

A Multiple Perspective Approach for Insider
Threat Risk Prediction in Cyber-Security

by

Nebrase Elmrabbit

A Doctoral Thesis

Submitted in partial fulfilment
of the requirements for the award of

Doctor of Philosophy
of
Loughborough University

Supervisors
Professor Shuang-Hua Yang
Dr Lili Yang

1st April 2018

Copyright 2018 Nebrase Elmrabbit

Abstract

Currently governments and research communities are concentrating on insider threat matters more than ever, the main reason for this is that the effect of a malicious insider threat is greater than before. Moreover, leaks and the selling of the mass data have become easier, with the use of the dark web. Malicious insiders can leak confidential data while remaining anonymous. Our approach describes the information gained by looking into insider security threats from the multiple perspective concepts that is based on an integrated three-dimensional approach. The three dimensions are human issue, technology factor, and organisation aspect that forms one risk prediction solution.

In the first part of this thesis, we give an overview of the various basic characteristics of insider cyber-security threats. We also consider current approaches and controls of mitigating the level of such threats by broadly classifying them in two categories: a) technical mitigation approaches, and b) non-technical mitigation approaches. We review case studies of insider crimes to understand how authorised users could harm their organisations by dividing these cases into seven groups based on insider threat categories as follows: a) insider IT sabotage, b) insider IT fraud, c) insider theft of intellectual property, d) insider social engineering, e) unintentional insider threat incident, f) insider in cloud computing, and g) insider national security.

In the second part of this thesis, we present a novel approach to predict malicious insider threats before the breach takes place. A prediction model was first developed based on the outcomes of the research literature which highlighted main prediction factors with the insider indicator variables. Then Bayesian network statistical methods were used to implement and test the proposed model by using dummy data. A survey was conducted to collect real data from a single organisation. Then a risk level and prediction for each authorised user within the organisation were analysed and measured.

Dynamic Bayesian network model was also proposed in this thesis to predict insider threats for a period of time, based on data collected and analysed on different time scales by adding time series factors to the previous model.

Results of the verification test comparing the output of 61 cases from the education sector prediction model show a good consistence. The correlation was

generally around $R^2 = 0.87$ which indicates an acceptable fit in this area of research.

From the result we expected that the approach will be a useful tool for security experts. It provides organisations with an insider threat risk assessment to each authorised user and also organisations can discover their weakness area that needs attention in dealing with insider threat. Moreover, we expect the model to be useful to the researcher's community as the basis for understanding and future research.

Keywords – Cyber security insider threats; Privileged user abuse; Multiple perspective approach; Insider threats predictions.

Acknowledgements

Significant parts of this research were funded by the Ministry of Higher Education and Scientific Research, Libya, through the cultural affairs at the Libyan embassy, UK.

Foremost, I would like to express my deepest appreciation to my supervisors Professor Shuang-Hua Yang and Dr Lili Yang for their support and guidance through my PhD study journey. Their vision, motivation and knowledge were always the source of my inspiration and ideas.

I extend my gratitude to the organisation that gives us the excellent opportunity to carry out and test the proposed model, in particular, their HR and IT management teams for their incredible collaboration. We would also like to thank all 71 volunteer participants for their time and feedback.

Special thanks goes to the five cyber-security researchers for their contribution and assistance with their opinions to validate the model in this study.

Finally, my heartfelt thanks go to my whole family, who have been an essential and indispensable source for moral support, selfless support, understanding, with constant love.

Contents

Acknowledgements	i
List of Figures	vi
List of Tables	viii
List of Abbreviations	ix
1 Introduction	1
1.1 Motivation	1
1.2 Research Questions	3
1.3 Aim and Objectives of the Study	3
1.4 Original Contributions	4
1.5 Research Methodology	5
1.6 Ethical Considerations	8
1.7 Overview of the Thesis	8
2 Insider Cyber-Security Background	10
2.1 Introduction	10
2.2 Information Security	10
2.3 Information Security Concepts	11
2.4 Insider Threat Definition	12
2.5 Reasons for Misusing Privileged Access	14
2.6 Insider Threat Categories	14
2.6.1 Insider IT Sabotage	16
2.6.2 Insider IT Fraud	16
2.6.3 Insider Theft of Intellectual Property	17
2.6.4 Insider Social Engineering	17
2.6.5 Unintentional Insider Threat Incident	18
2.6.6 Insider in Cloud Computing	19
2.6.7 Insider National Security	20
2.7 Summary	21

3	Insider Threats Mitigation Approaches	23
3.1	Technical Controls to Identify Insider Threats	23
3.1.1	Intrusion Detection Systems (IDS)	24
3.1.2	Security Information & Event Management (SIEM)	24
3.1.2.1	Universal Serial Bus (USB) Device Auditing to De- tect Possible Data Exfiltration by Malicious Insiders	25
3.1.3	Data Loss Prevention (DLP)	25
3.1.3.1	Traffic Inspection Approach	26
3.1.3.2	HTTPS Traffic Inspection Approach	27
3.1.4	Access Control System	27
3.1.5	Honey-tokens	28
3.2	Non-Technical Approaches	29
3.2.1	Psychology Prediction Model	29
3.2.2	Security Education and Awareness	30
3.2.3	Information Security Policy	31
3.3	Techniques and Psychology Prediction Model	33
3.4	A Framework for Characterising Attacks Approach	35
3.5	Summary	37
4	Insider Threat Risk Prediction Model	38
4.1	Introduction	38
4.2	The Framework	39
4.2.1	Human Factor Dimension	41
4.2.2	Technology Aspect Dimension	42
4.2.3	Organisational Impact Dimension	43
4.3	Modeling Framework	44
4.3.1	Network Construction	46
4.3.2	Prior Probabilities	46
4.3.3	Risk output	48
4.4	Summary	52
5	Data collection and Analysis	53
5.1	Survey Data Collection	53
5.1.1	Survey Questions (Data Requirements)	53
5.1.2	Data Collection	58
5.1.3	Data Processing and Exploitation Method	59
5.2	Modeling Prediction Results	62
5.2.1	Technology Factor Prediction Result	62
5.2.2	Organisational Aspect Prediction Result	65

5.2.3	Human Factor Prediction Result	67
5.2.4	Insider Threat Prediction Results	70
5.3	Agreement with Theory	76
5.4	Summary	79
6	Validation of the Prediction Model	80
6.1	Introduction	80
6.2	Concepts of Verification and Validation	81
6.3	Verification of the Insider Threat Prediction Approach	82
6.4	Validation of the Prediction Model	83
6.5	Summary	86
7	A Dynamic Model Approach for Insider Threats	87
7.1	Introduction	87
7.2	Model Formulation	87
7.3	The Architecture of Dynamic Insider Threat Prediction	88
7.3.1	Data Input	89
7.3.2	Data Analysis	89
7.3.3	Integration	90
7.3.4	Prediction Result	90
7.4	Case Study implementation	90
7.5	Summary	96
8	Conclusions, Limitation, and Future Research	97
8.1	Conclusions	97
8.2	Limitations	98
8.3	Contributions Revisited	98
8.4	Future Research	99
	References	110
	Appendix	110
A	Human Factors, Technology Aspects and Organisational Impact Survey	111
B	A list of all variables with changing of the probability for a selected Cases 4,20.22.69	137
C	Prediction Results with Different Time Period Table	148
D	Insider Threat Risk Prediction Validation Workshop	159

E	Ethics Approvals	170
F	A Snap-shot of Bayes Network for Case 4	177
G	A Snap-shot of Bayes Network for Case 22	179

List of Figures

Figure 1.1	How Insider Threats are Handled	2
Figure 1.2	Research Methodology and Plan	7
Figure 2.1	Main Security Goals	11
Figure 2.2	Insider Threat Definition Scope by CERT	13
Figure 2.3	Reasons For Misusing Privileged Access	15
Figure 2.4	Summarise of Insider Threat Categories	22
Figure 3.1	USB History.bat Script	25
Figure 3.2	Traffic Inspection Network Structure	26
Figure 3.3	Bayesian Network Variables and Structure	30
Figure 3.4	Greitzer’s Risk Indicators	30
Figure 3.5	Insider Threat Prediction Model	33
Figure 3.6	A Framework for Characterising Insider Attacks	36
Figure 4.1	McCumber Model	39
Figure 4.2	Insider Threat Risk Prediction Framework	40
Figure 4.3	Simple Bayes Network Sprinkler Example.	45
Figure 4.4	A Snapshot of Gender Distribution Editor and Domain	46
Figure 4.5	Insider Threat Risk Prediction Model Network	47
Figure 5.1	A Snapshot of the Survey Layout	55
Figure 5.2	A Snapshot of the Survey Introduction	55
Figure 5.3	Data Processing and Exploitation Method	59
Figure 5.4	Technology Factor Domain - Case 25	64
Figure 5.5	Organisational Impact Domain - Case 25	66
Figure 5.6	A Snapshot for Human Factor Nodes Variable - Case 25	68
Figure 5.7	A Snapshot for Insider Threat Risk Prediction Levels	70
Figure 5.8	Insider Threat Prediction Result	72
Figure 5.9	Insider Threat Prediction Result Line Chart	75
Figure 5.10	Bayes Network Example 1	77
Figure 5.11	Prior Probabilities	77
Figure 5.12	Bayes Network Example 2	78

Figure 6.1	Simulation Model Verification and Validation in a Simulation Study	81
Figure 6.2	Verification Test	84
Figure 7.1	Architecture of the Dynamic Insider threat Prediction	89
Figure 7.2	Case Number 4	93
Figure 7.3	Case Number 20	94
Figure 7.4	Case Number 22	95
Figure 7.5	Case number 69	95

List of Tables

Table 2.1	Insider Threat Categories	15
Table 3.1	Insider Threats Approaches Summary	32
Table 3.2	Threat Scour	35
Table 4.1	Mapping the Risk Band to Probability	52
Table 5.1	Human Factor Surveys' Questions	56
Table 5.2	Technology Aspect Surveys' Questions	57
Table 5.3	Organisational Impact Surveys' Questions	57
Table 5.4	Respond Values	58
Table 5.5	Missing Values	59
Table 5.6	Missing Values SPSS Analysis	60
Table 5.7	Data Processing and Exploitation Result	61
Table 5.8	Technology Factor Predictions	63
Table 5.9	Organisational Aspect Prediction	65
Table 5.10	Human Factor Result For All Cases	67
Table 5.11	Case 4 and Case 22 of the Human Factor Results	69
Table 5.12	Human Factor Result for All 12 Cases	69
Table 5.13	Insider Threat Prediction Result	71
Table 5.14	Case 4 Human Factors	73
Table 5.15	Case 22 Human Factors	73
Table 5.16	Insider Threat Prediction Result for the Small Enterprise	74
Table 5.17	Case 11 Human Factors	75
Table 5.18	Case 0 Human Factors	76
Table 6.1	Insider Threat Experts Judgement Result	85
Table 7.1	Part of Prediction Result within Different Time Period	91
Table C.1	Prediction Result with Different Time Period	148

List of Abbreviations

- DLP* Data Loss Prevention
- IDS* Intrusion Detection System
- DBN* Dynamic Bayesian Networks
- DAG* Directed Acyclic Graph
- CERT* Computer Emergency Response Team
- HSE* Health and Safety Executive
- SSL* Secure Sockets Layer
- IT* Information Technology
- HR* Human Resource
- BN* Bayesian Networks
- CIA* Confidentiality, Integrity and Availability

Chapter 1

Introduction

1.1 Motivation

Organisations nowadays depend on computers in every aspect of their daily operations, and because more than 80% of companies use remotely hosted services on the cloud [93], most governments have started to centralise citizens' information in huge data service centres, while the citizens themselves also rely on cloud computing to store their confidential data. All these make data theft easier. Most of the decision makers in organisations and government are focusing on external cyber-attacks such as unauthorised access to their networks, denial of service attacks, viruses, Trojan Horses, Worms, etc. In order to protect such networks from external attack, they spend around 10% of their IT budget on securing their assets [93].

However, new evidence shows that both external attacks and insider threats are significant [93], while the damage caused by insider attack is more damaging than that of outsider attacks [36]. This means that anyone who has authorisation to access organisation's data assets is more dangerous than any other security threat. Regardless of this, insider threat has been undervalued, and underestimated.

Insider attacks are the most expensive form of information security breach, in that the average cost per insider incident is £115,000 according to a recent report by the Ponemon Institute LLC [73]. This is because the insider has knowledge of, and access to, their employer's assets, This has come about because such an individual has had the trust of the organisation causing him or her to be supplied with authorised access so that it is possible to bypass all physical and electronic security measures.

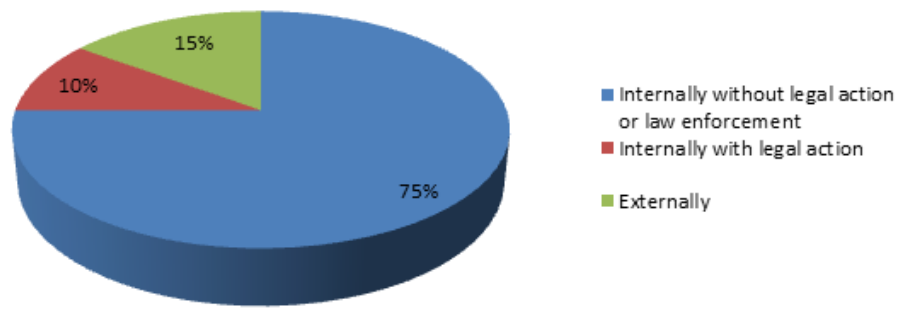


Figure 1.1: How Insider Threats are Handled

However, the number of insider threat incidents have continued to increase to a significant extent. In fact, a recent study by the Ponemon Institute found that 88% of IT experts believe that the risk of insider threat will stay the same or increase in the next two years [72]. But more than three-quarters of these incidents usually go unreported and are handled internally, with few referrals to law enforcement agencies and no legal action taken, because of a lack of sufficient evidence in order to prosecute the insider, or because organisations are concerned about their reputation and negative publicity [11] [89]. Figure. 1.1 shows how insider threats are handled.

Over the last ten years, there have been numerous studies that have tried to define insider threat problems in order to come with one solution to solve current security data breaches. In addition, security research incorporating survey results in the last three years has shown an increase in insider threat breaches, with a strong level of incident effects on organisations from the activities of insiders[89], However, studies of insider threats prevention are divided into two main parts, non-technical mitigation and technical mitigation - in which researchers have focused on the non-technical aspect even though technical controls have improved. This is because privilege users are the greatest vulnerability to organisations. Part of this is because these peoples' knowledge of technical controls allows them to avoid existing technical controls.

Considering the above information we define the problem statement for this research as designing a new approach that helps organizations to mitigate the risk level of insider threat by considering different techniques.

1.2 Research Questions

Whether it is intentional or unintentional insider threat breaches carried out by trusted people, what could be the approach that helps us to prevent of such threats, and to deal with any potential insider breach before it can take place?

1.3 Aim and Objectives of the Study

The aim of this research, as established in our problem statement, is to design and develop a prediction framework that will assist decision makers to eliminate cyber security insider threat.

This thesis contains the context and details of a set of objectives we define as necessary to present our final solution. These objectives provide a clear definition of the scope of our work. The main objectives of the research are as follows:

- To review the current literature in the area of insider threat.
- To define the nature of the insider threat problem and identify various categories of insider threats.
- To present a new framework that help organisations to predict potential malicious insider threats before a breach takes place.
- To implement the framework by modelling the proposed prediction framework.
- To conduct empirical investigation “data collection”.
- To extend the proposed static prediction model to a dynamic model.
- To validate and test the proposed framework.

1.4 Original Contributions

The study made during this PhD study has resulted in several contributions in the field of insider threat mitigation to achieve the research aims and objectives. The following list summarises the contributions this research achieves.

- We provide a detailed definition of the insider threat that makes a clear distinction between malicious or unintentional breaches, with the authorisation access, that impact the information security goals ([chapter 2](#)).
- We divide the insider threat category into seven sub-categories, based on the manner in which they affect the organisation's information security goals (confidentiality, integrity, and availability), and the human factors which lead an insider to act in a malicious manner (motive, opportunity, and capability ([chapter 2](#)).
- An in-depth literature review of the current state of the art in insider threat mitigation approaches. We classified these approaches into two main categories: a) technical mitigation approaches and b) non-technical mitigation approaches. The limitations of the current insider threat mitigation approaches are identified ([chapter 3](#)).
- We propose a novel multiple perspective framework to help reducing the risk of insider threat by predicting who could be an insider threat ([chapter 4](#)).
- We develop a computational statistical Bayesian model to implement the proposed framework ([chapter 4](#)), and tested the model by data collected using surveys ([chapter 5](#)).
- A dynamic insider threat prediction model with time series is proposed ([chapter 7](#)).

1.5 Research Methodology

In this thesis, a constructive research approach is used, which means problem-solving through the construction of models, diagrams, plans, organisations, etc. This method of research is widely used in technical sciences to develop a new theory, algorithm, model, software, or a framework, to solve the research problem.

Kasanen et al. [50] characterised the constructive method by dividing the research process into a number of stages, as listed:

- Find a practically relevant problem which also has research potential.
- Obtain a general and comprehensive understanding of the topic.
- Innovate, i.e., construct a solution idea.
- Demonstrate that the solution works.
- Show the theoretical connections and the research contribution of the solution concept.
- Examine the scope of applicability of the solution.

Our research is comprised of seven stages. The first addresses the literature review, the second stage focuses on framework design, the third stage is on model implementations, fourth stage is model test, fifth stage improves and extends the prediction model, sixth stage is to validate the proposed prediction model, and final stage is the conclusions, limitation, and any future Research. Figure. 1.2 shows flowchart of this research plan.

Stage 1: Literature Review.

- Setting the scope
- Find out insider threat categories.
- Find out insider threat approaches.
- Find out research caps.
- Publish paper based on the previous points.

Stage 2: Framework Design.

- Multi-perspective approach thinking.
- To find out Key Insider Threat Indicators.
- To set up the relations between all indicators in a single framework.

Stage 3: Model Implementations.

- Choose the proper statistic method to calculate the prediction levels.
- Apply the proposed model to selected statistic application.
- Set the conditional probabilities for all nodes.

Stage 4: Model Test.

- Survey Design (Data Requirements)
- Survey Responded Data (Data Collection).
- Data Processing and Exploitation.
- Data Product (Predictive Analytics).

Stage 5: Validation of the Prediction Model.

- Choose the proper validation method to validate the result from prediction model.
- Prepare a workshop for expert judgement discussion.
- Analyse the findings.

Stage6: Extending the Previous Model to a Dynamic Model.

- Choose the proper dynamic method to calculate the predicting levels.
- Design a new architecture for the insider threat prediction model.
- Run and test this model.

Stage 7: Conclusion, Limitation, and Future Research

- To discuss the final Conclusion.
- To conclude our work limitation.
- To find out any potential research based on our conducted work.

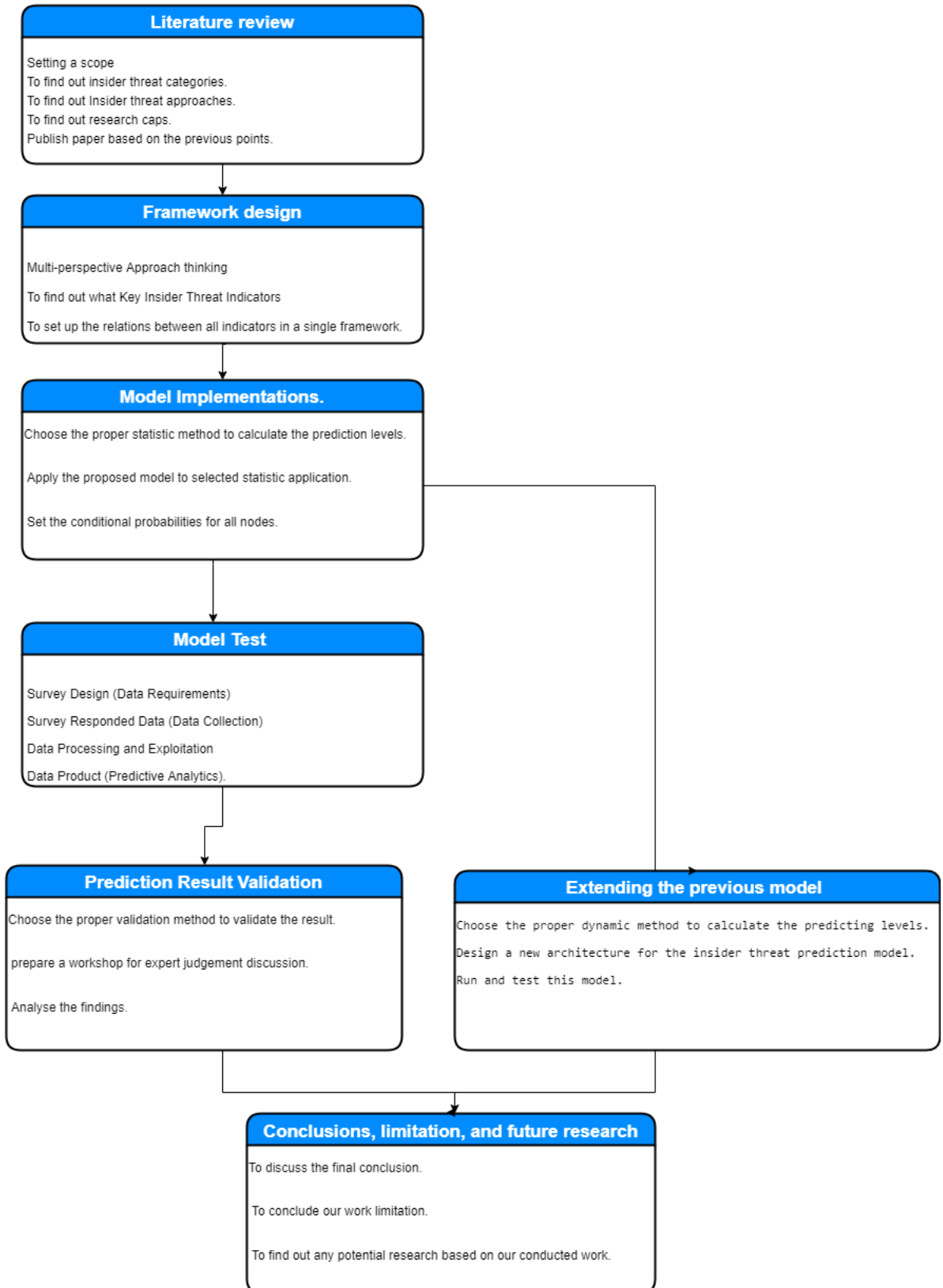


Figure 1.2: Research Methodology and Plan

1.6 Ethical Considerations

The project was reviewed and approved in according with the Loughborough University ethical clearance procedures for the School of Science. Participants were fully informed by the aims and objectives of the study and the use of the data collected at the start of the survey. Participants were informed of their right to withdraw from the study at any point.

Data collected were treated as confidential and cannot be used or disclosed for any other purpose. Further contact details of the researcher were made available to all participants. Please refer to Appendix E for the ethical clearance form.

1.7 Overview of the Thesis

Chapter 2: Insider Cyber-Security Background

In this chapter, we provide the necessary background for topics discussed throughout the thesis. We categorise different types of insider attack (e.g., sabotage, fraud, theft of Intellectual Property) against the main security principles (confidentiality, integrity, availability), and also against human factors (motive, opportunity, capability).

Chapter 3: Insider Threats Mitigation Approaches

In this chapter, a variety of current approaches in the context of insider threat detection, were classified into two categories a) technical mitigation approaches, such as intrusion detection systems, honey-tokens, access control systems, and security information and event management systems. and b) non-technical mitigation approaches, such as the psychological prediction models, and security education and awareness. Both of these categories are required by organisations in order to mitigate the insider threat problem.

Chapter 4: Insider Threat Risk Prediction Model

This chapter presents a new framework, the multiple perspective approach for insider threat risk prediction. We apply Bayesian network statistical methods to implement the proposed framework.

Chapter 5: Data Collection and Analysis

In this chapter, we evaluate the proposed model through the process of data collection by a survey, and modelling prediction result via Bayesian Network Software. Here the outcome of this prediction result is aimed at helping decision makers

to avoid insider threat breaches by indicating who could be a potential malicious insider threat within the organisation.

Chapter 6: A Dynamic Model Approach for Insider Threats

In this chapter, we propose a new approach to predict insider threats over a period of time, based on data collected and analysed on different time scales called a dynamic model.

Chapter 7: Validation of the Prediction Model Results

In this chapter, We evaluate the prediction result by comparing the model result with security expert's judgements result, by using different statistical methods to find how close the data are to the fitted regression line.

Chapter 8: Conclusions, Limitation, and Future Research

This chapter summarises our research and its findings and provides possible future Research. Also, research limitation were discussed in this chapter.

Chapter 2

Insider Cyber-Security Background

2.1 Introduction

In this chapter, we present the background information on insider threat; we start with various definitions of insider threat, followed by discussion of main reasons of misusing privileged access, Then, dividing insider threat categories into seven categories, each category is explained with a case example.

2.2 Information Security

Information Security can be defined as the process by which digital information assets are protected in order to ensure the three main security goals. These goals are *a) Confidentiality* To ensure that information assets are not disclosed to individuals or systems that are not authorised to receive them. It is also defined as the process of making sure that data assets remain secret and confidential, and that they cannot be viewed by unauthorised users, *b) Integrity* To ensure that information assets cannot be modified by any other party without authorisation. Integrity could also be described as the process that ensures that data assets are the same as they were when they were originally created, without any change over time, and *c) Availability* To ensure that information assets are available when requested, It could also be described as a situation in which data assets should be accessible for legitimate users when needed [92]. Figure 2.1 shows the main security goals.



Figure 2.1: Main Security Goals

2.3 Information Security Concepts

When we discuss information security, it is important and helpful that we mention and understand terms like vulnerabilities, threats, and attacks on IT and Network infrastructures, applications and services.

Vulnerability

Vulnerability is the weakness of an asset that is inherent in every IT and Network infrastructure, application and service. It is the weakness that make threats happen.

Threat

Threats refer to anything that has the potential to cause serious harm or damage to the IT and Network infrastructures, applications and services, such as people willing to take advantage of each security weakness which leads to attacks on your asset.

Attack

Attack means the action taken to exploit vulnerability or to create a threat to the IT and Network infrastructures, applications and services. Attack also could be defined as any attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset[47].

To summarise, a **threat** is a potential event that can adversely affect an asset, whereas a successful **attack** exploits **vulnerabilities** in your system[59].

2.4 Insider Threat Definition

Hunker[91] indicated that the research community has made little overall progress in mitigating the insider threat problem; which is not because of lack of research quality but rather from a lack of a framework to describe precisely what issues we are trying to solve. One of these problem questions is “ *What exactly is an insider threat?* ” The authors noted that “ if we cannot rigorously define the problem we are seeking to solve, then how can we approach it, or even know when the problem has been solved? ”.

To comprehend the definition of an insider threat, we should know what an insider is and what a threat means in relation to information security. ***The insider:*** A major workshop by the Advanced Research and Development Activity RAND Corporation [8] that was held in 2004 defined the term of insider as: “an already trusted person with access to sensitive information”. Greitzer et al. [30], definition of insider is “an individual currently or at one time authorised to access an organisation’s information system, data, or network ”. Bishop et al [7] also, defined an insider in terms of trust that includes organisation assets as “ a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organisation’s structure ” , or simply as: an individual who has logically or physically authorised access to any IT system.

A Threat, as in the previous section, refers to anything that has the potential to cause serious harm or damage to an organisation’s IT systems or assets.

Then, what is an Insider Threat: the CERT Guide to Insider Threats [11] defined Insider Threat as: “ A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems” . However, CERT updated their definition in March 2017 to cover both malicious and unintentional acts as: “ the potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization”[21]; Also, they developed a new diagram as shown in Figure 2.2 to assist further expansion of the definition.

Another definition by RAND is as follows: “ malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems”. Also, Greitzer et al, in their paper argue that an insider threat refers to: “ harmful acts that trusted insiders might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual ” [30].

A simple definition by Pfleeger et al[71] is “ An insider’s action that puts at risk an organization’s data, processes, or resources in a disruptive or unwelcome way” .

Finally, the UK CPNI [19] define the insider threat is: “someone who exploits, or has the intention to exploit, their legitimate access to assets for unauthorised purposes ” .

Our definition for Insider Threats is as follows:

Any malicious or unintentional activities that cause damage to an organisation’s IT and network infrastructure, applications, or services. On the part of an employee (current or former), contractor, subcontractor, supplier, or trusted business partner. Who has or has had authorised access to the organisation’s IT assets. And poses a significant negative impact on the information security elements (confidentiality, integrity, and availability) of the organization.

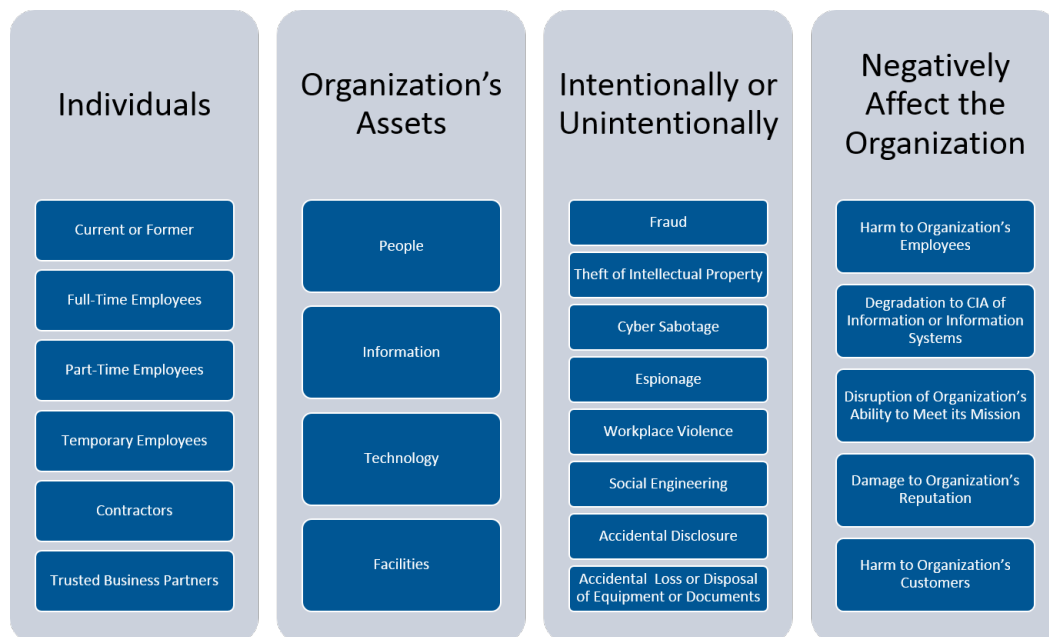


Figure 2.2: Insider Threat Definition Scope by CERT

2.5 Reasons for Misusing Privileged Access

Based on Wood's assumption [95], an insider threat requires three factors for the attacker to misuse his privileges: a) an insider attacker must have the motivation to attack *a motive*, b) must identify a target *an opportunity* and c) must be able to launch an attack *a capability*. A recent study by Colwill [17] reports that insider attacks are made with varying degrees of motivation, opportunity and capability. Motivation will come from internal, personal drives, whereas opportunity and capability will be given to insiders overtly by his/her former or current organisation to perform their role, or may be attained covertly once they are on the inside(191).

A motive: "The reasons for action - is what encourages an individual to act in a certain way or at least develop an inclination for specific behaviour. It can also be defined as the forces within an individual that push or drive him to satisfy his needs [69]. Motivation for an insider attack can be for profit, revenge, sabotage, provoking change, self-satisfaction, patriotism, stress, or ideological reasons [95] [25].

An opportunity: This is a set of circumstances that makes it possible for an insider to act out a malicious threat, with a low risk of being identified. Opportunities can consist of privileges to access the system, system authorised access level, extensive knowledge of the target, system role, or trust [95].

A capability this is the power or ability for a malicious insider to misuse his privileged access to achieve his goal. This then leads to an insider threat security breach. Capability can be through a set of skills, knowledge, and tactics on the part of the insider with regard to an attack [95] [51]. Figure 2.3 shows the main reasons for misusing privileged access.

2.6 Insider Threat Categories

We can divide the insider threat category into seven sub-categories, based on the manner in which they affect the organisation's information security goals (confidentiality, integrity, and availability), and the human factors which lead an insider to act in a malicious manner (motive, opportunity, and capability).

