

Ethical Auditors' Framework for Generative AI Cybersecurity

Running Head: Ethical Generative AI

Waymond Rodgers

University of Texas, El Paso, USA/ Hull University Business School, United Kingdom

Email: w.rodgers@hull.ac.uk

James M. Murray

Cardiff University (from Sep. 2023), United Kingdom

Email: MurrayJ11@cardiff.ac.uk

Leonard Strashnoy

Tata Consulting Services, USA

Email: leonard.strashnoy@tcs.com

Dmitry Lande

National Technical University of Ukraine

Igor Sikorsky Kyiv Polytechnic Institute

Email: dwlände@gmail.com

Conflict of Interest Statement: There is no conflict of interest for this paper.

Ethical Auditors' Framework for Generative AI Cybersecurity

Abstract

Ethical dilemmas and compromises are introduced when identifying, mitigating, and addressing solutions to cybersecurity vulnerabilities. The accelerated use of generative AI platforms presents opportunities for cybersecurity professional auditors to analyze possible approaches in identifying the drivers and possible solutions in addressing vulnerabilities such as fraud. In this paper we seek to introduce a structured approach to addressing ethics for auditors' cybersecurity decision-making, rooted in scenario-planning to support agility in cybersecurity. Building on Causal Network research using ChatGPT, we introduce an ethical framework for generative AI cybersecurity using algorithmic ethical pathways.

Keywords

Cybersecurity, Ethics, Causal Networks, ChatGPT, Generative AI, Throughput Model, Agility

Introduction

The convergence of human and generative artificial intelligence (AI) decision-making in a rapidly changing technological environment impacts connectivity and the agility of auditors making decisions. Auditors consequently need to develop skills to embrace the opportunity of supporting their work by using generative AI platforms.

In this paper we highlight the use of algorithmic ethical pathways when using generative AI in addressing cybersecurity vulnerabilities, and we propose their key role in supporting auditors' agility-focused cybersecurity threat mitigation strategies.

The nature of addressing cybersecurity vulnerabilities generates difficult choices and ethical dilemmas, complicating the delegation of decision-making via algorithms (Formosa et al., 2021). We propose a more structured approach to representing algorithms by offering a clear comprehension of the specific cybersecurity vulnerability drivers to incorporate into the application and use of generative AI support systems.

Whilst incorporating the 'black box' of generative AI to support auditors' decision-making is attractive as a speedy solution to organizations attempting to embrace technology to support their objectives, the inherently opaque nature of algorithms challenges perceptions of understanding of the process, and authenticity of information extracted for incorporation in auditors' decision-making (Rodgers & Nguyen, 2022).

Cybersecurity weaknesses are often rooted in decision-making based on users' ethical positions, (Sadeghi et al., 2023). Exploring causality network formation with ChatGPT (Lande & Strashnoy, 2023a, b), we propose a framework to open the 'black box,' providing pathways to decision choice and accountability, using generative AI scenario-planning process-apparatus for auditors to explore their strategy, structure, and accountability in addressing cybersecurity vulnerabilities (Rodgers, 2020; 2022).

Understanding ethical positions can support auditors, in terms of improved security, convenience, accountability, and fraud detection. Cultivating ethical judgment by cybersecurity professionals (Formosa et al., 2021) may also be generated by the application of ethical frameworks in system development.

Therefore, this paper provides the Throughput Model (TPM), which consists of a comprehensive conceptual framework for analysing the interconnected processes impacting the decision choices that influence auditors' identification and reaction to cybersecurity threats (Rodgers, Söderbom, & Guiral, 2015). The model's distinction is its ability to draw out and illuminate critical decision-making pathways, operating in parallel process rather than a serial process. The model integrates the constructs of perception (framing of situational context), information, judgment (evaluation of information/ situational context) and decision choice, supporting an auditor's agility in addressing vulnerabilities (see Figure 1).

Figure 1

Generative AI

AI is a machine's ability to perform the cognitive functions we usually associate with human minds (Rodgers, 2020; 2022). AI has potential for auditors to collect, analyse and act on data from multiple sources in real-time, on a vast scale, with increased speed and accuracy.

Machine Learning (ML) systems 'infer' instructions based on algorithms 'trained' on data to perform tasks (even when no instructions exist) from examples. The hierarchy of data features is established by a human. Deep Learning systems are a subset of ML that acts like the brain's neural networks, ingesting and processing unstructured data (e.g., photos and text), adjusting in a loop for accuracy. Analytical or 'traditional AI', analyses data, finds patterns, makes predictions and decisions.

Generative AI – is a class of ML that in response to a prompt generates (creates) something 'new', rather than just analysing existing information. We are experiencing accelerated use of generative AI on platforms such as ChatGPT, Stable Diffusion, GitHub Copilot etc.

Generative AI is a subset of digital technologies which will significantly influence global

competitiveness and productivity in forthcoming years, granting significant societal, economic, and strategic advantages to early adopters (Government of Ireland, 2021).

AI has potential for auditors to collect, analyse and act on data from multiple sources in real-time, on a vast scale, with increased speed and accuracy. AI can perform predictive (forecasting) analytics and offer prescriptive recommendations for auditors with increased speed and accuracy. Cybersecurity professional auditors can use generative AI to support in the Identification of vulnerability patterns and insights, with descriptive analytics to communicate findings, and prescriptive analytics to offer possible solutions. Understanding the application of “descriptive,” “predictive,” and “prescriptive” analytic techniques with generative AI will give auditors a competitive edge.

The creation of text and content to support auditors is one of the fundamental benefits that auditing firms can employ utilising the functions of generative AI platforms such as ChatGPT. Though several organizations use knowledge management platforms and solutions in enhancing explicit and tacit knowledge within their organizational levels, there is limited understanding of how generative AI-enabled currently assists in organizational learning (Baidoo-Anu & Owusu Ansah, 2023). This suggests that research in the use of ChatGPT in identifying cybersecurity vulnerabilities will support cybersecurity professional auditors’ agility in assisting organizational learning with regards to cyber risk.

The uncertainty resulting from the accelerated widespread use of advanced AI technology, impacts the identification, mitigation, and proposed solutions to cybersecurity vulnerabilities. Taking the perspective of embracing uncertainty as an opportunity, is a mindset that supports the critical analysis of accounting and administrative systems, (Girod & Kralik, (2021).

Embracing this perspective, understanding an organization’s philosophical stance and decision-making approach, within a framework allowing post-decision outcome analysis,

supports both decision-making agility and the potential opportunities resulting from the growing utilization of generative AI technology.

The ethical drivers of cybersecurity vulnerability.

The drivers of cybersecurity vulnerability are rooted in the ethical positions of both organizations and auditors. Decision choices in the design, implementation, operation, and effectiveness of control systems determine the security of systems.

