HIERARCHICAL FORMATION OF CAUSAL NETWORKS BASED ON CHATGPT

Dmitry Lande
National Technical University of Ukraine – Igor Sikorsky Kyiv Polytechnic Institute

Leonard Strashnoy
The University of California, Los Angeles (UCLA)

Annotation

This paper is devoted to a methodology of forming causal networks by applying the ChatGPT system repeatedly, and visualizing and analyzing these networks with Gephi. The methodology is based on the use of the ChatGPT system, a generative pre-trained transformer on large text corpora, which uses artificial intelligence capabilities to perform user prompts. The methodology covers the means of analysis and visualization of the formed networks using the Gephi program. The CSV format is used to upload data to the Gephi environment. The article shows the possibility of constructing causal networks of concepts based on the use of Chat GPT, which allows for solving problems that previously required the involvement of large resources (human and time). The methodology integrates means of intellectual text analytics and network analysis, as well as their visualization. The formed causal networks provide the possibility of further transition to scenario analysis. The article discusses the possibility of emulating a multitude of experts by repeatedly applying similar prompts to the ChatGPT system. The proposed comprehensive methodology can be applied to the construction of causal networks in various subject areas.

Keywords:

Chat GPT, causal networks, Domain model, Artificial experts, Graph visualization, Cyber Security

Introduction

Recently, large linguistic models, such as ChatGPT, are gaining more widespread use in many areas. The most common applications are machine translation, text summarization, various levels of generalization, for example, formulating questions for educational materials. In particular, ChatGPT from OpenAI is a Generative Pre-trained Transformer (GPT) that uses natural language processing to perform user prompts using the broad capabilities of the field of artificial intelligence [1].
Huge opportunities in extracting basic concepts, named entities, allow using ChatGPT in factographic systems, in particular, in medicine and economics [2]. Naturally,

intellectual chats are integrated with external systems, such as geographic information [2], systems for analyzing and visualizing graphs, and networks [3]. In particular, the authors in [4] showed how to form networks of connections between characters of literary works, networks of subject areas with "general-particular" connections.
This work is devoted to the description of the methodology for forming causal (causal) networks by repeatedly addressing the ChatGPT system, as well as visualizing and analyzing these networks using the Gephi system (gephi.org) - the most popular graph visualization program with a free license [5]. CSV format is quite suitable for uploading data to the Gephi environment, so all requests to ChatGPT will be accompanied by a requirement for the format.
Causal relationships are necessary when models are implemented in critically important areas such as healthcare, disaster management, theft detection, finance, and law [6].
The formed causal networks provide the possibility of further transition to scenario analysis. The main problem that arises when conducting scenario analysis based on causal networks is precisely the creation of such systems, which in traditional cases requires large resource costs, attracting experts. There are also successful attempts at automated formation of causal networks, for example, in [7] a rule-based SCANER system is presented, which transforms raw text into causal networks using a set of natural language processing tools.
The approach proposed by the authors for forming a swarm of virtual experts [4] will significantly simplify and speed up the process of forming causal networks.

Formation of a network based on simple hierarchical access to ChatGPT

So, our plans include describing the procedures for forming cause-and-effect networks in the field of cybersecurity through hierarchical refinement. Let's move on to the description of tasks and their solutions. It should be noted that not every subject area was sufficiently covered by ChatGPT during its training. Obviously, the system "knows" a subject area of such a scale. To build a network, it is necessary to obtain a CSV file and upload it to the Gephi program.
Let's say, for example, we are interested in the issue of data leakage. We will ask ChatGPT to provide known causes of this phenomenon. The central node of the future network should be the concept of "data_leakage". Successful processing of such a request will determine the second level of the hierarchy - concepts related to data leakage - its causes. After that, for each such concept, a set of reasons that influenced it is also requested. This process can continue indefinitely, but in this work, we will stop at three levels. Obviously, some concepts of the third level can influence different concepts of the second level, as well as the concept of the first level directly. Theoretically, looping is also possible, which can be interpreted as the paradox of primacy (which came first, the chicken or the egg?). Thus, despite the hierarchical formation of such a causal network, the resulting network will not be a strictly

hierarchical structure.