We can also name the insider threat categories in term of the impact and the actions that the insider uses to achieve his aims. These are: *a)* insider IT sabotage, *b)* insider IT fraud, *c)* insider theft of intellectual property, *d)* insider social engineering, *e)* unintentional insider threat incident, *f)* insider in cloud computing, and *g)* insider national security [11] [9] [14] [26]. However, organisa-

2.6.1 Insider IT Sabotage

Insider information technology (IT) sabotage are attacks in which the insider uses his/her IT experience and knowledge to launch an attack on an individual or an organisation. In general the attacker mainly targets the availability of the IT and network infrastructure, applications and services, when they feel they are under pressure or stress from their organisation or from colleagues. In general, insider IT saboteurs are former employees, working remotely, without authorised access to target systems, working outside normal hours, who prepare themselves and plan the attacks, and use tools to launch such attacks. The main targets are databases, systems, services, and network devices.

From the CERT insider threat cases database, an employee spreads rumours across his organisation, that annual bonuses would be smaller than in previous years. This drove a malicious IT employee to design and program a logic bomb from a remote distance. He used authorised VPN access to move the malicious program to all company servers as the foundation for his revenge if the rumour is proved to be true. After he found out that the company was going to reduce the annual bonuses of all staff, he resigned, and then set the logic bomb to go off two weeks later. This deleted company files and disrupted thousands of servers across the USA. However, the insider was convicted and sentenced to more than eight years in prison [11].

It is clear that this piece of IT sabotage was caused by an employee wanting revenge on his organisation in order to achieve self-satisfaction. Usually the employee has high stress levels caused by his organisation, or is aware of the danger of losing his job.

2.6.2 Insider IT Fraud

Insider IT fraud is the case where an insider uses authorised access for personal gain. This abuse can be in the form of creating, modifying, deleting or, in some cases, selling confidential data assets. This fraud also affects data asset confidentiality and integrity. Insider fraudsters in general are current employees, working in an office, who have authorised access to information assets, are in a non-technical position, who operate during normal hours, and who do not need tools to launch the attack. The main insider target is information assets.

A case study of insider IT fraud published by the Department for Business Innovation and Skills in the United Kingdom shows how a malicious insider working for a large utility company, having authorised access to sensitive company inform-

ation could harm the organisation's confidentiality and profits by selling customer data asset to competitors. However, the organisation accidentally discovered this breach after months following a huge financial impact on their business. The value of the losses was several hundred thousand pounds.

It is clear that IT fraud is caused by the greed of employees who work to benefit themselves for financial gain. Usually the employee is suffering from high financial pressures caused by the outside environment, and is unable to solve the problem through legitimate means. This is what motivates the fraud crime in the first place [83].

2.6.3 Insider Theft of Intellectual Property

Insider theft of intellectual property (IP) is that an insider uses the IT infrastructure to engage in espionage or steal information created and owned by the organisation which employs him. Insider thieves of intellectual property in general are current employees, or employees working in their resignation notice period, working in the office, who has authorised access to intellectual property. They tend to hold technical positions such as scientists, programmers, engineers, or sales, during normal hours, and do not need tools to launch an attack. The main insiders targets are source codes, business plans, strategic plans, product information such as designs formulas and schematics, and customer information [11].

In a case study of the theft of intellectual property in September 2013, a mobile telecommunication company in Germany suffered a data breach caused by an insider who had close knowledge of their IT infrastructure and system. He managed to take a copy of more than two million customers' records, such as customer names, customer addresses, date of birth and bank account details [55].

The theft of intellectual property is usually done by someone who has been a part of the process that creates the organisation's intellectual property. They think that the information asset belongs to them. Other types of people who steal intellectual property are those who want financial gain for themselves.

2.6.4 Insider Social Engineering

Insider social engineering is when malicious insiders act to psychologically manipulate another innocent employee without their knowledge to disclose confidential information or perform an action to harm the organisation's IT, network infrastructure, applications or services. However, insider social engineering occurs

when the insider or outsider does not have the authorisation to access part of, or all of, the organisation's assets. Insider social engineering in general involves an employee or outsider, using psychological manipulation, working inside normal hours, preparing them selves and planning before the attack, involving a human-based and technology-based attack. It may be a multiple-stage attack, on the part of individual who does not have authorisation access to target systems, and uses phishing tools to launch the attacks. The main targets are access user names and passwords to a database, systems, services, and network devices.

From the CERT insider threat cases database, government organisations have been the target to insider social engineering, in that employees have been tricked by a phishing email sent to them regarding human resource benefits that exploited a zero-day vulnerability and downloaded malicious code. The code hides itself on the target system and acts as the back door for the outsider allowing the malicious outsider to transfer government information [14].

It is apparent that insider social engineering is caused by someone who has no authorised access to the target systems, and whose main reason for social engineering is to sabotage the IT system, steal intellectual property, or commit fraud using IT systems.

2.6.5 Unintentional Insider Threat Incident

An unintentional insider threat incident is one in which an authorised user accidentally performs an action to harm the organisation's IT and network infrastructures, applications or services, without the motive or intention to mount a malicious attack [41]. Unintentional insiders in general are current employees, working in the organisation's office during normal hours, who have authorised access to the target system, who causes an unplanned incident, without a target or malicious motive.

A mistake by an accounts manager working in a pharmacy company in the USA drove her company to fire her after performing an accidental security breach. The unintentional insider downloaded a file containing the prescription information of 6,000 patients with full patient details onto a USB memory stick, which she then lost, because she did not realise that this was against company policy [75].

There is no doubt that unintentional insider threat incidents occur when the victim has no security awareness training, poorly understands organisation secur-

ity policy, poor management systems, work under high job pressure or stress, is involved in difficult tasks with a lack of knowledge, and uses drugs [41] [9].

2.6.6 Insider in Cloud Computing

Insider in cloud computing or insider in service providers, are those working inside service provider company environments, who perform malicious insider actions without the client's knowledge in order to harm their data asset confidentiality. However, there are neither possible ways of detecting such an attack during or even after the breach, as the client has no control over service provider infrastructures or any effective method and tools to prevent such an attack. Insiders in the cloud in generally current employees, working in a technical position, during normal hours, who have fully authorised access to target infrastructure, who are well planned, and have a malicious motive. The main insider targets are data assets such as databases, source codes, business plans, and strategic plans [26] [53] [96].

In a case study, an experienced IT administrator, working for a cloud computing server provider, used his skills to act as a malicious insider. He managed to take a copy of a client's virtual machine file as part of his duties, and then he broke into the client's administrator account by using password cracking tools. This gave him full access to the client's operating system on the virtual machine without the client's knowledge.

Malicious threats from inside the cloud computing providers and caused by their employees are increasing. Using their authorised access rights to the environment, they commit security breaches such as file recovery, coping virtual machine files, and removing disks from a RAID.

2.6.7 Insider National Security

Insider national security threats involve an insider using their authorised access to represent a threat or do harm to a country's national security. This threat can include damage to the country through espionage, sabotage, disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. Their main targets are the national security secret information.

The biggest intelligence leak in the U.S. history was launched by a malicious insider (a trusted IT contractor and infrastructure analyst) who worked for the National Security Agency (NSA). Edward Snowden managed to download millions of documents on classified intelligence collection programs, as he had the authorised access to mass electronic surveillance data as part of his job. Then he leaked classified material to media outlets. Since then he has released details of unwarranted NSA hacking of friends and foe alike, the fallout damage U.S. relations abroad and putting a spotlight on current security issues facing the U.S.

Insider national security threats usually come from insiders as they have the trust of the government. The motivations for their malicious actions are money, psychology, accident, revenge or, as in Snowden's case, " My sole motive is to inform the public as to that which is done in their name and that which is done against them, I do not want to live in a world where everything I do and say is recorded " [37].

2.7 Summary

The starting point of this study is to define the nature of the insider threat issues and identify the various categories of insider threats. In this chapter, we have provided the necessary background and literature review for the topics in the thesis. We started by reviewing the definitions of insider threats from different sources and we came out with one up-to-date definition of insider threats, that includes malicious and unintentional insiders motivation. Finally we have categorised the different types of insider attacks into sabotage, fraud, IP theft, etc. Based on the CIA security principles (confidentiality, integrity, availability), and also human factors (motive, opportunity, capability) , which has been summarised in Table 2.1.

Figure 2.4 shows the categories of insider threats. An organisation could be targeted in any of the categories or more than one categories at the same time. For example, a malicious insider could act to steal intellectual property by psychologically manipulating another innocent user and use social engineering to obtain higher privileges to access more resources.

In the next chapter, we will review the current approaches to mitigate the insider threats and discuss their advantages and limitations to find the research gaps.

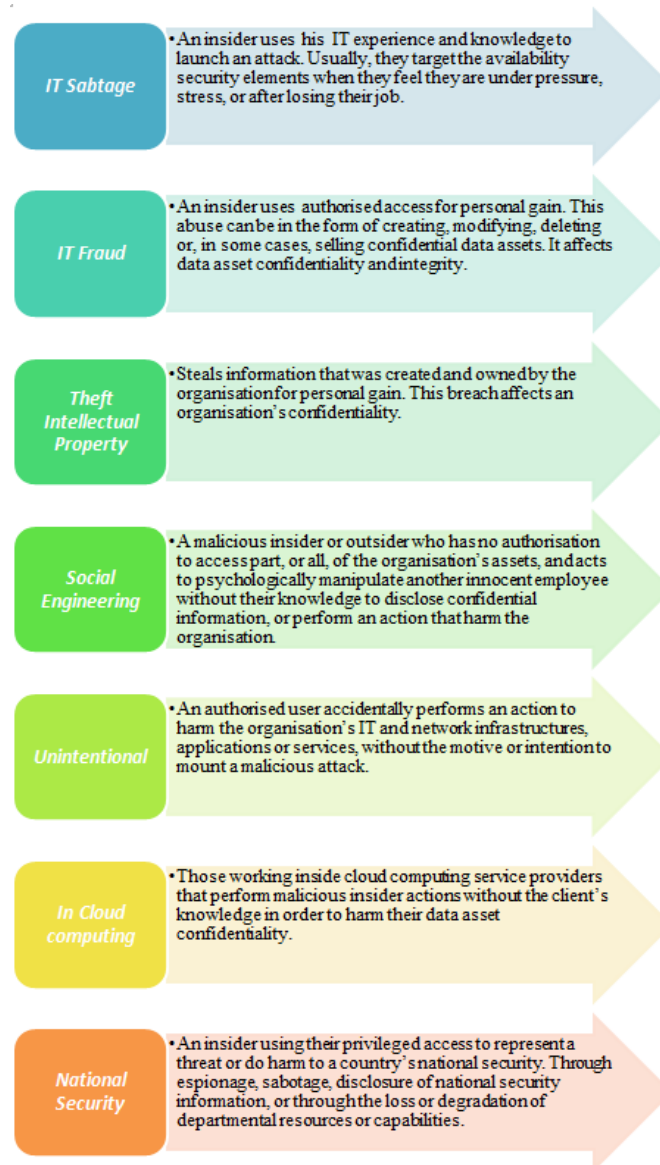


Figure 2.4: Summarise of Insider Threat Categories

Chapter 3

Insider Threats Mitigation Approaches

Regardless of significant work over the last years, the research community has made slight overall progress in mitigating the insider threat. As malicious insider threat activities are still detected by individuals who are not part of the organisation's security staff, with only one in five activities detected using a combination of automated tools for logging, monitoring and flagging suspicious activity, along with manual diagnosis and analysis [52] [97].

In this chapter, a research literature review of various approaches towards insider threats and controls are presented in order to explain how we could mitigate insider threat. These approaches can be broadly classified into two categories: *a)* technical mitigation approaches and *b)* non-technical mitigation approaches.

3.1 Technical Controls to Identify Insider Threats

In general technical controls are divided into two main categories: *a)* those that look for unauthorised malicious activity, and *b)* those that look for changing in behaviour that may indicate a malicious insider [31]. In addition to this, technical control tools could be implemented to concentrate on: *a)* network-based activities, *b)* host-based activities, or *c)* cloud-based activities.

3.1.1 Intrusion Detection Systems (IDS)

The National Institute of Standards and Technology (NIST) [82] defines Intrusion Detection (IDS) as the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. It also defines IDSs as software that automates the intrusion detection process.

Intrusion Detection Systems deployed to detect malicious intruders in real time originate from external threats, and are based on monitoring networks or endpoint devices through analysing activities and traffic patterns from any abnormal behaviour in the network and endpoint, or through matching the activities and traffic with a database of attack signature.

When intrusion detection system detects abnormal behaviour or an attack signature it initiates a security alert. As IDS gathers information over different platforms in real time, it is a helpful tool for discovering a malicious insider by analysing information of any change of user behaviour or activity that may lead to data breaches [2] [6].

However, IDS has its limitations in dealing with insider threats such as: a high number of false alarms, a huge database log file size, and requiring an administrator to analyse the traffic and behaviour. In addition, it cannot monitor encrypted traffic [97]. Furthermore, Cyber-Security Centre at the University of Oxford [26] concluded that IDSs are far from ideal for detecting insiders as they are primarily focused on external attackers and have a tendency to identify false positives.

3.1.2 Security Information & Event Management (SIEM)

Security Information and Event Management (SIEM) is a tool that is responsible for centralising and analysing logging in one management platform, it collects information through secure network channels from various security-related logs (ranging from client workstations and servers to application servers, antivirus software, network devices, honeypots, firewalls, IDSs), and any other sensors in the network, then correlating the events among them in a database by matching any related characteristics and events [28] [87].

This approach allows the information security administrator to quickly search for events and possibly identify malicious insider activity before it occurs, or as a

data-mining tool and evidence for forensic investigations after the accident occurs [88] [13].

3.1.2.1 Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders

Lewellen et al [88] implemented an approach to audit the use of USB device within a Microsoft Windows environment. In their approach they wrote batch scripts, installed in all user devices with host-based intrusion-detection system (HIDS).

Any activity done by users will be logged into log centre, by which information technology professionals analyse these logs for any malicious insider threat. Figure 3.1 shows a snippet of code from the usbHistory.bat script [88].

```
1 @ECHO OFF
2 SETLOCAL
3 :: The below line tells the script where it is stored and where working files will be kept
4 :: Change the path below to reflect where it will be on the local machine.
5 SET pth="C:\Admin_Tools\USB_Audit"
6 %pth%\usbHistory.exe > %pth%\newlog.tmp
7
```

Figure 3.1: USB History.bat Script

3.1.3 Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is a technology responsible for the early detection of data exfiltration attempts by a malicious or unintentional insider. It is performed in three steps:

- system discovery - scanning storage devices, capturing network data flow, and watching user behaviour on endpoint devices.
- leaked confidential data identification - information discovered in the system discovery step could be identified if they are secret information in three ways: keyword matching, regular expressions, or hashing fingerprinting.
- organisation policy enforcement - this step prevents any action that could cause any security breach in identified confidential data in the previous step [43].

The benefit of using a data loss prevention approach is that we can use it to protect three types of data in an organisation, or part of any type, depending on business need. These types are:

- Data at rest - refers to inactive data or static data that is stored physically on enterprise devices.
- Data in motion - refers to data captured in the moment of data traffic flow.
- Data in use - refers to active data assets under constant change, data in operation as they are processed by applications or endpoint agents [91] [43] [34].

However, these research groups use this technology to deploy new insider threat potential approaches such as: web traffic inspection [34] [56]; Virtual Private Network (VPN) data flow monitoring; and Correlating Events from Multiple Sources such as Universal Serial Bus (USB) [88] [86].

3.1.3.1 Traffic Inspection Approach

Silowash et al [34], developed a new system to detect and prevent data exfiltration through encrypted web sessions via traffic inspection, Their system acts as a Man-in-The-Middle¹ Proxy, where MiTMs is a type of attack that interrupts and inspects all uploaded attachment message encrypted with SSL encryption[29].

First they install Squid² to be working as MiTM over Ubuntu Linux platform. Afterwards they scan outbound web-based traffic using C-ICAP³ and ClamAV⁴. Finally redirect all clients requests to a proxy server by using Certificate. Figure 3.2 shows traffic inspection network structure [34].

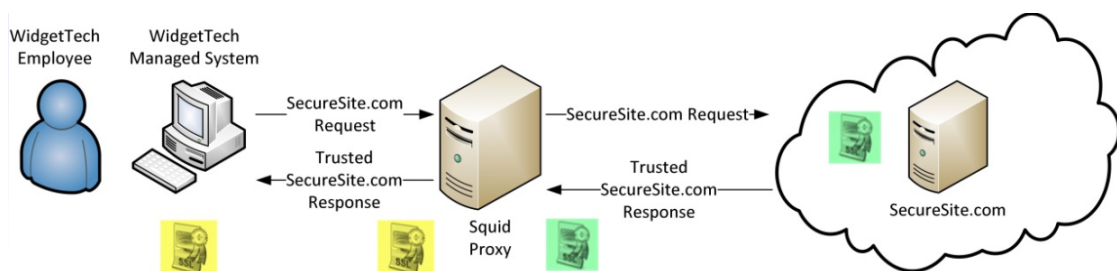


Figure 3.2: Traffic Inspection Network Structure

¹**Man-in-The Middle (MiTM)** attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party.

²**Squid** is a caching proxy for the Web supporting HTTP, HTTPS, FTP.

³**C-ICAP** is an implementation of an ICAP server. It can be used with HTTP proxies that support the ICAP protocol such as the Squid server to implement content adaptation/filtering services.

⁴**ClamAV** is an open-source, GPL licensed, anti-virus engine

It is important to note that, this approach could prevent intellectual property leakages with only tagged attached file. That means we need to tag all documents with known tag to proxy server to generate a signature, such as:

*FOR OFFICIAL USE ONLY: 0 : **
:464f52204f4646494349414c20555345204f4e4c59

3.1.3.2 HTTPS Traffic Inspection Approach

In the previous approach Silowash et al [34] did not add the scenario if an insider copied intellectual property and past the text into the body of webmail message. Consequently, Lewellen [56], implemented a new system based on the previous approach to inspect text-based HTTP/S traffic, to block the connection in near real time. To do this they have added java text indexer (Apache Lucene) to Squid proxy server.

The threat of these approaches is that the proxy server will act as a Intellectual Property warehouse, which could bean attack target for malicious insiders.

3.1.4 Access Control System

Access control is the system that manages and controls the access credentials to specific electronic resources based on a) authentication “who you are”, and b) authorisation “what you are authorised to do” components, in relation to the security policy of an organisation. The rules are based on different principles such as: **a)** least privilege, **b)** privilege escalation, and **c)** separation of task duties [46] [20].

Whether using Role-Based Access Control (RPAC), Mandatory Access Control (MAC), or Discretionary Access Control (DAC) models, the insider threat is granted access by system authentication and is authorised to perform the necessary tasks. An access control system ensures that an organisation’s security administrators have control of their asset and they can change the authorisation access level, or deny access at any time, when needed [81].

3.1.5 Honey-tokens

A honey-token is a method used to attract malicious insiders, and help to detect, identify and confirm a malicious insider threat [90]. Moreover, it may be effective in catching insiders who are snooping around a network. The honey-token is a technique that is a part of honeypot technology. However, it is different to other types because it could be any interactive digital entity, such as a Microsoft Office document, rather than a hardware device or software.

The main concept is that no one should interact with the trap, and any interaction with the digital entity will indicate to the security administrator that there could be the threat of a malicious insider.

As an example, if a company general manager (GM) suspects that one of his information technology (IT) staff is checking his emails, owing to the fact that an IT employee has full authorisation to access to emails, then they could use the honey-token approach to generate an email to the GM. This email should contain interesting information to attract an insider. Then, this honey-token leads the insider to use a user-name and password within the email to access the honey-token, as no one else has the user name and the password. When a malicious insider accesses the URL, insider information such as the IP address, device name and user domain name will be sent to the IT security team to deal with this breach.

From: Human.Resource@example.com

Subject: Important HR System Login

Date: Thu, 15 Jun 2015 06:11:44 +0800

To: GM@example.com

Dear GM,

please find below your new login and password for our new HR system.

You could use this information to view all employees information.

Please Do Not Share This Information With Anyone.

URL:<https://hr.example.com/login.php>. Login: GM001. Password: Gm001.

3.2 Non-Technical Approaches

From the fact that insider threat “is a people problem” and “the trust we give”, mitigating the threat level of a malicious insider is a difficult issue that requires dealing with human behaviour, instead of only dealing with this issue by using a technical approach. As we have seen in the past five years whistle-blowers have managed to avoid all major technical controls. At this point, institutions and researchers should start to look into the problem of insider threats from different points of view, such as - **a)** prediction, **b)** training and awareness, and **c)** security policy.

3.2.1 Psychology Prediction Model

Based on the psychology of user behaviours, researchers have found psychology indicators related to a malicious insider threat. These three factors are: **a)** insider attackers must have the motivation to attack, “a motive”, **b)** they must identify a target, “an opportunity” and **c)** they must be able to launch an attack, “a capability” [84].

Axelrad et al. [1] proposed a model to predict insider threats. The motivation behind their approach is to define 83 psychological variables potentially associated with insider threats. The approach was to analyse these variables and estimate a score power to each variable. Variables include: **a)** dynamic environmental stress, such as life and job stress; **b)** personal characteristics, such as job satisfaction; **c)** insider actions, such as personal attitude; and finally, **d)** the degree of interest, such insider threat profile.

To generate a single score to measure degree of interest for each authorised person they used Bayesian Network⁵, Figure 3.3 shows Bayesian network variables and structure [1]. However, the downside of their approach is depending on judgement of the score estimates of each variable of 83 variables.

Greitzer et al. [38] [40] proposed another classification method for malicious insider threats based on the case studies of previous insider crimes. Their approach began with setting 12 indicators associated with insider threats. These are: **a)** disgruntlement, **b)** not accepting feedback, **c)** anger management issues, **d)** disengagement, **e)** disregard for authority, **f)** performance, stress, **g)** confrontational behaviour, **h)** personal issues, **i)** self-centredness, **j)** lack

⁵**Bayesian Network** is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a directed acyclic graph

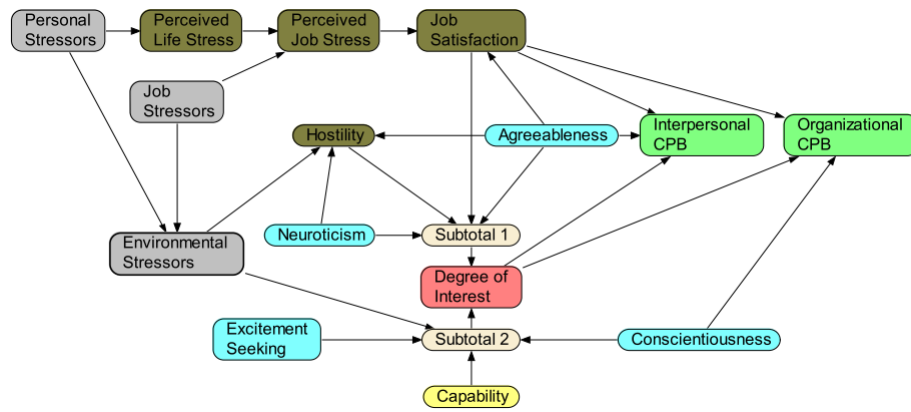


Figure 3.3: Bayesian Network Variables and Structure

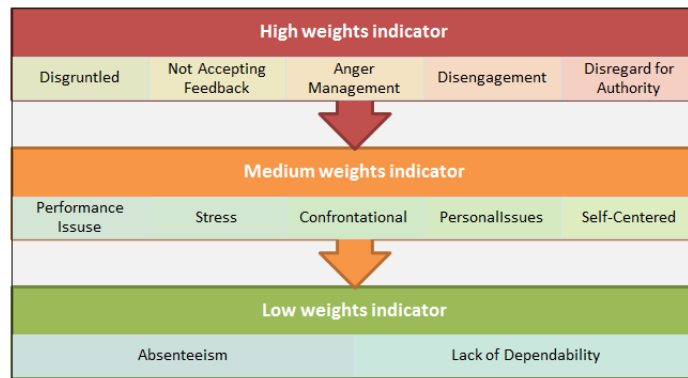


Figure 3.4: Greitzer’s Risk Indicators

of dependability, and finally *k*) absenteeism. Figure 3.4 shows Greitzer’s risk indicators classified by the weights of the indicator to risk levels.

Both models in this section claim to help decision makers to determine whether the user is a potential malicious insider threat or not, based on scoring indicators [65]. However, no evidence of any kind of real implementation of these models approves their claim.

3.2.2 Security Education and Awareness

Insider threat accidents could be avoided by the appropriate security education and awareness training [85], especially the category of the unintentional insider threat. The Ponemon Institute [72] reports that 62% of organisations conduct regular privileged user training programmes as part of their efforts to protect the organisation from insider threats, with 11% of the IT budget allocated to security education and awareness .

Educational and awareness training could include the following areas: *a)*

presentations by outside speakers, **b)** classroom courses, **c)** on-line training courses, **d)** the organisation's internal website, email and social media newsletters update feeds, and **e)** printed leaflets. Training objectives may include: **a)** incident reporting procedures and responsibilities, **b)** consequences and sanctions, **c)** handling of sensitive information, **d)** intellectual property protection, **e)** insider threat indicators, **f)** social engineering scams, and **g)** unintentional leaking.

3.2.3 Information Security Policy

Organisation's information security policies deliver the framework that sets the most critical controllers within the organisation once the organisation's objectives have been identified. It comes in a detailed statement of employees' expectations of an organisation, and what is expected from them in terms of information security, and the acceptable behaviour and culture within the organisation [48] [66] [78].

A recent paper by the Cyber Security Centre at the University of Oxford [9] focused on the ability of an organisation's information security policies to mitigate the level of a malicious insider threat. In their paper they pointed out the fact that the risk of an unintentional insider threat is potentially more pressing than that posed by other malicious insider categories. From this point, they found that 45% of employees do not follow security policies for two main reasons: a) the policy was incomplete or poorly defined; or b) the employee was not aware of the security policy. They conclude in their paper that if the information security policy is not followed by all authorised users the unintentional insider treat level will increase.

In September 2014, the USA Department of Defence issued a directive that establishes and ensures appropriate national insider threat policy within the Department of Defence. This prevents, deters, detects, and mitigates actions by malicious insiders who represent a threat to the USA's national security, or Department of Defence personnel, facilities, operations, and resources [24], and that will help to reduce insider threat levels.

From the previous two sections on technical controls and non-technical controls, we can summarise the benefit and the limitation of each insider threats approaches that are described in previous sections on Table 3.1 .

Table 3.1: Insider Threats Approaches Summary

Categories	Approaches	Benefits	Limitations	
Technical	Intrusion Detection Systems	Network & endpoint devices Activity analysis in real time.	Primarily focused on external attackers.	
		Attack signature matching.	High false Alarms.	
		Abnormal behaviour detection.	Huge database log file size.	
			Limitation of dealing with encrypted traffic.	
	Security Information & Event Management	Activities & logging Centralising in one platform from various sensors in network.	Not in real time.	
		Activity analysis by matching any related characteristics and events.	Manual detection.	
	Data Loss Prevention	Early detection of data exfiltration attempts.	Unable to inspect encrypted data if the key is not provided.	
		Keyword matching, regular expressions or hashing fingerprinting.	Not reliable in detecting unsupported file format.	
		Real time policy enforcement.		
	Access Control System	Manages and controls access credentials in various platforms.	N/A	
		Change user authorisation access level, or deny access at any time.		
	Honey-tokens	Malicious attraction.		
		Detect, identify and confirm a malicious insider threat.	No interact with the honey-token as the insider knows the trap.	
		Interactive digital entity.		
Psychology Prediction Model	Prediction a malicious insider before the breach.	High false Alarms.		
	Helps decision makers to determine if the user is a potential malicious insider.	Complexity of getting data to the model from various platforms.		
		Complexity of implementation in real system.		
		N/A		
Non-Technical	Security Education and Awareness	Improve employee behaviour.		
		Increase employees responsible for their actions.		
	Information Security Policy	Helping employees identify and respond appropriately to any security concerns.		
		Reduce unintentional Insider threat accidents.	Employees do not follow organisation security policies.	
	Helps to guarantee the best practices.	Employees do not understand organisation security policies.		
	Detailed statement of acceptable behaviour and culture within the organisation.			

3.3 Techniques and Psychology Prediction Model

Kandias et al. [51] proposed an insider threat prediction model, which focuses on combining two approaches, techniques and psychology⁶. First part of their model is analysing misbehaviour in information systems in real time, based on information gathered from Honeypot⁷, Intrusion Detection System⁸, and system calls⁹. Second part of their model is analysing psychological profiling component such as stress level, system role, and user sophistication. Figure 3.5 shows insider threat prediction model [51].

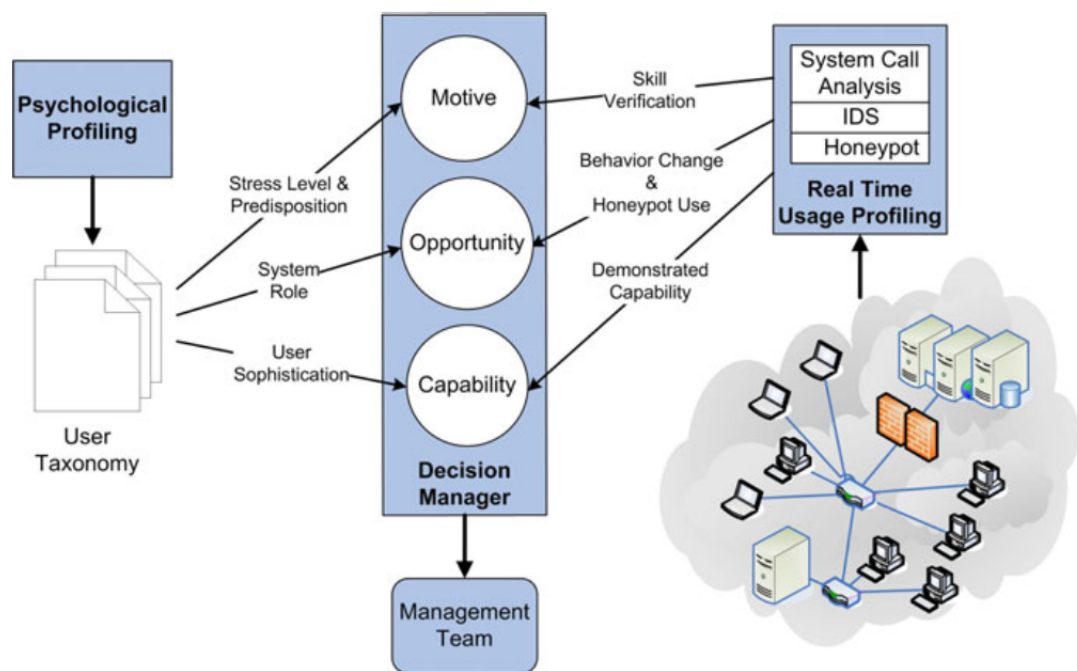


Figure 3.5: Insider Threat Prediction Model

To allow management team to predict a potential insider threat, they have discovered a relationship between all parameters collected from psychological profiling and technical control sources with the three factors motive, opportunity, and capability. where each factor receives an assessment score of the following form: low (1-2), medium (3-4) , and high (5-6) .

⁶**Psychology** is the scientific study of the human mind and its functions, especially those affecting behaviour in a given context.

⁷**Honeypot** is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorised use of information systems.

⁸**Intrusion Detection System(IDS)** (IDS) is a device or software application that monitors network or system activities for malicious activities

⁹**System Calls** is how a program requests a service from an operating system's kernel that it does not normally have permission to run.

Motive of a user M_i is assessed using three parameters: predisposition to malicious behaviour P_i , stress level S_i , and skill verification V_i .

$$M_i = f(P_i + S_i + V_i) \quad (3.1)$$

To measure level of predisposition to malicious behaviour they used the Computer Crime Index and Social Learning Questionnaire¹⁰ (CCISLQ)[79]. Second parameter to measure is the stress level which is based on psychometric test[74], evaluating both personal and professional stress. Finally, skills verification level declared users' skills during the psychometric test.

Opportunity for a user O_i is assessed using three parameters: change of work behaviour B_i , system role R_i , and honeypot use H_i .

$$O_i = f(B_i + R_i + H_i) \quad (3.2)$$

Change of work behaviour measured during the interaction with the IT infrastructure could indicate that a user is in the process of finding a possible target in the system. Second parameter to measure is user systems role which is based on user organisational structure position, which can be “novice, “advanced or “administrator”, Finally, if user interacts with the honeypot system, it will indicate a high risk of an attack.

Capability for a user C_i is assessed using two parameters: Demonstrated Capability D_i , and User Sophistication S_i .

$$C_i = f(D_i + S_i) \quad (3.3)$$

Demonstrated capability is measured by system call analysis tools and IDS, where User Sophistication is measured from user psychometric test.