Though many cybersecurity vulnerabilities may be a consequence of accidental actions (e.g., programming error, or data privacy leak), malicious actions (such as ransomware attacks, hacking incidents, or data theft) to facilitate fraud are a consequence of actors' ethical positions dependent on circumstance.

Cybersecurity vulnerability exposes an organization to an economic or strategic loss, driven by competitors or adversaries to realize a gain (Rodgers, Söderbom, Guiral, 2015). The Bank for International Settlements has identified that whilst data breach vulnerabilities result in the highest cost to organizations, fraud results in the second highest cyber costs (Aldosoro et al., 2020). Fraud can occur because of internal controls working inappropriately (COSO, 1999). Fraud refers to a deliberate dishonesty that causes its injured party an economic loss and/or results in personal gain for the perpetrator (or their organizational network). Cybersecurity professionals understanding of the impact of system users' ethical choices is an area of cybersecurity vulnerability that has received minimal attention (Sadeghi et al., 2023). As the assessment of decisions may only manifest after the impact of vulnerabilities are identified, cybersecurity professional auditors need to understand the drivers of alternate ethical positions that are driven by situational events.

For fraud to transpire, there are typically three prerequisites: pressure, opportunity, and rationalization (Coleman & Cressey, 1980; AICPA, 2003; PCAOB, 2023) (see Figure 1).

Pressure arises from situational circumstances such as financial need, personal desires, or fear of failure. Opportunity involves access to a situation where a fraud can be carried out, including organizational internal control weaknesses, operational conditions, management practices, and corporate culture. Rationalization encompasses personal characteristics that include a predisposition to engage in fraudulent activities (Rodgers et al., 2015).

When both the opportunity and pressure to exploit cybersecurity vulnerabilities exist, rationalisation seamlessly connects the vertex completing the fraud triangle, see Figure 2, (Coleman & Cressey, 1980).

Figure 2

Formosa et al. (2021) recognise the principlist approach explored in cybersecurity ethics research has limitations such as application of principles to specific cases, and conflicts and tensions between ethical principles. They consequently proposed an ethical framework building on the four basic ethical principles of autonomy, nonmaleficence, beneficence and justice (Beauchamp & Childress, 2001) with a fifth principle of ‘explicitability’ explaining use of cybersecurity technology should be intelligible, transparent, comprehensible, and accountable. Their focus is on identifying conflicts between principles, and do not incorporate the construct of ‘judgment’ for conflict resolution, (Formosa et al., 2021). This paper extends cybersecurity vulnerability research by incorporating the ‘judgment’ construct within a cognitive analysis framework of decision choice pathways generated by ‘perception’ and ‘information’ constructs.

In the TPM, decision-making is defined as a multi-stage, information-processing activity in which cognitive processes are employed to produce a set of outcomes (Kohlberg, 1969; Rest, Narvaez, Bebeau, & Thoma, 1999; Rodgers, 2009, Rodgers et al., 2015).

The TPM's fundamental insight is that understanding *information* is inherently situated within a situational context that encompasses cognitive, behavioural, individual, and social aspects (Reynolds, 2006, 2008; Reynolds and Ceranic, 2007).

This insight is depicted as "*perception*" in Figure 1. *Perception* entails individuals framing their problem-solving perspective or worldview (Sitkin and Weingart, 1995). Rodgers (1997, 2006) built on this position, arguing that perception includes how a person's expertise, classifying and categorization of information is represented. The "*Information*" stage (Figure 1) encompasses the digital data, analogue data, intelligence research and other information available to a decision-maker for the purpose of problem solving. The "*judgment*" stage incorporates the process where knowledge and information are weighed, sorted, and classified (including influences rooted in perception) to facilitate problem-solving and decision-making. The final stage is "*decision-choice*", where an action is executed or deferred, (as depicted in Figure 1).

The interdependency relationship of perception and information ($P \leftrightarrow I$) is like Bayesian statistics (Bolstad & Curran, 2016), in that the 'information' element is continuously altering a decision maker's perception. That is, prior information is continually encapsulated within the 'information' element, a process comparable to that of neural network software (Rodgers, 2020) that simulates humans' biological neurons (Barnett & Cerf, 2017). There is a continuous revision of information (data) in the process. Neural networks support machine learning in that they can match similarities in the ($P \leftrightarrow I$) relationship, mimicking pattern recognition as they learn to decipher a problem (Rodgers, 2020). This learning characteristic of the TPM can offer a machine learning methodology (supervisory or non-supervisory) to support agility in organizations to learn and get better from experience.

In individual decision-making, the information part is subjectively processed through the five senses: vision, hearing, touch, taste, and touch. Through education, training, and experience

(i.e., perception), we discern the information set and arrive at a position pertaining to the relevance and reliability of information as it relates to our comprehension of the data. Perception is continually revised by updated external information, a process like Bayes' Theorem, which is at the heart of AI neural networks utilised in deep learning tools (Cui, Wong, & Lui, 2006). The ($P \leftarrow \rightarrow I$) neural network also exemplifies that 'perception' influences 'information', and that from a cognitive perspective information is warehoused in memory (i.e., judgment) for additional processing and encoding for decision-making purposes.

An ethical behavioral control system that is suitably implemented, can provide enhanced security, more convenience, heightened accountability, and support fraud detection, (Rodgers et al., 2011). Based on Figure 1, we identify six different ethical positions that support cybersecurity vulnerability causal network analysis. The six dominant ethical positions are discussed in terms of how cybersecurity control systems may use these in addressing vulnerabilities, and to encourage assessment by cybersecurity professionals of alternative decision pathways that might be better suited to individuals to modify their behavior to meet organizational objectives. These are: ethical egoism, deontology, utilitarianism, relativist, virtue ethics, and ethics of care positions (Rodgers and Gago, 2001; Rodgers, 2009; Rodgers & Nguyen, 2022; Rodgers, Murray, Stefanidis, Degbey, Tarba, 2023).

Based on Figure 1, the six ethical algorithmic pathways are:

- (1) $P \rightarrow D$ ethical egoism
- (2) $P \rightarrow J \rightarrow D$ deontology
- (3) $I \rightarrow J \rightarrow D$ utilitarianism
- (4) $I \rightarrow P \rightarrow D$ relativist
- (5) $P \rightarrow I \rightarrow J \rightarrow D$ virtue ethics

(6) $I \rightarrow P \rightarrow J \rightarrow D$ ethics of care

The six ethical algorithmic pathway positions are discussed below in more detail (Rodgers & Gago, 2001; Rodgers, 2009):

