its combination pair (x1 vs x2) will get 0 alert = yes shows the correlation is positive, meaning they tend to move in the same direction. IF the two attributes have different binary values (0,1 or 1,0) then its combination pair will get direction vector 0 alert = yes shows the correlation is negative, meaning they tend to move in the opposite direction. This approach helped us see attributes correlation alerts (c.f. chapter 8.7Annex VII).

Process:

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

Key Benefits:

- Helps maintain consistency in risk evaluation.
- Improves the accuracy of cybersecurity assessments.
- Reduces potential errors in risk classification.

3.2.3 Ranking Methodology

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

Process Overview:

- Employees are sorted based on their attribute values.
- Rankings are assigned, with a rank of 1 indicating the least risky value according to the attribute classification.
- 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 Prepare ranked Values 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.

Validation check for Rank Equality

Example: Two workers with identical "System Downtime" (4.2 hours):

- Assigns them the same rank (e.g., Rank 7 for both) rather than randomly choosing one to rank higher.
- Adjusts subsequent ranks (next worker receives Rank 8).

Technical Implementation: Uses LINQ's Group By to cluster identical values before assigning ranks.

Saving and Submitting Rankings

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. For assessing risks and identifying higher risk remote worker or object, the ranked data is transmitted to a Coco engine using an HTTP POST request through CURL.

Key Benefits:

Provides historical records for risk trend analysis.

Allows offline access for security reviews.

3.2.4 Automation Results

```
Ranked values saved to: E:\New folder\Curl\tempRankedValues.txt
Sending request to server...
Response from server:
1002
980
1009
1016
993
981
1012
985
1004
999
1006
1028
1025
985
982
994

Object 12 facing the highest risk: 1028

Help Section:
1. Input directions for attributes correctly based on correlation matrix.
2. Ensure the data file is correctly formatted.
3. Check for warnings about inconsistent directions.

Mitigation Strategy:
1. Provide training or tools to improve their weak attributes.
2. Use the correlation matrix to identify factors contributing to high risk.
Activate
```

Figure 6: Response from COCO Y0 Engine

(Source: Author's own software, 2025, Units Risk points).

Once the ranked data is processed by the COCO Y0 engine. The engine evaluates the A risk analysis of the data and generates an output, which is then stored locally for further examination. The engine sends the risk assessment results back to the software. Based on this response, the software shows the risk values for all objects and identifies which object faces the highest risk, as shown in Figure (c.f. Chapter 3.2.4), which is 1028 similar to the result of the COCO analysis (c.f. Figure 4).

Process Overview:

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

Key Benefits:

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

Highlighting remote worker with the Highest Risk Scores

Using the Display Highest Risk Objects method, the system identifies employees with the highest risk levels.

Process Overview

- Risk values are analysed to determine the highest recorded risk.
- Employees matching this risk level are identified.
- Their names and associated risk factors are displayed.

Key Benefits

Helps security teams prioritize threats.

Enables targeted security measures for high-risk employees.

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 Benefits

Enhances user experience by providing clear guidance.

Helps prevent input errors, improving assessment accuracy.

Validation Workflow Review

1. Data Import
2. Null/Format Checks
3. Correlation Validation
4. Rank Calculation
5. COCO Y0 Submission

3.2.5 How to involve AI

AI plays a key role in my thesis by helping assess security risks assessment and automate tasks of console-based software in the C# language (c.f. chapter 3). It supports the COCO Y0 model to identify remote workers at higher cybersecurity risk by analysing attributes like Internet Traffic, Packet Error Rate, Security Logs, Authentication Logs, and Key Length. For instance, if a worker has high internet traffic, many authentication errors, and uses weak key lengths, AI flags this worker as high-risk, reducing manual effort and speeding up results (c.f. chapter 3.1.12). To test the model, I used sample data generated by ChatGPT, an AI tool, to simulate real-world situations without using personal data (c.f. Figure 2).

AI is also used to build some incorporating features like a correlation matrix to check relationships between attributes. For example, if Internet Traffic and Packet Error Rate increase together, AI shows a positive correlation. If Key Length weakens while Security Logs show more threats, AI highlights a negative correlation and sends alerts, such as: Potential risk detected check for unauthorized access attempts (c.f. chapter 3.2.2).

In future, AI can predict risks by learning from past data. For example, if a worker shows unusual login behaviour every Friday, AI will recognize this pattern and send an early warning. It can also spot irregular activities, like if a worker suddenly uses much more internet, which might signal a security issue. If key length weakens, AI flags it as a risk. In the future, an AI chatbot could provide security tips, such as advising password resets if there are repeated login failures. These AI features will make the system smarter, faster, and more efficient by automating tasks and offering helpful advice, ultimately improving cybersecurity.

4 Discussions

I faced some challenges (different attributes, excel approach and automation) that made me think critically about my approach and methods. One of the biggest issues was that the attributes in my analysis were different, and each had different units. This made it difficult to calculate risk values and determine the overall risk of an object. For example, attributes like Key length (measured in Bits), Internet traffic (measured in Gigabytes), and security logs (count-based) could not be directly compared. To solve this issue, I ranked all attributes based on a direction vector (c.f. Figure 3: Ranked And Naive Table), which helped standardize them. This method ensured that the impact of each attribute on risk assessment was properly considered, making the risk calculation more structured and meaningful.

