Insider threat risk prediction based on Bayesian network

Elmrabit, Nebrase; Yang, Shuang-Hua; Yang, Lili; Zhou, Huiyu

Published in:
Computers & Security

DOI:
10.1016/j.cose.2020.101908

Publication date:
2020

Document Version
Author accepted manuscript

Insider Threat Risk Prediction based on Bayesian Network

Nebrase Elmrabit[a], Shuang-Hua Yang[b], Lili Yang[c] and Huiyu Zhou[d]

[a]Department of Cyber Security and Networks, Glasgow Caledonian University, G4 0BA, UK
[b]Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, China
[c]School of Business & Economics, Loughborough University,LE11 3TU, UK
[d]School of Informatics, University of Leicester, LE1 7RH, UK

ARTICLE INFO

Keywords:
Bayesian network model
Insider threats
Predictions
User abuse

ABSTRACT

Insider threat protection has received increasing attention in the last ten years due to the serious consequences of malicious insider threats. Moreover, data leaks and the sale of mass data have become much simpler to achieve, e.g., the dark web can allow malicious insiders to divulge confidential data whilst hiding their identities. In this paper, we propose a novel approach to predict the risk of malicious insider threats prior to a breach taking place. Firstly, we propose a new framework for insider threat risk prediction, drawing on technical, organisational and human factor perspectives. Secondly, we employ a Bayesian network to model and implement the proposed framework. Furthermore, this Bayesian network-based prediction model is evaluated in a range of challenging environments. The risk level predictions for each authorised users within the organisation are examined so that any insider threat risk can be identified. The proposed insider threat prediction model achieved better results when compared to the empirical judgments of security experts

1. Introduction

Insider threat incidents have increased to significant levels (Walker-Roberts et al., 2018). Attacks carried out by insiders are among the more expensive types of information security breaches. According to a recent report by the Ponemon Institute LLC, the average cost per insider incident is £220,000 (Ponemon Institute LLC, 2018). This is because insiders often have good knowledge of the environmental set-up, and ready access to the assets owned by their employers. Such individuals often have the trust of their organisation, which enables them to gain authorised access and bypass electronic and physical security controls (Mills et al., 2017). Nonetheless, more than 75% of these incidents are typically handled internally without being reported to law enforcement agencies, and often no legal action is taken (Cappelli et al., 2012).

A socio-technical approach employing multi-perspective concepts to aid the assessment of new and existing technologies was initially proposed by Linstone (Linstone, 1981) during the 1980s. Socio-technical methodologies identify interactions between people and technology, whether in the workplace or more generally in society. McCumber et al. (McCumber, 1991) applied this approach in a security context, presenting a security measure model for understanding the complex issues inherent in ensuring that information is secure. They identified three dimensions to this: (a) policy and practice, (b) technical, and (c) education, training and awareness.

Recently, Greitzer et al. (Greitzer et al., 2018) proposed a knowledge-based ontological framework of individual and organisational socio-technical factors that might be used to evaluate insider threats, which they referred to as SOFIT (Socio-technical and Organizational Factors for Insider Threat). This framework integrated several indicators previously reported on in (Greitzer et al., 2016) and imported from Costa et al.'s Insider Threat Indicator Ontology ITIO (Costa et al., 2016). Their framework demonstrates that non-technical controls can enhance the mitigation of the potential malicious insider activity. It is rare, however, to see an insider threat approach that has implemented this concept of addressing the problem from multiple perspectives in a real demonstration.

This paper focuses on presenting a comprehensive risk prediction framework that considers malicious insider threats. We develop the new prediction framework based on the outcomes of the research literature reviewed in Section 2. Bayesian Network (BN) based statistical methods are used to model and implement the prediction framework.

The rest of this paper is organised as follows. Section 2 presents the background and related work on insider threat detection. Section 3 presents the framework for insider threat risk prediction, where Bayesian network methods are used to construct the prediction model. Section 4 reports on case studies to predict potential insider threats, and Section 5 verifies and validates the prediction model. Finally, the paper is concluded and future work is presented in Section 6.

2. Background

Although significant work has taken place in recent years, relatively little progress has been made overall in mitigating insider threats (Walker-Roberts et al., 2018). Malicious insider threat activities may be detected by indi-

*Corresponding author: Nebrase Elmrabit (e-mail: nebrase.elmrabit@gcu.ac.uk
**Corresponding author: Shuang-Hua Yang (e-mail: yangsh@sustech.edu.cn [yangsh@sustech.edu.cn]).
ORCID(s):

viduals who are not part of the organisation's security staff. This is evidenced in (Keeney et al., 2005; Zeadally et al., 2012), where it is shown that only one in five occurrences of such activities are detected using a combination of automated tools for logging, monitoring and flagging suspicious activities along with manual diagnosis and analysis.

2.1. Definition of an Insider Threat

In order to arrive at a definition of an insider threat, we need to understand what an insider is, and what a threat means in the context of information security.

Firstly, what is an insider? The Advanced Research and Development Activity (a research organisation within the US intelligence community) held a major workshop in 2004, where the insider was defined as: "an already trusted person with access to sensitive information" (Brackney and Anderson, 2004) . Greitzer et al. (Greitzer et al., 2008), meanwhile, defined insider as "an individual currently or at one time authorised to access an organisation's information system, data, or network". Additionally, Bishop et al. (Bishop et al., 2008) defined an insider in terms of how s/he is trusted with respect to the assets of an organisation: "an insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure".

On the other hand, a threat refers to anything that has the potential to cause serious harm or damage to an organisation's IT systems or assets.

In this paper, we refer to insider threats as: "malicious or unintentional activities on the part of an employee (current or former), contractor or trusted business partner, who has, or has had, authorised access to the organisation's IT assets, that cause damage to the organisation's assets and/or has a significant negative impact on the information security elements of the organisation (i.e. confidentiality, integrity and availability of information)" (Elmrabit, 2018).

2.2. Insider Threat Categories

In our previous study (Elmrabit et al., 2015), we categorised insider threats into seven categories, based on how they can affect the organisation's information security goals (i.e. confidentiality, integrity and availability of information), and on the human factors which may potentially lead an insider to act in a malicious manner (motive, opportunity and capability).

Insider threat categories were also constructed in terms of their impact, and the actions that malicious insiders might use in order to achieve their aims. These are as follows: IT sabotage, fraud, theft of intellectual property, social engineering, unintentional insider threat incident, insider in cloud computing, and insider national security.

2.3. Current Insider Threat Mitigation Approaches

There are various approaches to the mitigation of malicious insider attacks and their causes. We classify these approaches into two different categories: (a) technical mitigation approaches, and (b) non-technical mitigation approaches.

2.3.1. Technical Approaches

In the category of technical approaches, there are two main sub-categories based on the techniques available to detect insider threats. The first sub-category involves detecting any unauthorised activity, while the second sub-category involves identifying any changes in behaviours that may lead to a malicious insider threat. Both of these sub-categories are operated based on digital devices or network operations (Elmrabit et al., 2015).

Although Intrusion Detection Systems (IDS), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), Access Control Systems (ACS), or honey-tokens are all technical controls designed to prevent attacks from unauthorised users from outside an organisation, they can also be used to identify and mitigate insider threats (Kandias et al., 2013; Chen et al., 2012).

IDS was first used to detect external malicious intruders by analysing any abnormal behaviour or activity in networks or endpoints through matching activities and traffic patterns with a database of attack signatures.

Virtual Private Network (VPN) data flow monitoring (Cappelli et al., 2012), Web traffic inspection (George J. Silowash, Todd Lewellen, 2013), and Correlating Events from Multiple Sources such as Universal Serial Bus (USB) (Silowash and Lewellen, 2013), are different types of DLP security controls. All of these controls can be used to mitigate insider threats by analysing information about changes in the behaviour or activities of authorised users.

SIEM is a single point management platform used to centralise and analyse data harvested from various security-related logs, such as servers, workstations, network devices, antivirus software, firewalls, honeypots, DLP, IDSs, and other sensors in the network. Any instances of recorded network activity are then checked against a database by matching a particular event or related characteristic. Utilising such an approach allows for the organisation to search for events quickly, potentially identifying malicious insider activity before it happens. Additionally, the database can provide a rich source of evidence for forensic investigations that may take place once an incident has occurred (Silowash et al., 2012).

Spitzner (Spitzner, 2003), meanwhile, discussed several strategies and technologies that may be adopted for the detection, identification and gathering of information related to authorised user breaches based on honey-token approaches.

2.3.2. Non-Technical Approaches

Proposing a model intended to predict insider threats, Axelrad et al.(Axelrad et al., 2013) defined eighty-three psychological variables which can potentially relate to insider threats. They analysed these variables, then estimated a scoring power for each variable. Variables include: dynamic environmental stress, personal characteristics, insider actions and the degree of interest. Greitzer et al. (Greitzer and Ho-

Table 1
Summary of Approaches to Insider Threats

Categories	Approaches	Benefits	Limitations
Technical	Intrusion Detection Systems	Network & endpoint devices. Matching attack signature. Detection of abnormal behaviour. Analysis activity in real-time.	Primarily focused on external attackers. High false alarms. Log file size is huge. Limitations in dealing with encrypted traffic.
	Security Information and Event Management	Activities & logging centralised in one platform from various network sensors. Analysis of activities by matching any related events with characteristics.	Implementation complexity. Can detect insiders after the breach occurs. High level of false alarms.
	Data Loss Prevention	Data exfiltration attempts can be detected early. Real time policy enforcement. Keyword matching, regular expressions or hashing fingerprinting.	Some limitations in inspecting encrypted traffic. Not reliable in detecting unsupported file formats.
	Access Control System	Manages and controls access credentials in various platforms. Change user authorisation access level, or deny access at any time.	Insider threat already has access to the systems. Social engineering.
	Honey-tokens	Malicious attraction. Detect, identify and confirm a malicious insider threat. Interactive digital entity.	Could have no interaction as the potential insider knows the trap.
Non-Technical	Psychology Prediction Model	Predicts a potential insider threat before the breach occurs. It can differentiate between malicious and unintentional insider threats. Helps decision makers to determine if the user is a potential risk.	Complexity of data integration from various platforms. High false alarms. Complexity of implementation in real systems.
	Security Education and Awareness	Reduces unintentional insider threat accidents. Makes employees more responsible for their actions. Improves employee behaviour. Users can identify and respond appropriately to security concerns.	High cost for small businesses
	Information Security Policy	Helps to achieve cyber-security best practices.	Employees do not follow organisation's security policies.
		Detailed statement of acceptable behaviour within the organisation.	Cyber-security policy may not be understandable to all users.

himer, 2011; Greitzer et al., 2012) proposed another classification model based on case studies of previous insider crimes. Their approach started by setting up twelve psychosocial risk factors associated with insider threats.

Yang et al. (Yang et al., 2008) proposed the first integrated framework between three perspectives in the employee security risk assessment, namely: technical, organisational and human perspectives, with the security vulnerabilities being identified based on the BS ISO/IEC 27001 standard.