Threat score T_i is measured using a simple scoring system, the sum of Motive, Opportunity, and Capability. T_i reflects the user into four scouring categories: no risk (3, 4), medium risk (5, 6), high risk (7, 8), and very high risk (9).Table 3.2 shows overall thereat score of T_i [51].

$$T_i = f(M_i + O_i + C_i) \quad (3.4)$$

However, there are limitations in their approach. First limitation is on IDS, as it depends on monitoring the ports of network switches (SPAN switched port

¹⁰CCISLQ is a PhD thesis at Department of Psychology, University of Manitoba Winnipeg, Manitoba

Table 3.2: Threat Scour

Motive	Opportunity	Capability		
		Low	Medium	High
Low	Low	3	4	5
	Medium	4	5	6
	High	5	6	7
Medium	Low	4	5	6
	Medium	5	6	7
	High	6	7	8
High	Low	5	6	7
	Medium	6	7	8
	High	7	8	9

analysis), which cannot analyse encrypted data or traffic over encrypted channels such as secure virtual private network (VPN) or secure web connection using Secure Sockets Layer (SSL)¹¹. Second limitation is on using system logs as any action taken in the system should be logged and be processed in the real time, which will be limited by the resources and performances of information infrastructure.

3.4 A Framework for Characterising Attacks Approach

A framework for characterising insider attacks has been proposed by Cyber-Security Centre at University of Oxford [64][9]. They started with collecting 80 insider threats cases from the UK's Centre for the Protection of National Infrastructure (CPNI) [19], CMU- CERT[11], and published reports. Additional to that they collect data by creating a survey, then they started analysing collected data by adopting grounded theory approach¹².

Figure 3.6 shows the framework they proposed, which contains four classes of components: **a)** Catalyst refers to the overarching reason for the incident, **b)** Actor characteristics which capture the state of the insider, **c)** Attack characteristics detail the elements relating to the attacker, **d)** Finally organisation characteristics include organisational assets and the vulnerability, while solid arrows indicate a definite relationship between the elements and dashed lines potential relationships[64].

¹¹**Secure Sockets Layer (SSL)** is a standard security technology for establishing an encrypted link between a server and a client

¹²**Grounded Theory** is a qualitative research approach, which is a systematic methodology in the social sciences involving the discovery of theory through the analysis of data

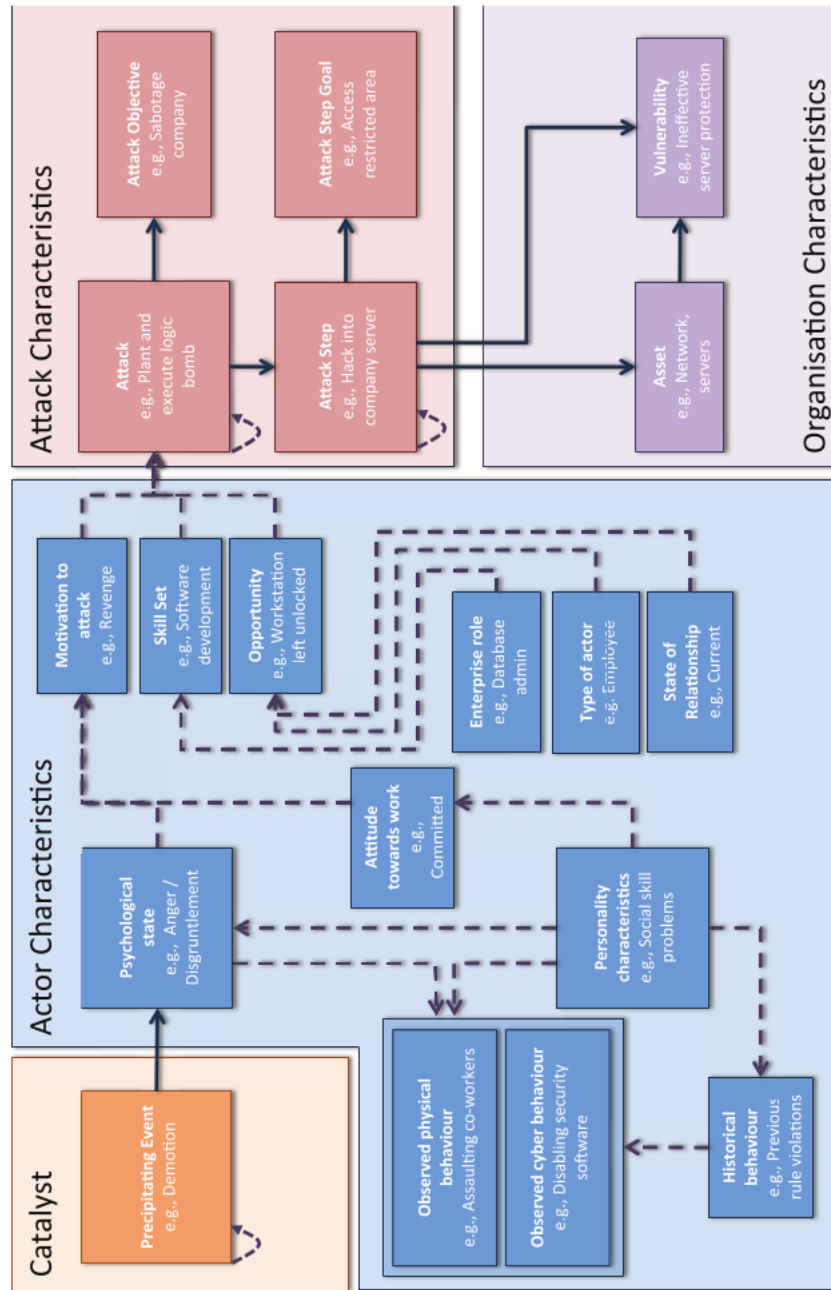


Figure 3.6: A Framework for Characterising Insider Attacks

3.5 Summary

In previous years, organisations, governments and armed forces all around the world, have failed to mitigate malicious insider threats through their regular security measures. Moreover, these kinds of security breaches have started to affect our entire society. In this chapter, we have considered the current approaches and controls associated with mitigating the level of insider threats.

The main approaches presented in this chapter have been classified into two categories: technical mitigation and non-technical mitigation approaches. Their advantages and drawbacks for each of these techniques have been summarised in Table 3.1.

The approaches presented in this chapter can prevent and reduce the risk of insider threats, Unfortunately we have found that there is no one solution, which can fully eliminate insider threats within an organisation. In addition, a technical approach by itself may not be the most effective way to prevent and detect malicious insider threats.

It has been concluded that no single approach alone could solve the security problem. In order to mitigate insider threats more research in the domain of insider cyber-security threats is needed, and the right approach should be identified for dealing with malicious insider threat from different perspectives.

In the next chapters, we will propose and implement a new framework that will help organisations to prevent from such threats and to deal with any potential insider breaches before it takes place, by adopting the three perspective approaches and extend the hybrid approaches that we have discussed in this chapter.

Chapter 4

Insider Threat Risk Prediction Model

4.1 Introduction

Insider threat issue is complex for the researcher community to address, and to deal with this kind of security breach we have to think differentially, as most of previous approaches address this problem from one aspect - usually a technical solution which is applied to particular applications or systems. We conducted our research using an applied constructive research methodology and injected with other methodologies such as empirical Bayes' methods and a quantitative ¹ method that is related to data collection and analysis.

The novel aspect of this study is that we adapt a multiple perspective approach to mitigate malicious insider threats. The term perspective is used to distinguish how we are looking at what we are looking at. Linstone et al. [57] first proposed a socio-technical approach using multiple perspective concepts in the 80s with regard to applications in terms of technology assessment. The three-dimensions this research is focusing on are: *a)* personal *b)* organisational and *c)* technical perspectives.

Socio-technical approach is a methodology for complex organisational work design that identifies the interaction between people and technology in the workplace. The term also refers to the interaction between human behaviour and society's complex infrastructures.

In addition, McCumber et al. [58] presented a security measures model in nine

¹**Quantitative method** Explaining phenomena by collecting numerical data through polls, questionnaires, or surveys that are analysed using statistical, mathematical, or numerical analysis methods.[61]

distinct boxes, each three layers deep to help us understand the comprehensive nature of information security. The three layers are: **a)** technical **b)** policy and practice and **c)** education, training and awareness. However, it is rare to see any insider threat approach or a real application which has implemented the multiple perspective concept. Figure 4.1 shows the McCumber model.

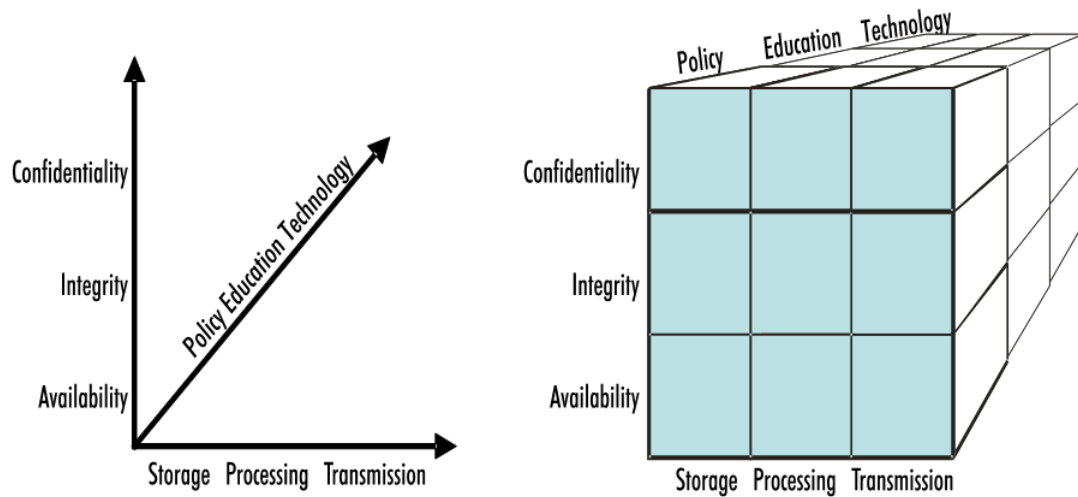


Figure 4.1: McCumber Model

4.2 The Framework

In this thesis we developed a new framework that helps organisations to predict potential malicious insider threats before a breach takes place. The emergency insider threat risk prediction framework is based on a multiple perspective approach integrated with Key Insider Threat Indicators; we predict who could be an insider threat based on the three-dimensions calculation: **a)** Technology Aspect, **b)** Organisational Impact, and **c)** Human Factor. Moreover, every dimension in this framework is divided into a number of layers. Figure 4.2 shows the proposed insider threat risk prediction framework.

Where in this figure, the middle triangle represents prediction risk levels of insider threat, layer one represents our main three-dimensions, layer two and three represent Key Insider Threat Indicators;

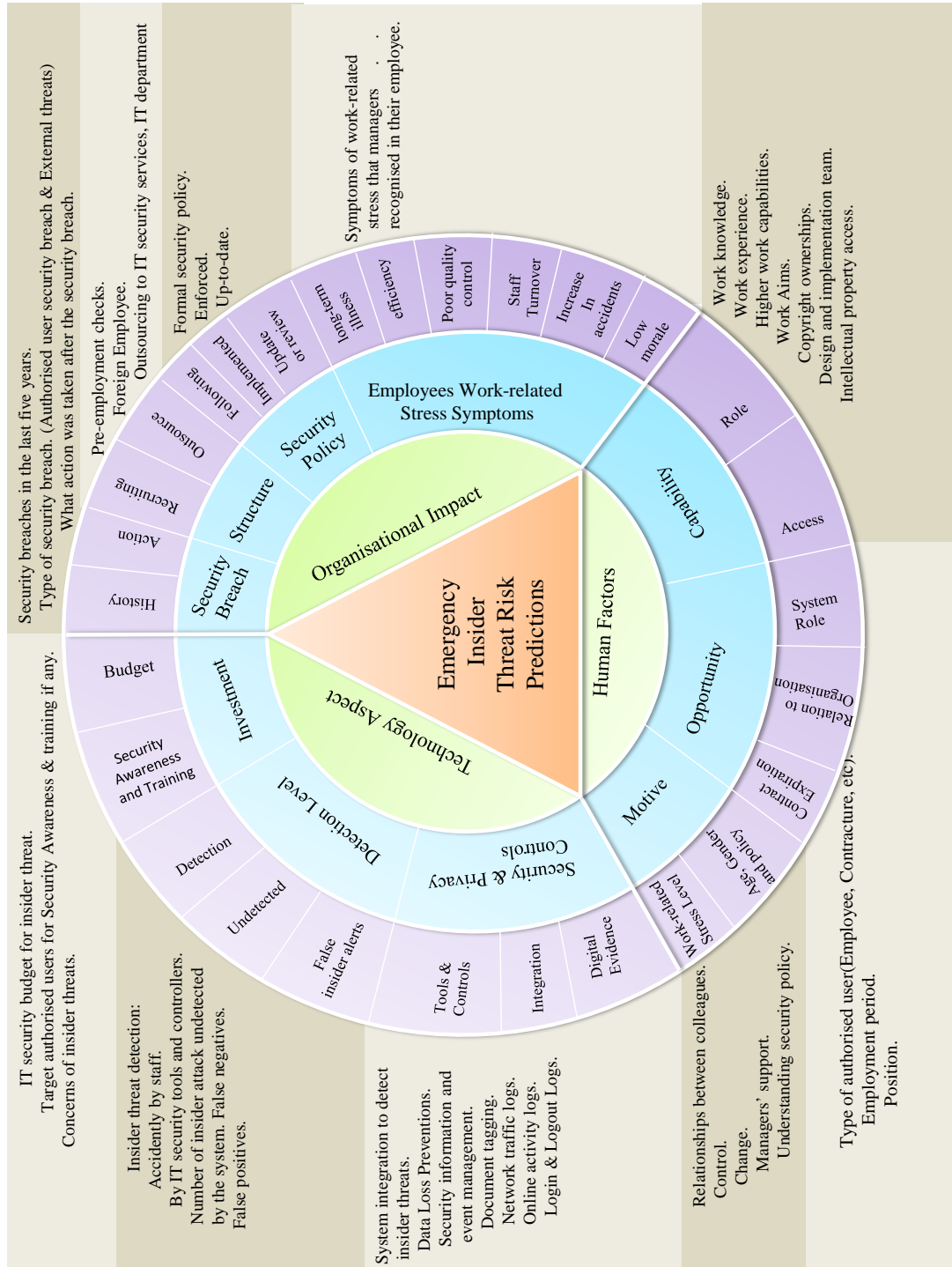


Figure 4.2: Insider Threat Risk Prediction Framework

4.2.1 Human Factor Dimension

As the human factor is always the weakest link in the information security chain, human factors in the context of insider threat started to gain increased attention, mainly where the use of security technologies has failed to protect organisations from malicious or unintentional insider threat [44, 42]. Researchers have argued that insiders have specific psychological characters (behavioural indicators) that need to be under our attention when measuring the level of insider threat risk [65].

In this dimension we measured each authorised user's psychological profiling level. Based on Wood's assumption,[95] a malicious insider threat requires three factors before it comes to the attacker misusing his privileges. These are: Motivation, Opportunities and Capabilities. To measure these factors, we designed our model based on these assumptions as listed below:

- The employee's **motivation** to act as a malicious insider threat, are complex and multifaceted to measure, where it's common for abusers to have more than one motivation for their actions. In this proposed framework motivations are measured by work related stress levels, such as considering authorised users attitude towards the workplace, the support that employees get from line manager or colleagues, relationships between colleagues, and the knowledge of organisation security policy. Also, employee age and gender affect motive levels.[68, 19, 38, 45, 65]
- The **opportunities** that authorised users have to enact any malicious insider threat, as human are expected to realise their intentions when the opportunity arises. In this proposed framework opportunities are measured by authorised user system role, contract expiration dates, and their relationship to the organisation (current employee, formal employee, contractor, etc).[19, 60, 88, 35]
- The **capabilities** factor is to measure the ability and skills of employees have to act on any kind of security breach, where insiders have the privileges and access rights to organisation data assets for a long time that gives the authorised users to know what security measures in place are. We measured the capabilities levels through, for example, employees' access rights to intellectual property and their work knowledge. [4, 60, 49]

4.2.2 Technology Aspect Dimension

Most medium and large organisations have their own Information Technology (IT) department. One of their critical roles is to ensure that they protect an organisation's information assets from any type of security breach [27] such as intellectual property (IP) data leaks. To do this, organisations need to invest in IT security, and also invest in carrying out security awareness training for all authorised users. Then organisations should implement some tools and controls to monitor their systems and take the right action before or after a breach has taken place. Finally, organisations should regularly evaluate their system, and make sure that all security measures are in place.

In our approach, the technology aspect domain is focused on the IT department within the organisation under consideration; we collected information related to the organisation's IT security measures, and how it ensures that insider threat breaches are kept to a minimum. To measure the technology factor level, we collected information in the following three categories:

- **Balance Investment:** between outsider and insider threats is a key to show how executive managers are aware of insider threat breaches. In investment we look into: security awareness and training, and budget spending aimed at minimising the threat from malicious or unintentional insider sources. [17, 93, 94]
- **Detection level:** an important aspect is to measure the level of detection of previous insider attacks with the proportion of false alerts and the techniques used to detect previous insider threat cases, if there is any. [90, 43]
- **Security and privacy controls:** in this category, we focused on forensic evidence, such as network traffic and email logs. [16] In addition, we measured system integrations in terms of detecting insider threats, technical tools and controls (such as security information and event management), and data loss prevention, which organisations commonly use to avoid any security breach. [39, 49, 97, 18]

4.2.3 Organisational Impact Dimension

The UK's Centre for the Protection of National Infrastructure (CPNI) [19] has found that “ where an insider act takes place there is often an exploitable weakness with the employers own protective security or management practices which enables the insider to acting ”. Organisational issues that may affect the risk levels of insider threat should be identified.

In this proposed framework, the organisational impact dimension represents information related to how organisations are structured, and how they manage insider threat breaches. To measure the organisational aspect level, we collect information in the following four main categories:

- **Security breaches:** In this category, we focused on the history of any kind of security breach and also collecting information regarding malicious or accidental insider breaches in the last five years [94]. The other part of this category is the action the organisation has taken in respect to any such previous breaches. [63]
- **Structure:** Here, we collected information in relation to the recruiting procedure, pre-employment screening and IT department outsourcing services [19].
- **Security policy:** This is all the information related to the organisation's security policies: whether they have one and they believe that it is followed by all authorised users or not. [10]
- **Employee work-related stress symptoms:** In this category we collect information relating to the visible stress symptoms to top managers for overall employees that affect the organisation's productivity, such as: increasing accidents, increasing long-term illnesses, and poor performance in tasks. [67][1]

4.3 Modeling Framework

Bayesian network statistical methods were used to implement and test the proposed framework. This is because we can represent the probabilistic relationships between all factors (Human, Organisation, and Technology) by using a directed acyclic graph. where each factor has dependency relation condition with other variable in various layers.

The term Bayesian Networks (BN) was coined by Judea Pearl in 1985 [70] and, in recent years, a number of insider threat approaches have started to rely on this statistical method to implement their models. For example, Greitzer et al. deployed a psychosocial model to assess employee behaviour associated with an increased risk of insider abuse based on a BN model [40]. Also, Axelrad et al. introduced a BN model of the motivation and psychology of malicious insider threats [1]. Moreover, in the cyber-security fields such (Forensic, risk management) BN is increasingly in popular modelling technique. [15].

A Bayesian network is a Directed Acyclic Graph (DAG) in which each node is a collection of random variables of X . The set of random variable values X_i can be referred to as the space of X , where the joint probability distribution of variables of X is $\{X_1, X_2, \dots, X_N\}$.

A network structure specifies the dependency relation condition of variables in X . Each node in the network has a one-to-one relationship with one space of X .

If a node is conditionally independent of its non-descendants given its parents, with a graph network implemented based on the order of the parent's node before its children, as $(1, 2, \dots, N)$. This means that we can find the representation of a Bayesian network joint probability distribution as follows, based on the multiplication law.

$$P(X) = P(X_1, X_2, \dots, X_N) = P(X_N | X_{N-1}, X_{N-2}, \dots, X_1) \dots P(X_2 | X_1) P(X_1) \quad (4.1)$$

$$= \prod_{i=1}^N P(X_i | X_{1:i-1}) \quad (4.2)$$

$$= \prod_{i=1}^N P(X_i | Parents(X_i)) \quad (4.3)$$

where $X_{1:i-1} = (X_1, X_2, \dots, X_{i-1})$, and $Parents(X_i)$ are the parents of node X_i , this formally shows that node X_i is dependent on its parents only and is independent of all its ancestors.

For example, Figure 4.3 represent a simple example to implement a BN. In this example the wet grass (W) can either be caused by rain (R) or by a water sprinkler (S). Where clouds (C) make it less likely that the sprinkler will turn on, but more likely that it will rain.

Based on the previous formulation 4.3, we can represent Figure 4.3 as follows:

$$P(C, S, R, W) = P(C)P(S|C)P(R|C)P(W|R, S) \quad (4.4)$$



Figure 4.3: Simple Bayes Network Sprinkler Example.

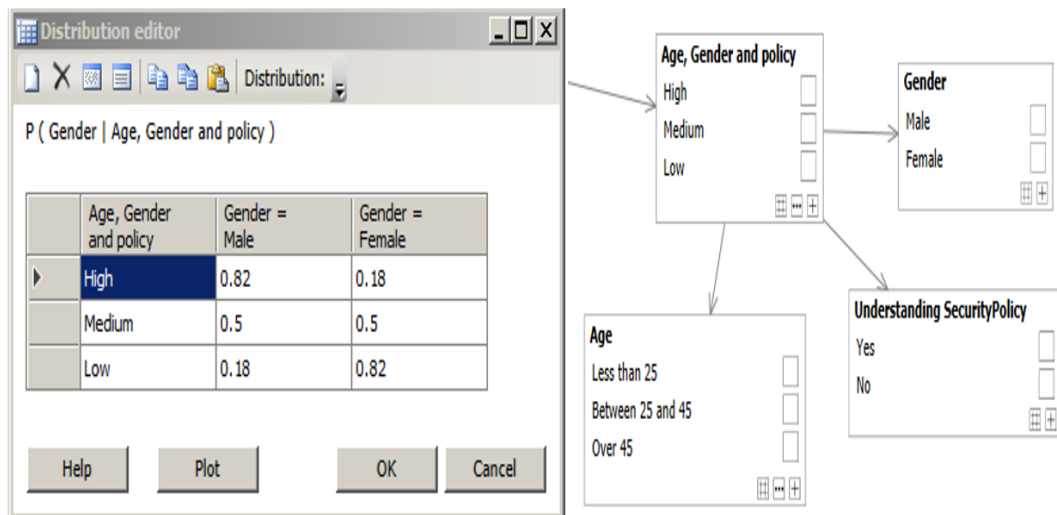


Figure 4.4: A Snapshot of Gender Distribution Editor and Domain

In our approach we went through three stages to implement and develop the model for the proposal framework: a) network construction, b) Prior probabilities, and c) Risk output.

4.3.1 Network Construction

In this phase the network is constructed with linked conditional nodes with different variables that each end node takes one value from a collected data. In our model, we divided the network into three main domains based on the three-dimension factors. Figure 4.5 shows the insider threat risk prediction network model.

4.3.2 Prior Probabilities

After creating all nodes, and linking each child nodes to their partners, we then assigned prior probabilities to each random variable in the network. These priors, which were estimated by us based on literature reviews and domain expert experience, reflect the frequencies at which random variables take on values from their domains. For example, the prior probability that an employee's gender is male, given the probability of (age, gender and policy) is high, is 82 % [19] [60]. Figure 4.4 shows a snapshot of gender distribution editor and domain.

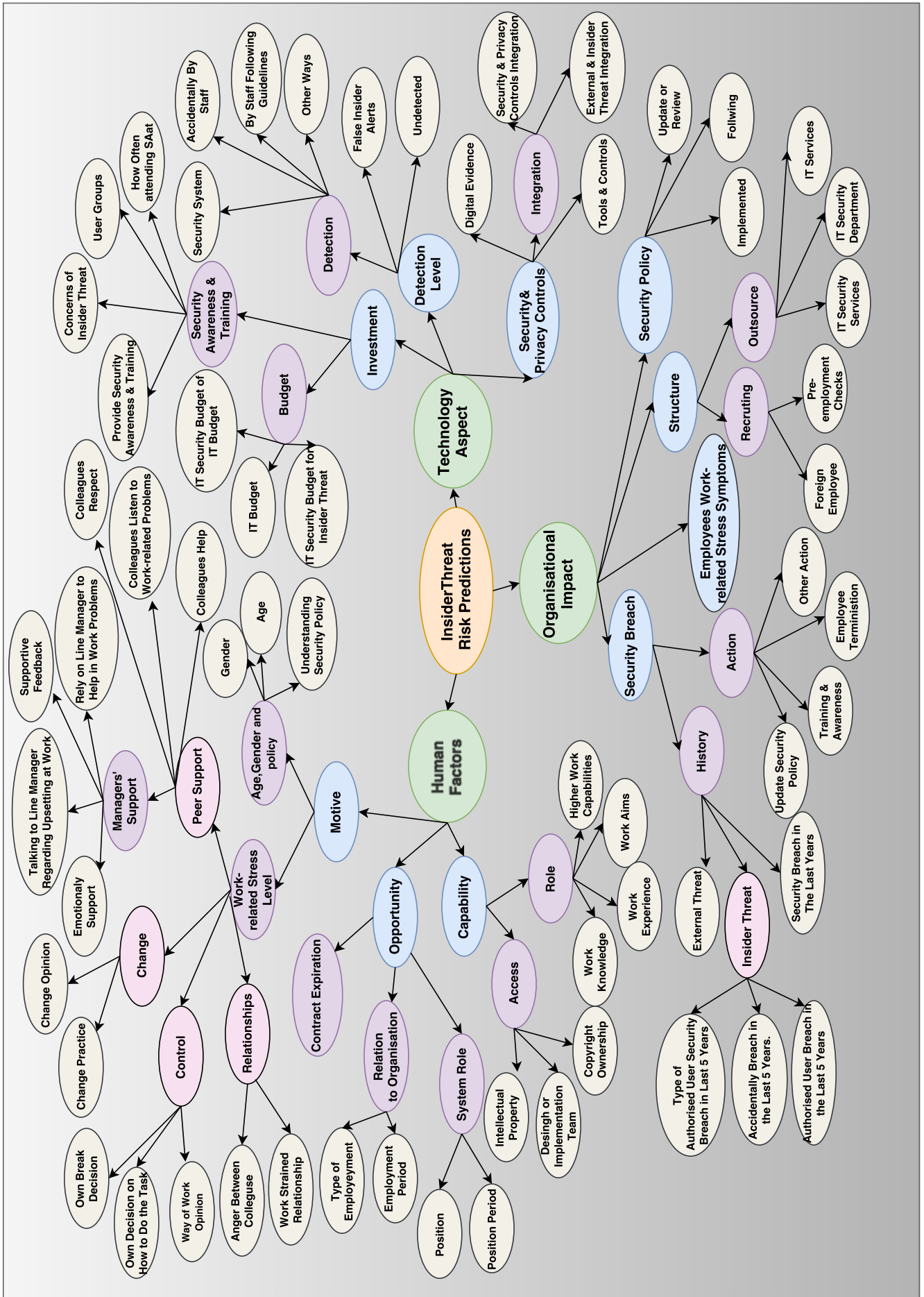


Figure 4.5: Insider Threat Risk Prediction Model Network

4.3.3 Risk output

The purpose of this phase of deploying a Bayesian network is to calculate the effects of the random variables on each internal node until we get to the central node which called Emergency Insider Threat Risk Predictions (**E**).

The probability of insider threat (**E**) given human factor (**H**), organisational impact (**O**), and technology aspect (**T**), can be generated based on these steps:

$$P(E, H, O, T) = P(E | H, O, T) P(H, O, T) \quad (4.5)$$

$$= P(E | H, O, T) P(H|O, T) P(O, T) \quad (4.6)$$

$$= P(E | H, O, T) P(H|O, T) P(O | T) P(T) \quad (4.7)$$

This is based on the multiplication law, where $P(O, T) = P(O | T) P(T)$
 $= P(T | O) P(O)$

Also

$$P(E, H, O, T) = P(H | E, O, T) P(E, O, T) \quad (4.8)$$

$$= P(H | E, O, T) P(E|O, T) P(O | T) P(T) \quad (4.9)$$

Also

$$P(E, H, O, T) = P(O | E, H, T) P(E, H, T) \quad (4.10)$$

$$= P(O | E, H, T) P(E|H, T) P(H | T) P(T) \quad (4.11)$$

Also

$$P(E, H, O, T) = P(T | E, H, O) P(E, H, O) \quad (4.12)$$

$$= P(T | E, H, O) P(E|H, O) P(H | O) P(O) \quad (4.13)$$

From the joint distributions we can get the Bayes formula.

First we can conclude that:

Equation's 4.7 = Equation's 4.9 = Equation's 4.11 = Equation's 4.13

According to Bayes' Rule, therefore, one option is to rearrange the above to get:

$$P(E | H, O, T) = \frac{P(H | E, O, T) P(E | O, T) P(O | T) P(T)}{P(H | O, T) P(O | T) P(T)} \quad (4.14)$$

$$= \frac{P(H | E, O, T) P(E | O, T)}{P(H | O, T)} \quad (4.15)$$

(O and T) can be removed from $P(H | E, O, T)$ as they are a child of variable (E) in the network.

$$P(E | H, O, T) = \frac{P(H | E) P(E | O, T)}{P(H | O, T)} \quad (4.16)$$

Next step is to get $P(E | O, T)$ and $P(H | O, T)$ in equation 4.16 :

$$P(E, O, T) = P(E | O, T) P(O, T) \quad (4.17)$$

$$= P(E | O, T) P(O|T) P(T) \quad (4.18)$$

Also

$$P(E, O, T) = P(O | E, T) P(E, T) \quad (4.19)$$

$$= P(O | E, T) P(E|T) P(T) \quad (4.20)$$

Equation's 4.18 = Equation's 4.20

$$P(E, O, T) = P(E | O, T) P(O|T) P(T) = P(O | E, T) P(E|T) P(T) \quad (4.21)$$

$$P(E | O, T) = \frac{P(O | E, T) P(E|T) P(T)}{P(O|T) P(T)} \quad (4.22)$$

$$P(E | O, T) = \frac{P(O | E, T) P(E|T)}{P(O|T)} \quad (4.23)$$

Remove T as T is the child of E in the network

$$P(E | O, T) = \frac{P(O | E) P(E|T)}{P(O|T)} \quad (4.24)$$

According to the general equation for conditional probability of:

$$P(E|T) = \frac{P(E) P(T|E)}{P(T)} \quad (4.25)$$

Also, According to the law of the total probability of:

$$P(T) = \sum_i P(T|E_i)P(E_i) \quad (4.26)$$

Where $i = 0, 1, 2, 3, \dots, n$ and n is the number of total probabilities.

Then from equations 4.24, 4.25, and 4.26.

$$P(E | O, T) = \frac{P(O | E) P(E) P(T|E)}{P(O|T) P(T)} \quad (4.27)$$

$$P(E | O, T) = \frac{P(O | E) P(E) P(T|E)}{P(O|T) \sum_i [P(T|E_i)P(E_i)]} \quad (4.28)$$

And

$$P(O|T) = \sum_i P(O|E_i) P(E_i|T) \quad (4.29)$$

To get $P(O, T)$, variables (E) is added to the joint probability distribution $P(O, T, E)$, as (E) comes between them on network.