Another issue was that the Excel-based approach required ranking the raw data of each attribute for every remote worker based on the direction vector (c.f. chapter 3.1.4 Figure 3). After this, I determine the risk levels for each remote worker using a naïve risk assessment, but the results were not very reliable. To improve accuracy, I performed COCO Y0 analysis (c.f. chapter 3.1.5 Figure 4: COCO Y0 Analysis), which provided a more structured and optimized risk assessment. However, during the ranking process in the COCO engine, I had to manually copy and paste data, which introduced a high risk of human error. A small mistake in copying could lead to incorrect risk assessments, affecting the overall accuracy of the results. Additionally, this manual process was time-consuming and inefficient, making automation necessary for improved reliability and efficiency.

To solve this issue, I implemented automation (c.f. chapter 3.2 Implementation of Automation), which reduced human errors and made the process faster. Automation ensured that data was transferred to the COCO engine correctly without the risk of copy-paste mistakes, providing more accurate and reliable results. However, another challenge emerged: how to verify whether the automated results were correct.

To investigate this, I compared the risk assessment results generated by COCO Y0 with the results obtained through automation. This comparison helped ensure that the automated process maintained the same level of accuracy as the manually processed COCO Y0 results (c.f. chapter 3.2.4 Figure 6: Automation Results). The findings confirmed that automation not only saved time but also improved consistency in risk assessment.

Another point for improvement is the level of automation. While AI helps automate many tasks, some security decisions still require manual input. This means that my system is not fully autonomous yet. In the future, I would like to develop a more advanced AI system that can learn from past incidents and take immediate action without waiting for human intervention. However, this also raises concerns about AI making incorrect decisions, so finding the right balance between automation and human control is essential.

Finally, my thesis could benefit from more testing to face real world problems such as incorrect missing and excessive data by user. Although I used various data sets for testing the software (c.f. chapter 3.2.1 Testing the Program). but testing the system in a real company environment would provide better insights into its performance. This would help identify practical challenges and ensure the software is useful for actual users. In future research, I plan to conduct more real-world tests and collect feedback from cybersecurity professionals to improve the system further.

Despite these challenges, my thesis successfully shows how structured risk assessment can help improve cybersecurity for remote workers in OT environments. The project proves that an automated and optimized approach to risk assessment is more effective than relying on naïve solution or personal judgment.. Future improvements will focus on better automation, considering human factors, and testing the system in more real-world scenarios to make it even more reliable.

5 Conclusion

I identified several weaknesses, especially in four key layers: Data Collection, Ranking Process, Human Factors, and Automation. Each of these areas had challenges (collect data, correct ranking and human mistakes) that affected the overall effectiveness of my cybersecurity risk assessment system.

The first weakness lies in Data Collection. For OAM risk assessment, we need data from different sources and user, but gathering high-quality, real-time data was difficult. Some data points were missing, wrong format and others were not unexpected and additional data, which can affect the process of risk assessments and give wrong results. There was need to improve data integration by using AI working model ensuring that collecting data will be more accurate.

The second issue is Ranking Process. AI plays a major role in analysing cybersecurity risks, but it depends on how well the model is trained. During testing, I noticed that some of the objects were not ranked correctly (e.g. two remote workers with same value of internet traffic received different ranks because the current model didn't account for value equality). This showed that my AI model still needs improvements, especially in learning from new changes (e.g. Same raw values will get same rank) in an OAM. To overcome this, I need to refine the coding process, add a condition if two objects have the values they will get the same rank to improve the ranking process.

Another weakness is related to Human Factors. My thesis primarily focuses on technical solutions, but cybersecurity is not just about technology it also depends on how people behave. Even the best AI system cannot prevent risks if users make mistakes. e.g. assigning incorrect directions for attributes, connecting to public or unsecured networks or ignoring correlation alerts about correlation of attributes which effect the result of risk analysis due to high unauthorized access events, response time and Internet Traffic. My current system does not directly address this human aspect, which limits its effectiveness. In future work, I need to include cybersecurity awareness training and behaviour monitoring to reduce human-related risks (e.g. encouraging to the use of private, fast, and secure networks and prompting users to follow correlation alerts).

The final challenge is Automation. Although AI helps automate risk assessment, my system is not fully autonomous. Some security decisions still require human interaction such as assigning direction to the attributes and uploading csv file, which slows down response times. On the other hand, allowing AI to make automatic decisions carries risks, as it could react incorrectly

in complex situations. Finding the right balance between automation and human control is still a challenge.

Overall, my thesis successfully explores the use of AI in cybersecurity risk assessment, but it also highlights several areas (e.g. data collection, ranking method, human involvement, and automation).for improvement. Recognizing these weaknesses (e.g. missing or wrong data, different ranks for same values, user mistakes) is important because it allows me to refine my system and develop better software. By addressing data quality, improving AI accuracy, considering human factors(e.g. public or unsecured networks), and enhancing automation, I can create a more reliable and effective cybersecurity risk assessment tool for remote workers in operational technology environments. 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 the higher and lower risk values,. It is made in a simple and flexible way, so it can be added to other security tools (e.g. security monitoring or alert systems), and is useful for different organizations (e.g. schools, government offices, and software companies) that want to keep their remote workers safe.

