The application of algorithmic cognitive decision trust modeling for cyber security within organisations

Professor Waymond Rodgers
Dr Rexford Attah-Boakye
Dr Kweku Adams

Abstract

Cybercrime continues to cause increasing threat to business processes, eroding stakeholders' trust in internet technologies. In this research paper, we explore how six dominant algorithmic trust positions facilitate cognitive processing, which, in turn, can influence an organisation's productivity and align its values and support structures for combating cybercrimes. This conceptual paper uses a cognitive perspective described as a Throughput Model. This modeling perspective captures several dominant algorithmic trust positions for organisations, providing a new and powerful approach which seeks to enhance our understanding of the cognitive representation of decision-making processes. These trust positions are (1) rational-based trust, (2) rule-based trust, (3) category-based trust, (4) third-party based trust, (5) role-based trust, and (6) knowledge-based trust. Finally, we provide conclusions and implications for future research.

Keywords: Cybercrime, cognitive processing, decision-making model, fraud triangle, Throughput model, trust pathways

Managerial Relevance Statement

Artificial intelligence is one of the most fascinating and promising technological development of the twenty-first century. Further, it has the potential to dramatically change society and organizations in the manner we live in a relatively short amount of time. A decision-making model (called the Throughput Model) is implemented in this paper in order to explain six dominant algorithms that can assist individuals and organisations in the employment of trust modelling. Trust issues can indelibly influence our understanding and usability of artificial intelligence platforms to almost every human endeavour, such as biology, chemistry, engineering, mathematics, finance, medicine, architecture, games, and even art. However, the profound benefits of artificial intelligence do not come without risks. Therefore, this paper explores two major issues in establishing an algorithmic artificial intelligence system, which are type 1 and 2 errors. Type 1 and type 2 errors may exist due to the interconnectedness of people, processes, and technology bias (observer, instrument, recall, etc.). Hence, as a practical matter, this research paper has identified appropriate trust positions to implement in order to address type 1 and type 2 errors. Type 1 error may fuel inefficiencies and higher transaction costs, which can spell inadequate productivity, as depicted by an artificial intelligence system. Likewise, inclusion of type 2 error may generate fraud triangle characteristics consisting of *perceived opportunity*, *perceived pressure/incentive*, and *rationalisation justification* of fraud. These characteristics are systematic of a problematic artificial intelligence system. The Throughput Modeling viewpoint discussed in this paper buttresses the fact that dissimilar algorithmic pathways are dependent upon risk factors entrenched in trust positions signifying cognitive, behavioural, individual and social inputs that transforms individuals or organisations' decision choices.

1. INTRODUCTION

One of the major concerns for managers is the threat from cybercrime that influences trust systems in organisations [1, 2]**.** Thus, organizations have built artificial intelligence systems to use human reasoning as a model to solve fraudulent problems [3]. Fraud is an intentional dishonesty that harms a person or organisation by causing an economic loss and/or the individual(s) responsible to realise a gain [4, 5]. Risk refers to the possibility of loss, which arises because of uncertainties or our inability to foresee the future [5-7]. This study uses a cognitive decision-modeling approach that allows for the examination of individual algorithmic pathway levels. Decision-making is the process by which we utilise our perceptions and information in order to form judgments to make choices to accomplish our goals [8]. Recent research has confirmed that people vary in the degree to which they form normative judgments and preferences on thinking bias tasks [9-11]

The work of Tombu and Mandel [23] has demonstrated that the way people perceive cognitive filters, such as decision heuristics, can influence information. That is, when confronted with an expected loss and a choice between a sure option and a risky option, the gain–loss framing of the problem has been shown to influence option preference. With regards to the prospect theory, this framing effect is the consequence of contradictory attitudes pertaining to risks involving gains and losses.

Building on this seminal work, Culbertson and Rodgers, [12], Rodgers[13], and Foss [14, 15], and Rodgers and Al Fayi [9] found that by implementing a Throughput Modeling approach, it was possible to represent risky decision making as including perception (P), information (I), judgment (J), and decision choice (D). The Throughput Model assumes that information inputs pass through the cognitive filters of perception and judgment before decision choices are made (see Figure 1).

Insert Figure 1 about here

In addition, this research paper utilizes propositions to suggest a link between concepts, which suggest promising areas of inquiry for researchers. Further, we use propositions to spur further research on several "trust questions," especially as it relates to artificial intelligence, in hopes that further evidence or experimental methods will be discovered that will make testable hypotheses. Finally, propositions serve as a common assumption that can support further speculation. This can occur in extremely complex artificial intelligence algorithms, such as those dealt with by sociology and economics of artificial intelligence impact on users, where an experimental test would be prohibitively expensive or difficult [28].

Furthermore, the Throughput Model advances six distinct algorithmic pathways tied to six dominant trust positions [16, 17]. Thus these algorithms are part of an artificial intelligence model (i.e., Throughput Model), which allows us to find solutions to a problem [18]. These trust positions tied to the Throughput Model are (1) rational-based trust (P→D), (2) rule-based trust (P→J→D), (3) category-based trust (I→J→D), (4) third-party-based trust (I→P→D), (5) role-based trust (P→I→J→D), and (6) knowledge-based or historical/dispositional trust (I→P→J→D) [4, 9, 19-21]. In sum, these algorithms provide a sequence of steps implemented to solve a problem. The sequence offers a unique way of addressing an issue by delivering a particular solution. Based on Figure 1.1, we can establish six general pathways that can be applied to the six dominate trust positions below:

(1) $\mathbf{P \rightarrow D}$ *Trust as a rational choice*

(2) $\mathbf{P \rightarrow J \rightarrow D}$ *Rule-based trust*

(3) $\mathbf{I \rightarrow J \rightarrow D}$ *Category-based trust*

(4) $\mathbf{I \rightarrow P \rightarrow D}$ *Third parties as conduits of trust*

(5) $\mathbf{P \rightarrow I \rightarrow J \rightarrow D}$ *Role-based trust*

(6) $\mathbf{I \rightarrow P \rightarrow J \rightarrow D}$ *Knowledge-based trust*

This research revealed that the resulting model was applicable across a wide range of general business decision-making contexts. Moreover, this line of research was expanded to incorporate risky decision-making activities along with "trust" and "ethical" positions [4, 9, 20]. In light of this, this paper proposes a Throughput Model that draws from computer science, economic and psychology literatures to model a perceptual and judgmental process whereby trust might be implemented to reduce fraud and risks [6, 20] (see Figure 2).

Insert Figure 2 about here

Prospect theory offers an elegant account of the perception framing effect. We add to the literature by asserting that there are six dominant algorithmic pathways to a decision choice that allows for greater potential in terms of examining how risk attitudes are assessed in risky-choice framing problems. Some studies questioned the generalisability of the framing effect due to predictable eliminations and reversals of the framing effect [22, 23]. In other words, findings that cannot be accommodated by the explanation that preference reversals (i.e., framing effects) are mediated by concomitant reversals of risk attitudes.