Pfleeger et al. (Pfleeger et al., 2010) presented a framework for describing insider threat behaviours and actions, based on four perspectives: the organisation, the environment, the system and the individual. Moreover, their framework is designed to categorise different insider threats according to how they interact with the defined attributes. Yaseen and Panda (Yaseen and Panda, 2010), meanwhile, introduced the Threat Prediction Graph (TPG) to predict and prevent insider threat}textcolorredss.

Kandias et al. (Kandias et al., 2010) proposed a prediction model that consists of two aspects. The first of these is psychological profiling, which includes the user system role, capability, predisposition and user stress level. The second is the real-time use of profiling, which also includes: system calls monitoring, intrusion-detection systems and honeypots. Authorised users' motives, opportunities and capabilities are scored according to these two aspects in order to determine whether they are a potential insider threat or not. Liu et al. (Liu et al., 2008) proposed a prediction technique for insider threat identification based on a game-theoretic model, which they called "an insider game", intended to help organisations to understand malicious insiders' motivations and decision-making processes, and then to identify the optimal defence strategy.

Cyber-security education and awareness training may avoid unintentional insider threats (Shaw and Fischer, 2005). It was found in a report by The Ponemon Institute (Ponemon Institute, 2014) that "62% of organisations conduct regular privileged user training programs as part of their efforts to protect the organisation from insider threats, with 11% of the IT budget allocated to security education and awareness".

The Cyber Security Centre at the University of Oxford (Buckley et al., 2014) carried out a study that focused on organisations' information security policies and their ability to mitigate the severity of a malicious insider threat. They suggested that that the risk posed by a threat originating from the 'unintentional insider threat' category is potentially more severe than that posed by some of the other identified categories. Further to this, their results suggested that there are two key reasons why 45% of employees do not follow security policies: (a) the policy was poorly or incompletely defined;(b) the security policy was not known to the employee in question. They concluded that if information security policies put in place by an organisation are not followed by a large number of authorised users this can result in an increased risk of unintentional insider threats.

Based on the previous paragraphs, we summarise in Table 1 both the limitations and benefits of each of the insider threat approaches that are detailed within this section.

Furthermore, based on this review, we can conclude that we should deal with malicious insider threat from different angles; we note however that no singular approach can entirely solve the problem. This particular observation will drive more research in the area of insider threats to cyber-security, in an attempt to understand the nature of those threats, as well as identify the right approach for tackling them. In the next section, we put forward a proposal for a new model and provide details as to its implementation. The aim of the proposed model is to provide organisations with a means of preventing insider threats, as well as a means of dealing with any potential insider breaches before they occur.

3. Proposed Method

3.1. Conceptual Model for Insider Threat Predictions

Insider threat risk prediction is a complex task for the research community to address, and recent studies such as those of (Greitzer et al., 2019, 2018; Legg et al., 2017) have started to consider insider threat issues from a different perspective of attempting to mitigate the risk of insider threats. Our work is inspired by the methodology proposed by (Kasanen et al., 1993) in combination with an empirical Bayes' method (Pearl, 1985). Our proposed framework for insider threat risk prediction is shown in Figure 1, and considers technological aspects, organisational impact, and human factors.

3.1.1. Technological Aspects

Most medium and large sized organisations have their own Information Technology (IT) departments, one of whose tasks is to protect the organisation's information assets from all types of security breach (Fenz et al., 2007), e.g. intellectual property (IP) data leaks. The technological aspect of our approach has the goal of ensuring that the IT department within the organisations under consideration is able to deal with such breaches. To that end, information was collected about the organisations' IT security measures and we then considered those particular measures seeking to ensure that insider threat breaches are kept to a minimum. In order to measure the level of these technological factors, we placed the collected information into one of the following three categories:

- Investment Balance: The balance between investment in insider and outsider threats is the key to determining the extent to which executive managers are aware of insider threat breaches. In this category, we considered security awareness and training, as well as budget spending aimed at minimising the threats from malicious or unintentional insider actions. (Colwill, 2009; The Department for Business Innovation and Skills, 2013; The UK National Cyber Security Programme, 2015)

- Detection level: One important aspect is the measurement of how accurate detection systems have been with regards to previous insider attacks. To measure this, the ratio of false alerts to legitimate ones was considered, as well as the techniques that were previously used to detect insider threats (if any had occurred) (Spitzner, 2003; Hart et al., 2011).

- Security and privacy controls: This category focuses on forensic evidence; for example, network traffic and email logs (Cohen, 2012). Additionally, we measured system integration in terms of insider threat detection, technical tools and controls (such as security information and event management), and data loss prevention, which organisations commonly use to avoid security breaches (Greitzer et al., 2010; Kandias et al., 2010; Zeadally et al., 2012; Costante et al., 2017).

3.1.2. Organisational Impact

The UK's Centre for the Protection of National Infrastructure (CPNI) (Centre for the Protection of National Infrastructure, 2013) has found that "where an insider act takes place there is often an exploitable weakness with the employer's own protective security or management practices which enables the insider to act". It can be concluded that it is important to identify any organisational issues that might increase the risk of insider threats.

Within the framework proposed in this paper, any information related to the way in which an organisation is structured, as well as how insider threat breaches are managed, are represented by the organisational impact dimension. In order to measure the level of the organisational aspect level, we collected information in the following four categories:

- Security breaches: Here, we focused on security breaches that have occurred historically within the organisations. We also collected any information regarding accidental/malicious insider breaches that may have occurred during last five years (The UK National Cyber Security Programme, 2015). The other element within this category was actions taken by the organisations with regards to any previous breaches (Negroponte, 2013).

- Structure: We collected information about recruitment procedures, previous employment screening, as well as any information pertaining to the outsourcing of services by the IT department (Centre for the Protection of National Infrastructure, 2013).

- Security policy: This encompasses all the information related to the organisations' security policies: whether there is one and if they believe that all the authorised users follow it or not. (Buckley et al., 2014)

- Employee work-related stress symptoms: In this category, we collected information related to visible stress symptoms of employees overall such as evidence of increasing numbers of accidents, increasing rates of long-term illness, and poor performance in tasks. (Palmer and Cary, 2013)(Axelrad et al., 2013)

3.1.3. Human Factors

The weakest link in any information security chain is always considered to be the human factor, and this has resulted in increasing attention being paid to human factors in the context of insider threats; mainly where the use of security technologies has failed to protect organisations from malicious insider threats (Herath and Rao, 2009; Hadlington, 2017). It has been argued by researchers that insiders have specific psychological characteristics (behavioural indicators) that need to be considered when measuring the severity of insider threat risk (Nurse et al., 2014) (Bell et al., 2018).

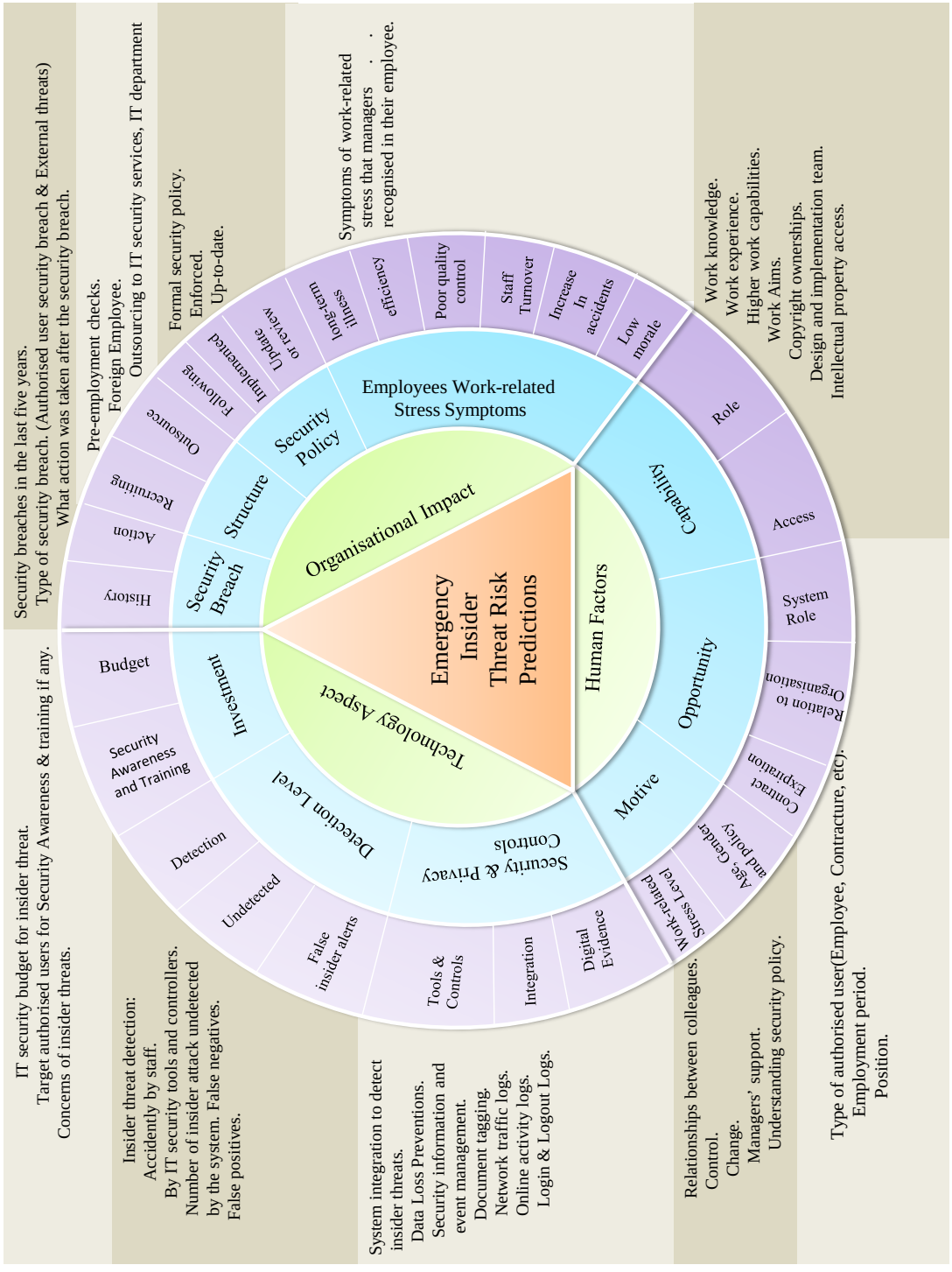


Figure 1: Framework for Insider Threat Risk Prediction

In this aspect, Wood's assumption (Wood, 2000), is used to calculate each authorised user's psychological profiling level. Three factors are required before a malicious insider misuses his or her privileges. These are: Motivation, Opportunity and Capability. In order to calculate these levels, our model was designed with the following assumptions:

- Motivations that drive an employee to launch a malicious attack are complex and multifaceted, making them difficult to measure. Within our framework, we measured motivations by work-related stress levels. For example, we considered the attitude of authorised users towards the workplace, the support that employees receive from their line manager or colleagues, relationships between colleagues, and employee knowledge of the organisational security policy. Also, employee age and gender affect the motivation levels (Palmer et al., 2001; Centre for the Protection of National Infrastructure, 2013; Greitzer and Hohimer, 2011; HSE; Nurse et al., 2014).
- Opportunities inform the likelihood of authorised users enacting a malicious insider threat, since humans are expected to realise their intentions should an opportunity arise. In the proposed framework, opportunities were measured by contract expiration dates, authorised user system role, as well as the employee's relationship to the organisation they work for (for example, a current employee, former employee, contractor, etc.) (Centre for the Protection of National Infrastructure, 2013; Moore et al., 2011; Silowash and Lewellen, 2013; Ghaffarzadegan, 2008).
- Capability refers to the skill and ability of an employee to carry out/enable different kinds of security breach. Insiders have privileged access rights to data assets owned by the organisation (potentially for extended periods of time), and this can potentially give these authorised users the ability to know and understand the security measures in place. We measured the capability levels through, for example, employees' access rights to intellectual property and their work knowledge (Bartram and Turley, 2009; Moore et al., 2011; Kandias et al., 2010).