Then

$$P(E, T, O) = P(E | T, O) P(T|O) P(O) \quad (4.30)$$

$$= P(O | T, E) P(T|E) P(E) \quad (4.31)$$

$$= P(T | E, O) P(E|O) P(O) \quad (4.32)$$

Equation's 4.30 = Equation's 4.31 = Equation's 4.32

$$P(O | T, E) = \frac{P(T | E, O) P(E|O) P(O)}{P(T|E) P(E)} \quad (4.33)$$

$$P(O | T, E) = \frac{P(E|O) P(O)}{P(E)} \quad (4.34)$$

$$P(O) = \sum_i P(O|E_i) P(E_i) \quad (4.35)$$

T is added to both side of equation 4.35.

$$P(O|T) = \sum_i P(O|E_i) P(E_i|T) \quad (4.36)$$

From equations 4.28 and 4.29 we get:

$$P(E | O, T) = \frac{P(O | E) P(E) P(T|E)}{\sum_i [P(O|E_i) P(E_i|T)] \sum_i [P(T|E_i)P(E_i)]} \quad (4.37)$$

Second we need to get $P(H | O, T)$

$$P(H|O, T) = \sum_i P(H|E_i) P(E_i|O, T) \quad (4.38)$$

$$P(H|O, T) = \sum_i \frac{P(E) P(H | E_i) P(O | E) P(T|E)}{\sum_i [P(O|E_i) P(E_i|T)] \sum_i [P(T|E_i)P(E_i)]} \quad (4.39)$$

Then

$$P(H | O, T) = \frac{P(O | H) P(H) P(T|H)}{\sum_i [P(O|E_i) P(E_i|T)] \sum_i [P(T|E_i)P(E_i)]} \quad (4.40)$$

From equation 4.37, and equation 4.39 we can get 4.16.

$$P(E | H, O, T) = \frac{P(H | E) \frac{P(O|E) P(E)P(T|E)}{\sum_i [P(O|E_i) P(E_i|T)] \sum_i [P(T|E_i)P(E_i)]}}{\sum_i \frac{P(E) P(H|E_i)P(O|E) P(T|E)}{\sum_i [P(O|E_i) P(E_i|T)] \sum_i [P(T|E_i)P(E_i)]}} \quad (4.41)$$

Then

$$P(E | H, O, T) = P(E) \frac{P(H | E) P(O | E) P(T|E)}{\sum_i [P(E_i) P(H | E_i) P(O | E_i) P(T|E_i)]} \quad (4.42)$$

Where: $P(E)$ is the probability of insider threat for a certain risk level, $P(H | E)$ is the probability of the human factor given the probability of insider threat in a certain risk level, $P(O | E)$ is the probability of the organisational aspect given the probability of insider threat in a certain risk level, $P(T | E)$ is the probability of the technology factor given the probability of insider threat in a certain risk level, $\sum_i [P(E_i) P(H | E_i) P(O | E_i) P(T|E_i)]$ is the sum probabilities for all risk levels from rare to be insider threat to certainly is an insider threat.

This output $P(E | H, O, T)$ is the final and main risk level prediction that

Table 4.1: Mapping the Risk Band to Probability

Rank	Risk Band	Probability Description
5	Certain	Continually experienced insider threats
4	Likely	Insider threat breach will occur frequently
3	Possible	Insider threat breaches will occur sometimes
2	Unlikely	Insider threat incidents will unlikely be expected to occur
1	Rare	Almost never authorised user will carry out an insider threat breach, but its possible

computes whether the employee may act as a malicious insider threat or not. We divided the risk level results into 5 levels based on the amount of harm that can be expected from each employee, ranging from **1)** rare to be insider threat, **2)** unlikely to be an insider threat, **3)** a possible insider threat, **4)** likely to be an insider threat, to **5)** certainly is an insider threat. (Tab. 4.1) shows the mapping between the risk band and probability.

4.4 Summary

In this chapter, we have considered the multiple perspective approaches of insider threat detection, by developing a new framework that helps organisations to predict potential malicious insider threats before a breach takes place. This framework is based on three dimensions: Human Factor, Organisational Impact, and Technology Aspect. Each of these dimensions was discussed to present main key insider threat indicators.

We also introduce the Bayesian Network in order to model the proposed framework. In the next chapter, we will go through the process of data collection and analysis to run the proposed prediction approach.

Chapter 5

Data collection and Analysis

5.1 Survey Data Collection

In this section we will go through the process of data collection and analysis to run the proposed prediction approach that helps organisations to discover any potential malicious or unintentional insider threat from the surveys' response data that we gathered from targeted organisations in three steps as below:

5.1.1 Survey Questions (Data Requirements)

Our research is based on quantitative methodology in relation to data collection by using questioners in the form of surveys. Three surveys were designed based on three-dimensions of the prediction model (human factor, technology factor, and organisational aspect) and each survey targeted a specific user group on a single organisation. The Human Factor surveys Table 5.1 were answered by all authorised users, the Technology Aspect survey Table 5.2 was answered by the department responsible for IT, and the Organisational Impact survey Table 5.3 was answered by the department responsible for Human Resources or any top management staff. Please refer to Appendix A for the full survey questions and answers options. This survey is based on the use of best strategies to implement and publish, as follows:

- We made it clear that the survey should focus on information that is required to run the proposed model and to fill 93 end node variables of the prediction model.
- We made the survey easy to answer; a multiple choice questions technique is used, with the option of a text box to add any extra information. Figure 5.1 shows a snapshot of survey layout.
- A logical flow is created by grouping questions that cover similar topics together in some places, and a mixed question flow on other places to make sure the responder's answers are accurate.
- As not all security breaches are reported to the Human Resource Department (HR), or are not reported to Information Technology Department (IT), we have listed 7 questions, which are related to previous security breaches in the organisational aspect and in the technology factor survey.
- The questions are ordered based on simplicity by making the first questions easy and interesting in order to engage the respondent and get them into the flow of the survey.
- We placed personal information at the end of the survey to avoid scaring people off. We believe that if a responder has taken the time to answer all related survey questions first, they are more likely to provide at least some of their personal information at the end.
- An online survey platform <https://www.qualtrics.com/> is used to make the survey easy to reach by the respondents.
- A clear survey introduction was shown before the responder starts answering questions. Figure 5.2 shows a snapshot of survey introduction.
- The survey was approved to have Ethical Clearance Appendix E.
- The survey was tested by a small group of people before it was published in order to get feedback regarding layout, overall flow, time spent to complete it, and the test entries were checked to ensure the answers' format will fill 93 end node variables.

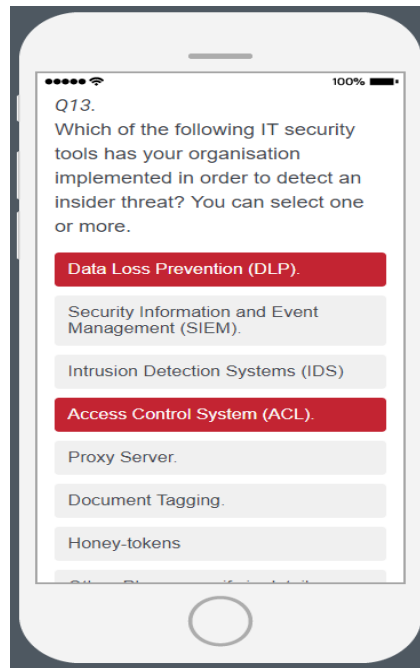


Figure 5.1: A Snapshot of the Survey Layout

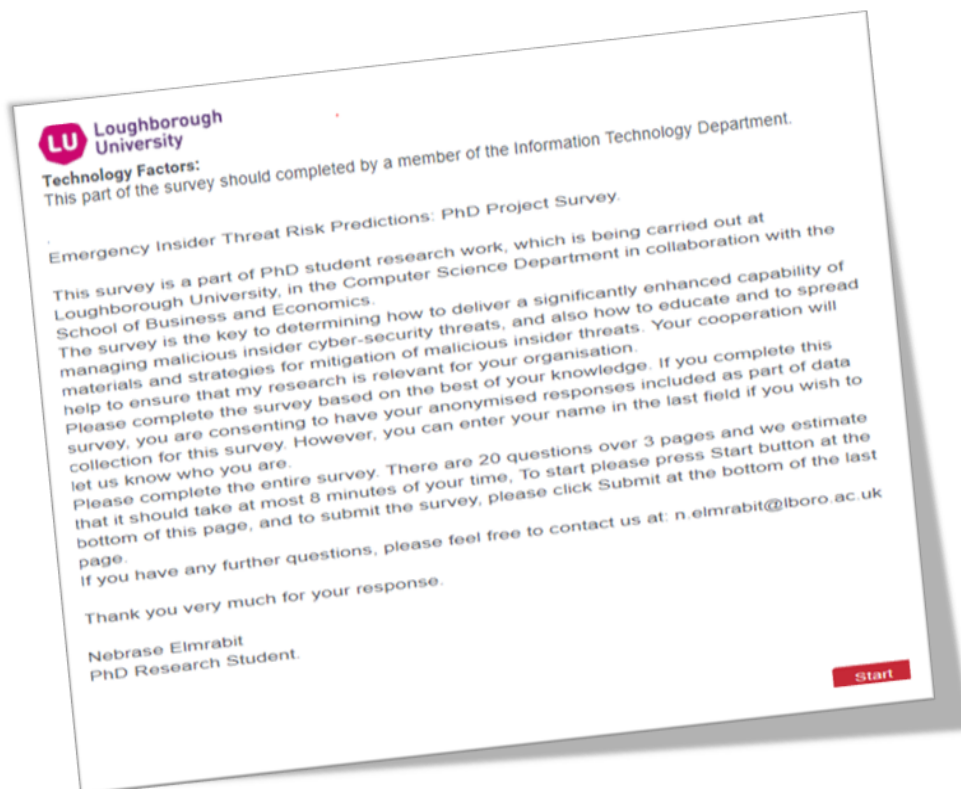


Figure 5.2: A Snapshot of the Survey Introduction

Table 5.1: Human Factor Surveys' Questions

Domain	Human Factor Surveys' Questions
Motive	How old are you?
	What is your gender?
	Do you understand your organisation's information security policy?
	If work gets difficult, do your colleagues help you?
	Do you receive the respect at work you feel you deserve from your colleagues?
	Are your colleagues willing to listen to your work-related problems?
	Is there friction or anger between colleagues?
	Are relationships at work strained?
	Do you have sufficient opportunities to question managers about changes at work?
	When changes are made at work, are you clear how they will work out in practice?
	Can you decide when to take a break?
	Do you have a choice in deciding how to do your work?
	Do you have some say over the way you work?
	Are you given supportive feedback with regard to the work you do?
	Can you rely on your line manager to help you out with a work problem?
Can you talk to your line manager about something that has upset or annoyed you about work?	
Are you supported through emotionally demanding work?	
Opportunities	How would you best describe your relationship with the organisation?
	How long have you been working for this organisation?
	How best do you describe your role within the organisation?
	How long have you been working in this role?
	If you are a current employee, when does your contract expire?
Capabilities	Is it clear what is expected of you at work?
	Do you know how to go about getting your job done?
	Do you understand how your work fits into the overall aim of the organisation?
	Do you have higher work capabilities than your colleagues?
	Are you a part of the design or implementation process team?
	Do you have access to the organisation's intellectual property?
	Do you feel that the copyright for your own created work is your own intellectual property and does not belong to your organisation?

Table 5.2: Technology Aspect Surveys' Questions

Domain	Technology Aspect Surveys' questions
Investment	How much does your organisation allocate to the IT budget in one year?
	How much of the IT budget is spent on IT security?
	How much of the IT security budget is spent on protection from insider threats?
	Do you have any concerns regarding security threats coming from authorised users?
	Does your organisation provide any security awareness and training strategy?
	Does your organisation encourage all authorised users to attend security awareness and training programmes?
	How often do your employees attend security awareness and training programmes?
Detection Level	What proportion of false insider alerts are generated by the security system?
	In previous security breaches, how did your organisation detect an insider threat?
	In previous security breaches, how many insider attacks has your system failed to detect?
Security and Privacy Controls	Which of the following IT security tools has your organisation implemented in order to detect an insider threat?
	Which of the following statements best describes how security and privacy controls are integrated to detect insider threats?
	Which of the following statements best describes how the external and insider threat detection systems are integrated?
	Which of the following data are logged on the organisation's system to help detect an insider threat?
Related to Organisation Impact	Has your organisation suffered any information security breach in the last 5 years?
	Has your organisation suffered any security breach that was accidentally caused by an authorised user in the last 5 years?
	Has your organisation been under attack from external threats?
	Has your organisation suffered any security breach caused by an authorised user in the last 5 years?
	If Yes to the previous question, please let us know which type of authorised user security breach your organisation suffered?
	What action was taken against any malicious authorised user?
	Has your organisation applied any extra measurement to monitor user activity in the termination period,?

Table 5.3: Organisational Impact Surveys' Questions

Domain	Organisational Impact Surveys' questions
Security Breach	Has your organisation suffered any information security breach in the last 5 years?
	Has your organisation suffered any security breach that was accidentally caused by an authorised user in the last 5 years?
	Has your organisation been under attack from external threats?
	Has your organisation suffered any security breach caused by an authorised user in the last 5 years?
	If Yes to the previous question, please let us know which type of authorised user security breach your organisation suffered?
	What action was taken against any malicious authorised user?
Structure	What sector does your organisation belong to?
	What is your organisation size in terms of employee numbers?
	Does your organisation have its own IT security department?
	Does your organisation outsource IT services?
	Does your organisation outsource IT security services?
	Does your organisation apply criminal records checks for people it employs before giving them access to IT systems?
Security Policy	Does your organisation recruit people from overseas?
	Does your organisation have a written security policy?
	How often does your organisation update or review its security policy?
Work-related stress symptoms	Do all authorised users follow your organisation's security policy?
	Do you recognise any of the following symptoms at work?

5.1.2 Data Collection

The main objectives of this stage were to collect high-quality raw data from specific organisations. We conducted our study on two organisations: first in the education sector, and second in a small enterprise. Both are based in United Kingdom.

For the education sector, we circulated the human factor survey to 15 heads of department and managers at this organisation, we asked them to forward the survey link to their department staff. Many of them complied with our request.

For the technology factor survey we conducted two interviews with two IT Services' management teams. The first interview was with the Assistant Director (Infrastructure and Operations), and the second interview was with the Assistant Director (Service Management and Governance).

For the organisational aspect we conducted our interview with the head of department for the Computer Science Department.

The number of responses to the human factor survey was 70 authorised users from this organisation. Also, two responded to the technology factor survey and one responded to organisational aspect survey, as shown in Table 5.4.

For the small enterprise, we conducted an interview with the company director to collect answers regarding the technology factor and organisational aspect. Also, he forwarded the human factor survey to all his employees and encouraged them to answer it.

To encourage staff to answer this survey on time, we set a deadline date to participate. We also asked them to enter their names in the last field of the survey if they wished to enter in a prize draw. The number of responses to the human factor survey was 12 authorised users from this organisation. Also, one responded to the technology factor survey and one responded to organisational aspect survey, as shown in Table 5.4.

Table 5.4: Respond Values

	Human Factor	Organisation Aspect	Technology Factor
Education Sector	70	1	2
Small Enterprise	12	1	1

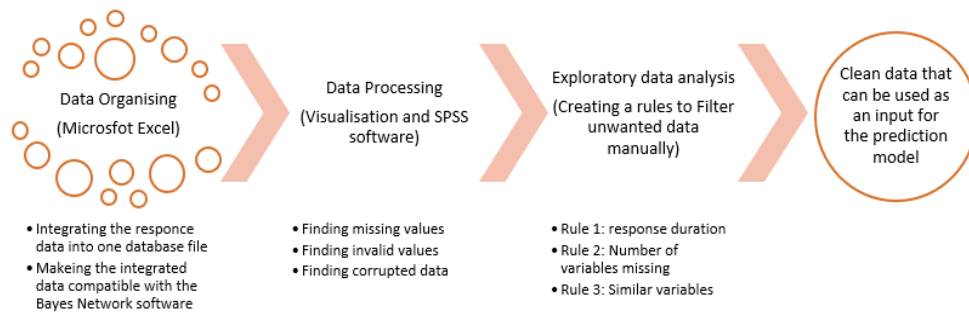


Figure 5.3: Data Processing and Exploitation Method

Table 5.5: Missing Values

	Number of Cases	Completed	Uncompleted	Missing all Variables
Education Sector	70	42	27	1
Small Enterprise	13	7	5	1

5.1.3 Data Processing and Exploitation Method

In this phase, we prepare collected survey data by making them compatible with modelling software and removing any unwanted data from the dataset. To do this, we created a method that allow us to divide the process into three steps: Data Organising, Data Processing, and Exploratory data analysis, as described below, also Figure 5.3 shows a data processing and exploitation process method.

- Data Organising:** Data initially obtained must be processed or organised for analysis. In our case, data processing was the process that was required to convert collected survey responses into a format compatible with Bayes Network Software ¹ (experimental environment) and compact all collected raw data onto one database file. In this step, we integrated all human factor variables of each response with the technology factor and organisation aspect directly from survey responses to one database file, for each organisation.
- Data Processing:** In this phase, we aimed to find any invalid values or corrupted data. Data cleaning is the process that helps us in detecting, correcting, or deleting corrupted or inaccurate cases from the database that we created in the last step.

After we integrated all aspects in the database, we reviewed all the variables in the data file and we determined their valid values using SPSS software. For the Education Sector, we found 42 cases were fully completed, 27 cases

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

were missing some variables, and one case was missing all data. Also, the same steps were carried out for small enterprise and we found that 7 cases were fully completed, 5 cases were missing some variables, and one case was missing all data. Table 5.5 summarises the number of completed and uncompleted responses.

Table 5.6 shows the missing values analysis for the human factor, using SPSS software for the education sector on the left-hand side and for the Small Enterprise on the right-hand side.

It is clear that in education sector's case, most of the variables in the survey questionnaire were over 90% completed. However, the last three variables were less than 30% completed. In the small enterprise's responses most of the variables are completed, except Contract Expiration and for the last three variables, less than 10% are uncompleted.

Table 5.6: Missing Values SPSS Analysis

	Education Sector			Small Enterprise		
	Responses	Missing		Responses	Missing	
		Count	Percent		Count	Percent
Age	69	0	0	12	0	0
Gender	69	0	0	12	0	0
Type of Employment	65	4	5.8	12	0	0
Employment period	69	0	0	12	0	0
Position Period	69	0	0	12	0	0
Contract Expiration	64	5	7.2	8	4	33.3
Understanding Security Policy	69	0	0	12	0	0
Colleagues Help	63	6	8.7	12	0	0
Colleagues Respect	63	6	8.7	12	0	0
Colleagues listen to work related problems	63	6	8.7	12	0	0
Anger between colleagues	63	6	8.7	12	0	0
Work strained relationships	63	6	8.7	12	0	0
Change opinion	63	6	8.7	12	0	0
Change practice	63	6	8.7	12	0	0
Own break decision	63	6	8.7	12	0	0
Own decision of how to do the task	63	6	8.7	12	0	0
Way of work opinion	63	6	8.7	12	0	0
Supportive feedback	63	6	8.7	12	0	0
Rely on line manager to help with a work problem	62	7	10.1	12	0	0
Talking to line manager regarding upsetting from work	63	6	8.7	12	0	0
Emotionally support	62	7	10.1	12	0	0
Work knowledge	63	6	8.7	12	0	0
Work experience	63	6	8.7	12	0	0
Work aims	62	7	10.1	12	0	0
Higher work capabilities	62	7	10.1	12	0	0
Design or implementation team	55	14	20.3	11	1	8.3
Intellectual property	54	15	21.7	11	1	8.3
Copyright ownership	49	20	29	11	1	8.3

- **Exploratory data analysis:** We created Cross-variable rules, which are applied to a combination of variables by defining a logical expression that flags invalid values.

The first rule is to find any response finished in less than 2 minutes, as we believe that the survey takes more than 2 minutes to complete and the average time to complete this part of survey is 4 minutes. We found that 4 cases responded in less than two minutes. We deleted these 4 cases as they are uncompleted with regard to the education sector, and no cases were found with regard to small businesses.

To ensure the accuracy for the final risk prediction result a second rule is created to find out whether there are more than 3 variables missing from 29 variables in the Human Factor survey for each case, as if the case has more than 3 variables missing this will directly affect the result. Then we can delete this cases. We found 4 cases matching this rule and we deleted them with regard to the education sector, and no cases were found relating to small businesses company.

The third rule is to find any suspicious or invalid cases by looking into some questions that are related to stress levels and find out whether their values are equal to each other, for example, if all values are equal to Never. Also, in this step, we made sure that there was no duplication. Table 5.7 shows the number of cases that we can use to run our model that results from the data processing and exploitation phase

Table 5.7: Data Processing and Exploitation Result

	Number of Cases Before Filtering	Completed Under Minutes	More than three Variables Missing	Missing all Human Factor Variables	Number of Cases After Filtering
Education Sector	70	4	4	1	61
Small Enterprise	13	0	0	1	12

5.2 Modeling Prediction Results

The outcome of this prediction aims at helping decision makers to avoid insider threat breaches by indicating who could be a potential malicious insider threat within the organisation. Further, we can identify which model domain within the organisation requires attention from an organisation team to make the right decisions to improve their defences and mitigate the level of such a threat. In this section, we will present prediction results for both selected organisations in four steps, as follows:

5.2.1 Technology Factor Prediction Result

To demonstrate the technology factor prediction results, we have divided it into four risk levels based on the organisation's performance and measures of detecting any potential insider threat. These levels from high to low risk levels are:

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

For the education sector, the proposed model predicted that this organisation is “ a moderate performance and low focus on insider threat ” organisation in relation to the detecting and controlling of insider threat incidents. That is because of the effect of 30 end node variables that we imported from the survey questions related to this organisation. Table 5.8 shows the state of each of main indicators and the main reason why this model predicts this level. Also, Figure 5.4 shows case number 25 Technology Factor level with all end node variables.

Table 5.8: Technology Factor Predictions

	Indicator	State	Reason
Education Sector	Investment	Low	IT security budget for Insider Threat is less than 5%.
			No concerns regarding Insider Threat from top management.
			No security awareness and training is provided.
	Detection Level	High	Over 90% of insider alert are true.
			All insider breach was detected.
	Security and privacy controls	Medium	They keep record of (Network traffic, online activity, Emails, etc.).
They take an extra measure on the employee termination period.			
Using (SIEM, IDS, ACL, Proxy Server, etc.)			
No Security & Privacy controls integration to detect Insider			
Small Enterprise	Investment	Low	IT security budget for Insider Threat is less than 5%.
			No concerns regarding Insider Threat from top management.
			No security awareness and training is provided.
	Detection Level	Low	No insider threat detection method is found.
			Two ends nod are not entered.
	Security and privacy controls	Medium	They keep record of (Emails).
They take an extra measure on the employee termination period.			
Using (ACL only)			
No Security & Privacy controls integration to detect Insider			

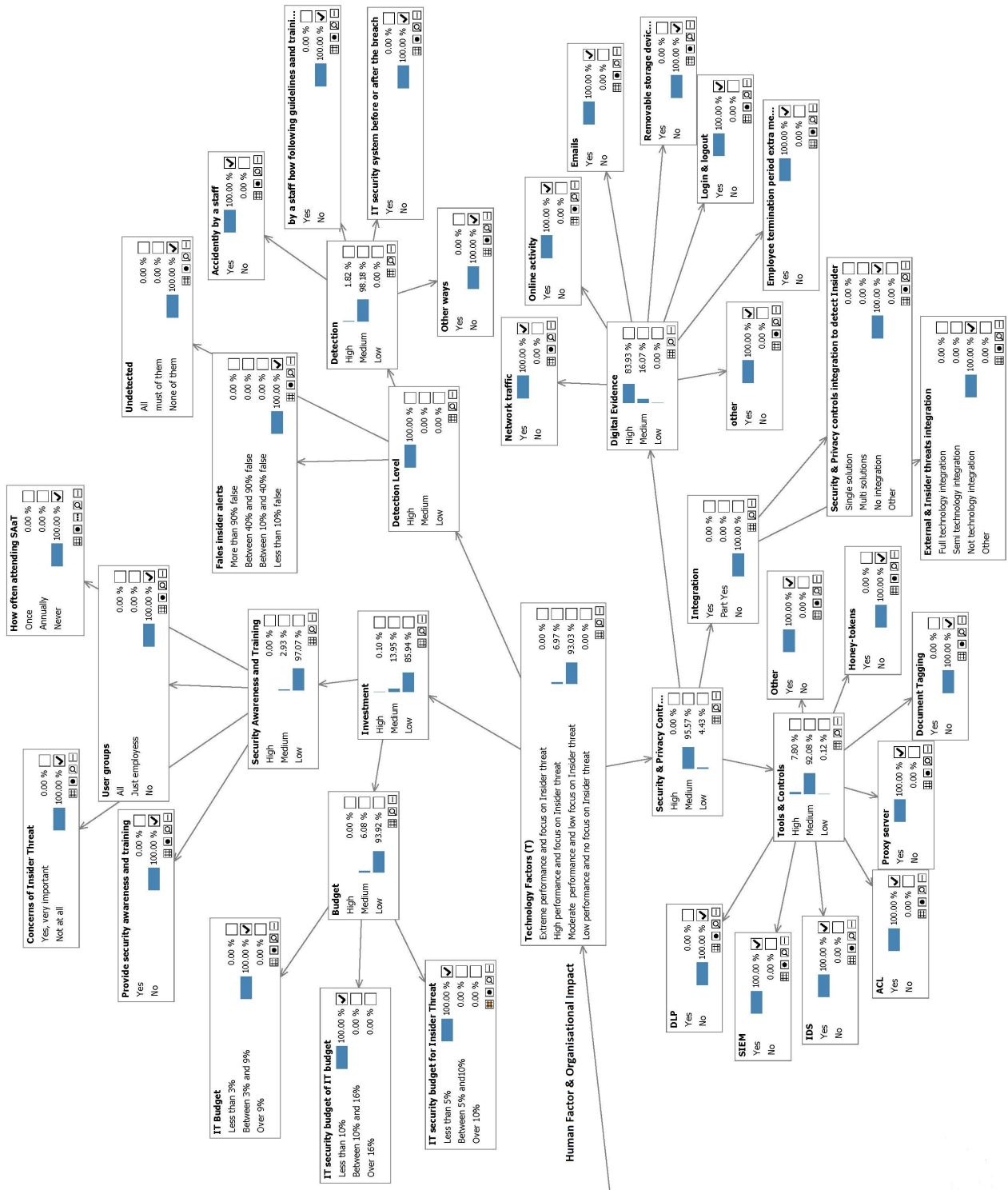


Figure 5.4: Technology Factor Domain - Case 25

5.2.2 Organisational Aspect Prediction Result

To determine organisational aspect prediction results, we have divided it into three risk levels, based on the organisational environment and culture that affects the risk level of insider threat. These levels from low- to high-risk levels are:

- Non-fertile environmental culture for insider threat.
- Neutral culture.
- Moderate performance and low focus on insider threat.
- Fertile environmental culture for insider threat.

For the education sector, neutral culture is predicted for this organisation. Table 5.9 shows indicators' states and the reason for this prediction level. Also, Figure 5.5 shows case number 25 organisational aspect level with all end node variables. For the small enterprise, there are mixed prediction levels for this aspect, as it predicts that 54% of this organisation is a neutral culture and also predicts that 43% is a non-fertile environmental culture for insider threat. Table 5.9 shows indicators' states and the reason for this prediction level

Table 5.9: Organisational Aspect Prediction

	Indicator	State	Reason		
Education Sector	Security Breach	Medium	No Authorised user breach in last 5 years of any type.		
			There is one or more accidental authorised user breach in last 5 years.		
			No action was taken when insider security breach is taken place.		
	Structure	Medium	No pre-employment checks. Outsource some of IT services.		
Security Policy	Medium	No enforcement system. Update or review every 5 years.			
		Employees Work-related Stress Symptoms	Medium	Some indicators indicate (low morale, increase in long-term illness, high turnover, etc.)	
Small Enterprise	Security Breach	Medium	Authorised user breach in last 5 years. Intellectual property insider breach. An action is taken when the breach takes a place		
			Structure	Medium	No pre-employment checks. Outsource IT services.
			Security Policy	Low	No security policy
	Employees Work-related Stress Symptoms	Low	Just one indicator indicates (deadlines not being reached)		

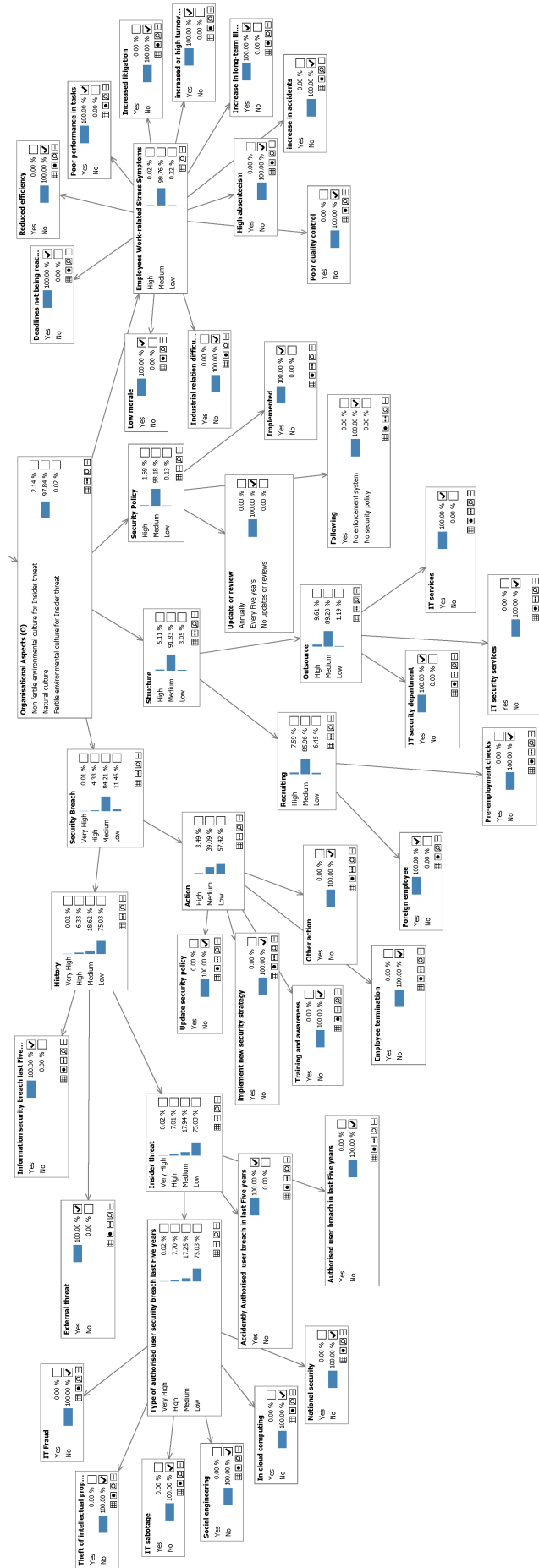


Figure 5.5: Organisational Impact Domain - Case 25

5.2.3 Human Factor Prediction Result

There are five prediction levels for the human factor that are based on personal characteristics of each employee to be a potential insider threat. These levels are listed from very high to very low risk levels. Figure 5.6 shows a snapshot for all human factor node variables. In this factor, as we explained earlier, we consider all of the organisation's employees, and each employee has his own case number.

For the education sector, Table 5.10 illustrates the human factor result for all cases that we have imported from the filtered survey data. The case number is the unique ID for each survey participant, the human factor prediction is what the proposed model is predicted, and finally prediction probability is the prediction percentage of this prediction level. We can see from this table result, 5 cases are indicated as high in human factor levels, also just 4 cases are indicated as low levels, and all the rest are indicated as medium levels of human factor.