This conceptual research paper embeds trust positions in the Throughput Model based on two types of process errors. The type 1 process error is where decision makers are expected to avoid the risk in a risky decision-making situation or intervene actively in an alternative with the help of a risk-defusing action. The type 2 process error is where the decision maker can select a less risky alternative (passive risk avoidance) [24]. Dual process theories of cognitive

processing distinguish unconscious, emotional, intuitive and effortless (Type I processing) with conscious, controlled and effortful characteristics (Type 2) (e.g., [25]; [26])

The type 1 error process represents a rejection of individuals who should be admitted from entering a system (e.g., accounting/auditing/information system) or network (i.e., type 1 error or false rejection rate). The type 2 process error represents an acceptance of individuals who should not be admitted to a system or network (i.e., type 2 error or false acceptance rate). In this paper, we investigate differences between active (type 1) and passive (type 2) risk avoidance in trust situations. More specifically, this paper aims to identify appropriate trust positions to reduce/increase the type 1 and type 2 process errors, and then discusses the implications of using a particular trust position in relation to people, processes and technology [4, 6, 20, 27]. Sections 2 and 3 clarify and highlight the issue of trust and trustworthiness. The discussion explores the relationship between the Throughput Model and dominant trust positions (see Table 1).

Insert Table 1 about here

The aforementioned processes help to tie trust positions to the Throughput Modeling paradigm, which in turn generates propositions. An initial stage in the scientific process is not observation, but the generation of hypotheses or propositions, which may then be tested critically by observations and experiments. Thus "proposition generation" is a necessary step in addressing critical issues surrounding people, processes, and technology. Likewise, Popper [28] also makes the vital assertion that the goal of the scientist's efforts is not the verification but the falsification of the initial hypothesis. It is understandably unattainable to confirm the truth of a general law by repeated observations. Nonetheless, at least in principle, it is possible to falsify such a law by a single observation. Therefore, the propositions assist in identifying

and exploring the dominant six-trust positions' relationship with fraudulent transactions and risk factors.

Finally, we conclude with a summary outlining implication for research and practice dealing with forensic and fraud organisational systems.

2. Definition of trust

Most literature on trust fails to distinguish trust from trustworthiness. Trust is a social psychological factor, which includes the reduction of control, willingness to accept vulnerability and risk based upon the positive expectations of the actions of the trustee [29]. Trustworthiness, on the other hand, involves the ability, benevolence and integrity of a trustee [30, 31]. Some scholars view trust as synonymous with trustworthiness and explain trust in the context of personal attributes that impel positive expectations on the part of the trustee [32, 33]. Whilst some scholars view trust as a behavioral intention rather than a psychological factor [30, 33], others view trust as a biological component within the individual, which develops early in life and remains relatively stable through adulthood Webb & Worchel [34] In this regard, Mayer, Davis & Schoorman [30] adopted an integrative model to define trust by using the trustworthy variables (benevolence, ability and integrity) as antecedent of trust. Their model attempts to separate the trustworthy variables into two major components such as ability component and character component. The ability component measures the 'can do' aspects, whereas the character component measures the 'will do' aspects. Trust decisions affect a company's relationship with its community, customers, employees, stockholders and suppliers [35, 36]. Thus, the roles of trust positions in achieving competitive advantage are becoming increasingly popular amongst organisations of all kinds and sizes [9, 19, 37]

The impact of trust on organisational performance and increase in productivity has received considerable interest in recent research such as cyber decision-making [38-40] e-

commerce [41], and accounting/auditing research [42-46]. In the trust literature, trust serves as a lubricant to the wheels upon which all business transactions and relationships are based [47, 48]. Trust plays a central role in every sustainable business endeavor because trust can reduce agency and transaction costs, ensure the smooth operation of transaction, and increase innovation and productivity [49]. Trust decisions occur in an environment of uncertainty, where stakeholders face vulnerable situation (risk/uncertain situation) leading to a dependence or reliance on management for security [50, 51]. Shareholders must trust managers, employers must trust employees, buyers must trust sellers, the public must trust business, and the government must trust business. Unfortunately, there is a scarcity of trust following the prevalence of recent corporate scandals (e.g., Arthur Anderson, Enron, Tyco, Adelphia, WorldCom etc.). The impact of these corporate scandals on stakeholders' trust is significant.

Furthermore, Rodgers [5, 19, 20] argues that there are two primary trust algorithmic pathways of rational choice; rule-based trust and category-based trust, which underscore the basis of trust relationships. Expertise level, incomplete information, rapidly changing environments, and/or time pressure sturdily influence the implementation of these primary trust algorithmic pathways [20]. However, the refinement of the interaction of people, process and technology will influence information exchange and individuals' perceptions. As a result, this can further yield three secondary higher-level trust algorithmic pathways of third-party-based trust, role-based trust and knowledge-based trust [19, 20, 27]. To avoid increasing threats (e.g., cybercrimes resulting in fraud, errors and risks) to business processes and shareholders' trust, we analyse and explore how fraudulent schemes are affected differently by employing one, or a combination of the three trust positions. We also investigate the interrelated processes of the Throughput Model and trust algorithmic pathways that have an impact on decisions affecting organisations.

Advanced Internet technology has now reached a point where achieving improved safety would occur through a better understanding of human error mechanisms [52] and trust relationships [21]. Human error is a causal or contributing factor in accidents, particularly in the security industries. Consequently, these trust positions could protect information systems and electronic commerce and the cyber-based technologies and the business environment [53]. For example, cyber-related security threats have presented debilitating consequences for organisations and have negatively impacted economic activities significantly [20, 41, 54]. As errors are intimately bound with the notion of intention, organisations are compounded with decisions regarding type 1 versus type 2 process errors [25]. In this regard, Zapf and Reason [54] suggested that errors lead to "the non-attainment of corporate goals, therefore, the dominant trust positions introduced in this study works on the assumption that errors should be potentially avoidable."

Moreover, it has been recognised that there is constructive magnitude of trust building system embedded within daily operations of organisations [55-57]. In particular, the challenges of increasing interpersonal communication and online transaction in a system or network have led many researchers to investigate the impact of online trust on cognitive processes [41, 58-62]. The overwhelming conclusion is that cybercrime continues to cause increasing threat to people, processes and technology of businesses, impacting upon organisational values and eroding stakeholders' trust. Trust plays a critical role in developing organisational relationships internally and externally because of its related uncertainty, risk, fear, and interdependence factors in the decision-making process [60-63] (see Table 2).

Insert Table 2 about here

---

3. Throughput Model Methodology

This paper utilises the Throughput Model (see Figure 1) to gain further insight on how organisations can create an environment that engenders trustworthy behavior. To our knowledge, this is the first study integrating different trust positions, fraud, risks and errors in decision-making algorithmic pathways that might be useful in reducing fraudulent behaviours.

Figure 3 illustrates the key three enablers, which can be captured by implementing the fraud triangle. The fraud triangle consists of *perceived opportunity*, *perceived pressure/incentive,* and *rationalisation justification* of fraud [5, 64]. The fraud triangle diagnoses high-risk fraud situations. Perceived opportunity is the possibility of entry into a situation where fraud can be carried out, for example, where there are weaknesses in an internal control system. Perceived pressure/incentive addresses the motivation or underlying drive for individuals to commit fraud. Rationalisation represents the propensity for individuals to 'bend' their ethical positions, moral standards, among others, to justify their fraudulent activities [5].