By offering ChatGPT to process a certain prompt, we will get a set of reasons for the primary concept. The ChatGPT system can help in obtaining the content of the CSV file (fields corresponding to character names, separated by a semicolon). To do this, you can use, for example, such a request (prompt) to the ChatGPT system:

> List the causes of **data leakage** in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; **data leakage**". Each such entry - from a new line

The system gives an answer of approximately this kind:

```
human error; data leakage
weak passwords; data leakage
insider threats; data leakage
misconfigured systems; data leakage
phishing attacks; data leakage
unpatched software; data leakage
malware infection; data leakage
social engineering; data leakage
third-party access; data leakage
stolen devices; data leakage
```

Prompts of the next level will relate to the concepts presented in the answer and have a form fully corresponding to the primary prompt, for example:

> List the causes of **human error** in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; **human error** ". Each such entry - from a new line

The set of all prompts and answers is given in Appendix 1.
The combined answers of ChatGPT in one CSV file are uploaded for analysis and visualization in the Gephi program.
After loading the obtained data into the Gephi system, we select the node size proportional to the degree (number of adjacent connections) and dividing the network into clusters according to the modularity criterion, we get a clear graph (Fig. 1).

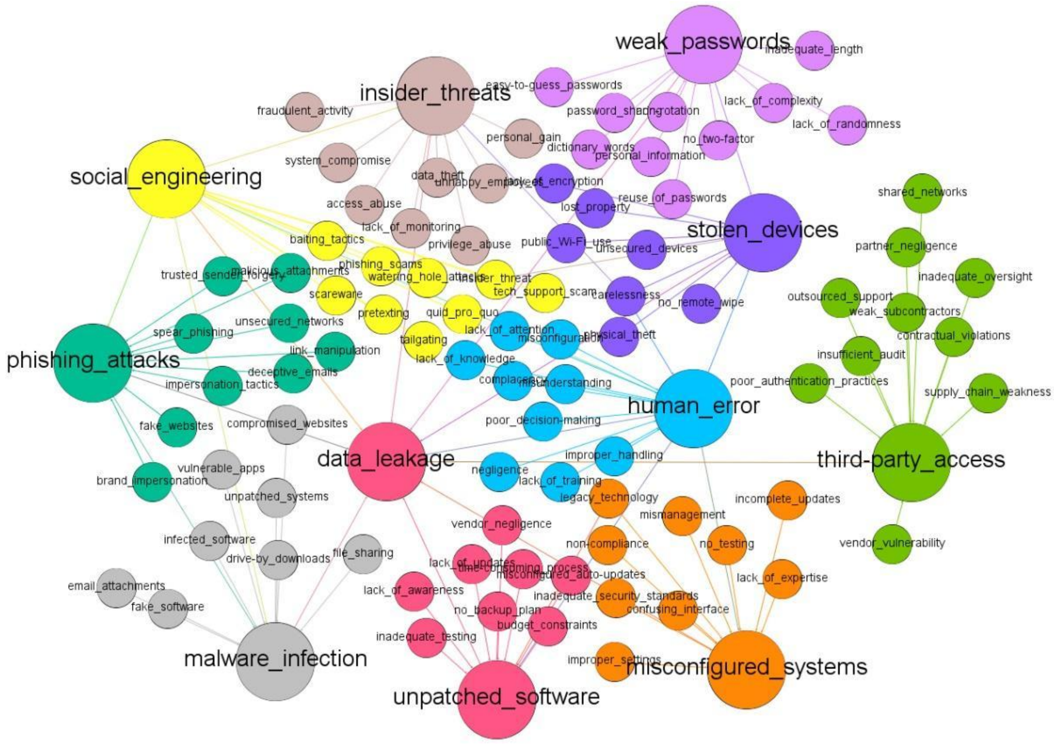

Figure 1. The Directed primary causal network obtained by simple hierarchical access to ChatGPT

The main parameters of the nodes in this network are provided in Appendix 2, item 1. The most influential nodes in this network (highest Out-Degree) are: human_error (5), social_engineering (4), weak_passwords(3), and phishing_attacks(2). It is evident that the formed network is weakly connected, incomplete, and the concepts represented in it may not accurately reflect causes and consequences. We will consider this as a network obtained from a survey of only one artificial expert.