- (1) $P \rightarrow D$ embodies an *ethical egoism* position, emphasising that individuals are driven to act in accordance with their perceived self-interest. This standpoint is supported by ‘utility theory’ (Von-Neumann & Morgenstern, 1947), and is characterised by an approach that gives less emphasis to non-supporting information and analysis. A situation is perceived, and a decision is made by diminishing the significance of prior information or judgments.
- (2) $P \rightarrow J \rightarrow D$ embodies the *deontology* position, placing emphasis on an individual’s rights, and judgment linked to a specific process rather than choice. An example is that of Kant (1996), taking the position that moral actions stem from a “supreme principle of morality”, namely the categorical imperative, which is objective, rational, and voluntarily embraced. Deontology extends a property rights perspective, supporting a right of contract enjoyed by all, with a conditioning construct (judgment) rooted in rules and laws before a decision is rendered. Difficulties may arise where perception is conditioned by judgment where rules are unclear, or decision-making perception is immature (Rodgers et al., 2015).
- (3) $I \rightarrow J \rightarrow D$ embodies the *utilitarian* position, concerned with focusing on outcomes and striving for the greatest benefit for the most individuals. It is an extension of ethical egoism in terms of expanding the impact of good whilst minimising harm to society. This position is rooted in the work of Adam Smith (1776) and extended by Friedman (1970) whereby organizations may strive for their economic objectives if they refrain from engaging in deceit or fraudulent activities. Judgment is initially generated by information, and the decision-choice is then conditioned by the information data.

- (4) $I \rightarrow P \rightarrow D$ embodies the *relativist* position, where the decision-makers ethical standards are contingent on reflecting the standards of their own culture or situation, with other specific social environments reflecting their own specific moral standards., i.e., universal moral standards cannot be universally applied in all circumstances. Holders of this position take the view that the only ethical criteria that an organization's actions can be evaluated are those established within the organization itself (Velasquez, 2006).
- (5) $P \rightarrow I \rightarrow J \rightarrow D$ embodies the *virtue ethics* position, where the cultivation in one's character of virtuous traits is considered morality's primary function (Rodgers et al., 2015). Rooted in the Hellenistic tradition represented by Plato and Aristotle, the concept of an individual citizen implies the capacity to understand, to be aware of rights and responsibilities, and be able to act in appropriately in accordance with these duties (Marshall, 1964). In the virtue ethics position, a conscious look for information is generated by one's perception, and this information conditions judgment and decision choice.
- (6) $I \rightarrow P \rightarrow J \rightarrow D$ embodies the *ethics of care* position, which reflects a willingness to attentively consider diverse and unacknowledged viewpoints. This position is focused on responding to needs rooted in cultivating empathetic understanding. It emphasises the interpersonal connections among people over the preferences or inclinations of individual entities or organizations. This position viewpoint is that all stakeholders have property rights (the organization's suppliers, customers, employees, and the wider community). This position has been extended, with the suggestion that organizations should measure the incorporation of obligations to various constituencies and the cost in fulfilling these commitments (Cornell & Shapiro, 1987).

Table 1 illustrates the six ethical pathways (ethical egoism, deontology, utilitarianism, relativist, virtue ethics, and ethics of care), viewed in the context of decision making governed by the influences represented in the fraud triangle (Rodgers et al., 2015).

Table 1

Typical drivers of pressure are generated by the social and economic environment of the individual or organization, and typical opportunity drivers are generated by the social environment and physical cybersecurity environment. When any of these environments are subject to change, such as the widespread adoption and use of generative AI, cybersecurity vulnerabilities may manifest for exploitation by malicious actors. To mitigate the impact of these vulnerabilities, development of organizational control systems is discussed in subsections of this paper.

Generative AI Cybersecurity vulnerability identification

The accelerated use of generative AI requires organizations to fully engage with the technology to understand its impact on their organization. Ethical issues arise in particular with cybersecurity research are relevant to cybersecurity professionals concerned with identification of vulnerabilities, and includes (1) accidental discovery (of unanticipated activities), (2) accidental disclosure of private data, (3) damage to networks/ servers, (4) misuse/ dual use by malicious actors, (5) knowledge dissemination of vulnerabilities, (6) reprisal actions against those discovering vulnerabilities, (7) opaque aspect of consent (8) reputational damage to organization arising from identifying vulnerabilities (9) malicious researcher behaviour, (Reidsma et al., 2023). Using ChatGPT to simulate acting in a neutral research position, allows for the subsequent introduction of ethical positions to determine alternate outcomes to a research question.

Collecting data from various sources for decision-making, with an understanding of how to frame a problem to reduce decision-bias, serves as the foundation for developing text prompts in data collection using generative AI. Lande and Strashnoy (2023b) utilised methods using the ChatGPT generative AI system, trained on a linguistic network, to extract examples of cybersecurity vulnerabilities and create a cyber security vulnerability causality network. This paper builds on a generative AI approach, with the subsequent integration of an ethics-focused decision pathway model to support using generative AI in identification, mitigation, and accountability in addressing cybersecurity vulnerabilities.

The first approach adopted (Lande & Strashnoy, 2023b) involved scenario planning, in simulating the activity of multiple experts addressing the same problem i.e., identifying the reasons for the concept of ‘cybersecurity vulnerability’. Using a simple prompt, 10 reasons for the term ‘cyber security vulnerabilities’ were generated by the ChatGPT system. They repeatedly executed the same prompt to the system, generating a set of reasons for a simulated team of ‘virtual experts’, (see upper part of Figure 3). This approach created a network list of cybersecurity vulnerability descriptors, or nodes, illustrated as a hierarchical frequency network list of 77 nodes.

The second approach adopted (Lande & Strashnoy, 2023a) involved decomposition of the given problem (concept) instead of virtual expert simulation. In this approach ChatGPT was firstly asked to decompose the problem concept into 10 partial concepts, followed by a similar prompt to determine 10 reasons for the main causes of each partial concept (see lower part of Figure 3). The two phases of this approach were combined, creating a network list of cybersecurity vulnerability descriptors (nodes), illustrated as a hierarchical frequency network list of 102 nodes.

Figure 3

The results of both approaches were then combined, creating a network list of cybersecurity vulnerability descriptor (nodes), illustrated as a hierarchical frequency network list of 162 nodes, with '*insider threats*' as the most frequent descriptor node, closely followed by '*weak passwords*' and '*social engineering*'. A characteristic of AI systems is their ability to rapidly illustrate knowledge visually to communicate issues addressed, and visual communicate complex information to broader audiences. Lande and Strashnoy (2023b) utilized AT&T's GaphViz graph visualization library to create graphs in SVG format to communicate the cybersecurity vulnerability causal networks generated in their approaches using ChatGPT (see Figure 4).

Figure 4

The integration of an ethics-focused decision pathway model such as the TPM with a causal approach (Lande & Strashnoy, 2023b), will support organizations using generative AI in the identification of the drivers of cybersecurity vulnerabilities, the mitigation of their impact, and in accountability when analysing decision choice outcomes.