6 Future

To improve cybersecurity effectiveness, the software will incorporate the following features:

- **AI-Driven Risk Analysis:** Machine learning will analyse historical data to better assess risks, helping to identify which remote workers are more likely to face high or low risks based on past incidents in order to compare with new data (e.g., detecting patterns in previous data breaches or vulnerabilities).
- **Instant Risk Detection:** The system will continuously monitor data to quickly detect risks and categorize remote workers as high-risk or low risk (e.g., spotting workers with irregular login behaviour, identifying workers using outdated software that may increase vulnerability).
- **Flexible Risk Configuration:** Organizations (e.g., companies in finance, healthcare, or government) will be able to adjust risk factors (e.g., setting specific criteria for worker access, prioritizing risk assessments based on location or device type) based on their unique security requirements.
- **Advanced Data Visualization:** Interactive dashboards (e.g., heatmaps, risk score charts) will help decision-makers visualize which remote workers face the highest risks (e.g., workers accessing systems from insecure networks, workers with weak password practices).
- **Automated Risk Response:** The system will automatically take action (e.g., flagging high-risk workers for review, locking accounts for workers identified with risky behaviours) to reduce potential damage as soon as risks are detected

7 Summary

My thesis presents an AI-assisted approach to analysing cybersecurity risks faced by remote workers in Operational Technology environments. It introduces a structured method called the Object-Attribute Matrix for risk assessment (c.f. chapter 3.1: OAM for Risk Assessment), which helps organize and evaluate different risk factors (c. f chapter 3.1.5) more accurately than naïve approaches (c.f. chapter 3.1.4). This optimized, anti-discrimination-based method ensures that cybersecurity risks are measured properly by using function-symmetry-based similarity analysis such as COCO Y0 (c.f. chapter 3.1.5: Figure 4: COCO Y0 Analysis) and identify which remote worker is facing the highest risk (c.f. chapter 3.1.8 Results Of COCO Y0 analysis). As remote worker becomes more common, the chances of cyber threats like system downtime, internet traffic, and network vulnerabilities have increased (c.f. chapter 1.2: Problem). My thesis focuses on creating a model/methodology that identifies high/low/norm-risk remote workers and suggests ways to reduce these risks (c.f. chapter 1.3: Aims/Goals).

This work is useful for industries where secure remote work is important, such as software companies, educational institutions, insurance firms, and government offices (c.f. chapter 1.4: Target Group and Usefulness).

Automation plays a key role in my thesis by making risk assessment more efficient (process of identifying high, medium and low risk quickly) and facilitate the efficient management of user inputs (c.f. chapter 3.1.8: Implementation of Automation). C# programming language help improve the steps and speed, and accuracy of risk assessments compared to manual methods (c.f. Chapter 3.1.13 How to Involve AI). The main contributions of my thesis automation include creating an automated ranking system and testing risk assessment methods (c.f. Chapter 3.1.9: Testing the Program) of raw data (c.f. Figure 2: Raw Data Table). Traditional (naive) risk assessment methods rely on simple risk detection methods (e.g. taking average of all attributes for each remote worker), which can be inconsistent (c.f. chapter 2.3: Risk Detection). My AI-based risk assessment model improves accuracy by using an optimized risk approach such COCO engine. Additionally, I also compare my work with other benchmark methodology on home-office security (c.f. chapter 2.1 Relationship to Other Theses), because it focuses on OT environments and uses real data for risk analysis, while studies relied on real test subjects. My benchmark Aadi and me used naïve approach (c.f. Figure#3) that use subjective scores and weights for the risk assessment, which are just approximations of optimal solutions, my automation (c.f. chapter 3.2) approach includes a correlation matrix (c.f. chapter 3.2.3) for generating alerts in case of arbitrary (inconsistent) user-direction-parameters base on rule to

detect positive and negative correlation between attributes (c.f. chapter 3.2.1: Testing the Program). The presented methodology can be adapted for quasi all arbitrary OAM-oriented analytical problems (e.g. Employees performance evaluation in different areas in a factory and Risk assessment in remote working etc). My thesis provides a structured and scalable cybersecurity risk assessment framework for remote work environments. By using automation, COCO Y0 analyses (a direct one and an indirect one), and correlation-matrix alerts, it reduces errors and improves accuracy in understanding the relationships between attributes, helping to choose the attributes direction for risk assessment. This approach can also be applied to other cybersecurity risk assessment problems (e.g. cloud security evaluations, insider threat detection, phishing attack and hacking simulations, and malware outbreak analysis). Future improvements could include further automation, deeper AI integration, and stronger cybersecurity defence mechanisms for OT systems (c.f. chapter 6: Future). My thesis lays a strong foundation for AI-powered cybersecurity risk evaluation and protection, opening new possibilities for innovation in this field.

8 Annexes

This chapter includes extra information such as the Raw Data & Ranked Table, Abbreviations, Figures, and References. These annexes help to support and explain the thesis more clearly.

8.1 Annex I: Raw Data & Ranked Table based on ChatGPT-conversations

Excel-generated raw data for each attribute of the 16 remote workers. (Source: *ChatGPT-4 simulation* <https://chatgpt.com/share/6803b600-8fa8-800d-ab32-4efd10be4e91> (prompt: "Generate 16 remote workers with...")).

8.2 Annex II: Abbreviations

- OT: Operational Technology
- IT: Information Technology
- ICS: Industrial Control Systems
- SCADA: Supervisory Control and Data Acquisition
- MFA: Multi-Factor Authentication
- AI: Artificial Intelligence
- OAM: Object-Attribute-Matrix
- IDE: Integrated Development Environment
- COCO Y0: Component-based Object Comparison for Objectivity

8.3 Annex III: Figures

- **Figure 1:** Steps Flow Chart...page#29
- **Figure 2:** Raw Data Table...page#32
- **Figure 3:** Ranked Raw Data Table...page#33
- **Figure 4:** COCO Y0 Analysis Results...page#35
- **Figure 5:** COCO Y0 Analysis Validation...page#36
- **Figure 6:** Response From COCO Y0 Engine ...page#43

8.4 Annex IV: References

The ordering-logic here in the list of references is ABC.