Forming a Network Based on Hierarchical Invocation of Swarm Virtual Experts to ChatGPT

The ChatGPT system can provide different answer options at different times during text processing, with some being more accurate and logically sound from a human perspective. Each such answer can be perceived as an answer from some virtual expert [3]. It can be assumed that by generalizing answers from multiple (swarm) similar experts, we can obtain a more complete and accurate response. By implementing swarm virtual experts, we ask the same prompts several times related to both first- and second-level hierarchies. After receiving responses from the system, we combine them into a single CSV file for analysis and visualization using Gephi software. Loading the obtained data into Gephi results in the graph shown in Figure 2. In practice, the network can be expanded until it becomes sufficiently complete according to human expert evaluation.

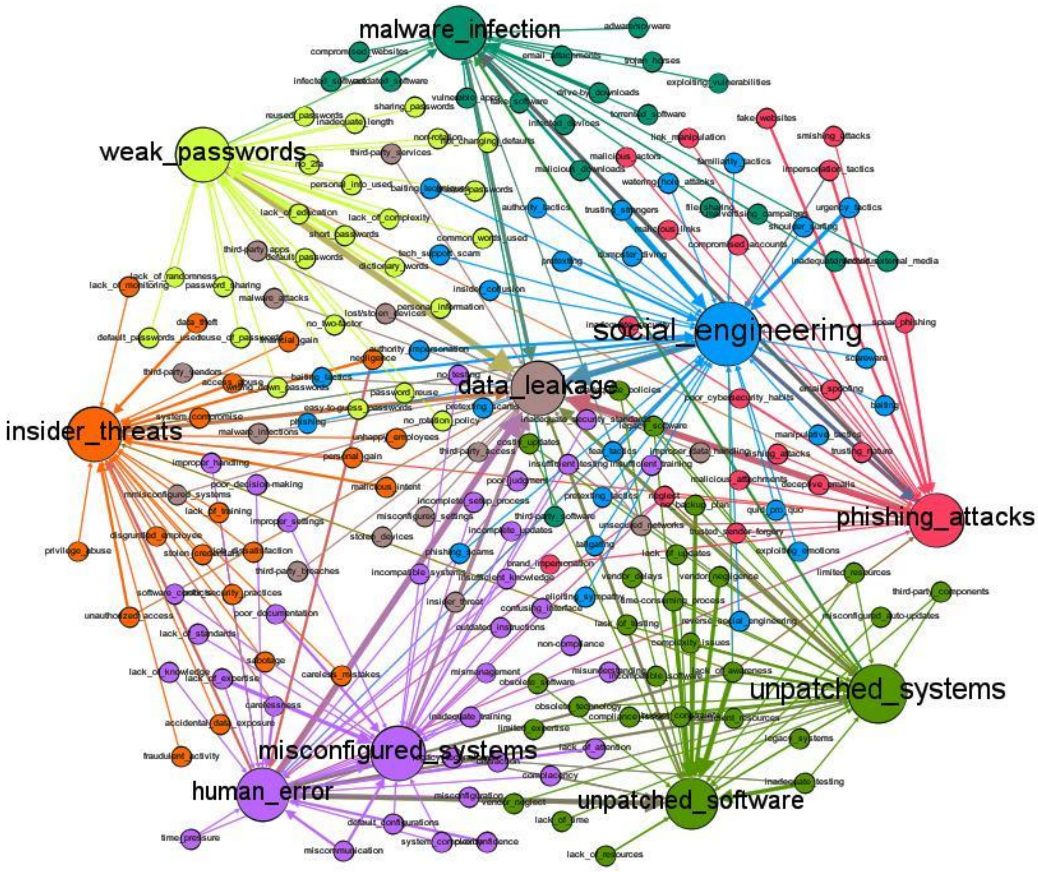

Figure 2. Directed full causal network obtained by hierarchically querying a swarm of virtual experts to ChatGPT

The main parameters of the nodes in this network are given in Appendix 2, item 2. The most influential nodes in this network (with the highest Out-Degree) are: human_error (7), social_engineering (4), weak_passwords(3), phishing_attacks(2), unpatched_systems(2), insider_threats(2).
As we can see, the number of important concepts has increased compared to the previous case.