Cybersecurity vulnerability threat mitigation

Organizations invest in cybersecurity to manage cyber risk (vulnerabilities) to mitigate cyber incident costs. Whilst most malicious actions are associated with lower costs, as they are identified and stopped before harm, successful malicious attacks are associated with extensive damage and higher costs (Aldosoro et al., 2020). As the accelerated use of generative AI technology is adopted in the wider community, potentially supporting malicious actions, agile organizations will need to develop skills to embrace the opportunity

of supporting their work by using generative AI platforms. Understanding ethical positions using generative AI can enhance organizational agility and behaviour, by assisting in identifying and addressing conflicts of interest, illegal or other improper actions, and develop data for cyber risk cost analysis.

Agility is characterised as the freedom and capability of accelerated decision-making (Prange & Hennig, 2019). Decisions are increasingly made within organizations by algorithms and data driven predictive analytics (Duggan et al., 2020), including the use of generative AI, where once these were conventionally made by just management and employees. The accelerated use of generative AI suggests auditors incorporate agility practices in their behavior at every decision level to anticipate and mitigate cybersecurity threats by malicious actors exploiting this technology to identify vulnerabilities. Scenario planning is a key component in anticipating cybersecurity circumstances and vulnerabilities, as perception, detecting shifts in environmental changes, and strategic foresight using scenario-planning are highlighted in agility-oriented literature as essential constituents of agility. Scenario-planning is proposed as an agility technique, with its emphasis on increasing flexibility in decision making flexibility and response speed, (Chermack et al., 2019, Worley & Lawler III, 2010).

Agility literature also reflects the circumstantial drivers for using AI, and the characteristics of AI systems, with an emphasis on:

- (a) Environmental changes both external and internal to an organization as drivers for change.
- (b) Perception, scenario-planning and transparent information as drivers of choice.
- (c) Speed, versatility, resilience, and fluidity as drivers for decision-making. (Rodgers & Murray, 2023)

Whilst cybersecurity professionals need to understand the impact of system users' ethical choices, (Sadeghi et al., 2023), they also need to understand the drivers of alternate ethical

positions that are driven by circumstance. Analysis of outcomes based on agility-focused scenario planning can act as drivers to address cybersecurity vulnerabilities. Integrating a causal network approach using ChatGPT with the TPM, will support auditors to develop control system scenario-planning, reflecting alternate ethical positions' juxtaposition with alternate cyber risk circumstances.

An example approach is illustrated below in Figure 5. Method 1 is used to examine alternate ethical approaches to a cybersecurity vulnerability scenario focused on mitigating fraud via 'insider threat'. Each 'virtual expert' (VE) is generated by a ChatGPT prompt reflecting their ethical position and takes a different approach in addressing the indicators of insider threat to an organization's data system. The results can be analysed separately (Causal Networks 1-6) and in parallel (Causal Network A) to support examination of alternate decision outcomes.

Figure 5

In Method 2, decomposition of the concept of '*fraud insider threat indicators*' is adopted (see Figure 6), instead of virtual experts. In this approach ChatGPT is firstly asked to decompose the concept of '*insider threat fraud indicators*' into 10 partial concepts, followed by a similar prompt to decompose the problem concept into the fraud triangle partial concepts of '*pressure*', '*opportunity*', and '*rationalisation*'. The results can be analysed separately (Causal Networks 7-12) and in parallel (Causal Network B) to support examination of alternate decision outcomes.

Figure 6

The results of both approaches can then be combined into Causal Network C, creating an advanced network list of cybersecurity fraud vulnerability (nodes) and a hierarchical

frequency network list of nodes. This approach will support cyber risk analysis, and examination of ethical positions in the identification of cybersecurity vulnerabilities.

The integration of the TPM with a causal network approach (Lande & Strashnoy, 2023b), can be explored further with regards to scenario-planning. Incorporation of a '*Decision Dashboard*' (Rodgers et al., 2023) helps to analyse and explain how the drivers of environmental circumstance (changes in the economic, social, and physical environment), time pressure, and organizational decision level influences how cybersecurity professional auditors may prioritise one ethical pathway to a decision over another. Generative AI technology such as ChatGPT can support cybersecurity agility in the following areas: (1) Time pressure decisions (where the cost of unhurried decisions is high), (2) Accuracy in Decisions (where the cost of wrong decision choices is minimized), (3) Resource Analysis (for large data size analysis). (4) Prediction Accuracy (more important than explanation or clarification). (5) Provision of information where regulatory requirements are slight (Rodgers & Murray, 2023).

We aim to explore in future studies development of the prompt generator with specific cybersecurity environments for scenario planning, including the influences of time pressure and the organization decision level of cybersecurity professionals in parallel ethical decision-making pathways. The next section explores the application of the TPM along with the ethical positions in AI algorithmic pathways.

Cybersecurity: Embedding the Ethical Principals and Rules

In accordance with the diagram in **Figure 1: Throughput Model (TPM)**, prompts are generated for each node:

Prompt 1: How is I = information influenced from outside?

What entities can influence the receipt of information about the possibility of committing a cybercrime? Define the entities briefly – up to 10 words. Print the answer as a list of entries. each of which consists of an entity, followed by the sign “;”, after which the word “information” is written - in the format “entity; Information”.

For example,

"Network vulnerabilities; Information"

"Weaknesses of the system; Information"

Prompt 2: How is P = perception influenced from the outside?

What entities can influence the receipt of Perception about the possibility of committing a cybercrime? Define the entities briefly – up to 10 words. Print the answer as a list of entries. each of which consists of an entity, followed by the sign “;”, after which the word “Perception” is written - in the format “entity; Perception”.

For example,

"Network vulnerabilities; Perception"

Weaknesses of the system; Perception"

Prompt 3: Decomposition I = information

What entities can influence the receipt of information about the possibility of committing a cybercrime? Define the entities briefly – up to 10 words. Print the answer as a list of entries. each of which consists of an entity, followed by the sign “;”, after which the word “information” is written - in the format “entity; Information”.

For example,

"Network vulnerabilities; Information"

"Weaknesses of the system; Information"

Prompt 4: Decomposition P = perception

Decompose the concept of “Perception of cyberspace vulnerability” into separate partial entities from the point of view of a computer-addicted hacker programmer. Define partial entities briefly – up to 4 words. Output the answer as a list of entries in the format “Perceptible; partial entity”. “Perception”, semicolon, entity

For example,

"Perception; Sensory Risk Assessment" "Perception; System weaknesses"

Prompt 5: What can lead an addicted hacker to J = judgment about the possibility of cybercrime

What entities can lead an addicted hacker to make judgments about the possibility of committing a cybercrime? Define the entities briefly – up to 4 words. Print the answer as a list of entries. each of which consists of an entity, followed by the sign “;”, after which the word “Judgment” is written - in the format “entity; Judgment”. an entity, semicolon, “Judgment”.

For example,

"Network vulnerabilities; Judgment"

"System weaknesses; Judgment"

Prompt 6: Decomposition J= judgment

Decompose the concept of “judgments about the possibility of committing a cybercrime” from the point of view of a hacker into separate partial entities. Define partial entities briefly – up to 4 words. Output the answer as a list of entries in the format “Judgment; partial entity”. “Judgment ”, semicolon, entity.