Insert Figure 3 about here

This model captures four major concepts (perception, information, judgment, and decision choice) which help explain, describe, and/or predict situations or environmental conditions in an ethical, trust, or general decision-making task [20, 65]. To clarify different algorithmic trust pathways, the Throughput Model separates the decision-making process into four key stages: perception as problem framing (P); information exchange (I); judgment representing the analysis of perception and information (J); and decision choice (D). Perception and information depend on each other in the Throughput Model because information can influence how a decision maker frames a problem (perception) or selects evidence (information) to be used in the decision-making process.

In Figure 1, perception (P) can be influenced by an individual's educational background, religion, belief, communal values, upbringing, etc. Perception depicts the framing of an organisational environment, which involves risk assessment, perceiving fraudulent transactions such as cyber fraud, high risk transactions, cyberattack etc**.** Previous studies posit that a change in framing (i. e. risk perception) influences risk preferences, and risk attitude. Thus changes in risk perception may lead to a pronounced shift from risk aversion to risk taking [23, 66]. brought into question rational-choice theories of human decision making due to violation to the description-invariance principle (i.e., fixed preferences across different descriptions of identical choice problems), one of the least questionable tenets of rational-choice theories.

Information (I) includes customer databases, organisations' databases, forensic evidence, social networks, financial information, governmental agencies' reports on fraud, etc. In the judgment (J) stage, financial and non-financial information are scrutinised and weight is placed on key information which is compared to other alternatives. We argue that experts such as auditors, forensic accountants, cybercrime investigators etc. usually retrieve from their knowledge base and expertise to examine situations to collect evidence. Finally, in the decision choice (D) stage, we argue that experts make trustworthy decisions based on combinations of perception, information, and judgment.

In addition, the Throughput Model in Figure 1 reflects interdependency between perception (P) and information (I). That is this relationship (P←→I) reflects a neural network that simulates human thought and make deep learning techniques possible for machine learning by drilling down on informational (I) databases [67]. Deep learning (also known as deep structured learning or hierarchical learning) is part of a wider family of machine learning methods based on learning data representations, as opposed to task-specific algorithms [68].

Rodgers [19, 20] argued that trust positions in the Throughput Model play a role as a cognitive process, which is rationally based on one's interest (incentive), for normative reasons, or for reasons of character or psychological disposition. Therefore, the underlying trust depends on the assessment of the trustworthiness of another in a particular situation [69]. Most importantly, the Throughput Model enables decision makers to understand why individuals have selected information which supports their trust positions and have ignored other information that does not support their positions. The following sub-sections discuss the six algorithmic trust pathways based on the Throughput Model. These algorithmic trust pathways represent:

1. *Trust as a rational choice*: a presumed understanding of the other party's desires and intentions.
2. *Rule-based trust*: trusting someone due to a strictly enforceable normative rule or legal system.
3. *Category-based trust*: social networks sharing some common experience, tradition, education, custom, culture, religion, and so forth.
4. *Third-party-based trust*: people use themselves or the people around them as their basis for defining trust.
5. *Role-based trust*: tied to formal societal structures, depending on individual attributes.
6. *Knowledge-based trust*: people have enough relevant and reliable information about others to understand them and accurately predict their likely behavior.

The following sub-sections discuss each algorithmic pathway and its proposition:

(1) P→D (rational-based trust)

According to Rodgers [19, 20, 70], the P→D algorithmic pathway represents trust as a rational choice, which is the quickest way to make a decision. Here, the trust decision takes perceptual preference as an important determinant for a decision choice because individuals are usually motivated to act in their perceived self-interest. In the rational-based trust, individuals prioritise the maximisation of their expected gains and the minimisation of their expected losses. This trust algorithmic pathway primarily manifests in a situation of low risk/high certainty. For example, where the momentary amount involved in a transaction is negligible, individuals may adopt a rational-based trust position. In addition, time pressure, difficulties in interpreting information and rapidly shifting environmental conditions are amongst the factors which can influence people to select this particular trust algorithmic pathway. In addition, the level of knowledge or expertise of individuals can influence people to select a rational-based trust position. Research suggests that time pressures may alter both the cognitive and emotional processes involved in risky decision making [71-73]. For example, time pressures may have a damaging effect on cognitive processes, such as impairing working memory capacity (e.g., [74, 75]) and plummeting decision accuracy (e.g., [75]). In addition, subsidiary anticipatory stress has a negative influence on learning and information processing abilities [73]. Hence, in a high-risk situation, certain individuals with a requisite level of expertise will ignore incomplete information and judgment and make a quick decision choice. For example, internet users may have many barriers to international cyber transactions resulting from disparate regulations in various foreign countries and an overall deficiency of familiarity and lack of information with webpage platforms.

Proposition 1a: In a time-pressured environment of incomplete information, high levels of expertise between the parties (online or offline) will result in a highly trustworthy relationship.

Proposition 1b: In a time-pressured environment of incomplete information, low levels of expertise between the parties (online or offline) will result in a poor trustworthy relationship.

(2) P→J→D (rule-based trust)

This trust position emphasises the 'power base', i.e. the use of rules, laws regulations etc. to influence the trust position of individuals [20]. The rule-based trust can be categorised under explicit and implicit contracts. Under the explicit contract, the individual trust position is influenced by factors including his/her contract of employment, job description and organisational policies and procedures. The implicit contract includes the individual's own personal values and the organisational culture, values, norms etc. In a risky/uncertain environment, organisations use structures and power to influence the individual trust position. The structural and interpersonal components of rules are likely to influence perceived trust [76]. With the rule-based trust, direct information is ignored due to either its unreliability or incompleteness. Currall and Epstein [77] argued that, "because rule-based trust involves personal consequences; trust position under the rule-based trust is individual oriented." Also, individuals may adopt the rule-based trust position as a result of certain influences such as some sets of spiritual doctrine, codes of trust for professionals (accountants and auditors), codes of conduct specific to certain organisations and social values etc. Rules, practices and mechanisms are unlikely to change suddenly. Rather, they are mentally represented as assimilated knowledge that can influence the individual trust decision. In a strong rule-based situation, results that depend entirely on trust are expected to decline in the long term. On the contrary, when an organisation's approach calls for fewer rules, employees are allowed to bring their innovations and initiative to bear in the production process. This will result in high productivity and less transaction cost [78-81].

When situations are less than rule-based, a higher level of trust will have the opportunity to result in certain situations where information on the internet is neither weak nor strong in directing a user toward an outcome. Trust helps to ‘‘tip the scales’’ as trust helps a person to interpret previous behavior and/or assess the future behavior of another party. For example, it is impractical to have written rules that deal with trust issues when communicating on a webpage based on feelings, values, and beliefs.

Proposition 2a: Trustworthy relationships that are based on high level transparent, responsible, accountable and enforceable rules and regulations will lead to low level false rejection and/or false acceptance into the network system.

Proposition 2b: Trustworthy relationships that are based on low level transparent, responsible, accountable and enforceable rules and regulations will lead to high level false rejection and/or false acceptance into the network system.