Formation of a network based on a generalization of hierarchical querying a swarm of virtual experts to ChatGPT

The graph formed in the previous example, having relatively high completeness of concepts, may contain inaccurate information mistakenly provided by ChatGPT when processing individual prompts. Assuming that the probability of encountering similar errors is relatively small, it is possible to exclude from consideration concepts that occur less frequently than a given threshold when constructing a network. In the case presented below (Fig. 3), concepts that occurred less than twice were not considered.

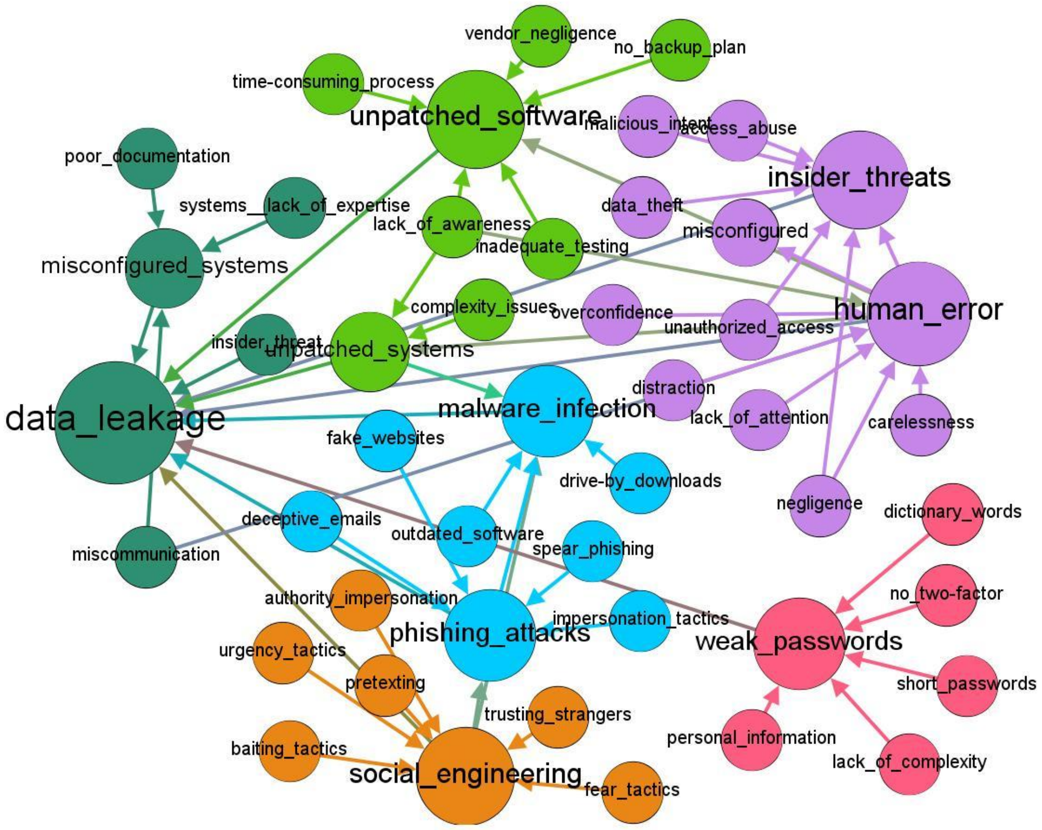

Figure 3. Directed causal network obtained by generalizing the hierarchical querying of a swarm of virtual experts to ChatGPT.

The main parameters of the network nodes are given in Appendix 2, section 3. The most influential nodes in this network (with the highest Out-Degree) are: human_error (5), social_engineering (3), phishing_attacks(2), unpatched_systems(2).

Conclusions:

Based on expert assessments, it can be concluded that the primary causal network obtained by simple hierarchical querying to ChatGPT covers the largest number of concepts that are relatively weakly connected (the network is close to hierarchical), but thanks to its completeness, it can be good "raw material for subsequent analytical processing."

The statistically processed second network, a causal network obtained by hierarchically querying a swarm of virtual experts to ChatGPT, is more accurate than the primary network and finally, the third network obtained by generalizing hierarchical querying from a swarm of virtual experts to ChatGPT has the highest average clustering coefficient indicating greater interaction between individual concepts influencing goals in this causality chain. This type of network is likely most suitable for further scenario analysis.