Table 5.10: Human Factor Result For All Cases

Case	Human Prediction	Factors	Predict Probability of Human Factors	Case	Human Prediction	Factors	Predict Probability of Human Factors
0	Medium		72.57%	33	Medium		80.14%
1	High		60.84%	34	Medium		74.37%
2	High		59.97%	35	Medium		78.48%
3	Medium		72.25%	36	Medium		82.74%
4	High		47.18%	37	Medium		69.41%
5	High		63.80%	38	Medium		65.10%
6	Medium		91.33%	39	Medium		68.23%
7	Medium		71.67%	40	Medium		58.16%
9	Medium		74.19%	41	Medium		77.11%
11	Medium		80.32%	42	Medium		75.05%
12	Medium		85.36%	43	Medium		73.48%
13	Medium		77.99%	44	Medium		74.72%
14	Medium		75.53%	45	Medium		59.59%
15	Medium		86.10%	46	Medium		87.41%
16	Low		52.30%	47	Medium		86.13%
17	Medium		66.99%	48	Medium		87.61%
18	Medium		76.12%	49	Medium		80.37%
19	Medium		66.97%	50	High		44.40%
20	Medium		70.40%	51	Medium		62.21%
21	Medium		81.12%	52	Medium		84.66%
22	Medium		83.39%	53	Medium		81.31%
23	Medium		83.58%	55	Medium		75.38%
24	Medium		67.41%	56	Low		70.18%
25	Medium		60.51%	57	Medium		69.20%
26	Medium		80.63%	58	Medium		66.96%
27	Medium		83.29%	62	Medium		65.73%
28	Medium		62.99%	63	Medium		69.70%
29	Medium		72.33%	64	Low		52.78%
30	Low		62.55%	65	Medium		81.48%
31	Medium		77.27%	69	Medium		74.32%
32	Medium		76.31%				

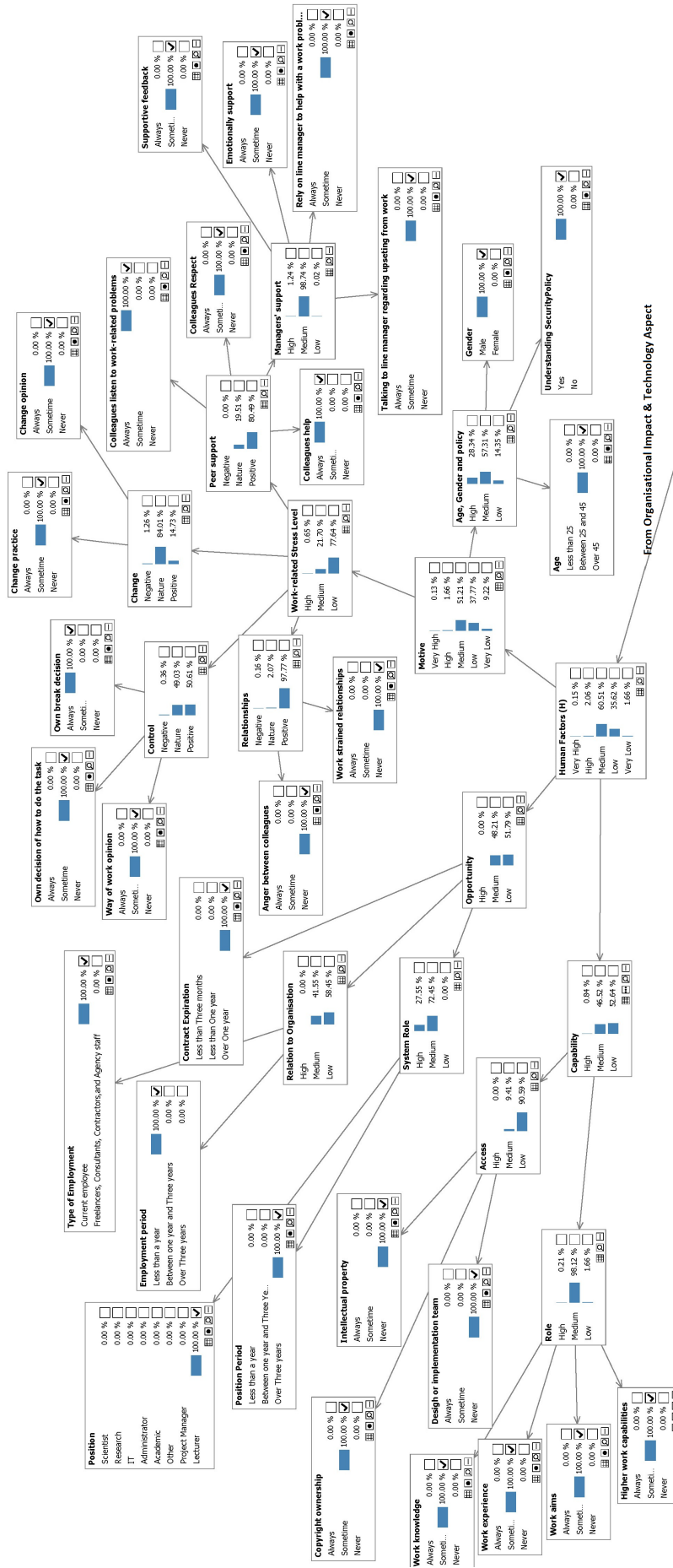


Figure 5.6: A Snapshot for Human Factor Nodes Variable - Case 25

Table 5.11: Case 4 and Case 22 of the Human Factor Results

Case number	Indicator	State	Reason
4	Motive	High	Do not understanding security policy.
			Work-related Stress Level is high.
	Opportunity	Medium	Position period is between one and three years.
4	Capability	High	Contract expiration is over one year.
			Copyright ownership.
22	Motive	Medium	Understanding security policy.
			Never get emotional support.
			Sometime anger between colleagues.
	Opportunity	Low	Position period is less than a year.
			Contract expiration is over one year.
Capability	Medium	No access to Intellectual property.	

Table 5.12: Human Factor Result for All 12 Cases

Case	Human Factors Predict	Predict Probability of Human Factors
0	Medium	74.260 %
1	Medium	80.351 %
2	Medium	69.101 %
3	High	69.742 %
4	Medium	71.804 %
5	Medium	54.965 %
6	Medium	68.281 %
7	Medium	74.057 %
8	Medium	75.616 %
9	Medium	54.130 %
10	Medium	73.022 %
11	High	62.237 %

In order to gain a better understanding, we have selected two different cases in this thesis, case number 4 and case number 22 “ please refer to Appendix F and Appendix G for full Bayes network digram. Case 4 is predicted with a high level and that is due to three main indicator variables: high motivation, medium opportunities with high capability. Also, case 22 is predicted as medium level and that is because the participant has medium motivation to enact malicious insider threat, and low opportunities with medium capability. Table 5.11 shows case 4 and case 22 of the human factor results.

For small enterprise, Table 5.12 illustrates the human factor result for all 12 cases that we imported from the filtered survey data. It is clear that only two cases are predicted to be high levels for the human factor and the others are medium levels. Therefore, it will affect the overall insider threat prediction in the next step.

5.2.4 Insider Threat Prediction Results

This output is the final and main risk level prediction that predicts whether the employee may enact any malicious insider threat or not. We have divided the risk levels result into 5 levels, from rare to be insider threat to a certain is an insider threat, as Figure 5.7 shows a snap-shot for Insider Threat Risk Prediction Levels, which is based on the amount of harm that can be expected from each employee. These levels from low to high risk levels are:

- Rare to be insider threat.
- Unlikely to be insider threat
- Possible insider threat.
- Likely to be insider threat.
- Certain is insider threat.

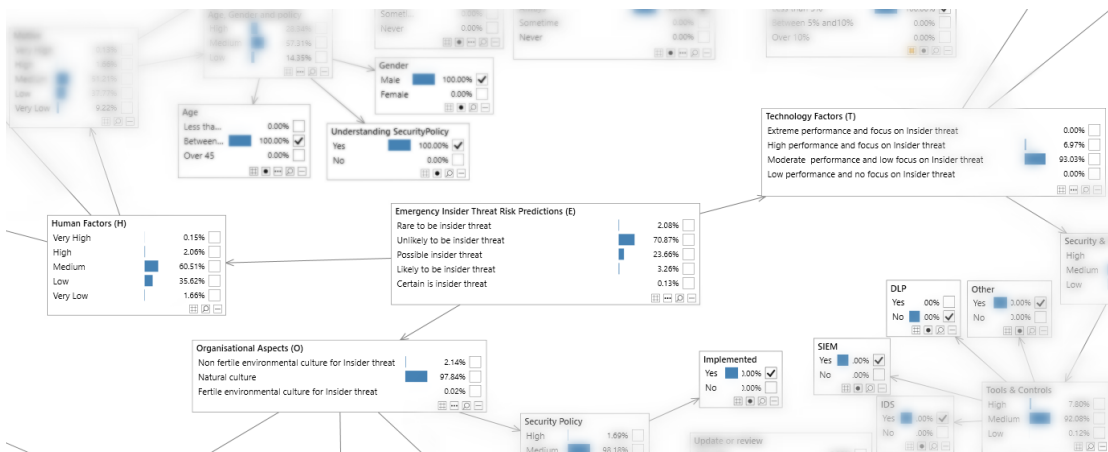


Figure 5.7: A Snapshot for Insider Threat Risk Prediction Levels

For the education sector, Table 5.13 illustrates the final result from the proposed prediction model. The first column displays case numbers ranging from 0 to 69 with some missing cases, as we deleted them during the data processing and exploitation phase. The second column displays the predicted risk level that has the highest prediction probability percentage. And the last five columns display the percentages of prediction probabilities for all risk levels.

Table 5.13: Insider Threat Prediction Result

Case	Insider Threat Risk Predictions	Predict Probability				
		Rare	Unlikely	Possible	Likely	Certain
0	Unlikely insider threat	0.045	46.735	43.063	8.658	1.5
1	Possible insider threat	0.002	22.413	55.65	15.185	6.749
2	Possible insider threat	0.006	22.827	55.391	15.035	6.741
3	Unlikely insider threat	1.073	64.519	29.71	4.337	0.362
4	Possible insider threat	0.058	30.845	50.985	12.763	5.349
5	Possible insider threat	0.002	22.002	56.129	15.642	6.226
6	Unlikely insider threat	0.065	56.489	37.591	5.548	0.307
7	Unlikely insider threat	0.224	50.234	40.112	7.551	1.879
9	Unlikely insider threat	0.063	47.832	42.347	8.271	1.487
11	Unlikely insider threat	0.689	62.232	32.243	4.601	0.234
12	Unlikely insider threat	0.073	53.591	39.193	6.506	0.637
13	Unlikely insider threat	0.753	64.699	30.251	4.104	0.193
14	Unlikely insider threat	0.029	47.712	42.627	8.318	1.314
15	Unlikely insider threat	0.268	58.061	35.924	5.374	0.373
16	Unlikely insider threat	3.232	77.647	16.824	2.228	0.07
17	Possible insider threat	0.042	43.694	44.454	9.25	2.56
18	Unlikely insider threat	0.641	59.312	33.964	5.415	0.668
19	Unlikely insider threat	0.971	59.599	32.734	5.6	1.096
20	Unlikely insider threat	0.027	45.11	44.004	9.075	1.784
21	Unlikely insider threat	0.17	53.56	38.746	6.606	0.918
22	Unlikely insider threat	0.288	57.307	36.226	5.657	0.522
23	Unlikely insider threat	0.194	55.261	37.747	6.131	0.667
24	Unlikely insider threat	1.336	64.888	28.887	4.414	0.475
25	Unlikely insider threat	2.081	70.867	23.664	3.262	0.126
26	Unlikely insider threat	0.489	59.523	34.299	5.226	0.462
27	Unlikely insider threat	0.361	59.774	34.413	5.07	0.382
28	Unlikely insider threat	1.799	71.042	23.92	3.159	0.08
29	Unlikely insider threat	0.034	46.253	43.363	8.749	1.601
30	Unlikely insider threat	4.34	81.464	12.547	1.625	0.024
31	Unlikely insider threat	0.112	50.681	40.39	7.306	1.512
32	Unlikely insider threat	0.885	62.853	31.357	4.601	0.304
33	Unlikely insider threat	0.256	54.94	37.6	6.279	0.924
34	Unlikely insider threat	0.042	47.271	42.668	8.281	1.738
35	Unlikely insider threat	0.338	55.637	36.9	6.153	0.972
36	Unlikely insider threat	0.075	52.253	39.918	6.913	0.84
37	Unlikely insider threat	0.081	45.937	43.182	8.786	2.014
38	Unlikely insider threat	1.568	67.691	26.59	3.854	0.296
39	Unlikely insider threat	0.974	60.046	32.549	5.478	0.953
40	Possible insider threat	0.239	42.184	44.589	9.834	3.154
41	Unlikely insider threat	0.16	51.284	40.09	7.353	1.113
42	Unlikely insider threat	0.466	56.271	36.088	6.127	1.047
43	Unlikely insider threat	0.247	51.341	39.536	7.3	1.577
44	Unlikely insider threat	0.015	47.019	43.034	8.484	1.448
45	Unlikely insider threat	1.6	64.963	27.995	4.641	0.801
46	Unlikely insider threat	0.209	57.431	36.52	5.478	0.364
47	Unlikely insider threat	0.352	60.911	33.863	4.712	0.162
48	Unlikely insider threat	0.289	60.217	34.487	4.79	0.216
49	Unlikely insider threat	0.733	64.984	30.266	3.954	0.063
50	Possible insider threat	0.078	29.99	50.761	12.362	6.808
51	Possible insider threat	0.155	43.547	43.979	9.334	2.986
52	Unlikely insider threat	0.389	59.717	34.565	5.042	0.287
53	Unlikely insider threat	0.71	64.625	30.61	4	0.055
55	Unlikely insider threat	1.017	64.729	29.873	4.191	0.19
56	Unlikely insider threat	5.212	84.151	9.411	1.212	0.013
57	Unlikely insider threat	1.267	65.628	28.583	4.213	0.31
58	Unlikely insider threat	1.358	65.805	28.209	4.242	0.387
62	Unlikely insider threat	1.425	66.886	27.264	3.994	0.431
63	Unlikely insider threat	0.016	44.612	44.237	9.145	1.99
64	Unlikely insider threat	3.322	77.805	16.608	2.196	0.068
65	Unlikely insider threat	0.117	52.655	39.478	6.837	0.913
69	Unlikely insider threat	0.273	52.375	38.871	7.04	1.44

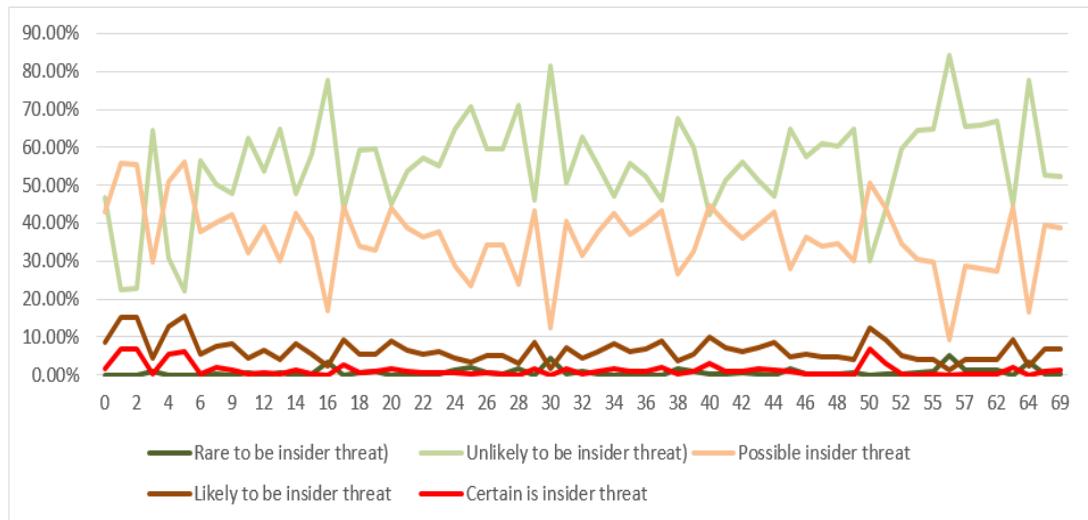


Figure 5.8: Insider Threat Prediction Result

By converting the previous table’s results into the line chart on Figure 5.8, we can analyse and understand the result by looking into the lines to discover any high-risk levels or abnormal behaviour. From the previous table, it is clear that there are 8 cases (1, 2, 4, 5, 17, 40, 50, and 51) that are predicted to be a possible insider threat, and the rest of the cases that are predicted as unlikely to be an insider threat.

However, if we analyse the line chart, we can conclude that there are some cases that are on the borderline between “possibly being an insider threat” and “unlikely to be an insider threat”, and we need to take them into our considerations. Next, we will explain two cases with different levels, and one case with two narrow prediction levels.

Please note that the result values are affected by the technology factor and organisational aspect as well. However, the organisational aspect and technology factor are the same values for all cases within the same organisation. For this reason, we will not mention these two in all cases. We will instead solely focus on the human factor.

Table 5.14: Case 4 Human Factors

Indicator	State	Reason
Motive	High	Do not understanding security policy.
		Work-related Stress Level is high, because of:
		No support from colleagues and managers.
		Change management resistant.
		Anger relationship between colleagues.
Opportunity	Medium	Position period is between one and three years.
		Contract expiration is over one year.
Capability	High	Copyright ownership.
		Access to organisation Intellectual Property.
		Part of design or implementation teams.
		Higher work capability than his colleagues.

Table 5.15: Case 22 Human Factors

Indicator	State	Reason
Motive	Medium	Understanding security policy.
		Never get emotional support.
		Sometime anger between colleagues.
Opportunity	Low	Position period is less than a year.
		Contract expiration is over one year.
Capability	Medium	No access to Intellectual property.

Case Number 04 Our model predicts that this case is more than 50% as a possible an insider threat with 12% as likely to be an insider threat. To understand why this model predicts these values we need to go through this survey response regarding the human factor. It is clear that the human factor levels are predicted as high levels, and this is affected by a high capability level, medium opportunity level, and high motivation level. Table 5.14 and Appendix B shows the reasons behind these values.

Case Number 22 In this case, our model predicted that this case is 55% unlikely to be an insider threat. The reason behind this prediction is that the human factor levels are predicted as 83% at medium level, and this is affected by a medium capability level, low opportunity level, and medium motivation level. Table 5.15 and Appendix B shows the reason behind these values.

Table 5.16: Insider Threat Prediction Result for the Small Enterprise

Case	Insider Threat Risk Predictions	Predict Probability %				
		Rare	Unlikely	Possible	Likely	Certain
0	Unlikely insider threat	0.02	52.883	29.936	15.633	1.529
1	Unlikely insider threat	0.016	54.411	30.264	14.539	0.77
2	Unlikely insider threat	0.029	54.617	28.459	15.219	1.676
3	Likely insider threat	0	10.141	36.459	36.617	16.783
4	Unlikely insider threat	0.001	37.297	35.929	23.174	3.599
5	Possible insider threat	0.003	31.128	35.274	25.818	7.778
6	Unlikely insider threat	0.01	42.091	33.182	20.556	4.16
7	Unlikely insider threat	0.018	52.761	29.99	15.787	1.445
8	Unlikely insider threat	0.021	52.699	30.302	15.827	1.151
9	Unlikely insider threat	0.011	36.441	33.017	23.464	7.067
10	Unlikely insider threat	0.024	54.989	28.891	14.735	1.361
11	Possible insider threat	0	12.804	36.025	34.23	16.94

Case Number 20 As we can see from the previous line chart for case 20, two lines are very narrow. The model predicts that 45% is unlikely to be an insider threat and 44% is a possible insider threat with just 1% difference. For this borderline type of case, a security analysis team should step in to analyse it manually and decide which risk level they will approve. In this case, the employee is between 25 and 45 years old, she does not understand security policies. She has access to the organisation's intellectual property and believes that she owns the copyright ownerships. On the other hand, her motivation level is a normal level. From this information, the security team can know the point at which to carry out analysis on her case to avoid any unintentional insider threat in the future. Giving her security awareness training will affect her insider risk levels in future assessments, as she then will understand the organisation's security policy and copyright ownership.

From 12 cases in this small enterprise, our prediction model predicted that 1 case is likely to be an insider threat, 2 cases were predicted as possible insider threats, and 9 cases were predicted as unlikely to be insider threats. Table 5.16 shows the final result from the proposed prediction model.

By converting the above table result into the line chart in Figure 5.9, we can analyse and understand the result by looking into the lines to discover any high-risk levels or abnormal behaviour. Next, we will explain three cases with different levels.

Table 5.17: Case 11 Human Factors

Indicator	State	Reason
Motive	High	Do not understanding security policy.
		Work-related Stress Level is high, because of:
		Negative peer support from colleagues and managers.
		Negative way of work control
Opportunity	Medium	Anger relationship between colleagues.
		Position period is less than one year.
Capability	High	Contract expiration is less than one year.
		Copyright ownership.
		Access to organisation Intellectual Property.
		Part of design or implementation teams.
		Higher work experience and capability than his colleagues.

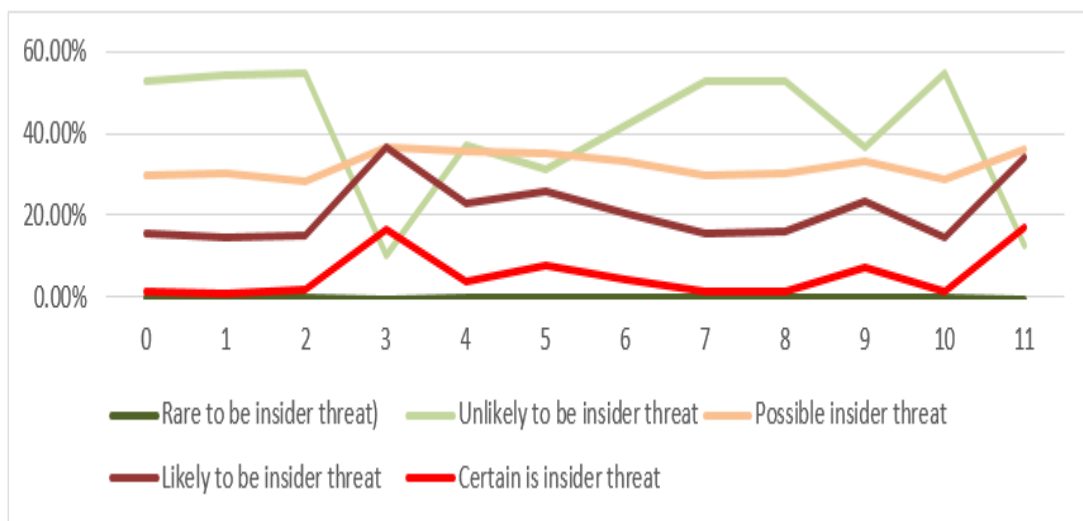


Figure 5.9: Insider Threat Prediction Result Line Chart

Case Number 11 Our model predicts that this case is to 36% a possible an insider threat with 34% likely to be insider threat and with more than 16% being certainly an insider threat. To understand why this model predicts these values, we need to go through the authorised user survey response values regarding the human factor. It is clear that human factor levels are predicted as high levels, and this is affected by a high capability level, a medium opportunity level, and high motivation levels, Table 5.17 shows the reason behind these values.

Table 5.18: Case 0 Human Factors

Indicator	State	Reason
Motive	Medium	Do not understanding security policy.
		Work-related Stress Level is low, because of:
		Positive peer support from colleagues and managers.
		Positive way of work control
		Positive relationship between colleagues.
Opportunity	Medium	Position period is less than a year.
		Contract expiration is less than one year.
Capability	Medium	Access to organisation Intellectual Property.
		Copyright ownerships belong to organisation.
		Not part of design or implementation teams.
		Higher work experience and capability than his colleagues.

Case Number 0 In this case, our model predicts that over 52% is unlikely to be an insider threat. The reason behind this prediction is the human factor levels, which are predicted to be 73% at the medium level, and this is affected by a medium capability level, a medium opportunity level, and medium motivation levels. Table 5.18 shows the reason behind these values.

Case Number 3 In this case, the model predicts that case 3 is likely to be an insider threat due to one missing value regarding the contract expiration date. Because the participant has not completed this question, our model assumes a threat in this case, as the contract will expire in less than three months. Other reasons are regarding work related-stress levels.

5.3 Agreement with Theory

Bayes network software was used as the experimental environment to implement the insider threat prediction model in this chapter, the risk levels output formula was created in section 4.3.3. In this section, we will calculate the risk levels using the equation (Eq. 4.42) and applied to a small sample from the proposed network, to approve that we will get the same result if we calculate it manually.

Example 1 By using the experimental environment, (Fig. 5.10) shows the result of 64.29 % is probability prediction for emergency insider threat risk prediction (E) to be possible insider threat where human factor (H) is high, organisational aspect (O) is natural culture, and technology factor (T) is moderate performance and low focus on insider threat.

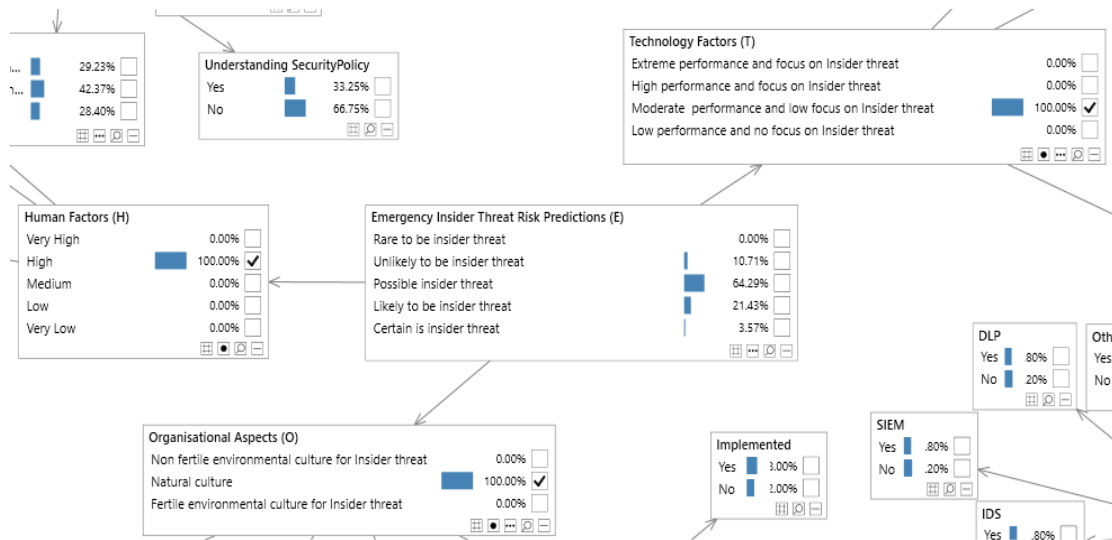


Figure 5.10: Bayes Network Example 1

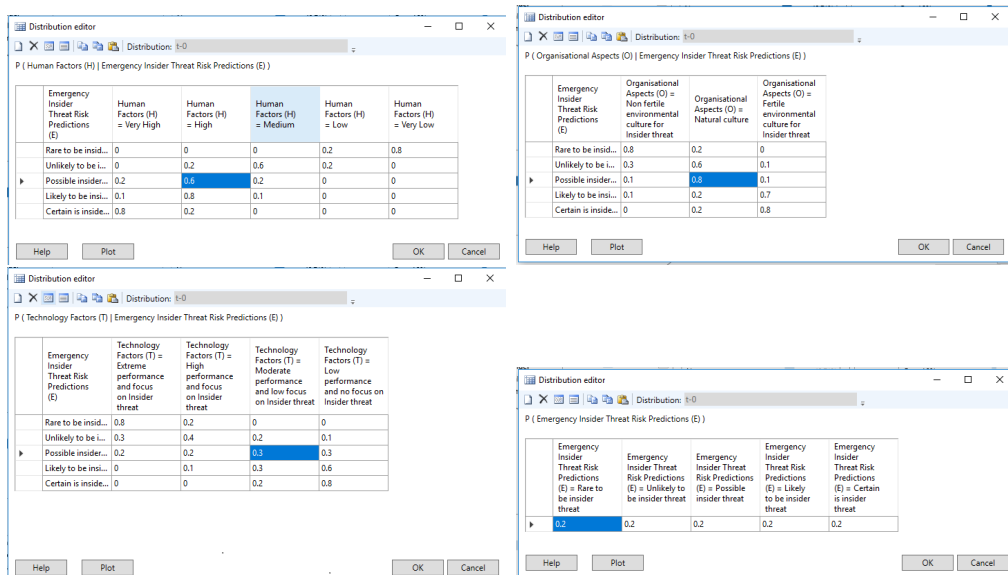


Figure 5.11: Prior Probabilities

As we have set on the design phase the prior probabilities for the H is high and E is possible to be 60%, the prior probabilities for the O is natural culture and E is possible is 80%, the prior probabilities for the T is moderate performance and low focus on insider threat and E is possible is 30%, and prior probabilities to be possible insider threat is 20%, as shown on (Fig. 5.11) .

Apply these numbers to the equation 4.42 we will get the same result as the experimental environment, which which proof that the result from (Fig. 5.10) is equal to result using (Eq. 4.42), as below:

$$P(E | H, O, T) = \frac{20 \cdot 60 \cdot 80 \cdot 30}{(20 \cdot 0 \cdot 20 \cdot 0) + (20 \cdot 20 \cdot 60 \cdot 20) + (20 \cdot 60 \cdot 80 \cdot 30) + (20 \cdot 80 \cdot 20 \cdot 30) + (20 \cdot 20 \cdot 20 \cdot 20)}$$

$$P(E | H, O, T) = 64.2857\%$$

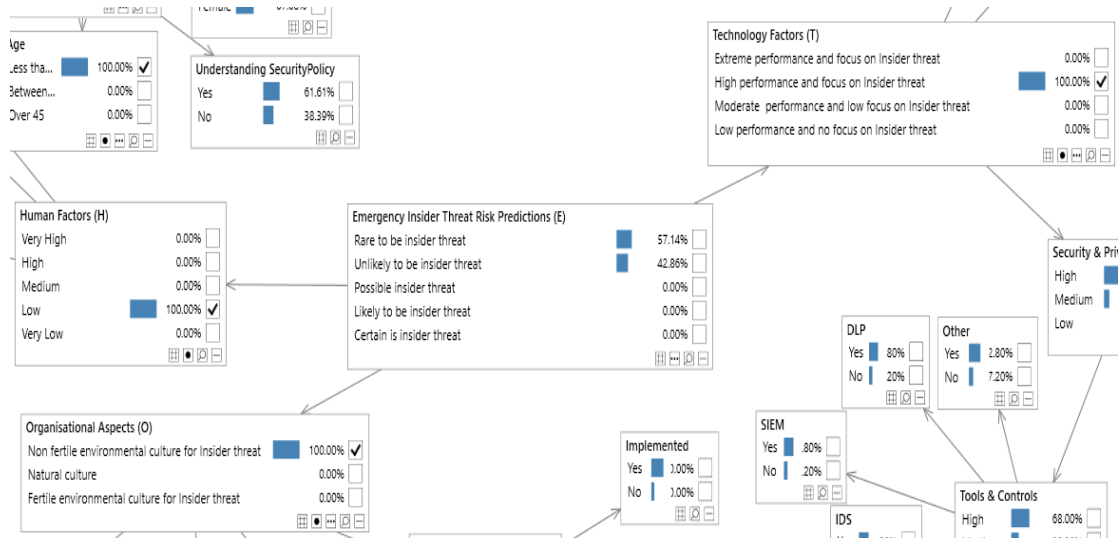


Figure 5.12: Bayes Network Example 2

Example 2 By using the experimental environment, (Fig. 5.12) shows the result of 57.14 % is probability prediction for emergency insider threat risk prediction (E) to be a rare insider threat where human factor (H) is low, organisational aspect (O) is non fertile environmental culture for insider threat, and technology factor (T) is high performance and focus on insider threat.

As we have set on the design phase the prior probabilities for the H is low and E is rare to be 20%, the prior probabilities for the O is non fertile environmental culture and E is rare is 80%, the prior probabilities for the T is high performance and focus on insider threat and E is rare is 20%, and prior probabilities to be possible insider threat is 20%, as shown on (Fig. 5.11) .

Apply these numbers to the equation 4.42 we will get the same result as the experimental environment, which proof that the result from (Fig. 5.12) is equal to result using (Eq. 4.42), as below:

$$P(E | H, O, T) = \frac{20*20*80*20}{(20*20*80*20)+(20*20*30*40)+(20*0*10*20)+(20*0*10*10)+(20*0*0*10)}$$

$$P(E | H, O, T) = 57.1428\%$$

5.4 Summary

In this chapter, we have implemented the proposed model based on the process of data collection. A survey was conducted and data was collected from a single organisation. Then a risk level and the prediction for each authorised user within the organisation were analysed and measured via Bayesian Network Software. The outcome from this prediction can help decision-makers by indicating who could be a potential malicious insider within the organisation so as to make proactive decisions and to avoid insider threat breaches happening. Please refer to Appendix B for the full list of all variables with changing of the probability for the selected cases 4, 20, 22, 69

In the next chapter, the validation of the prediction model will be carried out by comparing the model prediction results in Table 5.13 with the expert judgments that we collected via a workshop.

Chapter 6

Validation of the Prediction Model

6.1 Introduction

Insider threat prediction model provides facilities that support organisational decision makers to predict the risk of insider threat for each authorised user. However, before we can use this tool in practices, some steps should be carried out to evaluate the prediction model to ensure its validity.

Verification and validation (V&V) are the means by which the model is checked in each step in development stages, and by which its performance is demonstrated and assured to be a correct interpretation of the requirements. In short, validation means “ are we building the right product? ” [12] where verification means “ are we building the product right? ” [22] However, model validity is the process of increasing confidence in a model, and not one of demonstrating absolute accuracy [76].

The main aim of V&V is to ensure that the model is suitable for a particular use and increasing confidence in a model, by not being able to prove its invalidity, to the point that it will be used for decision-making [77].