For example,

"Judgment; Sensory Risk Assessment"

"Judgment; System Weaknesses"

Prompt 7: What entities can lead a hacker to D = decision

What entities can lead an addicted hacker to decide to commit a cybercrime? Define the entities briefly – up to 4 words. Print the answer as a list of entries. each of which consists of an entity, followed by the sign “;”, after which the word “Decision” is written - in the format “entity; Decision”. Entity, semicolon, “Decision”.

For example,

"Network vulnerabilities; Decision " "System weaknesses; Decision"

Each prompt was executed 10 times across virtual agents (VE), and the responses were combined. This ensured the implementation of the concept of a “swarm of virtual experts” (Lande & Strashnoy, 2023a, p. 111).

As a result, a network of entities was formed, presented as a CSV file, each line of which consisted of two entities separated by a semicolon. This network is sparse, with a total of 230 nodes and 306 links, and contains many leaves, nodes whose degree is only 1 (Figure 7).

Figure 7

After “trimming” the leaves, a support network remains, which is the basis for the formation of plot chains connecting two possible inputs to the diagram presented in Figure 1. This network contains a total of 29 connections and 57 connections (Figure 8).

Figure 8

The constructed network made it possible to construct plot chains connecting two possible inputs to the scheme - I= information and P= perception with the output D= decision choice.

For this purpose, two similar prompts were compiled:

Prompt 8:

For a network represented by pairs of nodes with directed connections, show all chains of nodes from the “Information” node to the “Decision” node. Rank chains of concepts based on the effectiveness of a cyber-attack. Here is the network:

"Perception; Software vulnerabilities"

"Perception; Potential attack vectors"

"Perception; System Vulnerabilities"

"Perception; Exploitable Weaknesses"

"Information; Exploitable Weaknesses"

"Information; Vulnerability Assessment"

...

Prompt 9:

For a network represented by pairs of nodes with directed connections, show all chains of nodes from the “Perception” node to the “Decision” node. Rank chains of concepts based on the effectiveness of a cyber-attack. Here is the network:

"Perception; Software vulnerabilities"
"Perception; Potential attack vectors"
"Perception; System Vulnerabilities"
"Perception; Exploitable Weaknesses"
"Information; Exploitable Weaknesses"
"Information; Vulnerability Assessment"
...

As a result of working out Prompts 8 and 9, answers were obtained that characterize the plots of transition from the states – I= information and P= perception to the state of decision making (D= decision).

ChatGPT: *To identify all chains of nodes from the "Information" node to the "Decision" node, let's first organize the information into a directed graph:*

P= perception □ D= decision choice

ChatGPT: *To find all chains of nodes from the "Perception" node to the "Decision" node, we can trace the connections in the given network. Therefore, we can list the chains and rank them based on their potential effectiveness for a cyber-attack:*

1. Perception → Software vulnerabilities → Judgment → Exploitable loopholes → Decision Choice.
 - This chain suggests that software vulnerabilities lead to the judgment of exploitable loopholes, which ultimately influences the decision-making process.
2. Perception → Potential attack vectors → Judgment → Exploitable loopholes → Decision Choice.

- Similar to the first chain, this one involves potential attack vectors leading to the identification of exploitable loopholes, affecting the decision choice.
3. Perception → Exploitable Weaknesses → Judgment → Exploitable loopholes → Decision Choice.
- This chain indicates that the perception of exploitable weaknesses leads to the judgment of exploitable loopholes, influencing the final decision.
4. Perception → System Vulnerabilities → Judgment → System vulnerabilities → Decision Choice.
- Here, the chain involves the perception of system vulnerabilities leading to the judgment of system vulnerabilities, which influences the final decision choice.
5. Perception → Cybersecurity gaps → Judgment → Exploitable loopholes → Decision Choice.
- This chain suggests that the perception of cybersecurity gaps leads to the judgment of exploitable loopholes, which in turn affects the decision-making process.
6. Perception → Exploitable software → Judgment → Exploitable loopholes → Decision Choice.
- This chain involves the perception of exploitable software leading to the judgment of exploitable loopholes, influencing the final decision choice.
7. Perception → Unpatched systems → Judgment → Exploitable loopholes → Decision Choice.
- This chain suggests that unpatched systems lead to the judgment of exploitable loopholes, ultimately influencing the decision choice.
8. Perception → Inadequate defenses → Judgment → Exploitable loopholes → Decision Choice.

- Here, the chain involves the perception of inadequate defenses leading to the judgment of exploitable loopholes, affecting the decision choice.

9. Perception → Weak access controls → Judgment → Exploitable loopholes → Decision Choice.

- This chain indicates that weak access controls in the perception phase led to the judgment of exploitable loopholes, influencing the final decision choice.

In sum, these chains are ranked based on the flow of concepts and their potential impact on the decision-making process in a cyber-attack scenario.

Conclusion

Cybersecurity accountability requires understanding of ethics, legal, and organizational controls. To deter cybersecurity vulnerabilities such as fraud, it is essential that an organization's management approach towards intervening or bypassing established controls should be endorsed and documented. An awareness of ethical positions should support auditors in accountability, with direction regarding typical circumstances and the frequency with which intervention is expected. Use of innovative technologies such as ChatGPT may offer auditors a sense of future-focused agility, however there is a tendency to incorrectly swap the terms 'capacity' (existing ability) with 'capability' (future higher ability) (Geiger et al., 2020). Accountability is key to cybersecurity performance measurement and feedback, including the ethical and legal aspects in the selection and analysis of data. Instances of management intervention (including remedial actions) should be documented and explained appropriately within the context of specific ethical positions. Where managerial overriding of system controls is explicitly prohibited, these should be communicated and documented.

Developing an understanding of ethical positions can contribute to improved conduct when managing situations involving conflicts of interest, illicit or inappropriate payments,

secondary employment, vendor gifts invitations, and other complex situations often involving parallel challenges. An accountability framework integrated with generative AI decision-making, will support auditors to identify, measure and track changes in cybersecurity vulnerability, enhancing agility in responding to cyber threats.

The scenarios utilised for constructing networks of causal relationships in cyber security vulnerability were fundamentally different. The first approach involving repeatedly executing the same prompt to the ChatGPT system, simulating the activity of multiple experts solving the same problem, suggests incorporation of the TPM will highlight how alternate ethical positions may result in identifying alternate cybersecurity vulnerabilities and outcomes for consideration. The second approach using primary decomposition contained significantly more nodes, with much less repetition, suggesting the combined approach with incorporation of the TPM may result in more accuracy in determining alternate ethical scenarios in cybersecurity strategic planning.