Aldrich, J.: *Correlations genuine and spurious in Pearson and Yule*. Statistical Science. 1995. p. 365. Retrieved from: <https://eprints.soton.ac.uk/32919/1/1177009870.pdf>

Alawida, M., Omolara, A. E., Abiodun, O. I., Al-Rajab, M.: *A deeper look into cybersecurity issues in the wake of Covid-19: A survey*. Journal of King Saud University - Computer and

Information Sciences. 34(10, Part A). 2022. pp. 8176–8206. Retrieved from: <https://doi.org/10.1016/j.jksuci.2022.08.003>

Babbs, A.: *How to leverage data security in a post-Covid world*. Computer Fraud & Security, 2020(10). 2020. pp. 8–11. Retrieved from: [https://doi.org/https://doi.org/10.1016/S1361-3723\(20\)30107-X](https://doi.org/https://doi.org/10.1016/S1361-3723(20)30107-X)

Barta, G.: *Application of Artificial Intelligence Methods in IT Systems Security Audit*. PhD Thesis. Bp.: MIAU. 2021. p. 1. Retrieved from: https://miau.my-x.hu/miau/292/Barta_Gergo_ertekezes.pdf

Corbet, Jonathan ["Code, conflict, and conduct"](#) (18 September 2018). Retrieved from: <https://lwn.net/Articles/765108/>

Chapman, P.: *Are your IT staff ready for the pandemic-driven insider threat?*. Network Security, 2020(4). 2022. pp. 8–11. Retrieved from: [https://doi.org/https://doi.org/10.1016/S1353-4858\(20\)30042-8](https://doi.org/https://doi.org/10.1016/S1353-4858(20)30042-8)

Fejes, Z. D., Pitlik, L., Rikk, J., Szűcs, D., Túri, P.: *E-volution in Defence Health Care: An overview of virtual educational and training opportunities*. Health Office. 2024(1-2). pp. 61–69. Retrieved from: https://miau.my-x.hu/miau/328/HealthOffice_Fejes.pdf

Furnell, S., Shah, J. N.: *Home working and cyber security – an outbreak of unpreparedness?*. Computer Fraud & Security, 2020(8). Retrieved from: [https://doi.org/10.1016/S1361-3723\(20\)30084-1](https://doi.org/10.1016/S1361-3723(20)30084-1)

Graham, L.: *Maximising protection in an era of remote working*. Computer Fraud & Security, 2021(3). 2021. pp. 16–17. Retrieved from: [https://doi.org/https://doi.org/10.1016/S1361-3723\(21\)00031-2](https://doi.org/https://doi.org/10.1016/S1361-3723(21)00031-2)

Goutam, R. K. *Cybersecurity fundamentals: Understand the role of cybersecurity, its importance and modern techniques used by cybersecurity professionals* (English ed.). BPB Publications. 2.1 History of computer and cybercrime. 2021a. Retrieved from: <https://books.google.hu/books?id=scUwEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>

Goutam, R. K. *Cybersecurity fundamentals: Understand the role of cybersecurity, its importance and modern techniques ued by cybersecurity professionals* (English ed.). BPB Publications. 1.1 Data. 2021b Retrieved from: <https://books.google.hu/books?id=scUwEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>

Goutam, R. K. *Cybersecurity fundamentals: Understand the role of cybersecurity, its importance and modern techniques used by cybersecurity professionals* (English ed.). BPB Publications. 1.1.1 Data versus information. 2021c Retrieved from: <https://books.google.hu/books?id=scUwEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>

Goutam, R. K. *Cybersecurity fundamentals: Understand the role of cybersecurity, its importance and modern techniques used by cybersecurity professionals* (English ed.). BPB Publications. 2.1 History of computer and cybercrime. 2021d Retrieved from: <https://books.google.hu/books?id=scUwEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>

Goutam, R. K. *Cybersecurity fundamentals: Understand the role of cybersecurity, its importance and modern techniques used by cybersecurity professionals* (English ed.). BPB Publications. 1.8 information system. 2021e Retrieved from: <https://books.google.hu/books?id=scUwEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>

Hijji, M., Alam, G.: *Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees*. Sensors 22(22). 2022. Article 866. Retrieved from: <https://doi.org/10.3390/s22228663>

HS Anhalt.: *Management von Cyber-Risiken*. Bernburg: HS Anhalt. 2015. p. 9. Retrieved from: https://www.hs-anhalt.de/fileadmin/Dateien/IT-Service-Center/Informationssicherheit/broschueren/handbuch_management_cyber_risiken_de.pdf

Kaspersky: *The great migration of cyberthreats: attacks on remote desktop protocols grew by 242% - reaching 3.3 billion - in 2020*. Kaspersky, 2020. Retrieved from: <https://www.kaspersky.com/about/press-releases/the-great-migration-of-cyberthreats-attacks-on-remote-desktop-protocols-grew-by-242-reaching-33-billion-in-2020>

Kaspersky MDR team: *Kaspersky experts report more than two critical cyber incidents per day in 2023*. Kaspersky. 2024. Retrieved from: <https://www.kaspersky.com/about/press-releases/kaspersky-experts-report-more-than-two-critical-cyber-incidents-per-day-in-2023>

Knuth, D. E.: *The Art of Computer Programming – Fundamental Algorithms* (3rd ed.). Boston: Addison-Wesley. 1997. p. 1. Retrieved from: <https://books.google.hu/books?id=x9AsAwAAQBAJ>

Mirza, M. N., Akram, M. S.: *3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare*. Islamabad: Strategic Studies Institute. 2022. p. 71 Retrieved from: https://strategicstudies.org.pk/index.php/strategic_studies/article/view/134/106