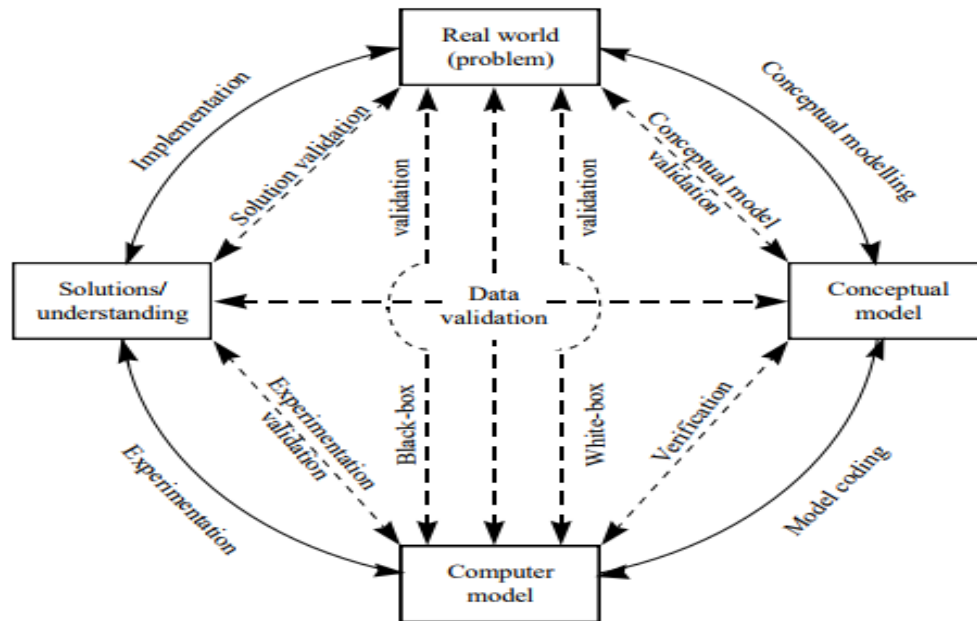


Figure 6.1: Simulation Model Verification and Validation in a Simulation Study

6.2 Concepts of Verification and Validation

Robinson [5] adapted a new framework of the life cycle for model development and use, illustrated on Figure 6.1, this model framework is based on V&V on each key activities. These V&V activities are defined by Robinson [5] for each process as follows:

- **Conceptual Model Validation:** define that the proposed model scope and level of detail are sufficient for the aim at hand.
- **Data Validation:** defining that the required data for model is sufficiently accurate .
- **Verification:** the method of ensuring that the conceptual model has been transformed into a computer model with sufficient accuracy.
- **White-box Validation:** defining that the essential parts of the computer simulations represent the corresponding real-world elements, with satisfactory accuracy.
- **Black-box Validation:** defining that the overall model represents the real world with sufficient accuracy.

- Experimentation Validation: determining that the experimental procedures adopted are providing results that are sufficiently accurate.
- Solution Validation: determining that the results obtained from the model of the proposed solution are sufficiently accurate.

6.3 Verification of the Insider Threat Prediction Approach

To ensure our approach is valid, we made sure from day one to take all the right steps and actions by verifying most of steps we take to implement the proposed model.

First, we asked ourselves if we are building the model, right? Is the project scope reflected to our aims? Do we carry out regular reviews, meetings and inspections? Is the required data for the proposed model sufficiently accurate? Did we make all the transformation from the proposed framework to a model without missing any part and correct? And where did model output reflect to what we have expected?

If we found the answer is “No” of any of the previous questions, then we take all the steps to make it right and start the verification procedure from where it failed.

An example of this verification process where the answer where “No” to the question “Is the required data for the proposed model sufficiently accurate?”. In [chapter 5](#), after collecting the survey questions answers, we found that some responses values are invalid. The step we carried out at that time to make the data input valid, is by applying cross-variable rules for all responses values. One of these rules were if the survey finished in less than 2 minutes, this would indicate that the participant does not take it seriously, we found 4 cases match this rule, these cases were deleted from the database, and a verification process started again by using the next rule.

6.4 Validation of the Prediction Model

The main challenge for the model validation is the need to compare the prediction result against real insider threat events. Due to the nature of this problem, however, real insider threat events are rarely published. However, Greitzer et al. validated their approach described in the previous chapters by comparing 24 case results with two HR experts judgments, giving a result correlation of R^2 ¹ = 0.598.[40]

We adopt a similar approach that Greitzer et al [40] used in our validation method, by comparing the results of the model prediction with the empirical judgements made by five researchers in the field of cyber-security, we refer to them in this report as a “security experts”.

Firstly, a validation workshop has been organised by us to validate the proposed prediction model result. 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, model, and its results.

A validation feedback form was provided to all experts participants, please refer to Appendix D for the feedback form. We then started describing the data collected in chapter 5 directly from the database file in a case by case procedure to all security experts.

They used a ranking probability election method ²to rank risk level from 1 to 5 for each case, where a rank of 1 signifies the most expected prediction (Certain), and a rank of 5 signifies the least expected prediction (Rare). Please refer to Appendix D for the expert participants contribution feedback forms at the validation workshop.

¹ R^2 In statistic, R-squared is to calculate how close the data are to the fitted regression-line. As well its known as the coefficient of multiple determination for multiple regression.

²**Probability Election Method** A method for protocols are used to assess and incorporate subjective probabilities in risk and decision analysis. various probability elicitation methods commonly used in risk analysis such as RR (Rank reciprocal), EW(Equal weight), RS(Rank Sum), ROC(Rank order centroid)

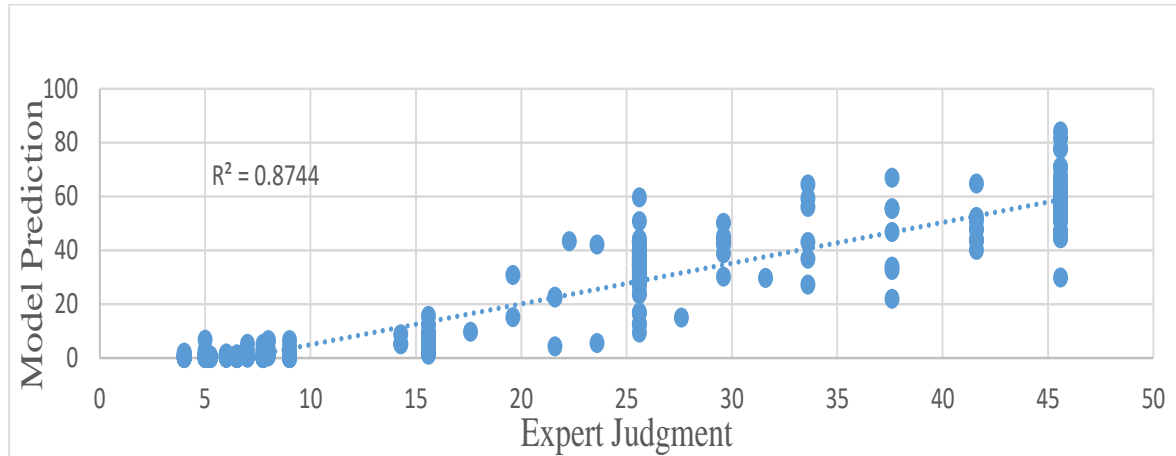


Figure 6.2: Verification Test

Barron and Barret in their research concluded that Rank order centroid (ROC) ³ weights are more accurate than the other rank-based formulae [3]. 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, (Tab. 6.1) illustrated the calculation result for ROC of Insider Threat Experts Judgement. The ROC formula used in this phase described as below:

$$wt_i = \left(\frac{1}{n}\right) \sum_{k=i}^n \left(\frac{1}{k}\right) \quad (6.1)$$

Where wt_i is the weight of each ranked order value, n is the total number of objectives and $i = 1, \dots, n$ & $\{wt_1 \geq wt_2 \geq \dots \geq wt_n\}$.

The model risk results were verified by examining the extent to which the model's results agreed with the experts' judgments, based on the results in Table 5.13 and Table 6.1.

Figure 6.2 shows the results of this verification test in respect to 61 cases from the selected organisation. The resulting correlation was generally around $R^2 = 0.87$, which indicates an acceptable fit in this area of research [40].

³ **Rank order centroid** In statistic, based on this the "ROC" weight method produces an estimate of the weights that minimises the maximum error of each weight by identifying the centroid of all possible weights maintaining the rank order of objective importance[32].

Table 6.1: Insider Threat Experts Judgement Result

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

6.5 Summary

This chapter described the important steps to verify and validate the insider threat prediction model result, to get enough confidence of the result. We evaluate the prediction results by comparing the model result with security expert's judgements results, by using different statistic methods to find how close the data are to the fitted regression line. In addition, the verification process has been carried out in each model development stage.

In the next chapter a dynamic model approach to mitigate the insider threat will be propose to try to improve the result of the validated static model over the time.

Chapter 7

A Dynamic Model Approach for Insider Threats

7.1 Introduction

Risk analysis strategies based on an assessment over an extended time period can help organisations to mitigate the risk of security breaches [33]. The previous chapters ([chapter 4](#) and [chapter 5](#)) in this thesis have presented a novel approach to predict the risk levels of insider threat based on a single period of data collection within an organisation, were described as a static model. In this part, we propose a new method to predict insider threats over a period of time, based on data collected and analysed on different time scales, called a dynamic model.

7.2 Model Formulation

Static Bayesian networks described in [chapter 4](#) can be extended with the concept of a time series - known as a Dynamic Bayesian network (DBN) [23]. DBNs model probability distributions over series of random variables of $Z = \{Z_1, Z_2, \dots\}$ where variables can be divided into $Z_t = (X_t, U_t, Y_t)$ to represent all observed variables (input, hidden and output) in a state-space model.

This means that DBNs can model time series or sequences; indeed they can model complex multivariate time series, thus encompassing the relationships between multiple time series within the same model [80].

Dynamic Bayesian networks are represented as a pair (B_1, B_{\rightarrow}) , where B_1 is a Bayesian network, which defines the prior $P(Z_1)$, while the second member

of the pair (B_{\rightarrow}) is called a two-slice temporal Bayesian network (2TBN), which is represented as $P(Z_t|Z_{t-1})$, with the use of Directed Acyclic Graph (DAG) as follows [54] [62]:

$$P(Z) = P(Z_1, Z_2, \dots, Z_t) = P(Z_t|Z_{t-1}, Z_{t-2}, \dots, Z_1) P(Z_2|Z_1)P(Z_1) \quad (7.1)$$

If we use the representation of $P(Z_t|Z_{t-1})$ we get:

$$P(Z_t | Z_{t-1}) = \prod_{i=1}^N P(Z_t^i | Parents(Z_t^i)) \quad (7.2)$$

Then:

$$P(Z_{1:T}) = \prod_{t=1}^T \prod_{i=1}^N P(Z_t^i | Parents(Z_t^i)) \quad (7.3)$$

Where Z_t^i is the i^{th} node at time t , and $Parents(Z_t^i)$ from $i = 1$ to N are the parents of Z_t^i in the DAG

7.3 The Architecture of Dynamic Insider Threat Prediction

The aim of this chapter is to provide a prediction method to support organisational decision makers to analyse the current situation and to establish long-term strategies to mitigate insider threats. This is based on the previous framework proposed in [chapter 4](#), which addresses the insider threat problem from three dimensions: the Technology Aspect Dimension, the Organisational Impact Dimension, and the Human Factors Dimension.

The novel aspect of the model development in this chapter is that it addresses insider threat issues from a fourth dimension, by adding a time series factor to the previous framework. A new architecture was therefore developed in this chapter to help organisations to predict potential malicious insider threats in the near future. ([Fig. 7.1](#)) shows the proposed architecture of the Dynamic Insider Threat Prediction Model, which is divided into four stages as follows:

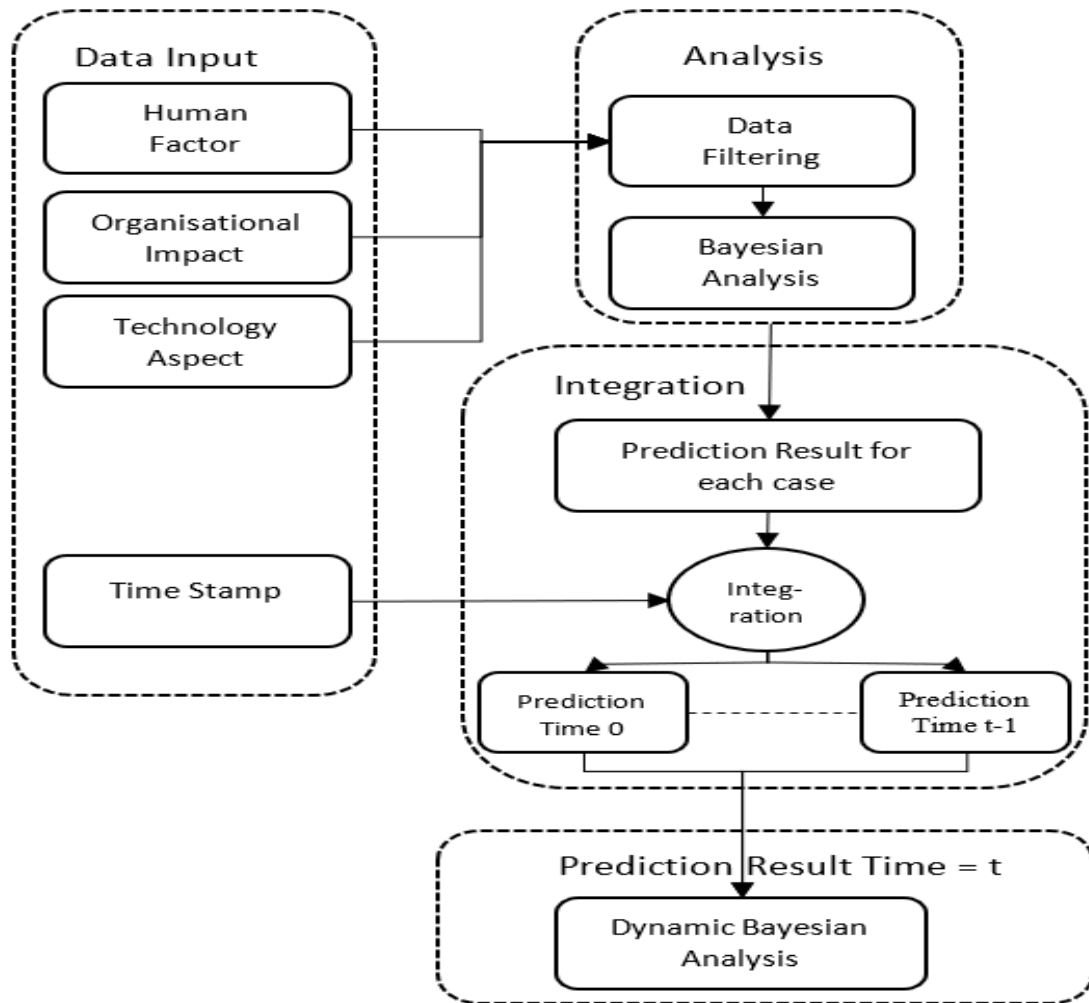


Figure 7.1: Architecture of the Dynamic Insider threat Prediction

7.3.1 Data Input

The first phase of this model is the data input phase where data should be collected from a single organisation over a period of time, to represent the Technology aspect, Organisational impact, Human factors and time frame. An online survey method is used to gather this information from a single organisation described in [chapter 5](#). The collected data then should be sorted into one database file.

7.3.2 Data Analysis

In this stage, the data collected in phase one will be filtered by various rules described in [chapter 5](#). Then import the filtered data into the Bayesian network data analysis model presented in previous chapters in order to predict insider threat risk levels for each case within one time series.

7.3.3 Integration

The main purpose of this stage is to integrate the prediction result from the previous step with the time stamp when the data was collected for each participant “case”. The output of this step is prediction levels for each participant for all time slots. For example, if we have six time stamps then we will get six prediction results for each participant case based on each time-frame, which we will explain later in this chapter.

7.3.4 Prediction Result

In this final step, the output from the previous stage for each case will be combined into the dynamic Bayesian Analysis model in order to predict potential malicious insider threats in the near future for each participant.

7.4 Case Study implementation

The objective of the case study is to implement the proposed Dynamic Bayesian model for predicting insider threats. The case study uses real data collected over a single time period, which has been extended with dummy data to represent another five periods of data. In total, therefore, six periods of data is used to run the proposed model.

The data was collected by means of a survey. Specifically, on the first collection three surveys were conducted as following: One Technology Aspect survey, One Organisational Impact survey, and Seventy Human Factor “participants” surveys were collected. Followed by the second collection three surveys identical to the first collection surveys were conducted as well on the same UK-based organisation with over 1000 employees. Around 70 members of staff volunteered to answer Human Factors part of the surveys questions.

The survey focused on the information needed to complete the 93 end node variables of the prediction model, as presented in [chapter 5](#), which comprised the data required to run the proposed model. However, due to the security restriction of the organisation to keep all participants anonymous we were unable to link cases from first and second surveys, for this reason we will base this analysis only on first collection followed by dummy data.

Each input from the six periods of data was processed using static Bayesian analysis to predict each input for each participant. A time-stamp was attached to each prediction result. Table 7.1 illustrates the prediction result from the proposed prediction model for each year period “ for full table please refers to Appendix C”. Where case means participant number, as we design this model to make the individual participants supplying data through the survey repeatedly in order to generate these different time stamps such as year 1, year 2 etc, then time represents the time order when data were collected, and Rare, Unlikely, Possible, Likely, and Certain represents the prediction percentage in respect to insider threat.

Table 7.1: Part of Prediction Result within Different Time Period

Case	Year	Rare	Unlikely	Possible	Likely	Certain
1	0	0.002	22.413	55.65	15.185	6.749
	1	0.002	22.122	55.537	15.374	6.965
	2	0.002	21.98	55.246	15.645	7.127
	3	0.001	20.28	56.097	16.124	7.499
	4	0.002	20.847	56.012	15.847	7.292
	5	0.002	20.847	56.012	15.847	7.292
4	0	0.058	30.845	50.985	12.763	5.349
	1	0.052	30.499	50.974	12.945	5.53
	2	0.051	30.336	50.76	13.188	5.664
	3	0.051	30.336	50.76	13.188	5.664
	4	0.089	32.909	49.542	12.427	5.032
	5	0.089	32.909	49.542	12.427	5.032
20	0	0.027	45.11	44.004	9.075	1.784
	1	0.024	44.751	44.139	9.235	1.85
	2	0.024	44.604	44.045	9.428	1.899
	3	0.024	44.604	44.045	9.428	1.899
	4	0.064	46.234	42.976	8.882	1.845
	5	0.064	46.234	42.976	8.882	1.845
22	0	0.288	57.307	36.226	5.657	0.522
	1	0.26	56.996	36.43	5.772	0.543
	2	0.256	56.885	36.401	5.9	0.558
	3	0.256	56.885	36.401	5.9	0.558
	4	0.234	52.315	39.228	7.187	1.037
	5	0.234	52.315	39.228	7.187	1.037
69	0	0.273	52.375	38.871	7.04	1.44
	1	0.246	52.035	39.048	7.175	1.496
	2	0.242	51.9	38.992	7.329	1.537
	3	0.027	42.724	44.664	9.64	2.946
	4	0.039	36.078	47.784	11.184	4.915
	5	0.039	36.078	47.784	11.184	4.915

The change we made for the first collection to generate dummy data for other five time-slots, are divided into three area of changes: a) change in personal circumstances of the participants over the period, similarly the change in the variables on the human factor described on [chapter 4](#) , b) change in organisational environment which reflect the organisational impact, one of theses changes is that the organisation has had any security breach on any time-slot, and d) the change to technical measures which impact on Technology aspect, these measures include adding new tools to prevent insider threat or providing security awareness training.

From [Table 7.1](#) and [Appendix C](#) prediction output table data, Insider Threat levels can be predicted using the Dynamic Bayesian Network. Next, we are going to choose three from the seventy cases as detailed examples: Case 4, Case 20 and Case 69, as explained in [chapter 5](#) in the section on emergency insider threat prediction result.

Case Number 04 From the previous predictions result in [chapter 5](#) using static Bayesian analysis our model predicts that this case is more than 50 % as a possible insider threat, with 12 % as likely to be an insider threat, and 30 % is unlikely an insider threat. Also, over six periods of data collected and analysed using static Bayesian, the prediction result is always being as a Possible insider threat. In [Table 7.1](#), it can be seen that case 4 at time 0 to 5 reveals an initial prediction result showing a 50.9% chance of this being a possible insider threat. At the later time frames, however, the risk of this being a possible insider threat decreases. In addition, the prediction of this case being unlikely to be an insider increases as time progresses. The reasons behind these prediction values changing over the time are mainly due to some change on personal circumstances such the change on understanding the organisational security policy, also, no change to work-related stress levels, which are still high over six-time periods.

In this case, after applying DBN to the previous data showed in [Table 7.1](#), we get the result shown in the chart [Figure 7.2](#). Our DBN model predicted that the risk level to be an insider threat would increase over two-time slots as it represented in dotted orange and red lines in the chart.

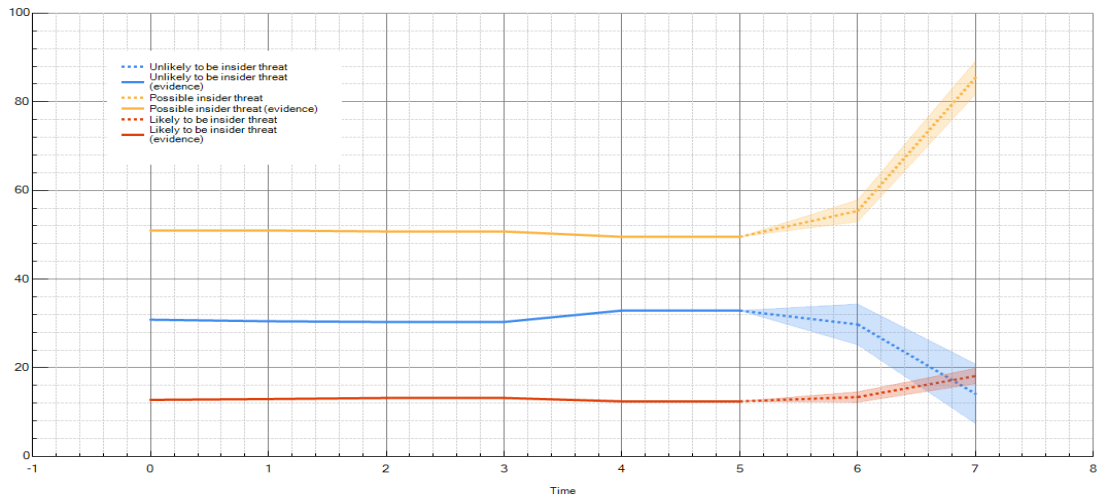


Figure 7.2: Case Number 4

Case Number 20 In the previous prediction model result in respect to emergency insider threat prediction in [chapter 5](#), we advised that the security analysis team should step into this case and analysis it manually to decide which risk level this case should belong to since in this case the prediction model predicted a borderline outcome between the case being unlikely to be an insider threat and a possible insider threat.

In [chapter 5](#) we introduce this case as “an employee is between 25 and 45 years old, she does not understand security policies, has access to the organisation’s intellectual property and believes that she owns the copyright ownerships. On the other hand, her motivation level is a normal level”. Then we advise the organisation to provide her with security awareness training which may reduce her insider risk levels in future assessments, as she then will understand the organisation’s security policy and copyright ownership.

Using the Dynamic Insider Threat prediction Model proposed in this chapter, however, it becomes clear that this participant over two-time slots will be possible an insider threat, as in all six time-slots prediction she still believes that she owns the copyright ownerships of the organisation property after the security awareness training that organisation provided to her. [Figure 7.3](#) illustrates the case number 20 prediction result, where the possibility to be an insider is represented in dotted orange line.

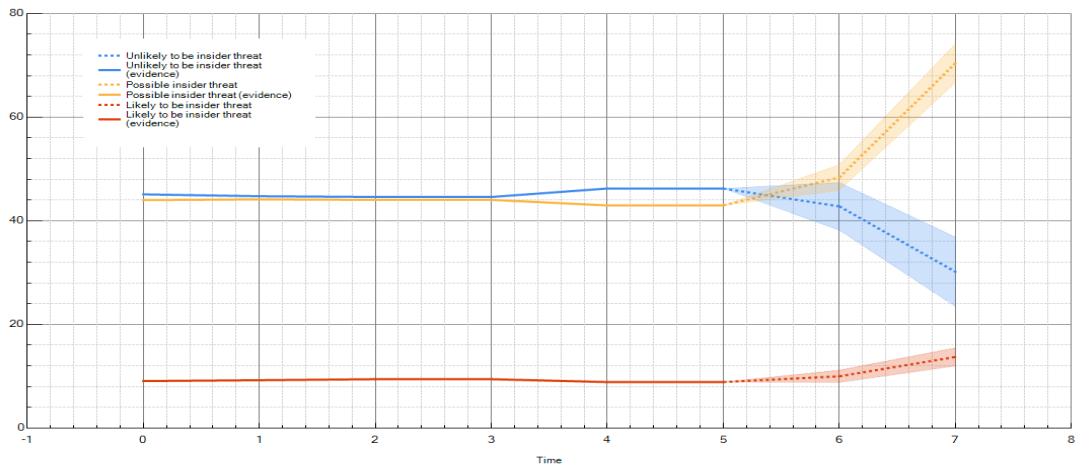


Figure 7.3: Case Number 20

Case Number 22 From the previous predictions result in [chapter 5](#) using static Bayesian analysis our model predicts that this case is 57.3 % is unlikely to be an insider threat, with 36.2% as a possible insider threat, and only 5.6 % as likely to be an insider threat. Also, over six periods of data collected and analysed using static Bayesian, the prediction result is always being as an unlikely insider threat. In [Table 6.1](#), it can be seen that case 22 at time 0 to 5 reveals an initial prediction result showing a 57.3 % is an unlikely insider threat. At the later time frames, however, the risk of this being an unlikely insider threat is decreases but stay over the prediction of possible insider threat, the reason behind no major change on the prediction result that because no change of the personal circumstances has been recorded.

In this case, after applying DBN to the previous data showed in [Table 7.1](#), we get the result shown in the chart [Figure 7.4](#) . Our DBN model predicted that the risk level to be an insider threat would decreases over two-time slots as it represented in dotted orange and red lines in the chart.

Case Number 69 In the previous prediction model result in respect to emergency insider threat prediction in [Table 5.13](#), this case is 52 % of being unlikely to be an insider threat. With different time collection showed in [Table 7.1](#), it reveals an initial prediction result as unlikely then changed to possible insider threat at time-slot 3. The reason of this is the change on the personal circumstances of the participants from time-slot 3, one of these changes was the participant's contract will expire in three mounts.

In this case, it is clear that the prediction result from [Figure 7.5](#) shows a

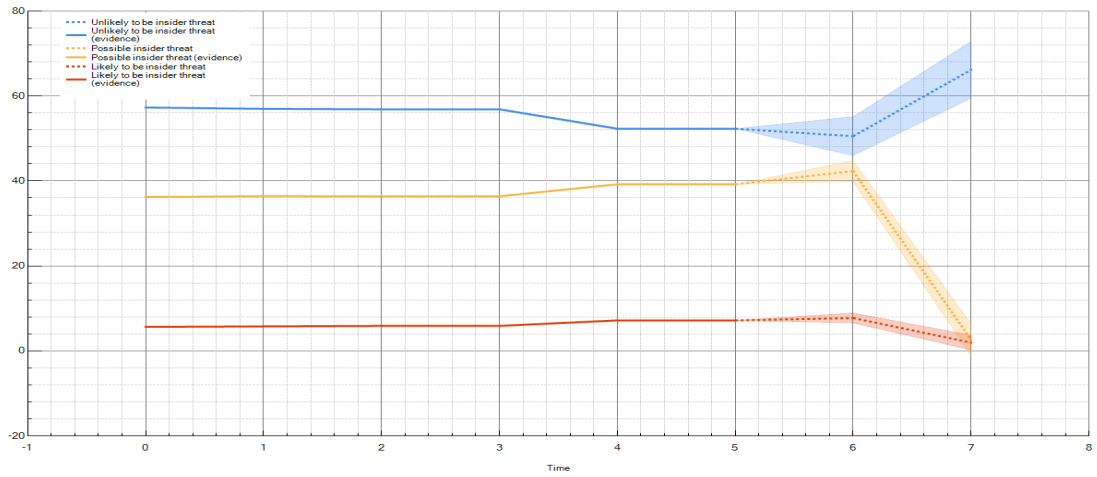


Figure 7.4: Case Number 22

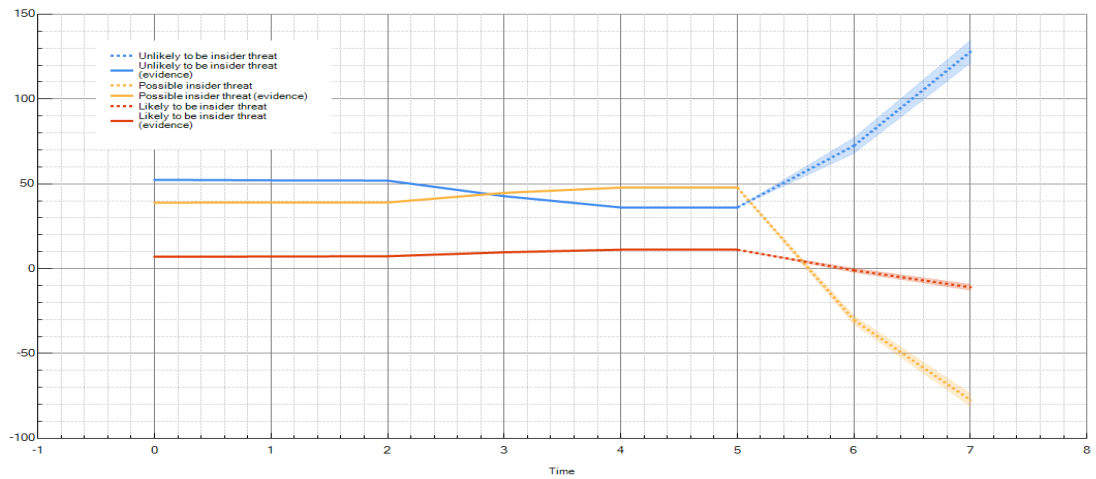


Figure 7.5: Case number 69

decrease in the risk of being an insider threat. The reason behind this is that the survey data shows a change in the contract expiration date, which previously been less than three months, which it may indicate this employee has left the organisation.

7.5 Summary

The previous chapters introduced the static insider threat prediction model, which is a way to measure the risk level for each authorised user within the organisation at a single time point. This chapter has focused on improving the insider threat risk assessment approach, by presenting the dynamic insider threat prediction. This model was introduced to a group of predictions results within one organisation based over a period of time the data was collected. This will help organisations to predict potential malicious insider threats in the near future.

Architecture of the Dynamic Insider Threat prediction was proposed and discussed in this chapter, followed by a case study implementation to predict malicious insider threat for the near future.

We have found that extending our model approach based on the Bayesian network to a new model based on a Dynamic Bayesian network has the potential to improving prediction results for the near future, also it provides the organisations with further information that is helpful to manage and mitigate insider threat.

Chapter 8

Conclusions, Limitation, and Future Research

8.1 Conclusions

Insider threat issue is one of the most pressing challenges that threaten an organisation's information assets. Unfortunately, no single approach can eliminate this kind of security breach; organisations need to carry out a regular security risk assessment in regard to insider threats, and to address any gaps on their environment. In this thesis, we presented a model that predicts a malicious insider threat before a security breach takes place. Insider threat problems are not like external threats, an insider has knowledge of all organisational security measures and has some degree of trust from the organisation.

We used a multiple-perspective approach, where more than 100 key insider indicators were collected for each authorised user, which were divided into three-dimensions. Then we used these indicator values to calculate the risk levels for each authorised user, based on Bayes theorem.

Also, we presented the emergency insider threat risk prediction level results for two selected organisations, the result shows that our model gives a worthy result in predicting any malicious insider threat, with the possibility to find and address the vulnerable area within the organisation that needs to improve to mitigate the risk.

Finally, we proposed a new method to predict insider threats over a period of time, based on data collected and analysed on different time scales, called a dynamic model Approach.

8.2 Limitations

This section considers the limitations for the proposed work in this thesis.

- The first limitation to this study was the use of a prior probability distribution which was based on judgement and literature review, as little insider threat evidence is available for researchers.
- Second, organisation policy prevents us from getting participant's names in this study, to compare the prediction result with any insider security breach which occurred. For this reason, it was hard to validate this approach within the organisation.

8.3 Contributions Revisited

The contributions of this study can be summarised as follows:

- A detailed definition of the insider threat has been introduced that makes a clear distinction between malicious or unintentional breaches, authorisation access, with the impact to the information security goals ([chapter 2](#)).
- Insider threat categories have been divided into seven sub-categories, based on the manner in which they affect the organisation's information security goals (confidentiality, integrity, and availability), and the human factors which lead an insider to act in a malicious manner (motive, opportunity, and capability ([chapter 2](#))).
- An in-depth literature review that presents an unique view of the current state of the art about insider threat mitigation approaches has been discussed. We classified these approaches into two main categories: a) technical mitigation approaches and b) non-technical mitigation approaches ([chapter 3](#)).
- A multiple perspective frameworks has been proposed to reduce the risk of insider threat by predicting who could be an insider threat ([chapter 4](#)).
- A Bayesian model has been developed to implement the proposed framework ([chapter 4](#)).