There are many typical cybersecurity circumstances where there are conflicts presented both between and within different ethical principles (Formosa et al., 2021). Development of scenario planning using ChatGPT within the TPM ethical framework to incorporate a broader range of cybersecurity vulnerabilities (including parallel vulnerabilities), will inform and support auditors in cybersecurity accountability, strategic planning, and cyber risk management.

REFERENCES

- AICPA. (2003). Statement of Auditing Standards No. 99: consideration of Fraud in a Financial Statement Audit New York AICPA Inc.
- Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020) The drivers of cyber risk. BIS Working Paper, issue 865 Bank for International Settlements, Switzerland.

- Baidoo-Anu, D., & Owusu Ansah, L. (2023). Education in the Era of Generative Artificial Intelligence (AI): Understanding the Potential Benefits of ChatGPT in Promoting Teaching and Learning. SSRN Electronic Journal. <https://doi.org/10.2139/SSRN.4337484>
- Barnett, S.B. & Cerf, M. (2017). A ticket for your thoughts: Method for predicting content recall and sales using neural similarity of moviegoers. *Journal of Consumer Research*, 44, 160-181.
- Beauchamp T.L. & Childress J.F. (2001) Principles of Biomedical Ethics. Oxford University Press.
- Bolstad, W.M. & Curran J.M. (2016). Introduction to Bayesian statistics, *John Wiley & Sons*.
- Chermack, T.J., Lindsey, K., Grant, C. & Barber, V.A. (2019). The Effects of Scenario Planning on Perceptions of Organisational Agility. *Journal of Futures Studies*, 24(1), pp.15-28.
- Coleman, J.W. & Cressey, D.R. (1980). *Social Problems*. New York: Prentice Hall.
- Cornell, B. & Shapiro, A. (1987). Corporate stakeholders and corporate finance. *Financial Management*, 16, 5-14.
- COSO - Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1999). *Fraudulent financial reporting: 1987-1997: An analysis of U.S. public companies*. New York: American Institute of Certified Public Accountants.
- Cui, G., Wong, M.L., & Lui, H-K. (2006). Machine Learning for Direct Marketing Response Models: Bayesian Networks with Evolutionary Programming. *Management Science* 52(4), 597-612.
- Duggan, J., Sherman, U., Carbery, R. & McDonnell, A. (2020). Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM. *Human Resource Management Journal*, 30(1), pp.114-132.
- Formosa, P., Wilson, M., Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, Volume 109, 102382.
- Friedman, M. (1970). The responsibility of business is to increase its profits. *New York Times Magazine*, September 13, 1970.
- Geiger, J., Elshaw, J. & Jacques, D., (2020). Establishing the Foundations to Measure Organisational Agility for Military Organisations. *Systems*, 8(4), p.44.
- Girod, S.J.G. & Kralik, M. (2021). *Resetting Management: Thrive with agility in the age of uncertainty*. Kogan Page USA
- Government of Ireland. (2021). *The National AI Strategy: AI - Here for Good*. Department of Enterprise, Trade and Employment. <https://www.gov.ie/en/publication/91f74-national-ai-strategy/>
- Kant, I. (1996). *Religion and Rational Theology*, edited by Allen Wood and George DiGiovanni. Cambridge: Cambridge University Press.

- Kohlberg, L. (1969). Stage and sequence. The cognitive developmental approach to socialization. In D. A. Goslin (Ed.), *Handbook of socialization theory* (pp. 347-480). Chicago: Rand McNally.
- Lande, D., & Strashnoy, L. (2023a). *GPT Semantic Networking: A Dream for the Semantic Web –The Time is Now*. Publisher: Kyiv Engineering Publishing Corp.
- Lande, D., & Strashnoy, L. (2023b). Causality Network Formation with ChatGPT. SSRN Electronic Journal. 10.2139/ssrn.4464477.
- Marshall, T.H. (1964). *Sociology at the cross roads*. NY: Doubleday.
- PCAOB. (2023). Public Company Accounting Oversight Board. AS 2401: Consideration of Fraud in a Financial Statement Audit. <https://pcaobus.org/oversight/standards/auditing-standards/details/AS2401>
- Prange, C. & Hennig, A. (2019). From strategic planning to strategic agility patterns. *Journal of Creating Value*, 5(2), pp.111-123.
- Reidsma, D., van der Ham, J. & Continella, A., (2023), February. Operationalizing cybersecurity research ethics review: from principles and guidelines to practice. In 2nd International Workshop on Ethics in Computer Security, *EthiCS 2023*. Internet Society.
- Rest, J., Narvaez, D., Bebeau, M. J., & Thoma, S. J. (1999). *Postconventional moral thinking: A neo-Kohlbergian Approach*. Mahwah, NJ: Lawrence Erlbaum.
- Reynolds, S. (2006). Moral awareness and ethical predispositions: Investigating the role of individual differences in the recognition of moral issues. *Journal of Applied Psychology*, 91, 233-243.
- Reynolds, S. (2008). Moral attentiveness: Who pays attention to the moral aspects of life? *Journal of Applied Psychology*, 93, 1027-1041.
- Reynolds, S., & Ceranic, T. (2007). The effects of moral judgment and moral identity on moral behavior: An empirical examination of the moral individual. *Journal of Applied Psychology*, 92, 1610-1624.
- Rodgers, W. (1997). *Throughput Modeling: Financial Information Used by Decision Makers*. Greenwich, Ct: Jai Press.
- Rodgers, W., (2006). *Process thinking: Six pathways to successful decision making*. iUniverse 2006.
- Rodgers, W. (2020). *Evaluation of Artificial Intelligence in a Throughput Model: Some Major Algorithms*. Florida: Science Publishers.
- Rodgers, W. (2022). *Dominant Algorithms to Evaluate Artificial Intelligence: From the view of Throughput Model*. UAE: Bentham Science.
- Rodgers, W. (2009). *Ethical beginnings: preferences, rules, and principles*. New York: iUniverse.
- Rodgers, W., & Gago, S., (2001). Cultural and ethical effects on managerial decisions: examined in a throughput model. *Journal of Business Ethics*, 31, 355-367.

Rodgers, W. & Nguyen, T. (2022). 'Advertising benefits from Ethical Artificial Intelligence Algorithmic Purchase Decision Pathways', *Journal of Business Ethics*, 178(4), 1043–1061. doi:10.1007/s10551-022-05048-7.

Rodgers W, Murray J, Stefanidis A, Degbey W, Tarba, S., (2023). An artificial intelligence algorithmic approach to ethical decision-making in human resource management processes. *Human Resource Management Review* 33:100925

Rodgers, W., & Murray, J.M. (2023). Are decision -making generative AI algorithmic pathways drivers for agility? Working Paper.

Rodgers, W., Söderbom, A., & Guiral, A. (2015). Corporate social responsibility enhanced control systems reducing the likelihood of fraud. *Journal of Business Ethics*, 131(4), 871-882

Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M.H.A., Hitchens, M. & Ryan, M. (2023). "Modelling the ethical priorities influencing decision-making in cybersecurity contexts", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. ahead-of-print No. ahead-of-print.