Mano, M. M.: *Computer System Architecture* (3rd ed.). 2006. Retrieved from: <https://www.mbit.edu.in/wp-content/uploads/2020/05/computer-systems-Architecture.pdf>

Peltier, T. R.: *Information Security Risk Analysis* (3rd ed.). Boca Raton: Auerbach Publications. 2010. p. 18. Retrieved from: <https://doi.org/10.1201/EBK1439839560>

Pakistan Parliament, Prevention of Electronic Crimes Act, 2016, https://na.gov.pk/uploads/documents/1470910659_707.pdf

Pitlik, L.: *Application of artificial intelligence methods in the security audit of IT systems. Hypotheses*. 2017. p. 2. Retrieved from: https://miau.my-x.hu/miau/phd/Barta_Gergo_Theses_of_the_doctoral_dissertation_0604.pdf

Pitlik, L., Pitlik, M., Pitlik, P.: *Attitude risk detection robot, Abstract*. 2018. Retrieved from: https://www.researchgate.net/publication/354695511_Attitud-kockazatfeltaro_robot

Pitlik, L., Rikk, J., Gángó, V., Tóth, C.: *Distance education as a kind of critical education operation and its IT-relevant aspects, or preparation for a dual education*. Informatics Journal. 2020. Retrieved from: https://miau.my-x.hu/bprof/kritikus_uzem.pdf#page=2

Pohlmann, N.: *IT-Sicherheitsleitfaden*. Bp.: Selbstverlag. 2019. p. 41. Retrieved from: <https://norbert-pohlmann.com/wp-content/uploads/2019/08/IT-Sicherheitsleitfaden-Prof.-Norbert-Pohlmann.pdf>

Qadri, Z.: *Cyber Threats in Pakistan: Rising Smishing Scams and the Double-Edged Sword of Hackers*. LinkedIn Article. 2023. Retrieved from: <https://www.linkedin.com/pulse/cyber-threats-pakistan-rising-smishing-scams-sword-hackers-qadri-uxmke/>

Rikk, J.: *Ethical hacking 1.0*. American Journal of Research, Education and Development, 2017a. p. 5. Retrieved from: https://red.devlart.hu/issues/2018_1.pdf#page=5

Rikk, J.: *Types of hackers*. American Journal of Research, Education and Development, 2017b. p. 7. Retrieved from: https://red.devlart.hu/issues/2018_1.pdf#page=7

Rajesh, A., Pitlik, L. & Pitlik, L.: *Risk-evaluation possibilities concerning IT-activities in home-office*. (conference presentation). 5th International Congress on Scientific Research. 2024. Retrieved from: https://miau.my-x.hu/miau/311/home_office_risks/full_home_office_risks.pdf

Rajesh, A., Pitlik, L. & Pitlik, L.: *Risk-evaluation possibilities concerning IT-activities in home-office*. (conference presentation). 5th International Congress on Scientific Research. 2025. Retrieved from: https://miau.my-x.hu/miau/319/itsec_III_20/more/aadi_rajesh.pdf

Sabin, J.: *The future of security in a remote-work environment*. Network Security 2021(10). 2021. pp. 15–17. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S1353485821001185>

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabae, S., Choo, K.-K. R., Al-Qirim, N.: *COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities*. Digital Communications and Networks 9(1). 2023. pp. 211–222. Retrieved from: <https://doi.org/10.1016/j.dcan.2022.08.005>

8.5 Annex V Conversations with LLMs

Prompt1 = ChatGPT was asked to create raw data for 16 remote workers based on security-related attributes.

Answer1 = Certainly! Here's a table presenting realistic, numerical data for 16 remote workers based on security-related attributes. These values are informed by industry reports and studies to reflect real-world scenarios.

Worker	Packets				Malware		Avg		Unauthorized Access Events (per month)	Intrusion		
	Internet Traffic (GB/month)	Packet Error Rate (%)	Security Logs (per day)	Authentication Logs (per day)	Key Length (bits)	Response Time (ms)	are infected (per month)	Time to Respond (hours)		System Availability (%)	Incidents (per month)	System Downtime (hours/month)
1	500	0.05	3,125	625	256	150	1	3	2	99.9	25	2
2	520	0.07	3,200	640	2048	140	1	2.5	2	99.8	20	2
3	480	0.04	3,000	600	2048	160	1	3	1	99.7	30	2.5

Worker	Internet Traffic (GB/month)	Packet Security			Authentication Logs (per day)	Key Length (bits)	Response Time (ms)	Malware Infections (per month)	Avg Time to Respond (hours)	Unauthorized Access Events (per month)	System Availability (%)	Intrusion Detection System	
		Error Rate (%)	Logs (per day)	Attempts (per month)								Downtime (hours/month)	
4	510	0.06	3,100	620	256	155	1	2.5	1	99.6	25	2.5	
5	530	0.05	3,250	650	2048	145	1	3	2	99.9	28	2	
6	490	0.08	3,050	610	2048	150	1	2.5	1	99.7	22	2	
7	515	0.06	3,200	640	256	145	1	3	2	99.8	27	2.5	
8	495	0.05	3,100	620	256	155	1	2.5	1	99.9	26	2	
9	520	0.07	3,200	640	2048	140	1	3	2	99.7	24	2.5	
10	510	0.06	3,150	630	2048	150	1	2.5	1	99.8	25	2	
11	530	0.05	3,250	650	256	145	1	3	2	99.9	29	2.5	
12	500	0.07	3,125	625	2048	160	1	2.5	1	99.6	23	2.5	
13	490	0.08	3,050	610	2048	155	1	3	2	99.8	28	2	
14	515	0.06	3,200	640	256	145	1	2.5	1	99.9	26	2.5	