3.2. Modelling for Insider Threat Risk Prediction

This section describes how we utilised a Bayesian network as a statistical method to model and implement the proposed framework. We describe the probabilistic relationships between all the factors (Human, Organisation, and Technology) by using a directed acyclic graph. Each factor then has a dependence relation with other variables in various layers.

Judea Pearl coined the term Bayesian Networks (BN) in 1985 (Pearl, 1985). In recent years, many insider threat approaches have started to use this statistical method to implement their models. For example, Greitzer et al. (Greitzer et al., 2012) deployed a psychosocial model to assess employee behaviours associated with an increasing risk of insider abuse based on a BN model. Also, Axelrad et al.(Axelrad et al., 2013) introduced a BN model for the motivation and psychology of malicious insider threats.

Recent work by Sticha et al. (Sticha and Axelrad, 2016) introduced the integration of two modelling approaches (Bayesian belief networks and system dynamics models) each of which have different strengths in respect to addressing the problem of insider threats. Moreover, BN is an increasingly popular modelling technique in cyber-security fields such as forensic, risk management and smart grid security, (Chockalingam et al., 2017; Ross et al., 2017; Poolsappasit et al., 2012; Wadhawan et al., 2018).

We consider a Bayesian prediction model in this study since the previous study by Greitzer et al. (Greitzer et al., 2012) indicates that BN outperforms other approaches such as Artificial Neural Networks, Linear Regression, and Counting Model, since it can handle missing values by using the prior probabilities.

Three stages were taken to implement and develop the model for the proposed framework as follows:

Stage 1: Network Construction

The prediction model is represented as a Directed Acyclic Graph (DAG) of variables denoted by $X = \{X_1, X_2, \ldots, X_n\}$, where each node represents a single random variable.

The graph network was constructed using Bayes Server Software[1] in the experimental environment, which enabled us to link the related nodes that have a conditional relationship between them. On the other hand, nodes that were not linked were considered as conditionally independent. Moreover, for each node, we had conditional probability tables (CPT) each of which described the conditional probability of the underlying random variable conditioned on its parent. Finally, all the links were directed from the parent to the child node.

Based on the conceptual model for insider threat prediction described in Section 3.1 and visualised in Figure 1, a full network model was structured, using the Bayes Server Software (Refer to Appendix B for the full insider threat prediction network graph). The network starts with the central main parent node, called "the emergency insider risk prediction (E)", and then moves into the three diminution nodes until it reaches the final child node of each parent, where each parent node has a CPT with a link pointing to the child node. An example of this is illustrated in Figure 2, which shows the part of the network model related to the human factor. In this figure, the end nodes, such as the Gender node, represent the collected data input with a single value, where the age, gender and policy node can be a parent node for the Gender node, and a child node for the Motive node. Also, the Human Factors (H) node is the parent node for the Motive node and a child node for the central node of the network.

[1] **Bayes Server** Version 6.17 is a tool for modelling Bayesian networks and Dynamic Bayesian networks. This software is widely used in the fields of Machine Learning, Data Science, Artificial Intelligence, Big data, and Time Series Analysis.

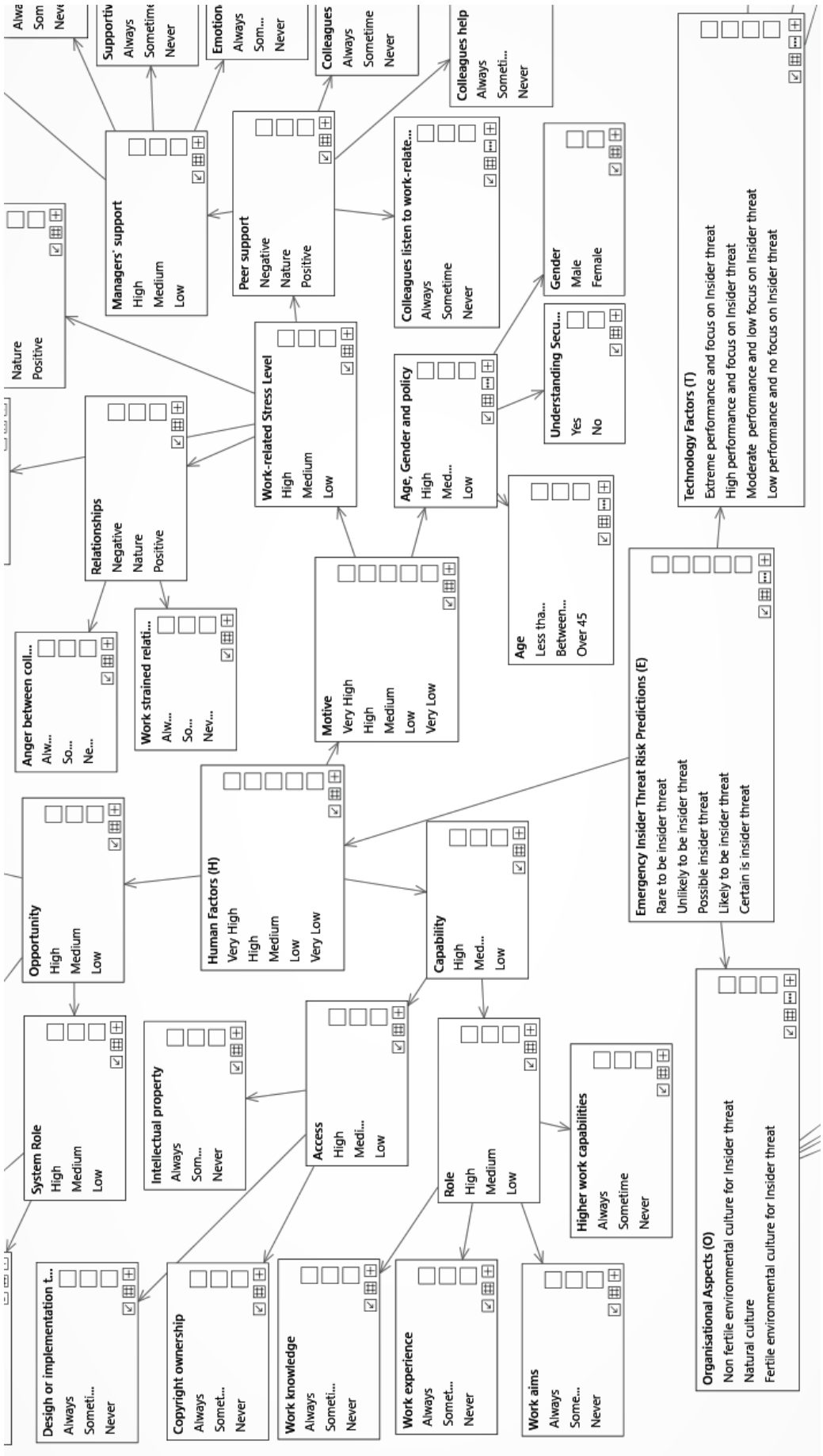


Figure 2: Part of the Insider Threat Risk Prediction Model Network

Table 2
Estimating Conditional Probability for the Gender Node.

Variables	Gender	
Age, Gender and Policy	**Male**	**Female**
High	0.82	0.18
Medium	0.5	0.5
Low	0.18	0.82

Table 3
Estimating Conditional Probability for the Access Node.

Variables	Access		
Capability	**High**	**Medium**	**Low**
High	0.7	0.3	0
Medium	0.2	0.6	0.2
Low	0	0.3	0.7

Stage 2: Estimated Conditional probabilities

After creating all the nodes, and linking each child node to its parent's node, we then determine conditional probabilities to each random variable in the network.

The procedure of assigning the conditional probability can be done based on data collected from different sources, such as surveys and publications. For example, the gender node has two variables (male and female) with one line directly connected to the parent node "Age, Gender and Policy", as shown in Figure 2. We set the conditional probability based on the evidence sourced from (Centre for the Protection of National Infrastructure, 2013) (Moore et al., 2011), which indicates that for malicious insider activities in which the gender of the perpetrator was know, 82% were committed by males, while 18% were committed by females. Using these two sources, we assigned the conditional probability to the gender node as shown in Table 2. In this case, the two sources gave the same information; in some other cases, however, the values reported differ between sources and in these cases we used the most recent publication source.

On the other hand, in some cases that no evidence available "non-informative" or "reference" data appears, we manually set the conditional probabilities using a number of heuristics (Sticha and Axelrad, 2016). In these cases, we set the conditional probabilities based on our empirical experience. For example, the node Access shown in Figure 2 has three variables (high, medium and low), with one link directly connected to the parent node "Capability" and three links to the child nodes. In this case, we set the conditional probabilities based on our experience and then manually established the best fit value where the best prediction result was obtained. Table 3 shows the estimated conditional probability for the Access node in the human factor domain. Another example from Figure 2 is that we assigned the same value of 0.2 to all five variables at the central node (E), thus summing to 1.

Stage 3: Risk output.

The purpose of this step in the Bayesian network deployment is to measure the effect of the random variables on each internal node until one arrives at the central node, which is called the Emergency Insider Threat Risk Prediction **(E)**. A small section of the risk prediction central node can be seenin the bottom middle of Figure 2.

Algorithm 1: Algorithm to compute the risk prediction result

Input: Prior Probability $P(Y_y)$; likelihood $P\left(X_i|Y_y\right)$ Where $i = 0, 1, 2 \dots n$ $y = 0, 1, 2 \dots k$.
As: k represents all the possible outcomes of Y.
n is the number of independent variables connected to the node Y.

Output: Prediction results

1 **foreach** *node of* Y **do**
2 Compute the posterior probability of $P\left(Y_y|X_1, X_2 \dots X_n\right)$ using Naive Bayes probability equation $= P\left(Y_y\right) \frac{\prod_{i=1}^{n} P(X_i|Y_y)}{\sum_y \Pi_i^n P(X_i|Y_y) P(Y_y)}$
3 Record the update of $P\left(Y_y|X_1, X_2 \dots X_n\right)$ and then propagate forward through the network. ;
4 Record the result of $P\left(Y_y|X_1, X_2 \dots X_n\right)$ as the probability of the insider threat.