(3) I→J→D (category-based trust)

Category-based trust refers to direct information that has an impact on judgment, which in turn influences decision choice. The category-based trust emphasises the fact that individuals are subject to preformatted information regarding relationship types [20]. The category-based trust operates on the philosophy that people and relationship types can be grouped into segments with similar characteristics. For example, organisations can categorise their suppliers or customers into different segments. In this situation, the level of trust is high because organisations have adequate and reliable information about each segment. On the other hand, the level of trust will be low if organisations have incomplete or unreliable information about the segment. Category-based trust highlights the relationships that exist amongst individuals within social networks [82-84]. Individuals within a particular social

group usually share similar values, cultures, norms, and belief systems etc. [84]. The strength of a category-based relationship is linked to its frequency, reciprocity, emotional intensity and trusting relationships to build slowly and incrementally over time, especially when it involves inclusion in a category. For example, relative knowledge regarding a particular website as well as other friends and family members use of the website can be reflected in completing future monetary transactions on the same website.

Proposition 3a: Complete and reliable information about the organisation' customer/supplier segments will lead to stronger online trust relationships.

Proposition 3b: Incomplete and unreliable information about the organisation' customer/supplier segments will lead to weaker online trust relationships.

These three primary algorithmic pathways either emphasise problem framing (P) or information (I), but not both [20]. Furthermore, the three primary algorithmic pathways encapsulate an understanding of trust and distrust within people relationships [85-87]. We can associate trust (high, low), no trust, and distrust (low, high) in the algorithmic pathways with values that vary from +1 (the highest trust) to -1 (the highest distrust). Each path can have a positive (+), negative (-) or zero (0) sign to represent the magnitude of *trust, distrust and no trust.*

Rodgers [20, 70, 88] argued that trust algorithmic pathways can be interrelated by perception and information via three secondary higher-level trust algorithmic pathways; rational-based trust (P→D), rule-based trust (P→J→D), or category-based trust (I→J→D). Firstly, information source (I) conciliates and changes trust as a rational choice into third-party-based trust (I→P→D). Next, problem framing (P) reconstructs category-based trust (I→J→D) into role-based trust (P→I→J→D). Finally, information (I) transforms rule-based trust (P→J→D) into knowledge-based trust (I→P→J→D). The remaining three secondary higher-

level trust algorithmic pathways supplement the primary algorithmic pathways by adding either problem framing (P) or gathering information (I), and this is discussed as follows.

(4) I→P→D (third-party-based trust)

This trust algorithmic pathway relies on the third party as a channel of trust [20]. In this instance, decision makers use people around them as a basis for defining their trust pathways to serve as reinforcement to their existing perception. As a result, one is more certain of his or her trust (distrust) in another. The third-party based trust therefore depends on the indirect connection between one entity and a third party and the indirect connection between two entities. For example, third parties as conduits of trust assume that an internet user desiring to purchase shoes on the internet relies on using people around them who promote buying shoes on a particular website. Third-party information serves to reinforce existing webpage use, making one's perception more certain of his or her trust (or distrust) in a particular webpage.

Proposition 4a: Relevant and reliable third-party information can result in a high trust relationship between two parties involved in a network transaction.

Proposition 4b: Non-relevant and unreliable third-party information can result in a low trust relationship between two parties involved in a network transaction.

(5) P→I→J→D (role-based trust)

The basis of trust in this algorithmic pathway depends on the role (profession, expertise, position, attribute, authority etc.) of the party to be trusted [20]. In this algorithmic pathway, people trust that specific role types can deliver specific desire outcomes. An example of role-based trust is gaining certification from an engineer, accountant, medical doctor etc. For

example, shareholders trust in the role of auditors because they believe that auditors have skills and professional expertise to audit the accounts of organisations. In addition, audit/accounting experts ensure that all of their members adhere to strict professional conduct. Furthermore, employees are prepared to accept a manager's decision due to the manager's organisational role and authority. Individuals' trust in their organisational authority (management) shapes their willingness to follow the rules and regulations of the organisation [89]. In addition, reliable information about personal qualities, social limitations of others and existence of trustworthy communication architecture are crucial for making trustworthy decisions [90-92]. In other words, trust "is cultivated out of productive inquiry rather than imperceptive acknowledgment" [93].

Examples of role-based trust are certification of a web-based plumber or medical doctor. That is, we trust a medical doctor since we trust the practice of medicine and believe that medical doctors are trained to apply valid principles of medicine. In addition, we have evidence every day that these principles are valid when we observe certain remedies recommended to save lives.

Proposition 5a: The level of expertise is high of the auditor, forensic accountant or cybercrime investigator can determine an individual's trustworthiness is high in order to minimise both false rejections and false acceptance into the network.

Proposition 5b: The level of expertise is low of the auditor, forensic accountant or cybercrime investigator can determine an individual's trustworthiness is low in order to minimise both false rejections and false acceptance into the network.

(6) I→P→J→D (knowledge-based trust)

This algorithmic pathway expands on the rule-based trust in that past and/or present information (knowledge-based), can influence individuals' perceptions, which in turn affects their judgment and decision choices [20]. The knowledge-based trust algorithmic pathway is influenced by fewer time pressures and a reasonable level of expertise in an unstructured environment in order to form judgment about the probability of trustworthy behavior of others [20]. In this trust algorithmic pathway, trust is considered as a function of 'general expectations' that is premised on past and present information. Knowledge-based trust transpires when individuals or organizations have enough, relevant, and reliable information about webpage-based companies in order to understand them and accurately predict their likely behavior. For example, organization' web pages on the internet vary by size and industry and the environment they carry out their operations is determined by legal traditions. Consequently, knowledge-based trust pathways permit flexibility in the design of mandatory and non-mandatory measures in a global cyber context.

Proposition 6a: Reliable and relevant information will encourage higher [94] levels of trustworthiness over and above rules and laws. The type and level of trust pathways employed by organisations may influence its productivity, competition and value.

Proposition 6b: Unreliable and irrelevant information will encourage higher [94] levels of trustworthiness over and above rules and laws. The type and level of trust pathways employed by organisations may influence its productivity, competition and value.

4. Conclusions and implications

Artificial Intelligence techniques such as trust decision-making algorithms can assist our understanding of employing machine learning and deep learning for solving fraud type problems in the future. This conceptual research paper has argued that the first step in the scientific process is not observation, but the generation of propositions (or hypotheses), which may then be tested critically by observations and experiments. Type 1 and type 2 errors can occur because of people, processes, and technology bias (observer, instrument, recall, etc.). Therefore, this theoretical research paper has identified appropriate trust positions to implement in order to address type 1 and type 2 errors. Type 1 error can contribute to inefficiencies and higher transaction costs, that can spell reduced productivity, as depicted by a cyber system. Furthermore, admittance of type 2 error creates fraud triangle characteristics consisting of *perceived opportunity*, *perceived pressure/incentive*, and *rationalisation justification* of fraud. These characteristics are systematic of a problematic cyber system.

Our implications of using a particular trust position depend on the controlling factors influencing type 1 and type 2 errors in relationship with people, processes and technology. Furthermore, the six dominant trust positions or algorithmic pathways were tied to situations that could lead to type 1 or type 2 errors. These trust positions denote: (1) rational-based trust, (2) rule-based trust, (3) category-based trust, (4) third-party-based trust, (5) role-based trust, and (6) knowledge-based trust.