- The model of Insider threat risk prediction has been tested on data collected using surveys and analysed using the model for the final result([chapter 5](#)).
- A new architecture has been introduced based on an extension to the previous framework, the novelty of this approach is on designing a dynamic insider threat prediction model with time series ([chapter 7](#)).
- The insider threat risk prediction result has been evaluated by using probability election method based on comparing the model results with experts judgements ([chapter 6](#)).

8.4 Future Research

This section provides intuition into how to extend the research reported in this thesis.

Dealing with trust is a difficult issue that involves researchers looking at the problem from a holistic perspective in terms of: a) Human behaviour, b)Technology controls and c) Organisational aspects. Future research is highly recommended by different institutions to cover the following points:

- More in-depth research is needed, to discover the cause behaviour that drives privileged users to act malicious insider threat. This will lead to the identification of the mitigating factors and indicators of malicious or accidental insider threats.
- To develop a comprehensive prediction model, which can integrate with all other approaches.
- Investigate the changing behaviour for human, organisation, and technology factors over a period of time to get accurate prediction results.
- To develop a model that provides guidance to mitigate such a threat based on the prediction result.
- Finally, research is required to identify the effects of information security policy for organisations in term of insider threat risk levels.

References

- [1] E. T. Axelrad, P. J. Sticha, O. Brdiczka, and Jianqiang Shen. A Bayesian Network Model for Predicting Insider Threats. In *2013 IEEE Security and Privacy Workshops*, pages 82–89. IEEE, may 2013. ISBN 978-1-4799-0458-7. doi: 10.1109/SPW.2013.35. URL <http://ieeexplore.ieee.org/document/6565234/>.
- [2] R. Bace and P. Mell. NIST special publication on intrusion detection systems. Technical report, Booz Allen & Hamilton, McLean, VA 22102, 2001. URL <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA393326>.
- [3] F. H. Barron and B. E. Barrett. Decision Quality Using Ranked Attribute Weights. *Management Science*, 42(11):1515–1523, nov 1996. ISSN 0025-1909. doi: 10.1287/mnsc.42.11.1515. URL <http://pubsonline.informs.org/doi/abs/10.1287/mnsc.42.11.1515>.
- [4] D. Bartram and G. Turley. *Managing the causes of work-related stress*, volume 31. HSE, sep 2009. ISBN 9780717662739. doi: 10.1136/inpract.31.8.400. URL <http://inpractice.bmj.com/cgi/doi/10.1136/inpract.31.8.400>.
- [5] A. Beck. Simulation: the practice of model development and use. *Journal of Simulation*, 2(1):67–67, mar 2008. ISSN 1747-7778. doi: 10.1057/palgrave.jos.4250031. URL <https://www.tandfonline.com/doi/full/10.1057/palgrave.jos.4250031>.
- [6] M. Ben Salem, S. Hershkop, and S. J. Stolfo. A survey of insider attack detection research. *Insider Attack and Cyber Security: Beyond the Hacker*, pages 69–90, 2008. ISSN 15682633. doi: 10.1007/978-0-387-77322-3_5. URL http://link.springer.com/chapter/10.1007/978-0-387-77322-3_5.
- [7] M. Bishop, D. Gollmann, J. Hunker, and C. W. Probst. Countering insider threats. In *Dagstuhl Seminar Proceedings 08302*, pages 1–18, 2008.

- URL <http://vesta.informatik.rwth-aachen.de/opus/volltexte/2008/1793/pdf/08302.SWM.1793.pdf>.
- [8] R. Brackney and R. Anderson. Understanding the Insider Threat. In *Advanced Research and Development Activity (ARDA)*, 2004. ISBN 0833036807.
- [9] O. Buckley, J. R. C. Nurse, P. a. Legg, M. Goldsmith, and S. Creese. Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat. *Workshop on Socio- . . .*, 2013. doi: 10.1109/STAST.2014.10.
- [10] O. Buckley, J. R. Nurse, P. A. Legg, M. Goldsmith, and S. Creese. Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*, pages 8–15. IEEE, jul 2014. ISBN 978-1-4799-7901-1. doi: 10.1109/STAST.2014.10.
- [11] D. Cappelli, A. P. Moore, and R. Trzeciak. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes*. Addison-Wesley Professional, 1st ed edition, 2012. ISBN 9780321812575.
- [12] J. Carson. Convincing users of model’s validity is challenging aspect of modeler’s job. *Industrial Engineering*, (18):6, 1986.
- [13] CERT Insider Threat Center. Insider Threat Control : Using a SIEM signature to detect potential precursors to IT Sabotage. *Software Engineering Institute, Carnegie Mellon University Carnegie Mellon University.*, (April), 2011.
- [14] CERT Insider Threat Team. Unintentional Insider Threats : Social Engineering. *Software Engineering Institute, Carnegie Mellon University, CMU/SEI-20* (January), 2014.
- [15] S. Chockalingam and W. Pieters. *Secure IT Systems*, volume 10674 of *Lecture Notes in Computer Science*. Springer International Publishing, Cham, 2017. ISBN 978-3-319-70289-6. doi: 10.1007/978-3-319-70290-2. URL <http://link.springer.com/10.1007/978-3-319-70290-2>.
- [16] F. Cohen. Forensic Methods for Detecting Insider Turning Behaviors. In *2012 IEEE Symposium on Security and Privacy Workshops*, pages 150–158. IEEE, may 2012. ISBN 978-1-4673-2157-0. doi: 10.1109/SPW.2012.21. URL <http://ieeexplore.ieee.org/document/6227699/>.

- [17] C. Colwill. Human factors in information security: The insider threat Who can you trust these days? *Information Security Technical Report*, 14(4): 186–196, nov 2009. ISSN 13634127. doi: 10.1016/j.istr.2010.04.004. URL <http://linkinghub.elsevier.com/retrieve/pii/S1363412710000051>.
- [18] E. Costante, J. den Hartog, M. Petković, S. Etalle, and M. Pechenizkiy. A white-box anomaly-based framework for database leakage detection. *Journal of Information Security and Applications*, 32:27–46, feb 2017. ISSN 22142126. doi: 10.1016/j.jisa.2016.10.001. URL <http://linkinghub.elsevier.com/retrieve/pii/S2214212616302629>.
- [19] CPNI. Insider data collection study- Report of man finding. Technical Report April, Centre for the Protection of National Infrastructure (CPNI), 2013.
- [20] J. Crampton and M. Huth. Towards an access-control framework for counter-ing insider threats. *Advances in Information Security*, 49:173–195, 2010. ISSN 15682633. doi: 10.1007/978-1-4419-7133-3_8. URL http://link.springer.com/chapter/10.1007/978-1-4419-7133-3_8.
- [21] DANIEL COSTA. CERT Definition of ‘Insider Threat’ - Updated, 2017. URL <https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html>.
- [22] P. K. Davis. *Generalizing Concepts and Methods of Verification, Validation, and Accreditation (VV&A) for Military Simulations*,. RAND, 1992. ISBN 0833012983. URL <http://handle.dtic.mil/100.2/ADA336851>.
- [23] T. Dean and K. Kanazawa. A model for reasoning about persistence and causation. *Computational Intelligence*, 5(2):142–150, 1989. ISSN 14678640. doi: 10.1111/j.1467-8640.1989.tb00324.x.
- [24] P. J. Dombrowski. The Department of Defense. *Routledge Handbook of American Foreign Policy*, (5205):1–16, 2011.
- [25] F. Doyle and V. Labs. Methods , Motivations and Mitigation of Insider Threats. Technical report, VeriSign, 2007.
- [26] A. Duncan, S. Creese, and M. Goldsmith. An overview of insider attacks in cloud computing. *Concurrency and Computation: Practice and Experience*, 27(12):2964–2981, aug 2015. ISSN 15320626. doi: 10.1002/cpe.3243. URL <http://doi.wiley.com/10.1002/cpe.3243>.
- [27] S. Fenz, G. Goluch, A. Ekelhar, B. Riedl, and E. Weippl. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. In

- 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)*, pages 381–388. IEEE, dec 2007. ISBN 0-7695-3054-0. doi: 10.1109/PRDC.2007.29. URL <http://ieeexplore.ieee.org/document/4459686/>.
- [28] L. Flynn, G. Porter, and C. DiFatta. Cloud Service Provider Methods for Managing Insider Threats : Analysis Phase II , Expanded Analysis and Recommendations. Technical Report January, Carnegie Mellon University CERT Program, 2014. URL <http://repository.cmu.edu/sei/765/>.
- [29] E. R. Ford. Man-in-the-Middle Attack to the HTTPS Protocol. *2009 IEEE Security & Privacy*, 7(1):78 –81, 2009.
- [30] Frank L. Greitzer ; Andrew P. Moore ; Dawn M. Cappelli ; Dee H. Andrews ; Lynn A. Carroll ; Thomas. Combating the Insider Cyber Threat. *IEEE Security & Privacy*, 6:61–64, 2008. doi: 10.1109/MSP.2008.8.
- [31] B. Gabrielson. Solving the Insider Threat Problem. *Presented at the University of Louisville Cyber Securitys Day*, (October):1–10, 2006.
- [32] P. H. Garthwaite, J. B. Kadane, and A. O’Hagan. Statistical Methods for Eliciting Probability Distributions. *Journal of the American Statistical Association*, 100(470):680–701, 2005. ISSN 0162-1459. doi: 10.1198/016214505000000105. URL <http://www.tandfonline.com/doi/abs/10.1198/016214505000000105>.
- [33] M. G. Gelles. *Insider Threat: Prevention, Detection, Mitigation, and Deterrence*. Candice Janco Elsevier, 2016. ISBN 9780128024102.
- [34] J. W. B. George J. Silowash, Todd Lewellen. Detecting and Preventing Data Exfiltration Through Encrypted Web Sessions via Traffic Inspection. *Software Engineering Institute, Carnegie Mellon University, CMU/SEI-20*(March), 2013.
- [35] N. Ghaffarzadegan. How a system backfires: Dynamics of redundancy problems in security. *Risk Analysis*, 28(6):1669–1687, 2008. ISSN 02724332. doi: 10.1111/j.1539-6924.2008.01132.x.
- [36] S. Gorniak, D. Ikonou, P. Saragiotis, I. Askoxylakis, P. Belimpasakis, B. Bencsath, M. Broda, L. Buttyan, G. Clemo, P. Kijewski, A. Merle, K. Mitrokotsa, A. Munro, O. Popov, C. W. Probst, L. Romano, C. Siaterlis, V. Siris, I. Verbauwhede, and C. Vishik. Priorities for Research on Current and Emerging Network Technologies. *European Network and Information Security Agency*, 2010.

- [37] G. Greenwald. Edward Snowden: the whistleblower behind the NSA surveillance revelations — US news, 2013. URL <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.
- [38] F. L. Greitzer and R. E. Hohimer. Modeling Human Behavior to Anticipate Insider Attacks. *Journal of Strategic Security*, 4(2):25–48, jun 2011. ISSN 1944-0464. doi: 10.5038/1944-0472.4.2.2. URL <http://scholarcommons.usf.edu/jss/vol4/iss2/3/>.
- [39] F. L. Greitzer, L. J. Kangas, C. F. Noonan, and a. C. Dalton. Identifying at-Risk Employees : A Behavioral Model for Predicting Potential Insider Threats. *Pacific Northwest National Laboratory*, pages 1–46, 2010. doi: 10.2172/1000159.
- [40] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer. Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. In *2012 45th Hawaii International Conference on System Sciences*, pages 2392–2401. IEEE, jan 2012. ISBN 978-1-4577-1925-7. doi: 10.1109/HICSS.2012.309. URL <http://ieeexplore.ieee.org/document/6149305/>.
- [41] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie. Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies. *2014 47th Hawaii International Conference on System Sciences*, pages 2025–2034, jan 2014. doi: 10.1109/HICSS.2014.256. URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6758854>.
- [42] L. Hadlington. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, (June):e00346, 2017. ISSN 24058440. doi: 10.1016/j.heliyon.2017.e00346. URL <http://dx.doi.org/10.1016/j.heliyon.2017.e00346>.
- [43] M. Hart, P. Manadhata, and R. Johnson. Text Classification for Data Loss Prevention. *Privacy Enhancing Technologies*, pages 18–37, 2011. doi: 10.1007/978-3-642-22263-4_2. URL http://link.springer.com/10.1007/978-3-642-22263-4_{_}2.
- [44] T. Herath and H. R. Rao. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009. ISSN 0960085X. doi: 10.1057/ejis.2009.6.

- [45] HSE. Work related stress - Tools and templates. URL <http://www.hse.gov.uk/stress/standards/downloads.htm>.
- [46] J. Hunker and C. Probst. Insiders and insider threats an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous ...*, 2(1):4–27, 2011. ISSN 20935374. URL <http://isyoud.info/jowua/papers/jowua-v2n1-1.pdf>.
- [47] ISO/IEC 27000:2009. Information technology - Security techniques - Information security management systems - Overview and vocabulary. Technical report, International Organization for Standardization, 2009.
- [48] G. Jabbour and D. a. Menascè. The insider threat security architecture: A framework for an integrated, inseparable, and uninterrupted self-protection mechanism. *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 3:244–251, 2009. doi: 10.1109/CSE.2009.278. URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5283555>.
- [49] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis. An Insider Threat Prediction Model. In *Trust, Privacy and Security in Digital Business*, chapter 3, pages 26–37. springer, 2010. doi: 10.1007/978-3-642-15152-1_3.
- [50] E. Kasanen, K. Lukka, and A. Siitonen. The Constructive Approach in Management Accounting Research. *Journal of Management Accounting Research*, 5(June 1991):243–264, 1993. ISSN 1049-2127.
- [51] S. M. Katsikas S, Lopez J. An Insider Threat Prediction Model. *Trust, Privacy and Security in Digital Business*, 7(LNCS 6264,):26–37, 2010. URL http://link.springer.com/chapter/10.1007/978-3-642-15152-1_{_}3.
- [52] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers. Study: Computer System Sabotage in Critical Infrastructure. *U.S.S. Service and C.M.U. Software Engineering Institute, Software Engineering Institute, Carnegie Mellon Universit*, (May):45, 2005.
- [53] M. T. Khorshed, a. S. Ali, and S. a. Wasimi. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, 28(6):833–851, jun 2012. ISSN 0167739X. doi: 10.1016/j.future.2012.01.006. URL <http://linkinghub.elsevier.com/retrieve/pii/S0167739X12000180>.

- [54] M. Koleini, M. R. Ahmadzadeh, and S. Sadri. A new efficient feature-combination-based method for dynamic texture modeling and classification using semi-random starting parameter dynamic Bayesian networks. *Multimedia Tools and Applications*, 76(14):15251–15278, 2017. ISSN 15737721. doi: 10.1007/s11042-016-3793-4.
- [55] M. Lennon. Insider Steals Data of 2 Million Vodafone Germany Customers, 2013. URL <http://www.securityweek.com/attacker-steals-data-2-million-vodafone-germany-customers>.
- [56] T. Lewellen and G. J. Silowash. Insider Threat Control : Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time. *Software Engineering Institute, Carnegie Mellon University*, CMU/SEI-20(October), 2013.
- [57] H. A. Linstone. The multiple perspective concept. *Technological Forecasting and Social Change*, 20(4):275–325, dec 1981. ISSN 00401625. doi: 10.1016/0040-1625(81)90062-7. URL <http://linkinghub.elsevier.com/retrieve/pii/0040162581900627>.
- [58] J. R. McCumber. Information systems security: A comprehensive model. In *14th National Computer Security Conference*, pages 1–6, 1991.
- [59] J. Meier, C. Farrre, J. Taylor, P. Bansode, S. Gregersen, M. Sundarajan, and R. Boucher. *Improving Web Services Security: Scenarios and Implementation Guidance for WCF Contributors*. Microsoft Corporation, 2008. ISBN 978-0735618428.
- [60] P. Moore, D. Cappelli, T. Caron, E. Shaw, D. Spooner, and R. Trzeciak. A preliminary model of insider theft of intellectual property. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2:28–49, 2011. ISSN 20935374.
- [61] D. Muijs. *Doing Quantitative Research in Education with SPSS*, volume 44. SAGE Publications Ltd, 1 Oliver’s Yard, 55 City Road, London EC1Y 1SP United Kingdom, feb 2011. ISBN 9781446287989. doi: 10.4135/9781849203241. URL <http://methods.sagepub.com/book/doing-quantitative-research-in-education-with-spss-2e>.
- [62] K. P. Murphy. Dynamic Bayesian Networks: Representation, Inference and Learning. *University of California, Berkeley*, Ph. D.:225, 2002. ISSN <null>. doi: 10.1.1.129.7714. URL <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.778{&}rep=rep1{&}type=pdf>.

- [63] J. Negroponte. A preliminary examination of insider threat programs in the U.S. private sector. Technical report, INSA, 2013. URL https://www.nist.gov/sites/default/files/documents/2017/06/08/20131213{}_charles{}_alsup{}_insa{}_part4.pdf.
- [64] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty. Understanding insider threat: A framework for characterising attacks. In *Proceedings - IEEE Symposium on Security and Privacy*, volume 2014-Janua, pages 214–228, 2014. ISBN 9781479951031. doi: 10.1109/SPW.2014.38.
- [65] J. R. C. Nurse, P. a. Legg, O. Buckley, I. Agrafiotis, G. Wright, M. Whitty, D. Upton, M. Goldsmith, and S. Creese. 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, pages 270–281. 2014. doi: 10.1007/978-3-319-07620-1_24. URL http://link.springer.com/10.1007/978-3-319-07620-1{}_24.
- [66] M. E. Palmer, C. Robinson, J. C. Patilla, and E. P. Moser. Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age. *Information Systems Security*, 10(2):1–15, may 2001. ISSN 1065-898X. doi: 10.1201/1086/43314.10.2.20010506/31399.4. URL <http://dx.doi.org/10.1201/1086/43314.10.2.20010506/31399.4>.
- [67] S. Palmer and C. Cary. *How to deal with strees (Creating Success)*. Kogan Page, 3 edition edition, 2013. ISBN 978-0749467067.
- [68] S. Palmer, C. Cooper, and K. Thomas. Model of organisational stress for use within an occupational health education/promotion or wellbeing programme - A short communication. *Health Education Journal*, 60(4):378–380, dec 2001. ISSN 0017-8969. doi: 10.1177/001789690106000410. URL <http://journals.sagepub.com/doi/10.1177/001789690106000410>.
- [69] R. Pardee. Motivation Theories of Maslow, Herzberg, McGregor & McClelland. A Literature Review of Selected Theories Dealing with Job Satisfaction and Motivation. *Synopsis of selected motivational theories*, pages 1–24, 1990. doi: 10.5539/gjhs.v4n2p2. URL <http://eric.ed.gov/?id=ED316767http://files.eric.ed.gov/fulltext/ED316767.pdf>.
- [70] J. Pearl. Bayesian Networks A Model of Self-Activated Memory for Evidential Reasoning. In *Proceedings of the 7th Conference of the Cognitive Science Society*, pages 329–334, 1985. doi: citeulike-article-id:3847802.

- [71] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford. Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *IEEE Transactions on Information Forensics and Security*, 5(1):169–179, mar 2010. ISSN 1556-6013. doi: 10.1109/TIFS.2009.2039591. URL <http://ieeexplore.ieee.org/document/5371836/>.
- [72] Ponemon Institute. Privileged User Abuse & The Insider Threat Commissioned. Technical Report May, Ponemon Institute, 2014. URL http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_{_}257010.pdf.
- [73] Ponemon Institute LLC. 2017 Cost of Data Breach Study. Technical Report March, IBM Security and Ponemon Institute, 2017. URL https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN{&}).
- [74] A. J. Puleo. *Mitigation Insider Threat Using Human Behavior Influence Models*. PhD thesis, 2006.
- [75] N. Robins, P. A. Williams, and K. Sansurooah. An investigation into remnant data on USB storage devices sold in Australia creating alarming concerns. *International Journal of Computers and Applications*, 39(2):79–90, 2017. ISSN 19257074. doi: 10.1080/1206212X.2017.1289689. URL <http://dx.doi.org/10.1080/1206212X.2017.1289689>.
- [76] S. Robinson. Simulation model verification and validation. In *Proceedings of the 29th conference on Winter simulation - WSC '97*, pages 53–59, New York, New York, USA, 1997. ACM Press. ISBN 078034278X. doi: 10.1145/268437.268448. URL <http://dx.doi.org/10.1145/268437.268448><http://portal.acm.org/citation.cfm?doid=268437.268448>.
- [77] S. Robinson and R. J. Brooks. Independent verification and validation of an industrial simulation model. *Simulation*, 86(7):405–416, 2010. ISSN 00375497. doi: 10.1177/0037549709341582.
- [78] F. Rocha and M. Correia. Lucy in the sky without diamonds: Stealing confidential data in the cloud. *Proceedings of the International Conference on Dependable Systems and Networks*, pages 129–134, jun 2011. doi: 10.1109/DSNW.2011.5958798. URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5958798>.
- [79] M. K. Rogers. A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior. *PHD Thesis. Dept. of Psychology, University of Manitoba*, (C):233, 2001.

- [80] S. Russel and P. Norwig. *Artificial Intelligence A Modern Approach*. Pearson Education, 2003. ISBN 0-13-080302-2. URL <http://www.ncbi.nlm.nih.gov/pubmed/22244610>.
- [81] R. S. Sandhu, H. L. Feinstein, and C. E. Youman. RoleBased Access Control Models. *IEEE*, 1996.
- [82] K. Scarfone and P. Mell. Guide to Intrusion Detection and Prevention Systems (IDPS). *National Institute of Standards and Technology Special Publication*, 2007.
- [83] K. F. Schuessler. Other People’s Money: A Study in the Social Psychology of Embezzlement. Donald R. Cressey. *American Journal of Sociology*, 59 (6):604–604, may 1954. ISSN 0002-9602. doi: 10.1086/221475. URL <http://www.journals.uchicago.edu/doi/10.1086/221475>.
- [84] E. Schultz. A framework for understanding and predicting insider attacks. *Computers and Security*, 21(6):526–531, oct 2002. ISSN 01674048. doi: 10.1016/S0167-4048(02)01009-X. URL <http://linkinghub.elsevier.com/retrieve/pii/S016740480201009X>.
- [85] E. D. Shaw and L. F. Fischer. 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, 2005.
- [86] G. Silowash and C. King. Insider threat control: Understanding data loss prevention (DLP) and detection by correlating events from multiple sources. Technical Report January, Carnegie Mellon University CERT Program, 2013. URL <http://repository.cmu.edu/sei/708/>.
- [87] G. Silowash and A. Nicoll. Managing The Insider Threat: What Every Organization Should Know. Technical report, Carnegie Mellon University CERT Program, 2013. URL <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69111>.
- [88] G. J. Silowash and T. B. Lewellen. Insider Threat Control: Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders. *Software Engineering Institute, Carnegie Mellon University*, (January):35, 2013. URL <http://repository.cmu.edu/sei/728/>.
- [89] Software Engineering Institute. 2014 US State of Cybercrime Survey, 2014. URL <http://resources.sei.cmu.edu/asset{ }files/Presentation/2014{ }017{ }001{ }298322.pdf>.

- [90] L. Spitzner. Honeypots: catching the insider threat. In *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, pages 170–179. IEEE, 2003. ISBN 0-7695-2041-3. doi: 10.1109/CSAC.2003.1254322. URL <http://ieeexplore.ieee.org/document/1254322/>.
- [91] S. Stolfo, S. Bellovin, and S. Hershkop. *Insider Attack and Cyber Security*, volume 39 of *Advances in Information Security*. Springer US, Boston, MA, 2008. ISBN 978-0-387-77321-6. doi: 10.1007/978-0-387-77322-3. URL <http://link.springer.com/10.1007/978-0-387-77322-3>.
- [92] M. Swanson. Security Self-Assessment Guide for Information Technology Systems. *National Institute for Standards and Technology Special Publication*, 800(26), 2001.
- [93] The Department for Business Innovation and Skills. 2013 Information Security Breaches Survey, Technical Report. Technical report, PWC, 2013.
- [94] The UK National Cyber Security Programme. 2015 Information Security Breaches Survey. Technical report, UK HM Government, 2015. URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.
- [95] B. Wood. An insider threat model for adversary simulation. *SRI International Research on Mitigating the Insider Threat to Information Systems*, 2:1–3, 2000. URL http://www.csl.sri.com/users/bjwood/Insider_threat_model_v02.pdf.
- [96] Z. M. Yusop and J. Abawajy. Analysis of Insiders Attack Mitigation Strategies. *Procedia - Social and Behavioral Sciences*, 129:581–591, may 2014. ISSN 18770428. doi: 10.1016/j.sbspro.2014.03.716. URL <http://www.sciencedirect.com/science/article/pii/S1877042814028985>.
- [97] S. Zeadally, B. Yu, D. H. Jeong, and L. Liang. Detecting insider threats solutions and trends. *Information Security Journal*, 21(4):183–192, jan 2012. ISSN 19393555. doi: 10.1080/19393555.2011.654318. URL <http://www.tandfonline.com/doi/abs/10.1080/19393555.2011.654318>.

Appendix A

Human Factors, Technology Aspects and Organisational Impact Survey

Technology Aspect

Start of Block: Introduction

Emergency Insider Threat Risk Predictions: PhD Project Survey.

This survey is a part of PhD student research work, which is being carried out at Loughborough University, in the Computer Science Department in collaboration with the School of Business and Economics.

The survey is the key to determining how to deliver a significantly enhanced capability of managing malicious insider cyber-security threats, and also how to educate and to spread materials and strategies for mitigation of malicious insider threats. Your cooperation will help to ensure that my research is relevant for your organisation.

Please complete the survey based on the best of your knowledge. If you complete this survey, you are consenting to have your anonymised responses included as part of data collection for this survey. However, you can enter your name in the last field if you wish to let us know who you are.

Please complete the entire survey. There are 20 questions over 3 pages and we estimate that it should take at most 8 minutes of your time, To start please press Start button at the bottom of this page, and to submit the survey, please click Submit at the bottom of the last page.

If you have any further questions, please feel free to contact us at: n.elmrabit@lboro.ac.uk

Thank you very much for your response.

Nebrase Elmrabit
PhD Research Student.

Page Break

End of Block: Introduction

Start of Block: Block 1

Q1 How much does your organisation allocate to the IT budget in one year?

- Less than 5% of overall budget.
 - Between 5% and 9% of overall budget.
 - Over 9% of overall budget.
-

Q2

How much of the IT budget is spent on IT security?

- Less than 10% of the overall IT budget.
 - Between 10 % and 25% of the overall IT budget.
 - Over 25% of the overall IT budget.
-

Q3

How much of the IT security budget is spent on protection from insider threats?

- Less than 10% of the overall IT security budget.
 - Between 10 % and 25% of the overall IT security budget.
 - Over 25% of the overall IT security budget.
-

Q4 Do you have any concerns regarding security threats coming from authorised users?

- Yes, very important.
 - Not at all, we trust all our authorised users.
-

Q5 Does your organisation provide any security awareness and training strategy?

- Yes.
 - No.
-

Q6 Does your organisation encourage all authorised users to attend security awareness and training programmes?

- Yes. All authorised user include employees, contractors or anyone who has authorised access to our system.
 - Yes, but just with regard to our employees.
 - No.
-

Q7 How often do your employees attend security awareness and training programmes?

- Once.
 - Annually.
 - Never.
-

Page Break

Q8 Has your organisation suffered any information security breach in the last 5 years?

Yes.

No.

Q9 Has your organisation suffered any security breach that was accidentally caused by an authorized user in the last 5 years?

Yes.

No.

Q10 Has your organisation been under attack from external threats?

Yes.

No.

Q11 Has your organisation suffered any security breach caused by an authorised user in the last 5 years?

Yes

No.

Display This Question:

If Has your organisation suffered any security breach caused by an authorised user in the last 5 years? = Yes

Q12-1

If you have answered Yes to the previous question, please let us know which type of authorised user security breach your organisation suffered? You can select more than one.

- Insider IT Fraud.
- Insider Theft of Intellectual Property.
- Insider IT Sabotage.
- Insider Social Engineering.
- Insider In Cloud Computing.
- Insider National Security.

Display This Question:

If Has your organisation suffered any security breach caused by an authorised user in the last 5 years? = Yes

Q12-2 What action was taken against any malicious authorized user ?

- Update security policy.
 - Implementing a new security strategy.
 - Training and awareness.
 - Termination of an employee.
 - Other action. Please specify
-

End of Block: Block 1

Start of Block: Block 2

Q13 Which of the following IT security tools has your organisation implemented in order to detect an insider threat? You can select one or more.

- Data Loss Prevention (DLP).
 - Security Information and Event Management (SIEM).
 - Intrusion Detection Systems (IDS)
 - Access Control System (ACL).
 - Proxy Server.
 - Document Tagging.
 - Honey-tokens
 - Other. Please specify in detail.....
-

Q14 Which of the following statements best describes how security and privacy controls are integrated to detect insider threats?

- A single solution that combines all alerts into a single insider threat report.
 - Multi solutions that generate a multi insider threats report or alert.
 - There is no integration at the moment.
 - Other. Please specify.....
-

Q15 Which of the following statements best describes how the external and insider threat detection systems are integrated?

- Fully technology integrated.
 - Semi technology integrated.
 - Not technology integrated.
 - Other. Please specify.....
-

Q16 Which of the following data are logged on the organisation's system to help detect an insider threat? You can select one or more.

- Network traffic.
 - Online activity.
 - Emails.
 - Removable Storage Devices.
 - User Login and Logout to IT systems.
 - Other. Please specify.....
-

Q17 What proportion of false insider alerts are generated by the security system?

- More than 90% are false alerts.
- Between 40 % and 90 % are false alerts.
- Between 10 % and 40 % are false alerts.
- Less than 10 % are false

Q18 In previous security breaches, how did your organisation detect an insider threat? You can select one or more.

- Accidentally detected by a member of staff.
- Detected by a member of staff who was following clear insider threat guidelines and training.
- Detected by IT security system after the breach had taken place.
- Detected by IT security system before the breach had taken place.
- Other, please specify.....

Q19 In previous security breaches, how many insider attacks has your system failed to detect?

- All or most of them were not detected by our system.
- Our system failed to detect most of them.
- None of them escaped our system.

Q20 Regarding employee termination period, has your organisation applied any extra measurement to monitor user activity in this period of time?

- Yes. Please specify what action was taken.....

- No.

Please enter your name and position if you wish to be knowing to us. You have the right not to answer this.

Name _____

Position _____

Any other information you would like us to know.

End of Block: Block 2

Organisational Impact

Emergency Insider Threat Risk Predictions: PhD Project Survey.

This survey is a part of PhD student research work, which is being carried out at Loughborough University, in the Computer Science Department in collaboration with the School of Business and Economics.

The survey is the key to determining how to deliver a significantly enhanced capability of managing malicious insider cyber-security threats, and also how to educate and to spread materials and strategies for mitigation of malicious insider threats. Your cooperation will help to ensure that my research is relevant for your organisation.

Please complete the survey based on the best of your knowledge. If you complete this survey, you are consenting to have your anonymised responses included as part of data collection for this survey. However, you can enter your name in the last field if you wish to let us know who you are.

Please complete the entire survey. There are 17 questions over 3 pages and we estimate that it should take at most 8 minutes of your time, To start please press Start button at the bottom of this page, and to submit the survey, please click Submit at the bottom of the last page.

If you have any further questions, please feel free to contact us at: n.elmrabit@lboro.ac.uk

Thank you very much for your response.

Nebrase Elmrabit
PhD Research Student.

Page Break

Start of Block: Block 1

Q1

What sector does your organisation belong to?

- Public.
 - Private.
 - Banking and financial.
 - Education.
 - Other. Please specify.....
-

Q2 What is your organisation size in terms of employee numbers?

- Fewer than 50 employees.
 - Between 50 and 250 employees.
 - More than 250 employees.
-

Q3 Does your organisation have its own IT security department?

- Yes.
 - No.
-

Q4 Does your organisation outsource IT services?

Yes.

No.

Q5 Does your organisation outsource IT security services?

Yes.

No.

Q6 Does your organisation have a written security policy?

Yes.

No.

Q7 How often does your organisation update or review its security policy?

Annually.

Every 5 years.

No reviews or updates.

Other, please describe.....

Q8 Do all authorised users follow your organisation's security policy?

