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

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

Presenter: Aadi Rajesh: Kodolányi János University

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

Full Text

Introduction

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

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

Evaluating risks associated with IT activities in a home-office environment involves identifying potential threats and vulnerabilities, assessing their likelihood and impact, and implementing measures to mitigate or manage these risks[1].

Literature

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

1. Security: It helps ensure the security of sensitive data and information. With the increasing prevalence of cyber threats such as malware, phishing, and ransomware, understanding and mitigating risks is essential to protect personal and business data.[2]

2. Compliance: Many industries and jurisdictions have regulations and compliance standards related to data protection and security. Conducting risk evaluations helps ensure compliance with these regulations, avoiding potential legal consequences and penalties.[3]

---

[1] Nwankpa & Datta, 2023

[2] Nwankpa & Datta, 2023

[3] Nwankpa & Datta, 2023

3. Business Continuity: Identifying and mitigating risks helps minimize the potential for disruptions to home-office activities. By proactively addressing vulnerabilities, individuals can reduce the likelihood and impact of incidents that could interrupt work or compromise productivity[4].

4. Protecting Assets: Home-office setups often include valuable assets such as computers, networking equipment, and intellectual property. Assessing risks helps safeguard these assets from theft, damage, or unauthorized access[5].

5. Reputation Management: A security breach or data loss can damage an individual's or business's reputation. By understanding and mitigating risks, individuals can demonstrate their commitment to security and protect their reputation among clients, customers, and stakeholders[6]

6. Cost Savings: Addressing risks proactively can help avoid the financial costs associated with security incidents, such as data recovery, legal fees, regulatory fines, and loss of business opportunities. Investing in security measures upfront can save money in the long run.[7]7.Peace of Mind: Knowing that risks have been identified and mitigated provides peace of mind for individuals working from home. It allows them to focus on their work without constantly worrying about potential security threats or disruptions.[8]

8. Compliance, trust and reliability: For a company, being able to be compliant, trusted and reliable is of utmost importance for its business continuity, customer satisfaction and future growth potential. Companies which invest in better cyber security can gain trust and confidence of their vendors and customers, which is cruital for a sustainable long-term business growth and continuity strategy[9].

…

---

[4] Hewitt, 2023

[5] Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events | NCCoE, n.d

[6] How to Manage Reputational Damage in Cyber Security | Institute of Data, 2023

[7] Nwankpa & Datta, 2023

[8] Eeckman, 2020

[9] Own abstract and presentation: Aadi Rajesh et al: Risk-evaluation possibilities concerning IT-activities in home-office

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

Own analyses

The risk potential concerning the IT activities in the home office can be described with a lot of abstraction/attributes (c.f. Compliance Violations, Remote Access Vulnerabilities, Cyber Attacks, Data Breaches, Third-party Software Risks etc.) By creating a system of most important objects and attributes, we can create parameters based on which we could analyses the risk based on an online AI-tool where anti-discriminative optimizations can be run using stair-case functions concerning the hypothesis whether each object can have the same risk index or not? Some of the attributes include Number of firewalls in the network, Scores from Intrusion detection and antivirus systems, no of users who access the device, number of non-authorized user logins, Password change frequency, etc. While creating an analytical model brough it its own challenges and issues, the most challenging task is the collection of real or realistic raw data. As most antivirus and threat detection software use proprietary access, and getting data from offices can be challenging due to various legal issues such as GDPR, company policies, data sharing rules etc. This task has been circumvented by first creating quasi-randomized data using real life research on the likelihood of various parameters and their minimum, maximum, average, mean, median and mode values and gain real life data, without names or any personalized information of the user.

Rational and OAM

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

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

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

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

Attribute ID

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

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

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

- Either our network is very unsafe

- Or the Firewall works too well

-Or Both

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

- Either our network is military grade secure

- Or our firewall doesn't work at all

- Or both

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

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

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

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

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

(Source: Own presentation)

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

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

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

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

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

Step 3: Using online COCO analysis

COCO Analysis is an AI based analytical tool which can help in predicting pointers and key data directions in large data sets. The AI program can be used as a ranking module and helps predict which attributes are more important than others and use ai to predict outcomes[10].

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

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

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

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

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

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

[10] Pitlik, László. (2010)

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

Figure 3: Excel Solver (Source: Own presentation)

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

But due to the complexities of the data and the need to analyze the entire data sets, with all the rankings per attributes and then predict from all the subjects, and attributes, which test subjects are at the higher risk. Coco AI analysis (online) was used Figure #4 and in Figure #5, Figure #6 and Figure #7, we can understand how the analysis predicted results and assisted us in providing a better analysis for the data.

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

Identifier:	5643774	Objects:	16	Attributes:	17	Stairs:	16	Offset:	0	Description:	COCO Y0: 5643774								
Ranking	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	Y	
O1	11	14	15	7	15	7	12	8	9	11	1	2	6	2	16	2	7	1000	
O2	1	13	15	4	14	3	11	16	1	7	5	15	14	11	14	15	9	1000	
O3	8	1	1	1	1	15	9	5	12	2	3	10	16	14	14	3	14	1000	
O4	13	9	12	4	7	11	7	9	8	13	12	7	13	5	13	16	16	1000	
O5	9	1	1	7	15	11	10	3	14	16	2	3	11	13	4	1	1	1000	
O6	13	10	1	7	3	7	16	13	4	5	13	16	10	9	9	6	12	1000	
O7	5	5	7	7	3	1	14	4	13	1	16	13	9	7	12	8	14	1000	
O8	9	4	6	7	2	2	5	2	15	8	4	12	8	10	4	8	1	1000	
O9	5	5	1	1	3	3	15	7	10	6	15	6	7	16	6	3	4	1000	
O10	13	14	1	7	10	3	4	12	5	10	6	14	4	3	9	12	9	1000	
O11	1	10	12	4	10	7	8	14	3	9	9	11	2	4	7	12	9	1000	
O12	1	5	7	7	10	10	1	1	16	4	8	5	15	15	1	5	5	1000	
O13	16	1	11	7	7	11	3	15	2	3	10	8	2	12	1	7	7	1000	
O14	1	5	12	7	3	3	6	10	7	15	11	1	12	8	7	12	5	1000	
O15	5	14	7	7	7	16	2	6	11	14	7	4	1	1	9	11	1	1000	
O16	11	10	7	1	13	11	12	11	6	12	14	9	5	6	1	10	12	1000	

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

Unit: Ranking based on Attributes: 1-16, 1= Least likelihood of Cyberthreat, 16: Highest

Unit for Y0: risk index/score

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

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

(Source: Own presentation)

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

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

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

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

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

Figure 7 Estimation of the risks (multidimensional optimized aggregation)

(Source: Own presentation)

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

Legend: Attribute ID

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

Results

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

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

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

Discussions

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

In a realist world view scenario, being actively prepared for threats and constant vulnerability testing is needed and for that I would appreciate constructive feedback and criticism of my structure, OAM approach, analysis and results. This feedback will help me

improve this project and assist in my personal and professional development as an aspirational cyber security expert.

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

Conclusions and Summary

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

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

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

Future Directions

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

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

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

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

References

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

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

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

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

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

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

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