Sitkin, S.B. & Weingart, L.R. (1995). Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity. *Academy of Management Journal*, 38, 1573-1592

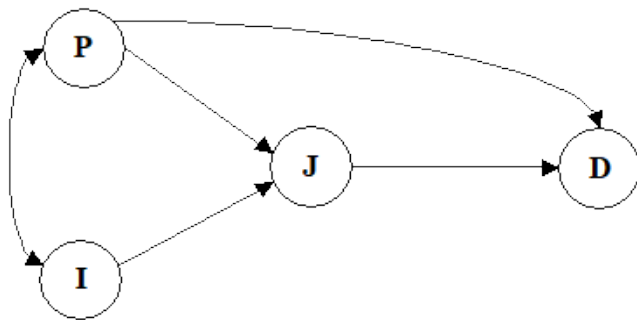
Smith, A. (1776). *The wealth of nations* (ed. 1991), Lancaster, UK: Prometheus Books.

Velasquez, M.G. (2006). *Business Ethics: Concepts and Cases* sixth edition. Upper Saddle River, NJ: Prentice-Hall, Inc.

Von-Neumann, J. & Morgenstern, O. (1947). *Theory of Games and Economic Behavior*. Princeton University Press, Princeton.

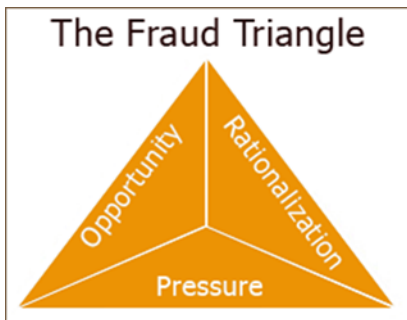
Worley, C.G. & Lawler, E.E. (2010). Agility and organisation design: A diagnostic framework. *Organisational Dynamics*, 39(2), pp.194-204.

Figure 1: Throughput Model (TPM)



P= perception, I= information, J= judgment, and D= decision choice.

Figure 2: Fraud triangle



From Rodgers et al., 2014

Figure 3: Causal Network Diagram (Lande and Strashnoy, 2023a).

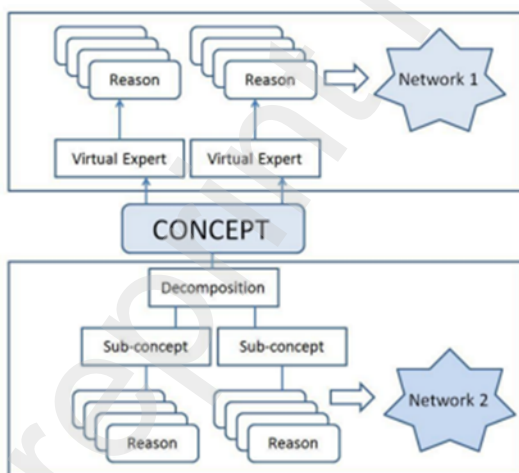


Figure 4: Combined approach Causal Network (Lande and Strashnoy, 2023a).