Worker	Pac						Malw Avg		Unauth	Intru		
	Intern et Traffic (GB/m onth)	ket Err or Rate (%)	Secu rity Logs (per day)	Authenti cation Logs (per day)	Key Len gth (bit s)	Resp onse Time (ms)	are Time Infect ions (per mont h)	Time Resp ond (hou rs)		Syste m Availa bility (%)	sion Atte mpts (per mont h)	System Downti me (hours/ month)
15	480	0.04	3,000	600	2048	160	1	3	2	99.7	22	2
16	500	0.05	3,125	625	256	150	1	2.5	1	99.9	25	2.5

Sources and References:

- **Internet Traffic (GB/month):** Remote workers typically use between 8 to 20 GB per month, depending on their activities. [Tech With Tech](#)
- **Packet Error Rate (%):** Standard packet error rates in reliable networks are around 0.05% to 0.1%.
- **Security Logs & Authentication Logs (per day):** The number of logs varies based on user activity and security policies.
- **Key Length (bits):** Common encryption standards include 256-bit and 2048-bit keys, depending on the encryption method used.
- **Response Time (ms):** Average response times for small business networks range between 140 ms to 160 ms.
- **Malware Infections (per month):** Small businesses may experience approximately one malware infection per month.
- **Average Time to Respond (hours):** Organizations take an average of 20.9 hours to respond to cyberattacks. [makeuseof.com+2VentureBeat+2businesswire.com+2](#)
- **Unauthorized Access Events (per month):** The frequency of unauthorized access events can vary; small businesses may experience 1-2 events per month.
- **System Availability (%):** High availability systems aim for 99.9% uptime. [crowdstrike.com](#)
- ****Intrusion Attempts (per).**

Prompt2 = Chat GPT can you tell me name of books related to computer and cyber security.

Answer2 = Here are some books:

Computer System Architecture (3rd ed.)

Information Security Risk Analysis (3rd ed.)

The Art of Computer Programming Fundamental Algorithms (3rd ed.)

Cyber Crime, Cyber Terrorism and Cyber Warfare

8.6 Annex VI: Test Cases

Test Case #1: Data Import and Validation

Steps:

#	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Remote Worker (below) / attributes for comparing	Internet Traffic (GB/month)	Packet Error Rate (%)	Security Logs (per day)	Authentication Logs (per day)	Key Length (bits)	Response Time (ms)	Malware Infections (per month)	Avg Time to Respond (hours)	Unauthorized Access Events (per month)	System Availability Percentage (%)	Intrusion Attempts (per month)	System Downtime (hours/month)
2	Remote Worker 1	500	0.05	3125	625	256	150	2	3	2	99.9	25	2
3	Remote Worker 2	520	0.07	3200	640	2048	140	1	2.5	2	99.8	20	2
4	Remote Worker 3	480	0.04	3000	600	2048	160	3	3	1	99.7	30	2.5
5	Remote Worker 4	510	0.06	3100	620	256	155	1	2.5	1	99.6	25	2.5
6	Remote Worker 5	530	0.05	3250	650	2048	145	2	3	2	99.9	28	2
7	Remote Worker 6	490	0.08	3050	610	2048	150	1	2.5	1	99.7	22	2
8	Remote Worker 7	515	0.06	3200	640	256	145	2	3	2	99.8	27	2.5
9	Remote Worker 8	495	0.05	3100	620	256	155	1	2.5	1	99.9	26	2
10	Remote Worker 9	520	0.07	3200	640	2048	140	1	3	2	99.7	24	2.5
11	Remote Worker 10	510	0.06	3150	630	2048	150	2	2.5	1	99.8	25	2
12	Remote Worker 11	530	0.05	3250	650	256	145	1	3	2	99.9	29	2.5
13	Remote Worker 12	500	0.07	3125	625	2048	160	2	2.5	1	99.6	23	2.5
14	Remote Worker 13	490	0.08	3050	610	2048	155	3	3	2	99.8	28	2
15	Remote Worker 14	515	0.06	3200	640	256	145	1	2.5	1	99.9	26	2.5
16	Remote Worker 15	480	0.04	3000	600	2048	160	1	3	2	99.7	22	2
17	Remote Worker 16	500	0.05	3125	625	256	150	2	2.5	1	99.9	25	2.5

1. Upload a CSV file containing objects and attributes (like failed login attempts, software update frequency, and network activity, etc.).
2. Verify if the system correctly reads the file and recognizes headers and object.
3. Ensure that unnecessary data is ignored and skipped, and valid data is processed.

Expected Outcome:

```

Sending request to server...
Response from server:
1002
980
1009
1016
993
981
1012
985
1004
999
1006
1028
1025
985
982
994

Object 12 facing the highest risk: 1028

```

- The system successfully uploads the data.
- Irrelevant columns are filtered out.
- No errors occur during the import process.