Algorithm 1, can be used to calculate the probability of an insider threat ***(E)*** given the human factor ***(H)***, organisational impact ***(O)***, and technological aspect ***(T)***. We generated the formula for this based on the following Bayesian theory:

$$P(E \mid H, O, T) = P(E) \frac{P(H \mid E)\ P(O \mid E)\ P(T|E)}{\sum_i \left[P(Ei)\ P\left(H \mid E_i\right) P(O \mid Ei)\ P(T|Ei)\right]} \quad (1)$$

Where $P(E)$ is the probability of an insider threat for a certain risk level. $P(H \mid E)$ is the probability of the human factor given the probability of the insider threat at a certain risk level. $P(O \mid E)$ is the probability of the organisational impact given the probability of the insider threat at a certain risk level. $P(T \mid E)$ is the probability of the technology aspect given the probability of an insider threat at a certain risk level.

$\sum_i \left[P\left(E_i\right) P\left(H \mid E_i\right) P\left(O \mid E_i\right) P\left(T|E_i\right)\right]$ is the sum of the probabilities for all the risk levels from a very low risk of an insider threat.

This output $P(E \mid H, O, T)$ is the final prediction of the risk of an employee acting as a malicious insider threat.

To get a comprehensive result, we divided the results for the risk levels into five bands: certain (continually experiencing threats from malicious insiders), likely (security breaches caused by malicious insiders will occur frequently), possible (breaches from malicious insiders will occur sometimes), unlikely (breaches from malicious insiders will be unlikely to occur), and rare (it is highly unlikely that security breaches caused by insiders will occur, i.e., almost never).

4. Case studies

4.1. Survey Data Collection

This section describes the process of data collection and analysis undertaken in order to execute the proposed model to help organisations to discover potential malicious or unintentional insider threats.

4.1.1. Survey Questionnaires to Reveal Data Requirements)

A quantitative methodology was employed in order to carry out this research. Data collection was carried out using questionnaires in the form of surveys. Three surveys were designed, based on each of the three aspects of the prediction model (human factor, technological aspect, and organisational impact). All the authorised users were required to answer the human factor survey, whilst the organisational impact survey was answered by the department responsible for human resources, and the technology aspect survey was answered by the IT department. The surveys were based on the best strategies published in the literature, as follows:

- It was made clear to respondents that the survey was being conducted in order to run the proposed model.
- The survey was designed in such a way that it was easy for the respondents to answer: Multiple-choice questions were employed, and there was an added option of using a text box for the respondents to add any extra information if they wished.
- Where possible, we ensured that the survey followed a logical flow by grouping questions covering similar topics together. Sometimes, however, a mixed question flow was utilised in order to be able to check the consistency of respondents' answers.
- Since not all security breaches are reported to either Information Technology departments (IT) or Human Resources departments (HR), in the the technological and organisational surveys we listed seven questions that were each in some way related to previous security breaches.
- Questions were ordered based on simplicity; i.e. we made the first question easy and interesting in order to engage respondents with the survey, thereby increasing the chances of them completing the entire survey with accurate and consistent answers.
- An online survey platform `https://www.qualtrics.com/` was employed so as to to make the survey readily accessible to respondents.
- Before the respondents begun answering any questions, a short but clear introduction was displayed in order to brief them.
- The survey was piloted with a small group of people before it was given to the entire group. This was to gather feedback regarding layout, overall flow, and time needed to complete the survey. The results generated by these pilot respondents were also checked to ensure that their answers could provide initial values for all the variables.

4.1.2. Data Collection

High-quality raw data was collected from two organisations: one from the education sector and a second that was a small enterprise. Both of the targeted organisations are based in the United Kingdom.

The human factor survey was circulated to fifteen heads of departments and managers, within the education sector organisation. They were also asked to forward the link to the survey to all their staff members within their respective departments. The majority of the heads of departments complied with this request.In summary, 70 responses were received from authorised users in respect to the human factor survey.

In order to gain information for the technology aspect survey, we conducted an interview with the IT Services manager, as well as an interview with the head of the Human Resources department for the organisational impact survey. This enabled us to answer all the organisational impact and technology aspect questions.

For the small enterprise, we conducted an interview with the company director. This was to collect answers related to the technology aspect as well as the organisational impact. The human factor survey was open to all the employees, who were actively encouraged to respond to the questions. There were twelve responses to the human factor survey in total.

4.1.3. Data Processing and Exploitation

During this phase of the study, the collected survey data was structured so as to be compatible with the software employed for analysis. This process was divided into three steps: Data Organisation, Data Processing and Data Exploration. Each of these steps is summarised in the paragraphs below, and Figure 3 shows the overall data processing and exploitation method.

- Data Organising: The data initially obtained had to be processed or organised for better analysis. Specifically, this involved converting the collected survey responses into a format compatible with Bayes Network Software (Bayes Server) and exporting all the collected raw data onto one data set file. In this step, we created a single data file for each organisation that integrated all the responses to each of the human factor variables and the responses to the technological and organisational aspects.
- Data Processing: During this phase, the aim was to cleanse the data by identifying invalid values or corrupted data within the data set that was generated during the Data Organisation step.

  Once all the aspects were integrated into the data set, variables within that data file were reviewed individually. For each variable, a valid range of values was determined. SPSS software was employed for this. For

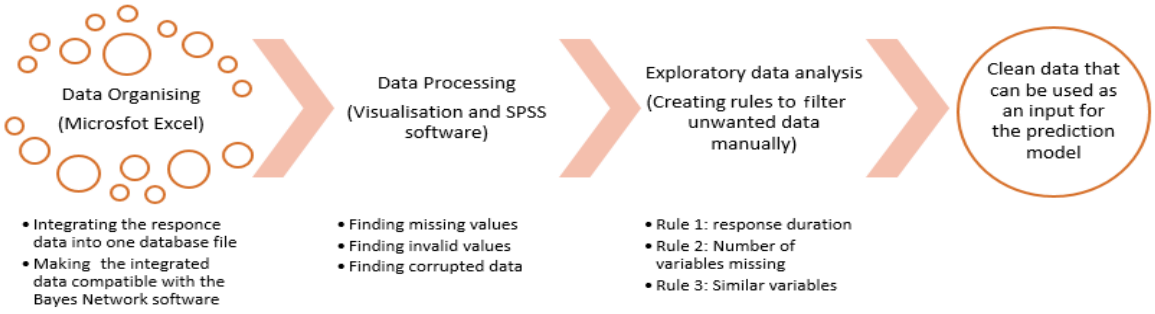


Figure 3: Data Processing and Exploitation Method

Table 4
Technological Factor Predictions

	Indicator	State	Reason
Education Sector	Investment	Low	Organisation spends less than 5% of its cyber-security budget on insider threats
			No attention from the top management regarding insider threats.
			providing no security training or awareness to authorised users.
	Detection Level	High	Most insider threat alerts are true (Over 90%).
			Detected all insider breaches.
	Security and privacy controls	Medium	Records of Emails, online activity, network traffic,etc. are logged.
			Extra security measures are taken during authorised users' termination periods.
			Use of security tools such: Proxy Server, IDS, SIEM, ACL, etc.
			No system integration to discover insider threat.
Small Enterprise	Investment	Low	Organisation spends less than 5% of its cyber-security budget on insider threats.
			No attention from the top management regarding insider threats.
			No security awareness and training is provided.
	Detection Level	Low	No tools to detect insider threats.
			(Missing two values since these were not entered).
	Security and privacy controls	Medium	Emails are logged.
			Extra security measures are taken during authorised users' termination periods.
			Use of security tools (ACL only)
			No system integration to discover insider threats.

the education sector organisation, 42 responses were fully completed, 27 had missing variables, and one contained no data at all. The same steps were then carried out for the small enterprise; here we found that seven responses were fully completed, five had some missing variables, and again, one had no data at all.

In the education sector, most variables within the survey questionnaire were over 90% completed. It should be noted, however, that in the case of the last three variables less than 30% were completed. For the small enterprise, most of the variables were completed, with the exception of "Contract Expiration". With the last three variables, we also found that less than 10% were incomplete.

- Exploratory data analysis: During this step, verification rules were created, and then applied to a combination of variables by defining a logical model to flag up any invalid values within the data.

  Our first rule was to invalidate responses that were finished in less than two minutes. During the pilot survey process described earlier, it was found that the average time taken to complete this section of the survey was four minutes. In the case of the education sector organisation only four surveys were completed in less than two minutes. These were removed from the analysis. For the small business organisation, no survey was completed in less than two minutes.

  The second rule was used to ascertain whether or not more than three of the 29 variables in the human factors survey were missing. If more than three variables were missing, then the completion percentage for that survey response was less than 87%, and therefore these survey responses were not used in our final analysis. We observed that there were four survey responses matching this rule from the education sector, and these were hence removed. Again, for the small enterprise organisation, no survey response omitted more than three variables.

  The purpose of the third rule was to identify any invalid/suspicious survey response by looking into the

Table 5
Organisational Aspect Predictions.

	Indicator	State	Reason
Education Sector	Security Breach	Medium	In the last five years there were no authorised user breaches of any type.
			In the last five years there was at least one accidental insider breach.
			When authorised user breaches occurred no action was taken.
	Structure	Medium	No pre-employment checks.
			Parts of IT services are outsourced.
	Security Policy	Medium	No enforcement system.
			Update or review every five years.
	Work-related Stress Symptoms	Medium	Some indicators indicate: (high turnover, increase in long-term illness, low morale, etc.)
Small Enterprise	Security Breach	Medium	Authorised user breaches in the last five years.
			Breach of intellectual property .
			When authorised users breaches occurred, action was taken.
	Structure	Medium	No pre-employment checks.
			Outsourced IT services.
	Security Policy	Low	Undefined security policy
	Work-related Stress Symptoms	Low	A single indicator indicates that deadlines are not being reached.

questions related to stress levels. By finding out whether or not their values were identified, an additional aspect of this step was to ensure that there was no duplication in the final data set.

4.2. Insider Threat Risk Prediction Results

The outcome of the predication was intended to inform decision making aimed at avoiding potential security breaches caused by insider threats. This was achieved by indicating which employees within the organisation had the potential to become a malicious insider. This could be identified from the technical, organisational and human factor aspects within the organisation and requires attention from a team within the organisation. The outcome helps the organisation to improve their defences and mitigate the level of such threats. In this section, we will present the prediction results regarding insider threats for each of the three perspective before offering an overall evaluation of the organisations in which we conducted the survey.

4.2.1. Analysis of Technological Aspects

For the purpose of demonstration, we have divided the technological factor prediction results into four risk levels based on the organisation's performance and its measures for detecting any potential insider threat. From lower to higher risk, these levels are:

- Extreme performance and focus on insider threats.
- High performance and focus on insider threats.
- Moderate performance and low focus on insider threats.
- Low performance and no focus on insider threats.