Trust behavior is a prerequisite for knowledge production and its exchanges. Individuals are not machines. They think and have feelings. When they pursue activities or communicate ideas, they are trusting in others. In addition, trust as a relational and institutional asset supports competitive advantages. Therefore, trust can be viewed as an intangible asset that adds value to an organisation.

A vast variety of Internet devices, including institutions, norms, cyber ware, etc., enables individuals/organisations to cooperate in an efficient and effective manner. The Throughput Model can be useful in understanding what causes individuals to act in a manner whereby they do not exploit cyber world for positive results. Trust augmented in a positive manner is 'good' for internet traffic, according to the ethical principles of normative philosophy, not according to the moral standards of a given group or culture. Beliefs about what is right, just and fair are possible influences on information network systems. The management of knowledge and technology in organisations is critical to competitive advantage and organisational success. This study highlights how decision-makers' perceptual framing, along with information can greatly influence decision choices. The Throughput Modeling perspective discussed in this paper reinforces the fact that different algorithmic pathways are dependent upon risk factors embedded in trust positions representing cognitive, behavioral, individual and social inputs, that modifies their decision choices.

Future research can investigate whether a particular trust position for cyber platforms supported by a particular decision-making pathway is more appropriate given a particular situation involving trust. In addition, future research can explore which decision-making pathway can typify better relationships between organisations and individuals when communicating across the Internet. Finally, the Throughput Model different algorithmic pathways can allow us to better understand how trust is nurtured and eroded as different parties interact.

References

[1] W. Rodgers, *Artificial Intelligence Evaluated in a Throughput Model: Some Major Algorithms,"* Florida: CRC Press, Taylor & Francis, 2020.

[2] W. Rodgers, Alhendi, E. and Xie, F, ""The Impact of Foreignness on the Compliance with Cybersecurity Controls,"" *Journal of World Business,* vol. 54, 2019.

[3] J. Liu, K. Xiangjie, F. Xia, X. Bai, L. Wang, Q. Qing, and I. Lee, "Artificial intelligence in the 21st century," *IEEE Access,* vol. 6, pp. 34403-34421, 2018.

[4] A. Guiral, W. Rodgers, E. Ruiz, and J. A. Gonzalo-Angulo, "Can expertise mitigate auditors' unintentional biases?," *Journal of International Accounting, Auditing and Taxation,* vol. 24, pp. 105-117, 2015.
[5] W. Rodgers, A. Söderbom, and A. Guiral, "Corporate social responsibility enhanced control systems reducing the likelihood of fraud," *Journal of Business Ethics,* vol. 131, no. 4, pp. 871-882, 2015.
[6] W. Rodgers, *Biometric and auditing issues addressed in a throughput model*. IAP, 2011.
[7] W. Rodgers and T. J. Housel, "The effects of environmental risk information on auditors' decisions about prospective financial statements," *European Accounting Review,* vol. 13, no. 3, pp. 523-540, 2004.
[8] W. Rodgers, G. N. Mubako, and L. Hall, "Knowledge management: The effect of knowledge transfer on professional skepticism in audit engagement planning," *Computers in Human Behavior,* vol. 70, pp. 564-574, 2017.
[9] W. Rodgers and S. Al Fayi, "Ethical pathways of internal audit reporting lines," in *Accounting Forum*, 2019: Taylor & Francis, pp. 1-26.
[10] W. Bruine de Bruin, A. M. Parker, and B. Fischhoff, "Individual differences in adult decision-making competence," *Journal of personality and social psychology,* vol. 92, no. 5, p. 938, 2007.
[11] P. Teovanović, G. Knežević, and L. Stankov, "Individual differences in cognitive biases: Evidence against one-factor theory of rationality," *Intelligence,* vol. 50, pp. 75-86, 2015.
[12] A. Culbertson and W. Rodgers, "Improving Managerial Effectiveness in the Workplace: The Case of Sexual Harassment of Navy Women 1," *Journal of Applied Social Psychology,* vol. 27, no. 22, pp. 1953-1971, 1997.
[13] W. Rodgers, "The influences of conflicting information on novices and loan officers' actions," *Journal of Economic Psychology,* vol. 20, no. 2, pp. 123-145, 1999.
[14] N. J. Foss, "Knowledge-based Approaches to the Theory of the Firm: Some Critical Comments," *Organization Science,* Article vol. 7, no. 5, pp. 470-476, 1996.
[15] J. M. Fossaceca, T. A. Mazzuchi, and S. Sarkani, "MARK-ELM: Application of a novel multiple kernel learning framework for improving the robustness of network intrusion detection," *Expert Systems with Applications,* Article vol. 42, no. 8, pp. 4062-4080, 2015.
[16] W. Rodgers, *"Trust Throughput Modeling Pathways."* Hauppauge, NY: Nova Publication, 2019.
[17] W. Rodgers, A. Guiral, and J. A. Gonzalo, "Trusting/Distrusting Auditors' Opinions," *Sustainability,* vol. 11, no. 6, p. 1666, 2019.
[18] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang., "Machine learning and deep learning methods for cybersecurity," *IEEE Access,* vol. 6, pp. 35365-35381, 2018.
[19] W. Rodgers, *Ethical beginnings: Preferences, rules, and principles influencing decision making*. iUniverse, 2009.
[20] W. Rodgers, "Three primary trust pathways underlying ethical considerations," *Journal of Business Ethics,* vol. 91, no. 1, p. 83, 2010.
[21] R. M. Kramer, "Trust and distrust in organizations: Emerging perspectives, enduring questions," *Annual review of psychology,* vol. 50, no. 1, pp. 569-598, 1999.
[22] D. R. Mandel and I. V. Kapler, "Cognitive style and frame susceptibility in decision-making," *Frontiers in psychology,* vol. 9, p. 1461, 2018.