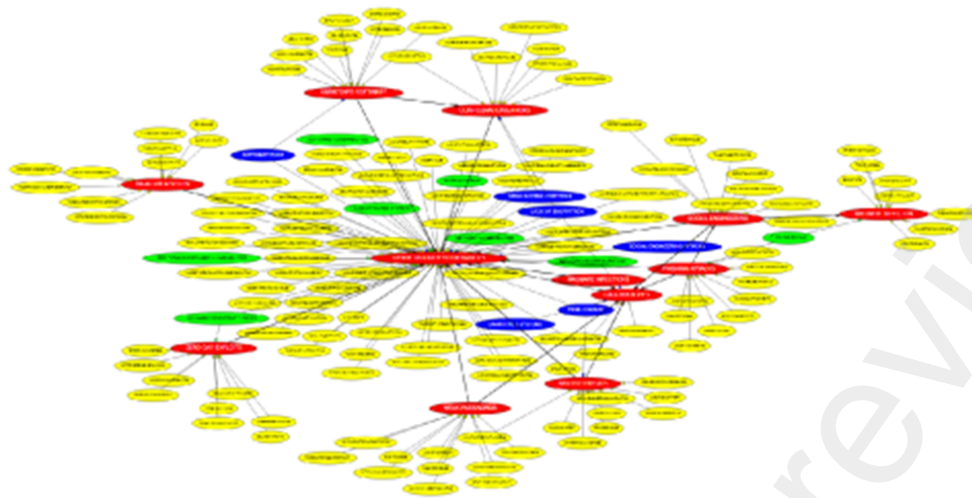


Figure 5: Ethical Causal Network Diagram – Method 1

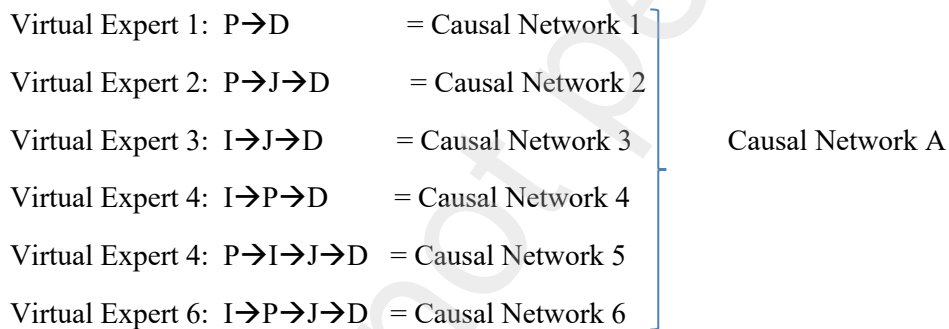


Figure 6: Ethical Causal Network Diagram – Method 2

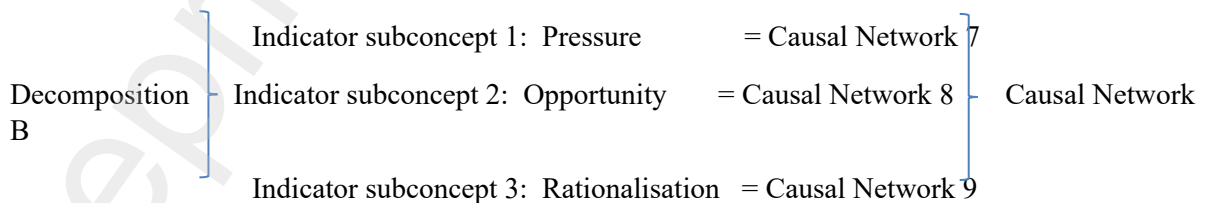


Figure 7. The complete network of concepts

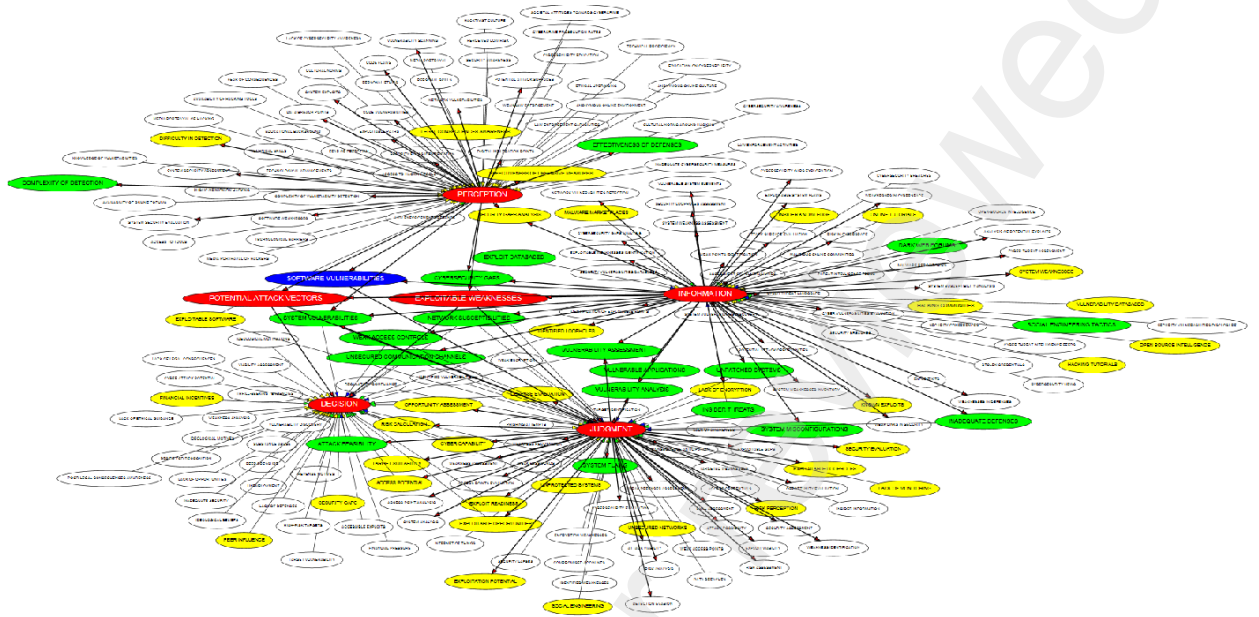


Figure 8. Supporting a network of concepts

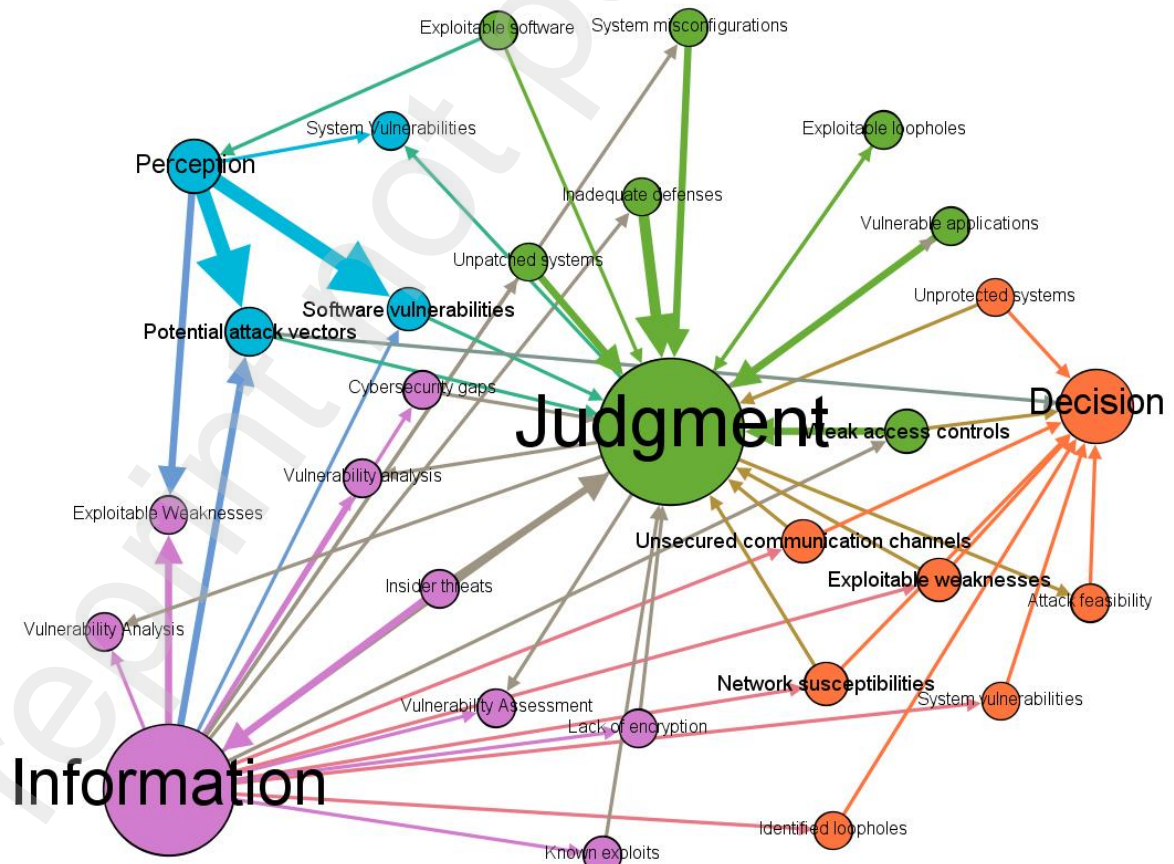


Table 1. TPM Pathways and Fraud Triangle (Rodgers et al., 2014).

TPM	Pressure	Opportunity	Rationalization
Ethical Egoism P→D	Wants, needs and desires are high	If I can get away with it	I deserve it
Deontology P→J→D	If rules do not cover situation, I may be pressured	New situation, no policy manual	No instructions or supervisory to contradict actions
Utilitarianism I→J→D	Goals are not achieved	Ends justify means-consequential oriented	Maximization of profits for shareholders
Relativist I→P→D	Cultural, up-bringing, etc. affected by wants needs and desires	Based on situation or environment	I deserve it
Virtue Ethics P→I→J→D	Virtues such as character, reputation reduces, but may not eliminate pressures	Organization has vastly different opinions on what constitutes a virtue.	Difficulty of establishing the nature of the virtues
Ethics of care I→P→J→D	Attempting to solve problems of stakeholders with confronting contradictory goals may not be possible.	Stakeholders are spread across a wide territory or international thereby difficult contact.	When carried to an extreme, this type of system can produce decisions that appear not simply subjective, but arbitrary.