For the education sector organisation, the proposed model predicts, a "moderate performance and low focus on insider threats". For the small enterprise, however, it predicts "Low performance and no focus on insider threats" . This is because of the effect of thirty end node variables that were imported from questions on the survey that were related to this particular organisation. The state of each one of the leading indicators, along with the key reasons why these levels are achieved by the model can be seen in Table 4.

4.2.2. Analysis of the Organisational Impact Aspect

The prediction results for the organisational aspect were divided into three distinct risk levels, based on how both the culture and the environment within the organisation can affect the risk of potential insider threats. The levels (from low to high) are outlined below:

- Non-fertile environmental culture in respect to insider threat.
- Neutral culture.
- Fertile environmental culture in respect to insider threat.

A "neutral environment" was predicted by the model for both the small enterprise and the education sector enterprise. The Table 5 shows the states of the indicators, as well as the reasons behind each of these predictions.

4.2.3. Analysis of the Human Factor Aspects

There were five prediction levels for the human factor aspect, based on how the personal characteristics of each employee inform his/her potential to be an insider threat. These levels are presented from higher to lower risk levels as shown in Figure 2. In this factor, as we have explained earlier, we consider all of the organisation's employees, each of which were assigned an anonymous case number.

4.2.4. Insider Threat Prediction Based on Multiple Perspectives

As described, the overall insider threat risks must be predicted from all the perspectives. For the education sector organisation, Table A2 "Appendix A" illustrates the final result of the proposed prediction model. The first column displays the case numbers ranging from 0 to 69, with the missing cases being those deleted during the data processing and exploitation phase, as discussed in section 4.1.3. The last five columns display (in percentages) the predicted probability of each case displaying each risk level (from rare through unlikely, likely, possible to certain). The second column uses these probabilities to summarise the predicted risk level that is most likely to be true.

From Table A2, it is clear that eight cases were predicted to be a possible insider threat, and 53 cases were predicted as unlikely to be an insider threat. It can also be seen, however, that some cases were on the borderline between possibly being an insider threat and unlikely to be an insider threat, and we need to take these into our considerations.

Next, we will explain cases with different risk levels. Note that these levels were calculated from multiple perspectives and the result values were also affected by both the technological and organisational impact aspects. Since the technological and organisational impact aspects had the same values for all these cases (because the employees are all from a single organisation) they can be effectively ignored in this analysis. We will therefore focus solely on the human factor.

Case Number 04 Our model predicted that there is a more than 50% likelihood of this case being a possible insider threat with a 12% probability of it being categorised as "likely to be an insider threat". The right-hand column in Table 6 gives the summarised responses from the case regarding the human factor. In this case, the human factor levels were predicted as being high, due to the high capability level, medium opportunity level and high motivation level. Refer to Appendix C for the full Bayes network diagram.

Case Number 22 In this case, the model predicted that there is a 55% probability of the case being "unlikely to be an insider threat". The human factor levels were predicted as being 83% at the medium level, and these were affected by a medium capability level, medium motivation level, and a low opportunity level. This explains how the 55% prediction is produced by the model. Consult Table 6 for more in-depth information about how these values were predicted by the model. Also, please refer to Appendix D for the full Bayes network diagram.

Case Number 20 As we can see from Table A2, in case 20, the probabilities of "possibly" being an insider threat and "unlikely" to be an insider threat are very close. The model predicted a 45% probability of the employee being unlikely to be an insider threat and a 44% probability of them being a possible insider threat.

With respect to this borderline case, a security analysis team should intervene in order to analyse the data more closely and then make a final decision as to which risk level they will assign. In the borderline case, the information regarding the employee is as follows: The employee is between 25 and 45 years old; she has access to the organisation's intellectual property and believes she owns the copyright; and finally, she does not properly understand the organisation's security policies. On the other hand, her motivation level is normal.

With this information in mind, the security team should be able to help her avoid causing any unintentional insider threat going forward. If she were further trained in the area of security awareness it is likely that her risk level would reduce during future assessments, since she would then properly understand the organisational security policy, as well as the details regarding the copyright ownership.

In the small enterprise, twelve cases were collected and our model predicted that one case is "likely to be an insider threat", two cases were predicted as "possible insider threats", and nine cases were predicted as "unlikely to be insider threats". Table A1 "Appendix A" shows the final result of the proposed prediction model. Next, we will explain three cases with different risk levels among the prediction.

Case Number 11 Our model predicted that this case has a 36% possibility of an insider threat definitely occurring. On the other hand, there is a 34% probability of the case being likely to be insider threat; and a more than 16% probability of it certainly being an insider threat. In order to understand why the model produces these values, it is necessary to examine the human factor survey response values. Clearly, human factor levels are predicted as being high, and this is affected by a high capability level, a medium opportunity level, and high motivation levels. This information is shown in Table 6.

Case Number 0 In this case, the model predicted a more than 52% probability of the case being unlikely to be an insider threat. This prediction is heavily affected by the human factor levels, which are predicted to be 73% at the medium level. A medium capability level, a medium opportunity level, and a medium motivation levels affect this result. Table 6 shows the reason why the model produced these particular values.

Case Number 3 Here, the model predicted that Case 3 is quite likely to be an insider threat. This is due to one missing value – the contract expiration date. The participant had not completed this particular question, and a threat has been assumed by the model in this case. This is because the contract will expire in less than three months. Another reason is due to high work-related stress levels.

Table 6
Human Factors Results for (Cases 4,22) from the Education Sector Organisation and (Cases 11,0) from the Small Enterprise Organisation

Case	Indicator	State	Reason
C-4	Motive	High	The security policy is unclear.
			High levels of work-related stress.
	Opportunity	Medium	The time spent in this job position is less than three years.
			Has more than one year of their contract left.
	Capability	High	Belief in copyright ownership.
C-22	Motive	Medium	The security policy is clear.
			No emotional support.
			Colleagues get angry between themselves sometimes.
	Opportunity	Low	Time spent in this job position is less than a year.
			Has more than one year of their contract left.
	Capability	Medium	No access to intellectual property.
C-11	Motive	High	The security policy is unclear.
			High levels of work-related stress, because of: Destructive peer support from colleagues and managers. A negative approach to task control Colleagues' relationship with anger.
	Opportunity	Medium	The time spent in this job position is less than one year.
			Has less than one year of their contract left.
	Capability	High	Copyright ownership.
			Has access to intellectual property.
			Member of project teams.
			Higher capability due to work experience.
C-0	Motive	Medium	Does not understand security policy.
			Getting support from line-managers and colleagues.
			Manages work in a positive way.
			Relations with colleagues are positive.
	Opportunity	Medium	The time spent in this job position is less than one year.
			Has less than one year of their contract left.
	Capability	Medium	Has access to intellectual property.
			Copyright ownership belongs to the organisation.
			N a member of any project teams.
			Higher capability due to work experience.

5. The Validation of the Prediction Model

The insider threat prediction model supports decision makers within an organisation to predict the risk of an insider threat from each authorised user. Before we can use this tool in practice, however, we must take some steps to evaluate the prediction model so as to gain some assurance as to its validity.

The main challenge for the model validation is the need to compare the prediction result against the real insider threat events. Due to the nature of this problem, however, real insider threat events are rarely published. Nonetheless, Greitzer et al. were able to validate their approach (described in the previous sections) by comparing twenty-four case results with the judgments of two Human Resources experts, giving a result correlation of R^2, [2] known as the coefficient of multiple determination for multiple regression (Elmrabit, 2018; Greitzer et al., 2012).

Our validation method adopts an approach similar to that proposed by Greitzer et al. (Greitzer et al., 2012, 2018), i.e. comparing the results of the model prediction with empirical results, obtained from a group of researchers in the field of cyber-security, referred as "security experts".

Firstly, a validation workshop was organised to validate the results of the proposed prediction model for the education sector organisation. We focused on this organisation because only a small data set was collected from the small enterprise organisation. Five security experts attended this meeting. We started the workshop by presenting the background of insider threat breaches within the organisations, followed by a brief discussion of the proposed prediction framework, the modelling, and its results.

A validation feedback form was provided to each of the expert participants. We then started presented the data collected in subsection 4.1 directly from the data set file in a case by case procedure.

The security experts used a ranking probability election method [3] to rank the risk level from 1 to 5 for each case,

[2] R^2. In statistics, "R-squared is a measure of how close the data is to the fitted regression-line.

[3] **Probability Election Method** "A method for protocols is used to assess and incorporate subjective probabilities in risk and decision analysis. Various probability elicitation methods are commonly used in risk analysis such as RR (Rank reciprocal), EW (Equal weight), RS (Rank Sum), ROC

where a rank of 1 signifies the most expected prediction (Certain), and a rank of 5 signifies the least expected prediction (Rare).

Barron and Barret concluded in their research that Rank order centroid (ROC)[4] weights are more accurate than the other rank-based formulae (Barron and Barrett, 1996). The ROC ranking-based method is used to calculate the weight of the probabilities of each risk level based on the selected values from the experts' judgments, Table A3 illustrates the calculation result for the ROC of the Insider Threat Experts Judgement. The ROC formula used in this phase is described below:

$$wt_i = \left(\frac{1}{n}\right) \sum_{k=i}^{n} \left(\frac{1}{k}\right) \tag{2}$$

Where wt_i is the weight of each ranked order value, n is the total number of the objectives and $i = 1, \ldots, n \;\&\; \{wt_i \geq wt_{i+1} \geq \ldots\ldots \geq wt_n\}$.

The model risk results were verified by examining the extent to which the results from the model agreed with the experts' judgments, based on the results shown in Tables A2 and A3. The resulting squared correlation is around $R^2 = 0.87$, which indicates a high level of agreement between the expert judgements and the prediction model compared with other related approaches that achieved from $R^2 = 0.60$ (Greitzer et al., 2012) to $R^2 \sim 0.9$ (Greitzer et al., 2018).

In summary, in this section, we describe the essential steps to validate the insider threat prediction model so as to gain confidence in its predictions. We evaluate the prediction results by comparing the model result with the security expert's judgements. A discussion comparing the proposed approach against Greitzer et al. (Greitzer et al., 2018) is given in the next section.

6. Conclusion and Future Research

In this paper, we have presented a Bayesian Network-based model that can predict the potential of a malicious insider threat occurring before a security breach takes place. A multiple-perspective approach was proposed to address the challenges from technical, organisational and human factors perspectives, with 93 key insider threat indicators being extracted across all aspects from individual authorised users. The values of these key indicators were used as the input into the model in order to calculate the risk levels for every authorised user, using Bayes theorem. This comprehensive prediction model can be used for a similar purpose in any organisation.

We expected the approach to be a useful tool for security experts: it provides organisations with an insider threat risk assessment for each authorised user, and also allows organisations to discover areas of weakness that need more attention if they are to mitigate the risk from insider threats. Moreover, we expect the model to be useful for the research community as a basis of knowledge and future research.

The prediction model was validated by a comparison with the empirical judgement of a group of experts in the field of cyber-security. The validation results show that the proposed prediction model produced the expected result in predicting the potential of malicious insider threats.

6.1. Reflection Against Related Works

There is no standard framework or data set available against which to compare our method. The most recent relevant research contribution in the area of insider threats, however, is that of Greitzer et al. (Greitzer et al., 2018). This section compares their approach against ours.