[23] M. Tombu and D. R. Mandel, "When does framing influence preferences, risk perceptions, and risk attitudes? The explicated valence account," *Journal of Behavioral Decision Making,* vol. 28, no. 5, pp. 464-476, 2015.
[24] O. Huber, O. W. Huber, and A. S. Bär, "Framing of decisions: effect on active and passive risk avoidance," *Journal of Behavioral Decision Making,* vol. 27, no. 5, pp. 444-453, 2014.
[25] D. Kahneman and F. Thinking, "Slow," *New York: Farrar, Straus and Giroux,* p. 73, 2011.
[26] B. Simonovic, E. J. Stupple, M. Gale, and D. Sheffield, "Stress and risky decision making: Cognitive reflection, emotional learning or both," *Journal of Behavioral Decision Making,* vol. 30, no. 2, pp. 658-665, 2017.
[27] W. Rodgers, *Process thinking: Six pathways to successful decision making*. IUniverse, 2006.
[28] K. R. Popper, "Unended Quest: An Intellectual Autobiography, 1974," *Fontana (London), S,* vol. 168, p. 171, 1993.
[29] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of Management Review,* vol. 23, no. 3, pp. 393-404, Jul 1998.
[30] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review,* vol. 20, no. 3, pp. 709-734, 1995.
[31] M. Hassan and F. Semerciöz, "Trust in personal and impersonal forms its antecedents and consequences: A conceptual analysis within organizational context," *International Journal of Management and Information Systems,* vol. 14, no. 2, pp. 67-83, 2010.
[32] J. K. Butler Jr and R. S. Cantrell, "A behavioral decision theory approach to modeling dyadic trust in superiors and subordinates," *Psychological reports,* vol. 55, no. 1, pp. 19-28, 1984.
[33] D. H. McKnight, N. L. Chervany, and L. L. Cummings, *Trust formation in new organizational relationships*. Management Information Systems Research Center, Curtis L. Carlson School of …, 1996.
[34] W. M. Webb and P. Worchel, "Trust and distrust," *Psychology of intergroup relations,* pp. 213-228, 1986.
[35] R. Bhattacharya, T. M. Devinney, and M. M. Pillutla, "A formal model of trust based on outcomes," *Academy of management review,* vol. 23, no. 3, pp. 459-472, 1998.
[36] E. L. Malone, "Intellectual capital: realizing your company's true value by finding its hidden brainpower," *NY: Harper Business,* 1997.
[37] J. B. Barney and M. H. Hansen, "Trustworthiness as a source of competitive advantage," *Strategic management journal,* vol. 15, no. S1, pp. 175-190, 1994.
[38] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 9, pp. 2167-2178, 2018.
[39] D. Pienta, J. Thatcher, H. Sun, and J. George, "Information Systems Betrayal: When Cybersecurity Systems Shift from Agents of Protection to Agents of Harm," *Information Systems,* vol. 6, pp. 26-2018, 2018.
[40] S. Banerjee, S. Bhattacharyya, and I. Bose, "Whose online reviews to trust? Understanding reviewer trustworthiness and its impact on business," *Decision Support Systems,* vol. 96, pp. 17-26, 2017.
[41] S. Y. Yousafzai, J. G. Pallister, and G. R. Foxall, "A proposed model of e-trust for electronic banking," *Technovation,* vol. 23, no. 11, pp. 847-860, 2003.
[42] L. Guiso, P. Sapienza, and L. Zingales, "Does culture affect economic outcomes?," *Journal of Economic perspectives,* vol. 20, no. 2, pp. 23-48, 2006.

[43] S. Knack and P. Keefer, "Does social capital have an economic payoff? A cross-country investigation," *The Quarterly journal of economics*, vol. 112, no. 4, pp. 1251-1288, 1997.
[44] P. J. Zak and S. Knack, "Trust and growth," *The economic journal*, vol. 111, no. 470, pp. 295-321, 2001.
[45] R. L. Porta, F. Lopez-De-Silane, A. Shleifer, and R. W. Vishny, "Trust in large organizations," National Bureau of Economic Research, 1996.
[46] P. Sapienza, A. Toldra, and L. Zingales, "Understanding trust (No. w13387)," ed: National Bureau of Economic Research, 2007.
[47] J. M. Hansen, G. Saridakis, and V. Benson, "Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions," *Computers in Human Behavior*, vol. 80, pp. 197-206, 2018.
[48] J. Yan, D. Wu, S. Sanyal, and R. Wang, "Trust-oriented partner selection in D2D cooperative communications," *IEEE Access*, vol. 5, pp. 3444-3453, 2017.
[49] S. L. Berman, A. C. Wicks, S. Kotha, and T. M. Jones, "Does stakeholder orientation matter? The relationship between stakeholder management models and firm financial performance," *Academy of Management journal*, vol. 42, no. 5, pp. 488-506, 1999.
[50] A. Iqbal, M. Guo, L. Gunn, M. A. Babar, and D. Abbott, "Game theoretical modelling of network/cyber security," *arXiv preprint arXiv:1901.08426*, 2019.
[51] A. Nagurney and S. Shukla, "Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability," *European Journal of Operational Research*, vol. 260, no. 2, pp. 588-600, 2017.
[52] J. Reason, *Human error*. Cambridge university press, 1990.
[53] M. E. Whitman, "Enemy at the gate: threats to information security," *Communications of the ACM*, vol. 46, no. 8, p. 91, 2003.
[54] D. Zapf and J. T. Reason, "Introduction: Human errors and error handling," *Applied Psychology*, vol. 43, no. 4, pp. 427-432, 1994.
[55] A. G. Hopwood, "Accounting and organisation change," *Accounting, Auditing & Accountability Journal*, vol. 3, no. 1, 1990.
[56] R. E. Miles and C. C. Snow, "Causes of failure in network organizations," *California management review*, vol. 34, no. 4, pp. 53-72, 1992.
[57] N. Garcia, M. J. Sanzo, and J. A. Trespalacios, "New product internal performance and market performance: Evidence from Spanish firms regarding the role of trust, interfunctional integration, and innovation type," *Technovation*, vol. 28, no. 11, pp. 713-725, 2008.
[58] D. Gefen, I. Benbasat, and P. Pavlou, "A research agenda for trust in online environments," *Journal of Management Information Systems*, vol. 24, no. 4, pp. 275-286, 2008.
[59] P. Palvia, "The role of trust in e-commerce relational exchange: A unified model," *Information & management*, vol. 46, no. 4, pp. 213-220, 2009.
[60] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building consumer trust online," *Communications of the ACM*, vol. 42, no. 4, pp. 80-85, 1999.
[61] C. Tomkins, "Interdependencies, trust and information in relationships, alliances and networks," *Accounting, organizations and society*, vol. 26, no. 2, pp. 161-191, 2001.
[62] M. Greenwood and H. J. Van Buren III, "Trust and stakeholder theory: Trustworthiness in the organisation–stakeholder relationship," *Journal of business ethics*, vol. 95, no. 3, pp. 425-438, 2010.
[63] K. Blomqvist, P. Hurmelinna, and R. Seppänen, "Playing the collaboration game right—balancing trust and contracting," *Technovation*, vol. 25, no. 5, pp. 497-504, 2005.