Test Case #2: Data Cleaning and Processing

Steps:

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Remote Worker (below) / attributes for comparing	Internet Traffic (GB/month)	Packet Error Rate (%)	Security Logs (per day)	Authentication Logs (per day)	Key Length (bits)	Response Time (ms)	Malware Infections (per month)	Avg Time to Respond (hours)	Unauthorized Access Events (per month)	System Availability Percentage (%)	Intrusion Attempts (per month)	System Downtime (hours/month)	Norm Value
2	Remote Worker 1	500	0.05	3125	625	256	150	2	3	2	99.9	25	2	1000
3	Remote Worker 2	520	0.07	3200	640	2048	140	1	2.5	2	99.8	20	2	1000
4	Remote Worker 3	480	0.04	3000	600	2048	160	3	3	1	99.7	30	2.5	1000
5	Remote Worker 4	510	0.06	3100	620	256	155	1	2.5	1	99.6	25	2.5	1000
6	Remote Worker 5	530	0.05	3250	650	2048	145	2	3	2	99.9	28	2	1000
7	Remote Worker 6	490	0.08	3050	610	2048	150	1	2.5	1	99.7	22	2	1000
8	Remote Worker 7	515	0.06	3200	640	256	145	2	3	2	99.8	27	2.5	1000
9	Remote Worker 8	495	0.05	3100	620	256	155	1	2.5	1	99.9	26	2	1000
10	Remote Worker 9	520	0.07	3200	640	2048	140	1	3	2	99.7	24	2.5	1000
11	Remote Worker 10	510	0.06	3150	630	2048	150	2	2.5	1	99.8	25	2	1000
12	Remote Worker 11	530	0.05	3250	650	256	145	1	3	2	99.9	29	2.5	1000
13	Remote Worker 12	500	0.07	3125	625	2048	160	2	2.5	1	99.6	23	2.5	1000
14	Remote Worker 13	490	0.08	3050	610	2048	155	3	3	2	99.8	28	2	1000
15	Remote Worker 14	515	0.06	3200	640	256	145	1	2.5	1	99.9	26	2.5	1000
16	Remote Worker 15	480	0.04	3000	600	2048	160	1	3	2	99.7	22	2	1000
17	Remote Worker 16	500	0.05	3125	625	256	150	2	2.5	1	99.9	25	2.5	1000

1. Upload a CSV file containing constant norm (=1000) value in last row.
2. Software ensures that if data is missing or irrelevant immediately inform to the user.
3. Validate, that columns with identical values e.g. norm(=1000) is excluded.
4. Check if only numerical (integer) attributes are retained for ranking.

Expected Outcome:

```

Sending request to server...
Response from server:
1002
980
1009
1016
993
981
1012
985
1004
999
1006
1028
1025
985
982
994

Object 12 facing the highest risk: 1028

```

- Only necessary data is kept and provide results.
- The system confirms that preprocessing is complete.

Test Case #3: Analysing file without headers and IDs

Steps:

#	A	B	C	D	E	F	G	H	I	J	K	L
1	500	0.05	3125	625	256	150	2	3	2	99.9	25	2
2	520	0.07	3200	640	2048	140	1	2.5	2	99.8	20	2
3	480	0.04	3000	600	2048	160	3	3	1	99.7	30	2.5
4	510	0.06	3100	620	256	155	1	2.5	1	99.6	25	2.5
5	530	0.05	3250	650	2048	145	2	3	2	99.9	28	2
6	490	0.08	3050	610	2048	150	1	2.5	1	99.7	22	2
7	515	0.06	3200	640	256	145	2	3	2	99.8	27	2.5
8	495	0.05	3100	620	256	155	1	2.5	1	99.9	26	2
9	520	0.07	3200	640	2048	140	1	3	2	99.7	24	2.5
10	510	0.06	3150	630	2048	150	2	2.5	1	99.8	25	2
11	530	0.05	3250	650	256	145	1	3	2	99.9	29	2.5
12	500	0.07	3125	625	2048	160	2	2.5	1	99.6	23	2.5
13	490	0.08	3050	610	2048	155	3	3	2	99.8	28	2
14	515	0.06	3200	640	256	145	1	2.5	1	99.9	26	2.5
15	480	0.04	3000	600	2048	160	1	3	2	99.7	22	2
16	500	0.05	3125	625	256	150	2	2.5	1	99.9	25	2.5

1. Upload a CSV file containing no headers (Attributes names) and column IDs (Object IDs).
2. Verify if the system correctly reads the file and recognizes headers and Column IDs are not present.
3. Ensure that first row and column is not skipped.

Expected Outcome:

```

Sending request to server...
Response from server:
1002
980
1009
1016
993
981
1012
985
1004
999
1006
1028
1025
985
982
994

Object 12 facing the highest risk: 1028

```

- The system successfully loads and processes the data and gives result.
- No errors occur during the import process.

Test Case 4: Single Attribute, Single Object

	A	B	C	D	E
1	comparable Remote Worker (below) / attributes for	Internet Traffic (GB/month)	Y		
2	Remote Worker 1	500	1000		
3					
4					
5					

Steps:

- Upload a CSV file containing with 1 attribute and 1 object.
- Ensure that attributes correlation is calculated to help the user to determine the direction.
- Process the ranking using the provided direction.
- Ensure that value of 1000 added in the last column after ranking.

- Save the ranked data in a Notepad file.