In Greitzer et al.'s paper, the authors report the design and development of a structured model that emphasises individual and organisational socio-technical factors with technical indicators from previous studies. Their Socio-technical and Organizational Factors for Insider Threat (SOFIT) model provides a mechanism to assess the risk presented by authorised users alongside organisational vulnerability, as well as to inform operational risk management practices. To achieve this it uses the estimated risk weights obtained from expert knowledge and elicitation exercises, with nine experts contributing to this task.

In addition, Greitzer et al. used a use case to demonstrate the application of the ontology. Four models were studied (counting model, simple sum of risks model, linear regression weight model and sequential weighted model) to assess the combined risk of multiple indicators to retain the expected result from the use case text. R^2 were calculated to compare the performance of the models, and they achieved between $R^2 = 0.1$ using the counting model and $R^2 = 0.9$ using the regression weight model.

Compared to the SOFIT model, our approach was deliberately designed to be implemented and tested for data from real organisations. In our approach, we structured the framework shown in Figure 1 by giving the same weight to the three aspects (technology aspect, organisational impact, and human factor) so as to reflect the importance of all of these aspects in the calculation of risk levels. Each of these aspects has a number of factors and different weights are assigned to different factors at the developing phase.

A Bayesian network model was developed to implement the framework, followed by a survey to collect data from real organisations to calculate the risk level of each authorised user within the organisation. In the validation stage, we managed to compare the model result with expert judgements, and achieved $R^2 = 0.87$.

These approaches, however, aim to mitigate the insider threat risk by looking at the problem from different perspectives. Thus we believe that the two methods can complement each other.

(Rank order centroid)" (Elmrabit, 2018).

[4] **Rank order centroid** "In statistics, the ROC method produces an estimate of the weights that minimises the maximum error of each weight by identifying the centroid of all the possible weights maintaining the rank order of objective importance"(Elmrabit, 2018).

6.2. Challenges of the Proposed Approach

Insider threats are one of the pressing challenges threatening organisations' information assets. Unfortunately, no single approach can eliminate this kind of security breach; organisations need to carry out regular security risk assessment regarding insider threats so as to address any vulnerability in their environment. In contrast to external threats, an insider may have knowledge of all the organisational security measures, and some degree of trust within the organisation (Sagan, 2004).

A limitation to this study was the use of a prior probability distribution that was based on judgement and a literature review, given that there is little insider threat evidence available to researchers. Second, the ethical issues in this research, and organisational policy, prevented us from accessing the participants' names so as to compare the prediction result with any insider security breach which may have occurred. For this reason, it was hard to validate this approach within the organisation. It is encouraging, however, to see that the selected organisation took extra measures to prevent their information assets from being leaked by authorised users after this study took place, by providing more frequent security awareness training to all authorised users.

Another limitation was that we had to assume that the targeted organisations perceived no risk from user such as former employees, contractors, visitors, etc., who may have access to the organisations' assets, since these categories were not included in the human resources records. The approach therefore only targeted authorised employees who had access to the organisations' asset based on HR records.

6.3. Future Work

Future research will focus on the changing behaviours of human, organisational and technology factors over a period of time so as to avoid adversarial answers and obtain more accurate prediction results. Also, a decision support system may be designed to provide guidance to mitigate potential threats based on the prediction result. Finally, simplification of this approach can be considered by limiting its scope to predicting a single category of insider threats so that those could be predicted more effectively; although the organisations will then remain vulnerable to the other types of insider threats discussed in section 2.2.

7. Acknowledgements

We would first like to thank the organisations that granted us the opportunity to implement and test the proposed approach, in particular, their human resources and information technology management teams for their incredible cooperation. Moreover, special thanks are due to all 71 volunteer participants for their time and feedback. In addition, we are also grateful to the five cyber-security experts for their efforts to validate this model.

8. Funding

The work was jointly funded by the National Science Foundation of China (NSFC) through the project 'Dealing with Security and Safety Contradictions and Intrusion Tolerant Control for Industrial Cyber-Physical Systems' (Project ID: 61873119) and by EU Horizon 2020 DOMINOES Project (Grant Number: 771066).

References

Axelrad, E.T., Sticha, P.J., Brdiczka, O., Jianqiang Shen, 2013. A Bayesian Network Model for Predicting Insider Threats, in: 2013 IEEE Security and Privacy Workshops, IEEE. pp. 82–89.

Barron, F.H., Barrett, B.E., 1996. Decision Quality Using Ranked Attribute Weights. Management Science 42, 1515–1523.

Bartram, D., Turley, G., 2009. Managing the causes of work-related stress. volume 31. HSE.

Bell, A.J.C., Rogers, P.M.B., Pearce, D.J.M., 2018. The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention. International Journal of Critical Infrastructure Protection 24, 166–176.

Bishop, M., Gollmann, D., Hunker, J., Probst, C.W., 2008. Countering insider threats, in: Dagstuhl Seminar Proceedings 08302, pp. 1–18.

Brackney, R., Anderson, R., 2004. Understanding the Insider Threat, in: Advanced Research and Development Activity (ARDA), p. 137.

Buckley, O., Nurse, J.R., Legg, P.A., Goldsmith, M., Creese, S., 2014. Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat, in: 2014 Workshop on Socio-Technical Aspects in Security and Trust, IEEE. pp. 8–15.

Cappelli, D., Moore, A.P., Trzeciak, R., 2012. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. Addison-Wesley Professional. 1st ed edition.

Centre for the Protection of National Infrastructure, 2013. Insider data collection study. Technical Report April.

Chen, Y., Nyemba, S., Malin, B., 2012. Detecting Anomalous Insiders in Collaborative Information Systems. IEEE Transactions on Dependable and Secure Computing 9, 332–344.

Chockalingam, S., Pieters, W., Teixeira, A., van Gelder, P., 2017. Bayesian Network Models in Cyber Security: A Systematic Review, in: Lipmaa, H., Mitrokotsa, A., Matulevičius, R. (Eds.), Nordic Conference on Secure IT Systems, Springer International Publishing, Cham.

Cohen, F., 2012. Forensic Methods for Detecting Insider Turning Behaviors, in: 2012 IEEE Symposium on Security and Privacy Workshops, IEEE. pp. 150–158.

Colwill, C., 2009. Human factors in information security: The insider threat. Who can you trust these days? Information Security Technical Report 14, 186–196.

Costa, D.L., Albrethsen, M.J., Collins, M.L., Perl, S.J., Silowash, G.J., Spooner, D.L., 2016. An Insider Threat Indicator Ontology. Technical Report May.

Costante, E., den Hartog, J., Petković, M., Etalle, S., Pechenizkiy, M., 2017. A white-box anomaly-based framework for database leakage detection. Journal of Information Security and Applications 32, 27–46.

Elmrabit, N., 2018. A Multiple Perspective Approach for Insider Threat Risk Prediction in Cyber-Security. Ph.D. thesis. Loughborough University.

Elmrabit, N., Yang, S.H., Yang, L., 2015. Insider Threats in Information Security Categories and Approaches, in: 2015 21st International Conference on Automation and Computing (ICAC), IEEE, Glasgow, United Kingdom. pp. 1–6.

Fenz, S., Goluch, G., Ekelhar, A., Riedl, B., Weippl, E., 2007. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard, in: 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007), IEEE. pp. 381–388.

George J. Silowash, Todd Lewellen, J.W.B., 2013. Detecting and Preventing Data Exfiltration Through Encrypted Web Sessions via Traffic In-

spection. Software Engineering Institute,Carnegie Mellon University CMU/SEI-20.

Ghaffarzadegan, N., 2008. How a system backfires: Dynamics of redundancy problems in security. Risk Analysis 28, 1669–1687.

Greitzer, F., Purl, J., Becker, D., Sticha, P., Leong, Y.M., 2019. Modeling Expert Judgments of Insider Threat Using Ontology Structure : Effects of Individual Indicator Threat Value and Class Membership, in: 52nd Hawaii International Conference on System Sciences, pp. 3202–3211.

Greitzer, F., Purl, J., Leong, Y.M., Becker, D.S., 2018. SOFIT: Sociotechnical and Organizational Factors for Insider Threat, in: 2018 IEEE Security and Privacy Workshops (SPW), IEEE. pp. 197–206.

Greitzer, F.L., Hohimer, R.E., 2011. Modeling Human Behavior to Anticipate Insider Attacks. Journal of Strategic Security 4, 25–48.

Greitzer, F.L., Imran, M., Purl, J., Axelrad, E.T., Leong, Y.M., Becker, D., Laskey, K.B., Sticha, P.J., 2016. Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk, in: The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security.

Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, a.C., 2010. Identifying at-Risk Employees : A Behavioral Model for Predicting Potential Insider Threats. Pacific Northwest National Laboratory , 1–46.

Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, A.C., Hohimer, R.E., 2012. Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats, in: 45th Hawaii International Conference on System Sciences, IEEE. pp. 2392–2401.

Greitzer, F.L., Moore, A.P., Cappelli, D.M., Andrews, D.H., Carroll, L.A., Hull, T.D., 2008. Combating the Insider Cyber Threat. IEEE Security & Privacy Magazine 6, 61–64.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon , e00346.

Hart, M., Manadhata, P., Johnson, R., 2011. Text Classification for Data Loss Prevention. Privacy Enhancing Technologies , 18–37.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems 18, 106–125.

HSE, . Work related stress - Tools and templates.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., 2010. An Insider Threat Prediction Model, in: Trust, Privacy and Security in Digital Business. springer. chapter 3, pp. 26–37.

Kandias, M., Virvilis, N., Gritzalis, D., 2013. The Insider Threat in Cloud Computing, in: 6th International Workshop in Critical Information Infrastructure Security, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 93–103.

Kasanen, E., Lukka, K., Siitonen, A., 1993. The Constructive Approach in Management Accounting Research. Journal of Management Accounting Researc 5, 243–264.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., Rogers, S., 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure. Technical Report May.

Legg, P.A., Buckley, O., Goldsmith, M., Creese, S., 2017. Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. IEEE Systems Journal 11, 503–512.

Linstone, H.A., 1981. The multiple perspective concept. Technological Forecasting and Social Change 20, 275–325.

Liu, D., Wang, X., Camp, J., 2008. Game-theoretic modeling and analysis of insider threats. International Journal of Critical Infrastructure Protection 1, 75–80.

McCumber, J.R., 1991. Information systems security: A comprehensive model, in: 14th National Computer Security Conference, pp. 1–6.

Mills, J.U., Stuban, S.M., Dever, J., 2017. Predict Insider Threats Using Human Behaviors. IEEE Engineering Management Review 45, 39–48.

Moore, A.P., Cappelli, D., Caron, T., Shaw, E., Spooner, D., Trzeciak, R., 2011. A preliminary model of insider theft of intellectual property. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2, 28–49.

Negroponte, J., 2013. A preliminary examination of insider threat programs in the U.S. private sector. Technical Report. INSA.