[64] B. A. S. a. W. Rodgers, "“Artificial Intelligence Algorithmic Approach in Enhancing Auditors’ Fraud Risk” " Presented at the American Accounting Association Conference, 2019.
[65] W. Rodgers, *Throughput modeling: Financial information used by decision makers*. Jai Press, 1997.
[66] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior,* vol. 75, pp. 547-559, 2017.
[67] A. L’heureux, K. Grolinger, H. F. Elyamany, and M. A. Capretz, "Machine learning with big data: Challenges and approaches," *IEEE Access,* vol. 5, pp. 7776-7797, 2017.
[68] G. Cui, M. L. Wong, and H.-K. Lui, "Machine learning for direct marketing response models: Bayesian networks with evolutionary programming," *Management Science,* vol. 52, no. 4, pp. 597-612, 2006.
[69] R. Hardin, *Trust and trustworthiness*. Russell Sage Foundation, 2002.
[70] W. Rodgers, H. L. Choy, and A. Guiral, "Do investors value a firm’s commitment to social activities?," *Journal of business ethics,* vol. 114, no. 4, pp. 607-623, 2013.
[71] K. Starcke, O. T. Wolf, H. J. Markowitsch, and M. Brand, "Anticipatory stress influences decision making under explicit risk conditions," *Behavioral neuroscience,* vol. 122, no. 6, p. 1352, 2008.
[72] L. Schwabe and O. T. Wolf, "The context counts: congruent learning and testing environments prevent memory retrieval impairment following stress," *Cognitive, Affective, & Behavioral Neuroscience,* vol. 9, no. 3, pp. 229-236, 2009.
[73] S. Preston, T. Buchanan, R. Stansfield, and A. Bechara, "Effects of anticipatory stress on decision making in a gambling task," *Behavioral neuroscience,* vol. 121, no. 2, p. 257, 2007.
[74] A. R. Otto, C. M. Raio, A. Chiang, E. A. Phelps, and N. D. Daw, "Working-memory capacity protects model-based learning from stress," *Proceedings of the National Academy of Sciences,* vol. 110, no. 52, pp. 20941-20946, 2013.
[75] S. R. Waldstein and L. I. Katzel, "Stress-induced blood pressure reactivity and cognitive function," *Neurology,* vol. 64, no. 10, pp. 1746-1749, 2005.
[76] J. Brockner, P. A. Siegel, J. P. Daly, T. Tyler, and C. Martin, "When trust matters: The moderating effect of outcome favorability," *Administrative science quarterly,* pp. 558-583, 1997.
[77] S. C. Currall and M. J. Epstein, "The fragility of organizational trust:: Lessons from the rise and fall of Enron," *Organizational Dynamics,* vol. 32, no. 2, pp. 193-206, 2003.
[78] J. H. Dyer, "Effective interim collaboration: how firms minimize transaction costs and maximise transaction value," *Strategic management journal,* vol. 18, no. 7, pp. 535-556, 1997.
[79] J. L. Pearce, I. Branyiczki, and G. A. Bigley, "Insufficient bureaucracy: Trust and commitment in particularistic organizations," *Organization Science,* vol. 11, no. 2, pp. 148-162, 2000.
[80] R. T. Sparrowe, R. C. Liden, S. J. Wayne, and M. L. Kraimer, "Social networks and the performance of individuals and groups," *Academy of management journal,* vol. 44, no. 2, pp. 316-325, 2001.
[81] B. Uzzi, "Social structure and competition in interfirm networks: The paradox of embeddedness," *Administrative science quarterly,* pp. 35-67, 1997.
[82] D. Good, "Individuals, interpersonal relations, and trust," *Trust: Making and breaking cooperative relations,* pp. 31-48, 2000.
[83] R. Dore, *Taking Japan seriously: A Confucian perspective on leading economic issues*. A&C Black, 2013.

[84] R. Singleton Jr, B. C. Straits, M. M. Straits, and R. J. McAllister, *Approaches to social research*. Oxford University Press, 1988.
[85] D. Woodward and T. Woodward, "The efficacy of action at a distance as a control mechanism in the construction industry when a trust relationship breaks down: an illustrative case study," *British Journal of Management,* vol. 12, no. 4, pp. 355-384, 2001.
[86] G. A. Bigley and J. L. Pearce, "Straining for shared meaning in organization science: Problems of trust and distrust," *Academy of management review,* vol. 23, no. 3, pp. 405-421, 1998.
[87] R. J. Lewicki, D. J. McAllister, and R. J. Bies, "Trust and distrust: New relationships and realities," *Academy of management Review,* vol. 23, no. 3, pp. 438-458, 1998.
[88] W. Rodgers, "E-commerce and biometric issues addressed in a Throughput Model," *Hauppauge, NY: Nova Publication,* 2010.
[89] T. Tyler and P. Degoey, "The influence of motive attributions on willingness to accept decisions," *Trust in Organizations, Sage Publications, Thousand Oaks,* pp. 331-356, 1996.
[90] G. Arfaoui *et al.*, "A security architecture for 5G networks," *IEEE Access,* vol. 6, pp. 22466-22479, 2018.
[91] B. Yang, Y. Lei, J. Liu, and W. Li, "Social collaborative filtering by trust," *IEEE transactions on pattern analysis and machine intelligence,* vol. 39, no. 8, pp. 1633-1647, 2016.
[92] M. Nitti, V. Popescu, and M. Fadda, "Using an IoT platform for trustworthy D2D communications in a real indoor environment," *IEEE Transactions on Network and Service Management,* vol. 16, no. 1, pp. 234-245, 2018.
[93] O. O'neill, *A question of trust: The BBC Reith Lectures 2002*. Cambridge University Press, 2002.
[94] J. Flower, "The international integrated reporting council: a story of failure," *Critical Perspectives on Accounting,* vol. 27, pp. 1-17, 2015.

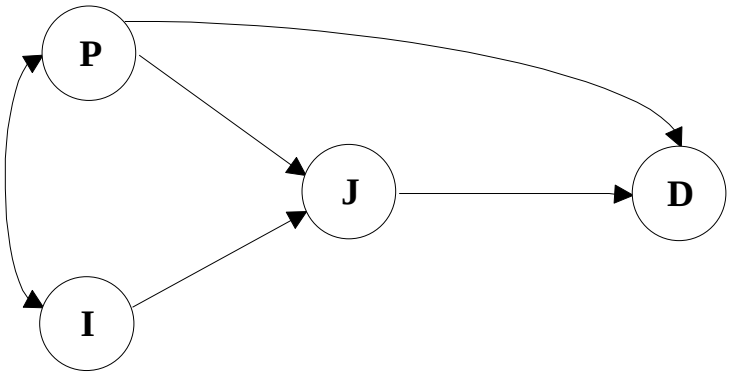
Table 1: Trust positions related to type 1 and 2 errors

Trust Positions	Type 1 Error / False Positive	Type 2 Error / False Negative
(1) Rational-based trust	Overly rigid presumption of other party's desires and intentions; thereby, denying the correct people entering or using cyber system.	Overly accommodating presumption of other party's desires and intentions; hence, allowing the inappropriate people entering or using cyber system.
(2) Rule-based trust	Guidelines and procedures are very strict. Result: prevent admission into cyber system of individuals who should be allowed in.	Guidelines and procedures are too lax. Result: Wrong individual's admission into cyber system.
(3) Category-based trust	Appropriate people in the same social networks (i.e., sharing some common experience, tradition, education, customs, culture, religion, etc.) NOT allowed in the cyber system due to strict system of classification.	Wrong people in the same social networks (i.e., sharing some common experience, tradition, education, customs, culture, religion, etc.) allowed in the cyber system due to WEAK system of classification.
(4) Third-party-based trust	People DENIED use of cyber system due to overly critical use of supporting information sources for reliability and relevance.	People ADMITTED to use cyber system due to weak supporting and relevant information.
(5) Role-based trust	People DENIED use of cyber system due to overly critical formal structures, judging individual attributes.	People ADMITTED to use cyber system due to weak formal structures, judging individual attributes.
(6) Knowledge-based trust	People DENIED use of cyber system due to overly critical evaluation of relevant and reliable information about others to understand them and accurately predict their likely behavior.	People ADMITTED to use cyber system due to weak evaluation of relevant and reliable information about others to understand them and accurately predict their likely behavior.