In this study we have demonstrated:

- The convenience of using ChatGPT for forming causal networks within specific subject areas such as cybersecurity is based on using ChatGPT & Gephi.
- We used a swarm-of-virtual-experts method through multiple prompt executions with ChatGPT.
- Our approach was applied specifically to cybersecurity but could be applied across various subject areas such as military, political or economic.

Limitations:

Despite significant gains in resources (both time and human capital), it's important to note that both constructing these causal networks and interpreting results require data scientists experienced in their respective fields and still require human observation for accuracy and precision purposes.

Bibliography

[1] St. Wolfram. "What Is ChatGPT Doing ... and Why Does it Work?". – Wolfram Media, Inc. March 9, 2023. 112 p.

[2] Brady D. Lund, Ting Wang, Nishith Reddy Mannuru, Bing Nie, Somipam Shimray, Ziang Wang. ChatGPT and a new academic reality: Artificial Intelligence-written research papers and the ethics of the large language models in scholarly publishing. JASIST, 2023. / Volume74, Issue5. Pages 570-581. DOI: https://doi.org/10.1002/asi.24750

[3] Tamilla Triantoro. Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT (March 30, 2023). ODSC Community.

[4] Lande, Dmitry and Strashnoy, Leonard, Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN. Available at http://dx.doi.org/10.2139/ssrn.4420452

[5] Ken Cherven. “Mastering Gephi Network Visualization”. – Packt Publishing, 2015. 378 p.

[6] Gunning D. Explainable Artificial Intelligence (Xai). Darpa-Baa-16-53. nd Web 2 (2), 1 (2017).

[7] Solat J. Sheikh, Sajjad Haider, Alexander H. Levis, On semi-automated extraction of causal networks from raw text, Engineering Applications of Artificial Intelligence, Volume 123, Part A, 2023, 106189, https://doi.org/10.1016/j.engappai.2023.106189.

Appendix 1. Prompts and Answers

Prompt 1. Data breach

□List the causes of data leakage in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause;data leakage". Each such entry - from a new line

human error; data leakage
weak passwords; data leakage
insider threats; data leakage
misconfigured systems; data leakage
phishing attacks; data leakage
unpatched software; data leakage
malware infection; data leakage
social engineering; data leakage
third-party access; data leakage
stolen devices; data leakage

Prompt 1.1. Human error

□List the causes of human error in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; human error ". Each such entry - from a new line

Poor decision-making;human error
Lack of attention;human error
Negligence;human error
Lack of knowledge;human error
Misconfiguration;human error
Improper handling;human error
Complacency;human error
Carelessness;human error
Lack of training;human error
Misunderstanding;human error

Prompt 1.2. Weak passwords

□List the causes of weak passwords in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; weak passwords ". Each such entry - from a new line

Password sharing;weak passwords
Reuse of passwords;weak passwords
Easy-to-guess passwords;weak passwords
Lack of complexity;weak passwords
Inadequate length;weak passwords
Lack of randomness;weak passwords
No two-factor;weak passwords
Non-rotation;weak passwords
Dictionary words;weak passwords
Personal information;weak passwords

Prompt 1.3. Insider threats

□List the causes of insider threats in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; insider threats ". Each such entry - from a new line

Unhappy employees;insider threats
Access abuse;insider threats

Data theft;insider threats
Fraudulent activity;insider threats
Carelessness;insider threats
Social engineering;insider threats
System compromise;insider threats
Lack of monitoring;insider threats
Privilege abuse;insider threats
Personal gain;insider threats

Prompt 1.4. Misconfigured systems

List the causes of misconfigured systems in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause;misconfigured systems ". Each such entry - from a new line

Human error;misconfigured systems
Lack of expertise;misconfigured systems
Incomplete updates;misconfigured systems
Improper settings;misconfigured systems
No testing;misconfigured systems
Inadequate security standards;misconfigured systems
Confusing interface;misconfigured systems
Legacy technology;misconfigured systems
Non-compliance;misconfigured systems
Mismanagement;misconfigured systems

Prompt 1.5. Phishing attacks

List the causes of phishing attacks in cyber security. The reason is to use no more than three words. The results should be presented in the format " cause;phishing attacks ". Each such entry - from a new line

Deceptive emails;phishing attacks
Impersonation tactics;phishing attacks
Link manipulation;phishing attacks
Malicious attachments;phishing attacks
Spear phishing;phishing attacks
Fake websites;phishing attacks
Social engineering;phishing attacks
Trusted sender forgery;phishing attacks
Brand impersonation;phishing attacks
Unsecured networks;phishing attacks