Nurse, J.R.C., Legg, P.a., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., Creese, S., 2014. A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches, in: Human Aspects of Information Security, Privacy, and Trust. volume 8533, pp. 270–281.

Palmer, S., Cary, C., 2013. How to deal with strees (Creating Success). Kogan Page. 3 edition edition.

Palmer, S., Cooper, C., Thomas, K., 2001. Model of organisational stress for use within an occupational health education/promotion or wellbeing programme - A short communication. Health Education Journal 60, 378–380.

Pearl, J., 1985. Bayesian Networks A Model of Self-Activated Memory for Evidential Reasoning, in: Proceedings of the 7th Conference of the Cognitive Science Society, pp. 329–334.

Pfleeger, S.L., Predd, J.B., Hunker, J., Bulford, C., 2010. Insiders Behaving Badly: Addressing Bad Actors and Their Actions. IEEE Transactions on Information Forensics and Security 5, 169–179.

Ponemon Institute, 2014. Privileged User Abuse & The Insider Threat Commissioned. Technical Report May. Ponemon Institute.

Ponemon Institute LLC, 2018. Cost of Insider Threats : Global Sponsored by ObserveIT. Technical Report April.

Poolsappasit, N., Dewri, R., Ray, I., 2012. Dynamic Security Risk Management Using Bayesian Attack Graphs. IEEE Transactions on Dependable and Secure Computing 9, 61–74.

Ross, K.J., Hopkinson, K.M., Pachter, M., Munoz-Gonzalez, L., Sgandurra, D., Barrere, M., Lupu, E., 2017. Exact Inference Techniques for the Analysis of Bayesian Attack Graphs. IEEE Transactions on Dependable and Secure Computing 4, 1–1.

Sagan, S.D., 2004. The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security+. Risk Analysis 24, 935–946.

Shaw, E.D., Fischer, L.F., 2005. Ten Tales of Betrayal : The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations. Technical Report September. Defense Personnel Security Research Center (PERSEREC). Monterey, CA.

Silowash, G., Shimeall, T.J., Cappelli, D., Moore, A., Flynn, L., Trzeciak, R., 2012. Common Sense Guide to Mitigating Threats. Technical Report December. Software Engineering Institute Carnegie Mellon University.

Silowash, G.J., Lewellen, T.B., 2013. Insider Threat Control: Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders. Technical Report January.

Spitzner, L., 2003. Honeypots: catching the insider threat, in: 19th Annual Computer Security Applications Conference, 2003. Proceedings., IEEE. pp. 170–179.

Sticha, P.J., Axelrad, E.T., 2016. Using dynamic models to support inferences of insider threat risk. Computational and Mathematical Organization Theory 22, 350–381.

The Department for Business Innovation and Skills, 2013. Information Security Breaches Survey, Technical Report. Technical Report. PWC.

The UK National Cyber Security Programme, 2015. 2015 Information Security Breaches Survey. Technical Report. UK HM Government.

Wadhawan, Y., AlMajali, A., Neuman, C., 2018. A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks. Electronics 7, 249.

Walker-Roberts, S., Hammoudeh, M., Dehghantanha, A., 2018. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access 6, 25167—-25177.

Wood, B., 2000. An insider threat model for adversary simulation. SRI International Research on Mitigating the Insider Threat to Information Systems 2, 1–3.

Yang, L., King, M., Yang, S.H., Armstrong, J., 2008. Integrating Technical Approaches, Organisational Issues, and Human Factors in Security Risk Assessment by Organising Security Related Questions, in: ICEIS - Proceedings of the Tenth International Conference on Enterprise Information Systems, Volume ISAS-1, Barcelona, Spain, pp. 311–315.

Yaseen, Q., Panda, B., 2010. Predicting and Preventing Insider Threat in Relational Database Systems, in: Information Security Theory and Prac-

tices. Security and Privacy of Pervasive Systems and Smart Devices. volume 6033 LNCS, pp. 368–383.
Zeadally, S., Yu, B., Jeong, D.H., Liang, L., 2012. Detecting insider threats solutions and trends. Information Security Journal 21, 183–192.

A. The Prediction Result Tables

Table A1
The Prediction of Insider Threat Result for the Small Enterprise

Case	Predictions of Insider Threat	Predict Probability %				
		Certain	Likely	Possible	Unlikely	Rare
C-0	Unlikely insider threat	1.52	15.63	29.93	**52.88**	0.02
C-1	Unlikely insider threat	0.77	14.53	30.26	**54.41**	0.01
C-2	Unlikely insider threat	1.67	15.21	28.45	**54.61**	0.02
C-3	Likely insider threat	16.78	**36.61**	36.45	10.14	0
C-4	Unlikely insider threat	3.59	23.17	35.92	**37.29**	0
C-5	Possible insider threat	7.77	25.81	**35.27**	31.12	0
C-6	Unlikely insider threat	4.16	20.55	33.18	**42.09**	0.01
C-7	Unlikely insider threat	1.44	15.78	29.99	**52.76**	0.01
C-8	Unlikely insider threat	1.15	15.82	30.3	**52.69**	0.02
C-9	Unlikely insider threat	7.06	23.46	33.01	**36.44**	0.01
C-10	Unlikely insider threat	1.36	14.73	28.89	**54.98**	0.02
C-11	Possible insider threat	16.94	34.23	**36.02**	12.80	0

Table A2
The Prediction Result of Insider Threat for the Education Sector

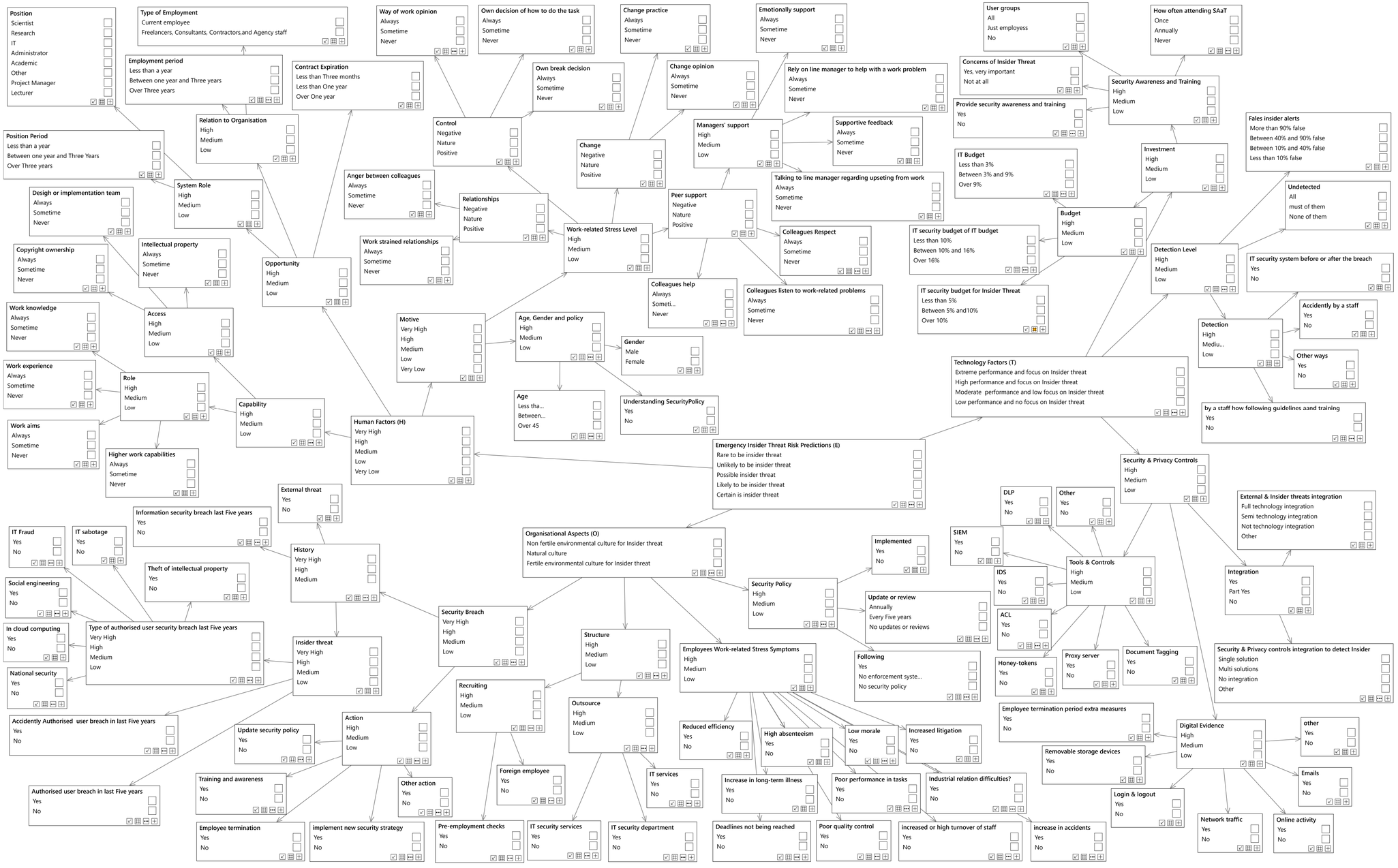
Case	Predictions of Insider Threat	Predict Probability %				
		Certain	Likely	Possible	Unlikely	Rare
C-0	Unlikely insider threat	1.5	8.65	43.06	**46.73**	0.04
C-1	Possible insider threat	6.74	15.18	**55.65**	22.41	0.00
C-2	Possible insider threat	6.74	15.03	**55.39**	22.82	0.00
C-3	Unlikely insider threat	0.36	4.33	29.71	**64.51**	1.07
C-4	Possible insider threat	5.34	12.76	**50.98**	30.84	0.05
C-5	Possible insider threat	6.22	15.64	**56.12**	22	0.00
C-6	Unlikely insider threat	0.30	5.54	37.59	**56.48**	0.06
C-7	Unlikely insider threat	1.87	7.55	40.11	**50.23**	0.22
C-9	Unlikely insider threat	1.48	8.27	42.34	**47.83**	0.06
C-11	Unlikely insider threat	0.23	4.60	32.24	**62.23**	0.68
C-12	Unlikely insider threat	0.63	6.50	39.19	**53.59**	0.07
C-13	Unlikely insider threat	0.19	4.10	30.25	**64.69**	0.75
C-14	Unlikely insider threat	1.31	8.31	42.62	**47.71**	0.02
C-15	Unlikely insider threat	0.37	5.37	35.92	**58.06**	0.26
C-16	Unlikely insider threat	0.07	2.22	16.82	**77.64**	3.23
C-17	Possible insider threat	2.56	9.25	**44.45**	43.69	0.04
C-18	Unlikely insider threat	0.66	5.41	33.96	**59.31**	0.64
C-19	Unlikely insider threat	1.09	5.6	32.73	**59.59**	0.97
C-20	Unlikely insider threat	1.78	9.07	44.00	**45.11**	0.02
C-21	Unlikely insider threat	0.91	6.6	38.74	**53.56**	0.17
C-22	Unlikely insider threat	0.52	5.65	36.22	**57.30**	0.28
C-23	Unlikely insider threat	0.66	6.13	37.74	**55.26**	0.19
C-24	Unlikely insider threat	0.47	4.41	28.88	**64.88**	1.33
C-25	Unlikely insider threat	0.12	3.26	23.66	**70.86**	2.08
C-26	Unlikely insider threat	0.46	5.22	34.29	**59.52**	0.48
C-27	Unlikely insider threat	0.38	5.07	34.41	**59.77**	0.36
C-28	Unlikely insider threat	0.08	3.15	23.92	**71.04**	1.79
C-29	Unlikely insider threat	1.60	8.74	43.36	**46.25**	0.03
C-30	Unlikely insider threat	0.02	1.62	12.54	**81.46**	4.34
C-31	Unlikely insider threat	1.51	7.30	40.39	**50.68**	0.11
C-32	Unlikely insider threat	0.30	4.60	31.35	**62.85**	0.88
C-33	Unlikely insider threat	0.92	6.27	37.6	**54.94**	0.25
C-34	Unlikely insider threat	1.73	8.28	42.66	**47.27**	0.04
C-35	Unlikely insider threat	0.97	6.15	36.9	**55.63**	0.33
C-36	Unlikely insider threat	0.84	6.91	39.91	**52.25**	0.07
C-37	Unlikely insider threat	2.01	8.78	43.18	**45.93**	0.08
C-38	Unlikely insider threat	0.29	3.85	26.59	**67.69**	1.56
C-39	Unlikely insider threat	0.95	5.47	32.54	**60.04**	0.97
C-40	Possible insider threat	3.15	9.83	**44.58**	42.18	0.23
C-41	Unlikely insider threat	1.11	7.35	40.09	**51.28**	0.16
C-42	Unlikely insider threat	1.04	6.12	36.08	**56.27**	0.46
C-43	Unlikely insider threat	1.57	7.3	39.53	**51.34**	0.24
C-44	Unlikely insider threat	1.44	8.48	43.03	**47.01**	0.01
C-45	Unlikely insider threat	0.80	4.64	27.99	**64.96**	1.6
C-46	Unlikely insider threat	0.36	5.47	36.52	**57.43**	0.20
C-47	Unlikely insider threat	0.16	4.71	33.86	**60.91**	0.35
C-48	Unlikely insider threat	0.21	4.79	34.48	**60.21**	0.28
C-49	Unlikely insider threat	0.06	3.95	30.26	**64.98**	0.73
C-50	Possible insider threat	6.80	12.36	**50.76**	29.99	0.07
C-51	Possible insider threat	2.98	9.33	**43.97**	43.54	0.15
C-52	Unlikely insider threat	0.28	5.04	34.56	**59.71**	0.38
C-53	Unlikely insider threat	0.05	4	30.61	**64.62**	0.71
C-55	Unlikely insider threat	0.19	4.19	29.87	**64.72**	1.01
C-56	Unlikely insider threat	0.01	1.21	9.41	**84.15**	5.21
C-57	Unlikely insider threat	0.31	4.21	28.58	**65.62**	1.26
C-58	Unlikely insider threat	0.38	4.24	28.20	**65.80**	1.35
C-62	Unlikely insider threat	0.43	3.99	27.26	**66.88**	1.42
C-63	Unlikely insider threat	1.99	9.14	44.23	**44.61**	0.01
C-64	Unlikely insider threat	0.06	2.19	16.60	**77.80**	3.32
C-65	Unlikely insider threat	0.91	6.83	39.47	**52.65**	0.11
C-69	Unlikely insider threat	1.44	7.04	38.87	**52.37**	0.27