Table 2: People, processes & technology related to type 1 and 2 errors

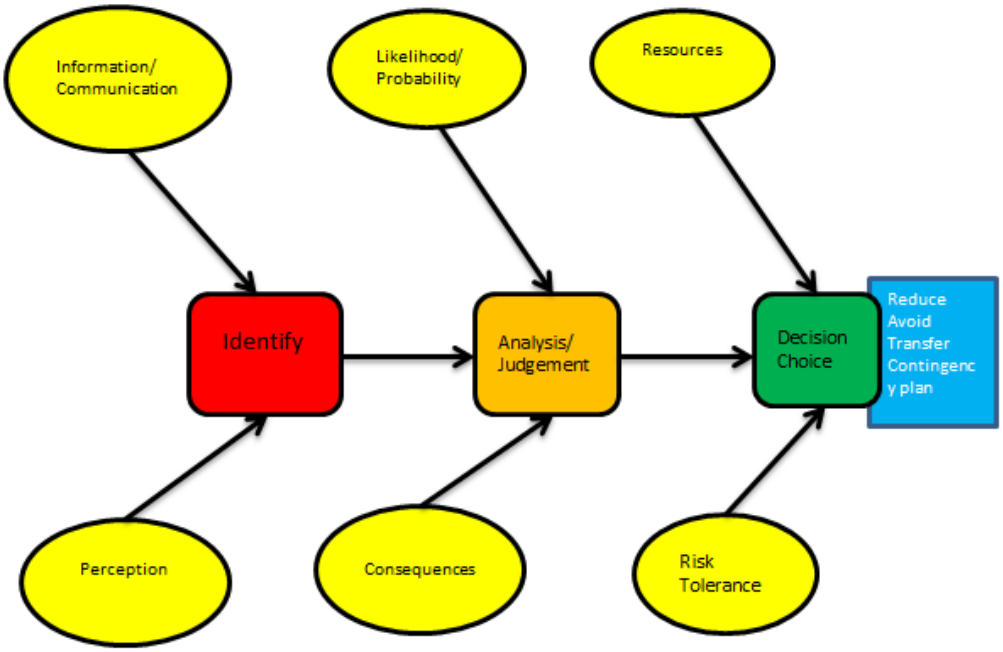
People, Processes & Technology	Type 1 Error / False Positive	Type 2 Error / False Negative
Computer Virus	Manager thinks virus is present when no virus is actually present.	Manager thinks virus is NOT present (manager does nothing) when a virus is actually present.
Cost Assessment	Costs (actual costs plus manager's credibility) associated with scrambling the organisation to find the non-existing virus.	Replacement cost for the damage done by the virus, and replacement cost for a new or modified system.

Figure 1: Throughput modelling process



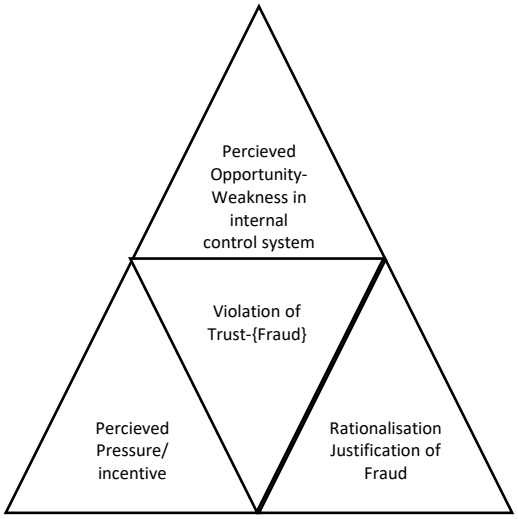
Where P= perception, I= information, J= judgment, and D= decision choice.
Source: Rodgers, 2006

Figure 2: Three key steps in risk management decision choices



Source: Adopted from Rodgers (2006)

Figure 3: Fraud triangle-unfolding the gateway to fraud/cyber-attacks



Source: Rodgers, Söderbom and Guiral, 2014

Title page and author biosketch

1. Professor Waymond Rodgers
Chair Professor of Accounting
Hull University Business School
Department of Accounting and Finance
University of Hull
Cottingham Rd
HU6 7RX
Email: w.rodgers@hull.ac.uk

2. Dr Rexford Attah-Boakye
Lecturer in Accounting
Department of Accounting and Finance
Hull University Business School
University of Hull
Cottingham Rd
HU6 7RX
Email: Rexford.Attah-Boakye@hull.ac.uk

3. **Dr Kweku Adams** ***(Corresponding Author)
Huddersfield Business School
University of Huddersfield
Department of Management
Queensgate
HD1 3DH
United Kingdom
Email: k.adams@hud.ac.uk
Tel +44 (0) 7428 775 516

Authors' Biographies

Waymond Rodgers received a Ph.D. in Accounting from the University of Southern California, and a cognitive psychology postdoctorate from the University of Michigan. He is a certified public accountant in California and Michigan. Professor Rodgers holds a professorship at the University of Texas, El Paso. Professor Rodgers' accounting, banking, and management expertise derives from his employment as an auditor at PricewaterhouseCoopers and Ernst & Young. He was also a commercial loan officer for Union Bank and his portfolio included Fortune 500 companies. He has received numerous research grants such as from the National Science Foundation, Ford Foundation and Citibank. Professor Rodgers has published ten books and in leading journals such as *Accounting Forum, Auditing: A Journal of Practice & Theory, European Accounting Review, Journal of Business Ethics, Journal of the Association of Information Systems, Journal of World Business, Management Science, Organization Studies*, among other journals.

Research interests: Artificial intelligence, auditing, cyber security, commercial lending decisions, decision modeling, ethics, trust issues, intellectual capital, and knowledge management.

Rexford Attah-Boakye, PhD (Accounting), MBA, MSc, FHEA, ACCA, ACICM, CQRM, B. Com (Hons), BMC, QTS, (Maths), TLA (Oxford) is a lecturer in Accounting at the University of Hull. He is also the faculty director of the degree apprenticeship program of university of Hull Business school. Rexford is also a module leader for financial control and information systems in Accounting and finance at university of Hull. As a qualified chartered accountant and a member of four professional bodies including ACICM, CQRM, QTS and FHEA, Dr Attah-Boakye has over ten years experience as Head of Audit of a major bank in Ghana. His His-area of specialty is in integrated financial reporting, accounting and accountability, corporate governance, social accounting, environmental accounting, taxation, auditing, merger and acquisition, quantitative risk management, financial analysis. His His-work has been published in international the *Journal of Finance and Economics and Technological Forecasting and Social Change*.

Dr Kweku Adams is a Senior Lecturer in Management (Strategy) at the Huddersfield Business School, University of Huddersfield. He is a Senior Fellow of the Higher Education Academy and holds a PhD from Swansea University. He has held academic positions in North America. First, as a Lecturer in Strategy and Global Management at the Haskayne School of Business, University of Calgary; and second, as a Visiting Lecturer of Management at the University of Lethbridge School of Management in Calgary, Canada. His research interests centers on business strategy and international business, specifically the management of headquarters-subsidiary relations, investigating the wider governance challenges facing multinational corporations. His work has appeared in outlets such as the *Journal of International Management*, *Critical Perspectives on International Business*, *Thunderbird International Business Review*, *The International Journal of Minerals Policy and Economics*, *The European Journal of Training and Development*, *Employee Relations*, *Technological Forecasting and Social Change*, among others. Dr Adams currently sits on the Editorial Review Board of the *African Journal of Management*.