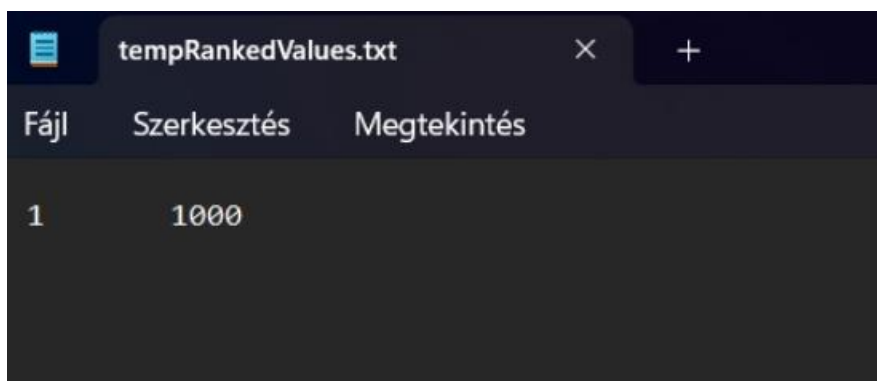
```
Sending request to server...
Response from server:
1000

All objects facing the same risk: 1000
```

```
Correlation Matrix (lower Triangular):
Attr\Attr      A1
-----
A1      1.00
```

Expected Outcome:

- The ranking file is successfully generated.
- The single object is ranked correctly.
- The last column contains 1000.



- The output is saved properly.

Test Case 5: Single Attribute, 432 Objects

Steps:

	A	B	C	D	E	F	G	H	I	J	K	L
1	500	0.05	3125	625	256	150	2	3	2	99.9	25	2
2	520	0.07	3200	640	2048	140	1	2.5	2	99.8	20	2
3	480	0.04	3000	600	2048	160	3	3	1	99.7	30	2.5
4	510	0.06	3100	620	256	155	1	2.5	1	99.6	25	2.5
5	530	0.05	3250	650	2048	145	2	3	2	99.9	28	2
6	490	0.08	3050	610	2048	150	1	2.5	1	99.7	22	2
7	515	0.06	3200	640	256	145	2	3	2	99.8	27	2.5
8	495	0.05	3100	620	256	155	1	2.5	1	99.9	26	2
9	520	0.07	3200	640	2048	140	1	3	2	99.7	24	2.5
10	510	0.06	3150	630	2048	150	2	2.5	1	99.8	25	2
11	530	0.05	3250	650	256	145	1	3	2	99.9	29	2.5
12	500	0.07	3125	625	2048	160	2	2.5	1	99.6	23	2.5
13	490	0.08	3050	610	2048	155	3	3	2	99.8	28	2
14	515	0.06	3200	640	256	145	1	2.5	1	99.9	26	2.5
15	480	0.04	3000	600	2048	160	1	3	2	99.7	22	2
16	500	0.05	3125	625	256	150	2	2.5	1	99.9	25	2.5

1. Upload a CSV file containing 12 attribute and 16 objects.
2. Ensure the last column contains a value of 1000 for all objects.
3. Save the ranked data in a Notepad file.

Expected

Outcome:

```
Sending request to server...
Response from server:
1002
980
1009
1016
993
981
1012
985
1004
999
1006
1028
1025
985
982
994

Object 12 facing the highest risk: 1028
```

- The ranking file is successfully generated.
- All 16 objects are ranked correctly.
- The last column contains 1000 for all objects.
- The data is saved properly.

8.7 Annex VII: Correlation Alerts

This annex shows attributes correlation alert patterns (Source <https://miau.my-x.hu/miau/323/rw2/rw2.xlsx>, Correlation Sheet, 2025).

Demo Raw Value Table

22	Binary	x1	x2	x3
23	Remote Worker 1	500	0.05	3125
24	Remote Worker 2	520	0.07	3200
25	Remote Worker 3	480	0.04	3000
26	Remote Worker 4	510	0.06	3100
27	Remote Worker 5	530	0.05	3250
28	Remote Worker 6	490	0.08	3050
29	Remote Worker 7	515	0.06	3200
30	Remote Worker 8	495	0.05	3100
31	Remote Worker 9	520	0.07	3200
32	Remote Worker 10	510	0.06	3150
33	Remote Worker 11	530	0.05	3250
34	Remote Worker 12	500	0.07	3125
35	Remote Worker 13	490	0.08	3050
36	Remote Worker 14	515	0.06	3200
37	Remote Worker 15	480	0.04	3000
38	Remote Worker 16	500	0.05	3125

This table contains the original binary values of selected attributes used for correlation alerts.

Binary Value Table

22	direction vectors (binary)	x1	x2	x3
23	1	0	0	0
24	2	0	0	1
25	3	0	1	0
26	4	0	1	1
27	5	1	0	0
28	6	1	0	1
29	7	1	1	0
30	8	1	1	1

I calculated all possible rows for an attribute (x1,x2&x3) using the formula. ($2^3= 8$ rows) means that when you have 3 attributes and each can be either 0 or 1, there are 8 possible combinations (since $2 \times 2 \times 2=8$).

Attributes Combination Pairs Table

	O	P	Q	R	S
22	OAM Raw	x1 vs x2	x1 vs x3	x2 vs x3	Y0
23	1	0	0	0	1000
24	2	0	1	1	1000
25	3	1	0	1	1000
26	4	1	1	0	1000
27	5	1	1	0	1000
28	6	1	0	1	1000
29	7	0	1	1	1000
30	8	0	0	0	1000

To find out how many different combination pairs could be formed among the attributes; I used the standard combination formula (3 under the 2 = $3*2/1*2=3$). The meaning of 3 under the 2 is selecting 2 attributes out of 3, which is a combination pair. The formula is: $(3 \times 2) \div (2 \times 1) = 3$, giving the total number of ways to choose 2 attributes from 3. When comparing two attributes like x1 and x2:

- If both have the same value as (x1=0 and x2=0 or x1=1 and x2=1 e.g. Binary Value Table). This shows a direct and positive correlation alert, so we write 0 for the pair.
- If they have different values (like x1=0 and x2=1 or x1=1 and x2=0 as in Binary Value Table), it means they move in opposite directions. This shows a negative correlation alert, so we also write 1 for the pair.