Table A3
Insider Threat Result by Experts Judgement

Case	Predictions of Insider Threat	Predict Probability %				
		Certain	Likely	Possible	Unlikely	Rare
C-0	Unlikely insider threat	8	15.6	33.6	**37.6**	5.25
C-1	Possible insider threat	9	19.6	**45.6**	21.6	4
C-2	Possible insider threat	8	27.6	**37.6**	21.6	4
C-3	Unlikely insider threat	7	21.6	31.6	**33.6**	6.5
C-4	Possible insider threat	7	25.6	**41.6**	19.6	6.5
C-5	Unlikely insider threat	8	15.6	33.6	**37.6**	5.25
C-6	Unlikely insider threat	7	15.6	25.6	**45.6**	5.25
C-7	Possible insider threat	7	15.6	**41.6**	29.6	5.25
C-9	Unlikely insider threat	6	15.6	29.6	**41.6**	6.5
C-11	Unlikely insider threat	7	15.6	25.6	**45.6**	6.5
C-12	Unlikely insider threat	7	15.6	25.6	**45.6**	6.5
C-13	Unlikely insider threat	6	15.6	29.6	**41.6**	7.75
C-14	Unlikely insider threat	6	15.6	29.6	**41.6**	7.75
C-15	Unlikely insider threat	6	15.6	25.6	**45.6**	7.75
C-16	Unlikely insider threat	6	15.6	25.6	**45.6**	7.75
C-17	Possible insider threat	7	15.6	**45.6**	25.6	6.5
C-18	Possible insider threat	8	15.6	**37.6**	33.6	5.25
C-19	Possible insider threat	8	23.6	**37.6**	25.6	5.25
C-20	Possible insider threat	6	15.6	**41.6**	29.6	7.75
C-21	Unlikely insider threat	6	15.6	25.6	**45.6**	6.5
C-22	Unlikely insider threat	6	15.6	25.6	**45.6**	7.75
C-23	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-24	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-25	Unlikely insider threat	4	15.6	25.6	15.6	9
C-26	Unlikely insider threat	4	14.28	25.6	**45.6**	9
C-27	Unlikely insider threat	4	14.28	25.6	**45.6**	9
C-28	Unlikely insider threat	5	15.6	25.6	**45.6**	9
C-29	Unlikely insider threat	4	15.6	22.28	**45.6**	9
C-30	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-31	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-32	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-33	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-34	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-35	Unlikely insider threat	6	15.6	33.6	**37.6**	7.75
C-36	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-37	Unlikely insider threat	4	14.28	25.6	**45.6**	9
C-38	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-39	Unlikely insider threat	4	15.6	25.6	**45.6**	9
C-40	Possible insider threat	5.25	23.6	**45.6**	17.6	8
C-41	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-42	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-43	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-44	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-45	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-46	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-47	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-48	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-49	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-50	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-51	Unlikely insider threat	5	15.6	29.6	**45.6**	7.75
C-52	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-53	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-55	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-56	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-57	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-58	Unlikely insider threat	5	15.6	25.6	**45.6**	7.75
C-62	Unlikely insider threat	6	15.6	33.6	**37.6**	6.5
C-63	Unlikely insider threat	5	15.6	25.6	**41.6**	7.75
C-64	Unlikely insider threat	5	15.6	25.6	**41.6**	7.75
C-65	Unlikely insider threat	5	15.6	25.6	**41.6**	7.75
C-69	Unlikely insider threat	5	15.6	29.6	**41.6**	7.75

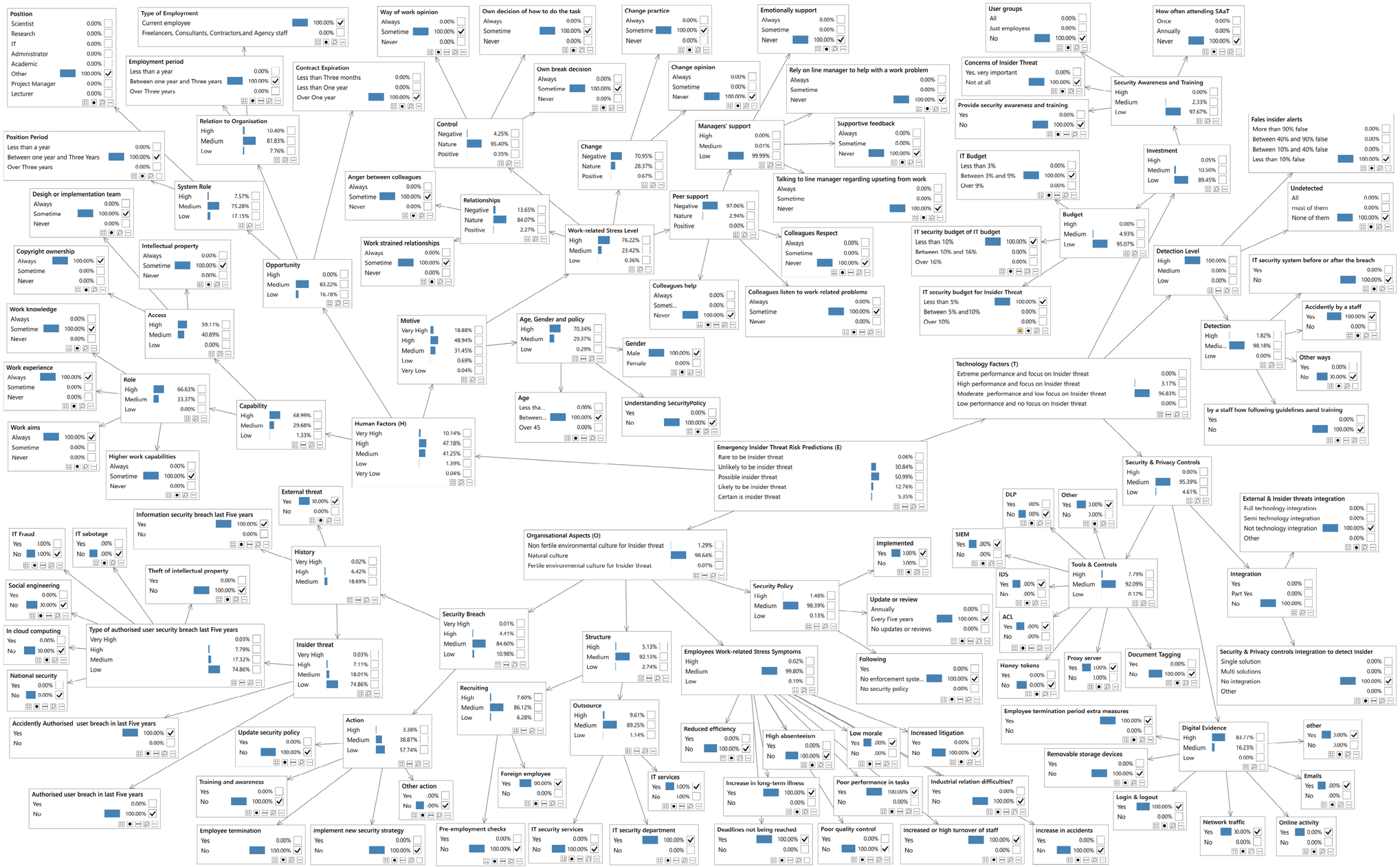
B. Full Insider Threat Prediction Network Graph

Please zoom in to view all details or print it on A3 paper.



C. A Snap-shot of Bayes Network for Case 4

Please zoom in to view all details or print it on A3 paper.



D. A Snap-shot of Bayes Network for Case 22

Please zoom in to view all details or print it on A3 paper.