Prompt 1.6. Unpatched software

List the causes of unpatched software in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause;unpatched software ". Each such entry - from a new line

Lack of updates;unpatched software
Vendor negligence;unpatched software
Time-consuming process;unpatched software
Legacy technology;unpatched software
Misconfigured auto-updates;unpatched software
Inadequate testing;unpatched software
Human error;unpatched software
Lack of awareness;unpatched software
Budget constraints;unpatched software
No backup plan;unpatched software

Prompt 1.7. Malware infection

List the causes of malware infection in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; malware infection". Each such entry - from a new line

Drive-by downloads;malware infection
Phishing attacks;malware infection
Email attachments;malware infection
File sharing;malware infection
Unpatched systems;malware infection
Infected software;malware infection
Vulnerable apps;malware infection
Social engineering;malware infection
Compromised websites;malware infection
Fake software;malware infection

Prompt 1.8. Social engineering

List the causes of social engineering in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; social engineering ". Each such entry - from a new line

Pretexting;social engineering
Phishing scams;social engineering
Baiting tactics;social engineering
Quid pro quo;social engineering
Tailgating;social engineering
Tech support scam;social engineering
Watering hole attacks;social engineering
Scareware;social engineering
Human error;social engineering
Insider threat;social engineering

Prompt 1.9. Third-party access

List the causes of third-party access in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause; third-party access ". Each such entry - from a new line

Vendor vulnerability;third-party access
Inadequate oversight;third-party access
Weak subcontractors;third-party access
Shared networks;third-party access
Outsourced support;third-party access
Partner negligence;third-party access
Poor authentication practices;third-party access
Contractual violations;third-party access
Supply chain weakness;third-party access
Insufficient audit;third-party access

Prompt 1.10. Stolen devices

List the causes of stolen devices in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause;stolen devices". Each such entry - from a new line

Unsecured devices;stolen devices
Lack of encryption;stolen devices
Carelessness;stolen devices
Physical theft;stolen devices
Weak passwords;stolen devices
Lost property;stolen devices
Insider threat;stolen devices
No remote wipe;stolen devices
Public Wi-Fi use;stolen devices
Human error;stolen devices

Appendix 2. Parameters of the most important nodes in networks

1. Parameters of the most important nodes in network 1 (primary causal network)

Concept	In-Degree	Out-Degree	Clustering Coefficient	Betweenness Centrality
human_error	10	5	0,02381	77,33333
social_engineering	10	4	0,027473	67,5
phishing_attacks	10	2	0,022727	18
weak_passwords	10	2	0,007576	20
misconfigured_systems	10	1	0,009091	8,5
stolen_devices	10	1	0,027273	6,833333
unpatched_software	10	1	0,009091	8,5
insider_threats	10	1	0,009091	8,333333
malware_infection	10	1	0,027273	8
third-party_access	10	1	0	10

2. Parameters of the most important nodes in network 2 (full causal network)

Concept	In-Degree	Out-Degree	Clustering Coefficient	Betweenness Centrality
social_engineering	31	4	0,011765	118,1667
data_leakage	24	0	0,032609	0
phishing_attacks	24	2	0,027692	58,91667
insider_threats	24	2	0,021538	55,16667
malware_infection	23	1	0,014493	18
human_error	23	7	0,032184	152,25
unpatched_software	22	1	0,005929	11,16667
unpatched_systems	27	2	0,006158	47,41667
misconfigured_systems	24	1	0,011667	17,91667
weak_passwords	24	3	0,004274	72

3. Parameters of the most important nodes in network 3 (generalized causal network)

Concept	In-Degree	Out-Degree	Clustering Coefficient	Betweenness Centrality
data_leakage	10	0	0,077778	0

human_error	7	5	0,045455	36,33333
social_engineering	6	3	0,041667	18
insider_threats	6	1	0,047619	4,5
unpatched_software	6	1	0,047619	4,333333
phishing_attacks	5	2	0,071429	8
malware_infection	5	1	0,133333	2
weak_passwords	5	1	0	5
unpatched_systems	3	2	0,15	10,33333
misconfigured_systems	3	1	0	2,5
misconfigured	1	0	0	0