- Yes.
 - No, because currently we do not have a system that controls and enforces this policy.
 - No, please specify why... _____
-

Q9 Does your organisation apply criminal records checks for people it employs before giving them access to IT systems?

- Yes.
 - No.
 - Other. Please specify.....

-

Q10 Does your organisation recruit people from overseas?

- Yes.
 - No.
-

Page Break _____

Q11 Has your organisation suffered any information security breach in the last 5 years?

Yes.

No.

Q12 Has your organisation suffered any security breach that was accidentally caused by an authorized user in the last 5 years?

Yes.

No.

Q13 Has your organisation been under attack from external threats?

Yes.

No.

Q14 Has your organisation suffered any security breach caused by an authorised user in the last 5 years?

Yes

No.

Display This Question:

If Has your organisation suffered any security breach caused by an authorised user in the last 5 years? = Yes

Q15-1

If you have answered Yes to the previous question, please let us know which type of authorised user security breach your organisation suffered. You can select more than one.

- Insider IT Fraud.
- Insider Theft of Intellectual Property.
- Insider IT Sabotage.
- Insider Social Engineering.
- Insider In Cloud Computing.
- Insider National Security.

Display This Question:

If Has your organisation suffered any security breach caused by an authorised user in the last 5 years? = Yes

Q15-2

What action was taken against any malicious authorized user?

- Update security policy.
 - Implementing a new security strategy.
 - Training and awareness.
 - Termination of an employee.
 - Other action. Please specify
-

Page Break

End of Block: Block 1

Start of Block: Block 2

Q16

Do you recognise any of the following symptoms at work? You can select one or more statements if applicable.

- Low morale.
- Industrial relation difficulties.
- High absenteeism.
- Increase in long-term illness.
- increased or high turnover of staff.
- Increased litigation.
- Reduced efficiency.
- Poor performance in tasks.
- Poor quality control.
- Deadlines not being reached.
- Increase in accidents.

Please enter your name and position if you wish to be knowing to us. You have the right not to answer this.

- Name _____
- Position _____
- Any other information you would like us to know.

Human Factor

Emergency Insider Threat Risk Predictions: PhD Project Survey.

This survey is a part of PhD student research work, which is being carried out at Loughborough University, in the Computer Science Department in collaboration with the School of Business and Economics.

The survey is the key to determining how to deliver a significantly enhanced capability of managing malicious insider cyber-security threats, and also how to educate and to spread materials and strategies for mitigation of malicious insider threats. Your cooperation will help to ensure that my research is relevant for your organisation.

Please complete the survey based on the best of your knowledge. If you complete this survey, you are consenting to have your anonymised responses included as part of data collection for this survey. However, you can enter your name in the last field if you wish to let us know who you are.

Please complete the entire survey. There are 29 questions over 3 pages and we estimate that it should take at most 4 minutes of your time, To start please press Start button at the bottom of this page, and to submit the survey, please click Submit at the bottom of the last page.

If you have any further questions, please feel free to contact us at: n.elmrabit@lboro.ac.uk

Thank you very much for your response.

Nebrase Elmrabit
PhD Research Student.

End of Block: Block 1

Start of Block: Human Factors

Page Break

Q1 How old are you?

- Less than 25 years old.
 - Between 25 and 45 years old.
 - Over 45 years old.
-

Q2 What is your gender?

- Female.
 - Male.
-

Q3 How would you best describe your relationship with the organisation?

- Current employee.
 - Contractor, Freelancer, Consultant.
 - Other, please specify..... _____
-

Q4 How long have you been working for this organisation?

- Less than a year.
 - Between one year and 3 years.
 - Over 3 years.
-

Q5 How best do you describe your role within the organisation?

- Scientist.
 - Engineer.
 - IT
 - Administrator.
 - Contractor.
 - Other, please specify..... _____
-

Q6 How long have you been working in this role?

- Less than 1 year.
 - Between one year and 3 years.
 - Over 3 years.
-

Q7 If you are a current employee, when does your contract expire?

- In less than 3 months.
 - Over 3 months and less than 1 year.
 - Over one year contract.
 - Other. Please describe

-

Q8 Do you understand your organisation's information security policy?

- Yes.
 - No.
 - Other, please specify. _____
-

Page Break _____

Q9 If work gets difficult, do your colleagues help you?

- Always.
 - Sometimes.
 - Never.
-

Q10 Do you receive the respect at work you feel you deserve from your colleagues?

- Always.
 - Sometimes.
 - Never.
-

Q11 Are your colleagues willing to listen to your work-related problems?

- Always.
 - Sometimes.
 - Never.
-

Q12 Is there friction or anger between colleagues?

- Never.
 - Sometimes.
 - Always.
-

Q13 Are relationships at work strained?

- Always. (15)
 - Sometimes. (16)
 - Never. (17)
-

Q14

Do you have sufficient opportunities to question managers about changes at work?

- Always.
 - Sometimes. (10)
 - Never.
-

Q15

When changes are made at work, are you clear how they will work out in practice?

- Always.
 - Sometimes. (10)
 - Never.
-

Q16 Can you decide when to take a break?

- Always.
 - Sometimes.
 - Never. (13)
-

Q17 Do you have a choice in deciding how to do your work?

- Always.
 - Sometime. (10)
 - Never.
-

Q18 Do you have some say over the way you work?

- Always.
 - Sometimes. (10)
 - Never.
-

Q19 Are you given supportive feedback with regard to the work you do?

- Always.
 - Sometimes.
 - Never. (10)
-

Q20 Can you rely on your line manager to help you out with a work problem?

- Always.
 - Sometimes.
 - Never.
-

Q21 Can you talk to your line manager about something that has upset or annoyed you about work?

- Always.
 - Sometimes.
 - Never.
-

Q22 Are you supported through emotionally demanding work?

- Always.
 - Sometimes.
 - Never.
-

Q23 Is it clear what is expected of you at work?

- Always.
 - Sometimes.
 - Never.
-

Q24 Do you know how to go about getting your job done?

- Always.
 - Sometimes.
 - Never.
-

Q25 Do you understand how your work fits into the overall aim of the organisation?

- Always.
 - Sometimes.
 - Never.
-

Q26 Do you have higher work capabilities than your colleagues?

- Always.
- Sometimes.
- Never.

End of Block: Human Factors

Start of Block: Block 2

Q27 Are you a part of the design or implementation process team?

- Always.
 - Sometimes.
 - Never.
-

Q28 Do you have access to the organisation's intellectual property?

- Always.
 - Sometime.
 - Never.
-

Q29 Do you feel that the copyright for you own created work is your own intellectual property and does not belong to your organisation?

- Always.
 - Sometimes.
 - Never.
-

Q37 Please enter your name and position if you wish to be knowing to us. You have the right not to answer this.

- Name _____
- Position _____
- Any other information you would like us to know.

End of Block: Block 2

Appendix B

A list of all variables with
changing of the probability for a
selected Cases 4,20.22.69

All Variables (end nodes and internal nodes)	Case number with changing of probabilities			
	4	20	22	69
Predict	Possible insider threat	Unlikely to be insider threat	Unlikely to be insider threat	Unlikely to be insider threat
Predict %	50.99%	45.11%	57.31%	52.38%
Predict Probability for Rare to be insider threat	0.06%	0.03%	0.29%	0.27%
Predict Probability for Unlikely to be insider threat	30.85%	45.11%	57.31%	52.38%
Predict Probability for Possible insider threat	50.99%	44.00%	36.23%	38.87%
Predict Probability for Likely to be insider threat	12.76%	9.08%	5.66%	7.04%
Predict Probability for Certain is insider threat	5.35%	1.78%	0.52%	1.44%
Predict(Technology Factors (T))	Moderate performance and low focus on Insider threat			
Predict Probability for Technology Factors	96.83%	96.17%	95.37%	95.61%
Predict Probability(Technology Factors (T)=Extreme performance and focus on Insider threat)	0.00%	0.00%	0.00%	0.00%
Predict Probability(Technology Factors (T)=High performance and focus on Insider threat)	3.17%	3.83%	4.64%	4.39%
Predict Probability(Technology Factors (T)=Moderate performance and low focus on Insider threat)	96.83%	96.17%	95.37%	95.61%
Predict Probability(Technology Factors (T)=Low performance and no focus on Insider threat)	0.00%	0.00%	0.00%	0.00%
Predict(Budget)	Low	Low	Low	Low
Predict Probability(Budget=High)	0.00%	0.00%	0.00%	0.00%
Predict Probability(Budget=Medium)	4.93%	5.13%	5.37%	5.30%
Predict Probability(Budget=Low)	95.07%	94.87%	94.63%	94.70%
Retracted Log Likelihood(Budget)	-75.6	-75.5	-80.8	-76.2
Predict(Security Awareness and Training)	Low	Low	Low	Low
Predict Probability(Security Awareness and Training=High)	0.00%	0.00%	0.00%	0.00%
Predict Probability(Security Awareness and Training=Medium)	2.33%	2.44%	2.56%	2.52%
Predict Probability(Security Awareness and Training=Low)	97.67%	97.56%	97.44%	97.48%
Predict(Security & Privacy Controls)	Medium	Medium	Medium	Medium

PredictProbability(Security & Privacy Controls=High)	0.00%	0.00%	0.00%	0.00%
PredictProbability(Security & Privacy Controls=Medium)	95.39%	95.43%	95.46%	95.45%
PredictProbability(Security & Privacy Controls=Low)	4.61%	4.58%	4.54%	4.55%
Predict(Integration)	No	No	No	No
PredictProbability(Integration=Yes)	0.00%	0.00%	0.00%	0.00%
PredictProbability(Integration=Part Yes)	0.00%	0.00%	0.00%	0.00%
PredictProbability(Integration=No)	100.00%	100.00%	100.00%	100.00%
Predict(Tools & Controls)	Medium	Medium	Medium	Medium
PredictProbability(Tools & Controls=High)	7.79%	7.79%	7.79%	7.79%
PredictProbability(Tools & Controls=Medium)	92.09%	92.09%	92.09%	92.09%
PredictProbability(Tools & Controls=Low)	0.12%	0.12%	0.12%	0.12%
Predict(Digital Evidence)	High	High	High	High
PredictProbability(Digital Evidence =High)	83.77%	83.80%	83.83%	83.82%
PredictProbability(Digital Evidence =Medium)	16.23%	16.20%	16.16%	16.17%
PredictProbability(Digital Evidence =Low)	0.00%	0.00%	0.00%	0.00%
Predict(Detection Level)	High	High	High	High
PredictProbability(Detection Level=High)	100.00%	100.00%	100.00%	100.00%
PredictProbability(Detection Level=Medium)	0.00%	0.00%	0.00%	0.00%
PredictProbability(Detection Level=Low)	0.00%	0.00%	0.00%	0.00%
Predict(Detection)	Medium	Medium	Medium	Medium
PredictProbability(Detection=High)	1.82%	1.82%	1.82%	1.82%
PredictProbability(Detection=Medium)	98.18%	98.18%	98.18%	98.18%
PredictProbability(Detection=Low)	0.00%	0.00%	0.00%	0.00%
PredictProbability(Undetected)	100.00%	100.00%	100.00%	100.00%
PredictProbability(Undetected=must of them)	0.00%	0.00%	0.00%	0.00%
PredictProbability(Undetected=None of them)	100.00%	100.00%	100.00%	100.00%
Predict(Investment)	Low	Low	Low	Low
PredictProbability(Investment=High)	0.05%	0.06%	0.07%	0.07%
PredictProbability(Investment=Medium)	10.50%	11.10%	11.83%	11.61%
PredictProbability(Investment=Low)	89.45%	88.84%	88.10%	88.33%
Predict(Organisational Aspects (O))	Natural culture			
PredictProbability(Organisational Aspects (O)=Non fertile environmental culture for Insider threat)	1.29%	1.48%	1.68%	1.61%

PredictProbability(Organisational Aspects (O)=Natural culture)	98.64%	98.47%	98.29%	98.35%
PredictProbability(Organisational Aspects (O)=Fertile environmental culture for Insider threat)	0.07%	0.05%	0.03%	0.04%
Predict(Security Policy)	Medium	Medium	Medium	Medium
PredictProbability(Security Policy=High)	1.48%	1.53%	1.57%	1.56%
PredictProbability(Security Policy=Medium)	98.39%	98.34%	98.30%	98.31%
PredictProbability(Security Policy=Low)	0.13%	0.13%	0.13%	0.13%
Following	No enforcement system	No enforcement system	No enforcement system	No enforcement system
Predict(Structure)	Medium	Medium	Medium	Medium
PredictProbability(Structure=High)	5.13%	5.12%	5.11%	5.12%
PredictProbability(Structure=Medium)	92.13%	92.07%	92.01%	92.03%
PredictProbability(Structure=Low)	2.74%	2.81%	2.88%	2.86%
Predict(Recruiting)	Medium	Medium	Medium	Medium
PredictProbability(Recruiting=High)	7.60%	7.60%	7.59%	7.60%
PredictProbability(Recruiting=Medium)	86.12%	86.08%	86.05%	86.06%
PredictProbability(Recruiting=Low)	6.28%	6.32%	6.36%	6.35%
Predict(Security Breach)	Medium	Medium	Medium	Medium
PredictProbability(Security Breach=Very High)	0.01%	0.01%	0.01%	0.01%
PredictProbability(Security Breach=High)	4.41%	4.38%	4.36%	4.37%
PredictProbability(Security Breach=Medium)	84.60%	84.53%	84.44%	84.47%
PredictProbability(Security Breach=Low)	10.98%	11.09%	11.20%	11.16%
Predict(History)	Low	Low	Low	Low
PredictProbability(History=Very High)	0.03%	0.02%	0.02%	0.02%
PredictProbability(History=High)	6.42%	6.39%	6.37%	6.38%
PredictProbability(History=Medium)	18.69%	18.68%	18.66%	18.67%
PredictProbability(History=Low)	74.86%	74.91%	74.95%	74.93%
Predict(Action)	Low	Low	Low	Low
PredictProbability(Action=High)	3.38%	3.41%	3.43%	3.42%
PredictProbability(Action=Medium)	38.88%	38.93%	38.98%	38.96%
PredictProbability(Action=Low)	57.74%	57.67%	57.59%	57.62%
Predict(Human Factors (H))	High	Medium	Medium	Medium
PredictProbability(Human Factors (H)=Very High)	10.14%	2.39%	0.66%	2.43%
PredictProbability(Human Factors (H)=High)	47.18%	26.26%	8.10%	15.92%
PredictProbability(Human Factors (H)=Medium)	41.25%	70.40%	83.39%	74.32%

PredictProbability(Human Factors (H)=Low)	1.39%	0.94%	7.66%	7.15%
PredictProbability(Human Factors (H)=Very Low)	0.04%	0.02%	0.20%	0.19%
Predict(Motive)	High	Medium	Medium	Medium
PredictProbability(Motive=Very High)	18.88%	0.63%	0.33%	0.22%
PredictProbability(Motive=High)	48.94%	16.56%	8.38%	3.40%
PredictProbability(Motive=Medium)	31.46%	74.34%	79.77%	65.12%
PredictProbability(Motive=Low)	0.69%	6.27%	9.53%	21.44%
PredictProbability(Motive=Very Low)	0.04%	2.21%	1.99%	9.83%
Predict(Opportunity)	Medium	Medium	Low	Medium
PredictProbability(Opportunity=High)	0.00%	0.00%	0.00%	1.55%
PredictProbability(Opportunity=Medium)	83.22%	96.98%	34.28%	64.47%
PredictProbability(Opportunity=Low)	16.78%	3.02%	65.72%	33.97%
Predict(Capability)	High	High	Medium	Medium
PredictProbability(Capability=High)	68.99%	54.86%	29.55%	47.10%
PredictProbability(Capability=Medium)	29.68%	43.35%	66.83%	51.22%
PredictProbability(Capability=Low)	1.33%	1.80%	3.62%	1.68%
Predict(Work-related Stress Level)	High	Medium	Medium	Low
PredictProbability(Work-related Stress Level=High)	76.22%	3.07%	1.58%	0.87%
PredictProbability(Work-related Stress Level=Medium)	23.42%	81.09%	80.98%	13.22%
PredictProbability(Work-related Stress Level=Low)	0.36%	15.85%	17.44%	85.91%
Predict(Age, Gender and policy)	High	Medium	Medium	Medium
PredictProbability(Age, Gender and policy=High)	70.34%	20.85%	34.87%	46.82%
PredictProbability(Age, Gender and policy=Medium)	29.37%	74.64%	57.47%	51.93%
PredictProbability(Age, Gender and policy=Low)	0.29%	4.51%	7.67%	1.26%
Predict(Relation to Organisation)	Medium	High	Medium	Medium
PredictProbability(Relation to Organisation=High)	10.40%	62.07%	4.29%	0.00%
PredictProbability(Relation to Organisation=Medium)	81.83%	37.93%	74.42%	51.55%
PredictProbability(Relation to Organisation=Low)	7.76%	0.00%	21.29%	48.45%
Predict(System Role)	Medium	High	Low	Low
PredictProbability(System Role=High)	7.57%	55.42%	0.00%	0.00%
PredictProbability(System Role=Medium)	75.28%	44.58%	18.56%	31.18%
PredictProbability(System Role=Low)	17.15%	0.00%	81.44%	68.82%

Predict(Role)	High	High	High	High
PredictProbability(Role=High)	66.63%	60.33%	87.56%	91.08%
PredictProbability(Role=Medium)	33.37%	39.67%	12.44%	8.92%
PredictProbability(Role=Low)	0.00%	0.00%	0.00%	0.00%
Predict(Access)	High	High	Medium	Medium
PredictProbability(Access=High)	59.11%	52.60%	0.00%	21.01%
PredictProbability(Access=Medium)	40.89%	47.40%	78.64%	74.71%
PredictProbability(Access=Low)	0.00%	0.00%	21.36%	4.28%
Age	Between 25 and 45	Between 25 and 45	Between 25 and 45	Between 25 and 45
Gender	Male	Female	Male	Male
Type of Employment	Current employee	Current employee	Current employee	Current employee
Employment period	Between one year and Three years	Over Three years	Between one year and Three years	Less than a year
Position	Other	Academic	Administrator	Scientist
Position Period	Between one year and Three Years	Over Three years	Less than a year	Less than a year
Contract Expiration	Over One year	Over One year	Over One year	Less than One year
Understanding Security Policy	No	No	Yes	No
Peer support	Negative	Nature	Nature	Positive
Colleagues help	Never	Sometime	Sometime	Sometime
Colleagues Respect	Never	Sometime	Always	Always
Colleagues listen to work-related problems	Sometime	Sometime	Always	Always
Own decision of how to do the task	Sometime	Always	Sometime	Always
Change practice	Sometime	Sometime	Sometime	Sometime
Change opinion	Never	Sometime	Sometime	Always
Anger between colleagues	Sometime	Sometime	Sometime	Sometime
Work strained relationships	Sometime	Sometime	Sometime	Sometime
Relationships	Nature	Nature	Nature	Nature
Change	Negative	Nature	Nature	Positive
Control	Nature	Positive	Nature	Positive
Way of work opinion	Sometime	Always	Sometime	Always
Own break decision	Sometime	Always	Always	Sometime
Managers' support	Low	Medium	Medium	Medium
Talking to line manager regarding upsetting from work	Never	Sometime	Sometime	Sometime
Rely on line manager to help with a work problem	Never	Sometime	Sometime	Sometime
Supportive feedback	Never	Sometime	Sometime	Sometime

Emotionally support	Never	Sometime	Never	Sometime
Work knowledge	Sometime	Always	Sometime	Always
Work experience	Always	Always	Always	Always
Work aims	Always	Sometime	Always	Always
Higher work capabilities	Sometime	Sometime	Always	Sometime
Intellectual property	Sometime	Sometime	Never	Sometime
Design or implementation team	Sometime	Sometime	Sometime	Sometime
Copyright ownership	Always	Always	Sometime	Sometime
Pre-employment checks	No	No	No	No
Foreign employee	Yes	Yes	Yes	Yes
Implemented	Yes	Yes	Yes	Yes
Update or review	Every Five years	Every Five years	Every Five years	Every Five years
Outsource	Medium	Medium	Medium	Medium
PredictProbability(Outsource=High)	9.61%	9.61%	9.61%	9.61%
PredictProbability(Outsource=Medium)	89.25%	89.24%	89.23%	89.23%
PredictProbability(Outsource=Low)	1.14%	1.15%	1.16%	1.16%
Predict(IT security department)	Yes	Yes	Yes	Yes
Predict(IT services)	Yes	Yes	Yes	Yes
Predict(IT security services)	No	No	No	No
Predict(Information security breach last Five years)	Yes	Yes	Yes	Yes
Predict(Authorised user breach in last Five years)	No	No	No	No
Predict(Type of authorised user security breach last Five years)	Low	Low	Low	Low
PredictProbability(Type of authorised user security breach last Five years=Very High)	0.03%	0.03%	0.03%	0.03%
PredictProbability(Type of authorised user security breach last Five years=High)	7.79%	7.76%	7.73%	7.74%
PredictProbability(Type of authorised user security breach last Five years=Medium)	17.32%	17.31%	17.29%	17.30%
PredictProbability(Type of authorised user security breach last Five years=Low)	74.86%	74.91%	74.95%	74.93%
IT Fraud	No	No	No	No
Theft of intellectual property	No	No	No	No
National security	No	No	No	No
In cloud computing	No	No	No	No
Social engineering	No	No	No	No
IT sabotage	No	No	No	No
Accidently Authorised user breach in last Five years	Yes	Yes	Yes	Yes
External threat	Yes	Yes	Yes	Yes

Predict(Insider threat)	Low	Low	Low	Low
PredictProbability(Insider threat=Very High)	0.03%	0.03%	0.02%	0.03%
PredictProbability(Insider threat=High)	7.11%	7.07%	7.05%	7.06%
PredictProbability(Insider threat=Medium)	18.01%	17.99%	17.98%	17.98%
PredictProbability(Insider threat=Low)	74.86%	74.91%	74.95%	74.93%
Update security policy	No	No	No	No
implement new security strategy	No	No	No	No
Training and awareness	No	No	No	No
Employee termination	No	No	No	No
IT Budget	Between 3% and 9%	Between 3% and 9%	Between 3% and 9%	Between 3% and 9%
IT security budget of IT budget	Less than 10%	Less than 10%	Less than 10%	Less than 10%
IT security budget for Insider Threat	Less than 5%	Less than 5%	Less than 5%	Less than 5%
Concerns of Insider Threat	Not at all	Not at all	Not at all	Not at all
Provide security awareness and training	No	No	No	No
User groups	No	No	No	No
How often attending SAaT	Never	Never	Never	Never
DLP	No	No	No	No
SIEM	Yes	Yes	Yes	Yes
Proxy server	Yes	Yes	Yes	Yes
ACL	Yes	Yes	Yes	Yes
IDS	Yes	Yes	Yes	Yes
Honey-tokens	No	No	No	No
Document Tagging	No	No	No	No
Other	Yes	Yes	Yes	Yes
Security & Privacy controls integration to detect Insider	No integration	No integration	No integration	No integration
External & Insider threats integration	Not technology integration	Not technology integration	Not technology integration	Not technology integration
Network traffic	Yes	Yes	Yes	Yes
other	Yes	Yes	Yes	Yes
Employee termination period extra measures	Yes	Yes	Yes	Yes
Login & logout	Yes	Yes	Yes	Yes
Removable storage devices	No	No	No	No
Emails	Yes	Yes	Yes	Yes
Online activity	Yes	Yes	Yes	Yes
False insider alerts	Less than 10% false	Less than 10% false	Less than 10% false	Less than 10% false
Accidently by a staff	Yes	Yes	Yes	Yes

by a staff how following guidelines aand training	No	No	No	No
IT security system before or after the breach	No	No	No	No
Other ways	No	No	No	No
Employees Work-related Stress Symptoms	Medium	Medium	Medium	Medium
Low morale	Yes	Yes	Yes	Yes
Poor performance in tasks	Yes	Yes	Yes	Yes
Reduced efficiency	No	No	No	No
Increased litigation	No	No	No	No
increased or high turnover of staff	Yes	Yes	Yes	Yes
Increase in long-term illness	Yes	Yes	Yes	Yes
High absenteeism	No	No	No	No
Industrial relation difficulties	No	No	No	No
increase in accidents	No	No	No	No
Deadlines not being reached	Yes	Yes	Yes	Yes
Poor quality control	No	No	No	No
Undetected	None of them	None of them	None of them	None of them
Following	No enforcement system	No enforcement system	No enforcement system	No enforcement system
Age	Between 25 and 45	Between 25 and 45	Between 25 and 45	Between 25 and 45
Gender	Male	Female	Male	Male
Type of Employment	Current employee	Current employee	Current employee	Current employee
Employment period	Between 1 year and 3 years	Over 3 years	Between 1 year and 3 years	Less than a year
Position	Other	Academic	Administrator	Scientist
Position Period	Between 1 year and 3 Years	Over 3 years	Less than a year	Less than a year
Contract Expiration	Over 1 year	Over 1 year	Over 1 year	Less than 1 year
Understanding Security Policy	No	No	Yes	No
Colleagues help	Never	Sometime	Sometime	Sometime
Colleagues Respect	Never	Sometime	Always	Always
Colleagues listen to work-related problems	Sometime	Sometime	Always	Always
Own decision of how to do the task	Sometime	Always	Sometime	Always
Change practice	Sometime	Sometime	Sometime	Sometime
Change opinion	Never	Sometime	Sometime	Always
Anger between colleagues	Sometime	Sometime	Sometime	Sometime

Work strained relationships	Sometime	Sometime	Sometime	Sometime
Way of work opinion	Sometime	Always	Sometime	Always
Own break decision	Sometime	Always	Always	Sometime
Talking to line manager regarding upsetting from work	Never	Sometime	Sometime	Sometime
Rely on line manager to help with a work problem	Never	Sometime	Sometime	Sometime
Supportive feedback	Never	Sometime	Sometime	Sometime
Emotionally support	Never	Sometime	Never	Sometime
Work knowledge	Sometime	Always	Sometime	Always
Work experience	Always	Always	Always	Always
Work aims	Always	Sometime	Always	Always
Higher work capabilities	Sometime	Sometime	Always	Sometime
Intellectual property	Sometime	Sometime	Never	Sometime
Design or implementation team	Sometime	Sometime	Sometime	Sometime
Copyright ownership	Always	Always	Sometime	
Pre-employment checks	No	No	No	No
Foreign employee	Yes	Yes	Yes	Yes
Implemented	Yes	Yes	Yes	Yes
Update or review	Every Five years	Every Five years	Every Five years	Every Five years
IT security department	Yes	Yes	Yes	Yes
IT services	Yes	Yes	Yes	Yes
IT security services	No	No	No	No
Information security breach last Five years	Yes	Yes	Yes	Yes
Authorised user breach in last Five years	No	No	No	No
IT Fraud	No	No	No	No
Theft of intellectual property	No	No	No	No
National security	No	No	No	No
In cloud computing	No	No	No	No
Social engineering	No	No	No	No
IT sabotage	No	No	No	No
Accidently Authorised user breach in last Five years	Yes	Yes	Yes	Yes
External threat	Yes	Yes	Yes	Yes
Update security policy	No	No	No	No
implement new security strategy	No	No	No	No
Training and awareness	No	No	No	No
Employee termination	No	No	No	No
Other action	No	No	No	No
IT Budget	Between 3% and 9%	Between 3% and 9%	Between 3% and 9%	Between 3% and 9%
IT security budget of IT budget	Less than 10%	Less than 10%	Less than 10%	Less than 10%

IT security budget for Insider Threat	Less than 5%	Less than 5%	Less than 5%	Less than 5%
Concerns of Insider Threat	Not at all	Not at all	Not at all	Not at all
Provide security awareness and training	No	No	No	No
User groups	No	No	No	No
How often attending SAaT	Never	Never	Never	Never
DLP	No	No	No	No
SIEM	Yes	Yes	Yes	Yes
Proxy server	Yes	Yes	Yes	Yes
ACL	Yes	Yes	Yes	Yes
IDS	Yes	Yes	Yes	Yes
Honey-tokens	No	No	No	No
Document Tagging	No	No	No	No
Other	Yes	Yes	Yes	Yes
Security & Privacy controls integration to detect Insider	No integration	No integration	No integration	No integration
External & Insider threats integration	Not technology integration	Not technology integration	Not technology integration	Not technology integration
Network traffic	Yes	Yes	Yes	Yes
other	Yes	Yes	Yes	Yes
Employee termination period extra measures	Yes	Yes	Yes	Yes
Login & logout	Yes	Yes	Yes	Yes
Removable storage devices	No	No	No	No
Emails	Yes	Yes	Yes	Yes
Online activity	Yes	Yes	Yes	Yes
False insider alerts	Less than 10% false	Less than 10% false	Less than 10% false	Less than 10% false
Accidentally by a staff	Yes	Yes	Yes	Yes
by a staff who following guidelines	No	No	No	No
IT security system before or after the breach	No	No	No	No
Other ways	No	No	No	No
Low morale	Yes	Yes	Yes	Yes
Poor performance in tasks	Yes	Yes	Yes	Yes
Reduced efficiency	No	No	No	No
Increased litigation	No	No	No	No
increased or high turnover of staff	Yes	Yes	Yes	Yes
Increase in long-term illness	Yes	Yes	Yes	Yes
High absenteeism	No	No	No	No
Industrial relation difficulties	No	No	No	No
increase in accidents	No	No	No	No
Deadlines not being reached	Yes	Yes	Yes	Yes
Poor quality control	No	No	No	No

Appendix C

Prediction Results with Different Time Period Table

Table C.1: Prediction Result with Different Time Period

Case	Time	Rare	Unlikely	Possible	Likely	Certain
0	0	0.045	46.735	43.063	8.658	1.5
0	1	0.04	46.38	43.211	8.813	1.556
0	2	0.04	46.237	43.127	8.999	1.598
0	3	0.04	46.237	43.127	8.999	1.598
0	4	0.067	47.033	42.611	8.752	1.537
0	5	0.067	47.033	42.611	8.752	1.537
1	0	0.002	22.413	55.65	15.185	6.749
1	1	0.002	22.122	55.537	15.374	6.965
1	2	0.002	21.98	55.246	15.645	7.127
1	3	0.001	20.28	56.097	16.124	7.499
1	4	0.002	20.847	56.012	15.847	7.292
1	5	0.002	20.847	56.012	15.847	7.292
2	0	0.006	22.827	55.391	15.035	6.741
2	1	0.005	22.532	55.283	15.223	6.957
2	2	0.005	22.389	54.995	15.493	7.119
2	3	0.002	20.494	55.95	16.021	7.533
2	4	0.003	21.066	55.861	15.745	7.325
2	5	0.003	21.066	55.861	15.745	7.325
3	0	1.073	64.519	29.71	4.337	0.362
3	1	0.971	64.288	29.932	4.433	0.377
3	2	0.956	64.198	29.925	4.534	0.388
3	3	0.956	64.198	29.925	4.534	0.388

Table C.1 continued from previous page

3	4	0.934	58.935	33.791	5.528	0.812
3	5	0.934	58.935	33.791	5.528	0.812
4	0	0.058	30.845	50.985	12.763	5.349
4	1	0.052	30.499	50.974	12.945	5.53
4	2	0.051	30.336	50.76	13.188	5.664
4	3	0.051	30.336	50.76	13.188	5.664
4	4	0.089	32.909	49.542	12.427	5.032
4	5	0.089	32.909	49.542	12.427	5.032
5	0	0.002	22.002	56.129	15.642	6.226
5	1	0.001	21.717	56.018	15.837	6.426
5	2	0.001	21.579	55.726	16.118	6.576
5	3	0.001	19.959	56.547	16.592	6.901
5	4	0.001	20.518	56.462	16.307	6.711
5	5	0.001	20.518	56.462	16.307	6.711
6	0	0.065	56.489	37.591	5.548	0.307
6	1	0.058	56.17	37.794	5.659	0.319
6	2	0.058	56.064	37.766	5.785	0.328
6	3	0.058	56.064	37.766	5.785	0.328
6	4	0.148	57.763	36.423	5.383	0.283
6	5	0.148	57.763	36.423	5.383	0.283
7	0	0.224	50.234	40.112	7.551	1.879
7	1	0.202	49.882	40.274	7.691	1.951
7	2	0.199	49.739	40.205	7.855	2.003
7	3	0.199	49.739	40.205	7.855	2.003
7	4	0.131	43.506	43.83	9.347	3.187
7	5	0.026	33.566	48.973	11.693	5.742
9	0	0.063	47.832	42.347	8.271	1.487
9	1	0.057	47.478	42.501	8.421	1.543
9	2	0.056	47.336	42.424	8.599	1.585
9	3	0.056	47.336	42.424	8.599	1.585
9	4	0.157	49.429	40.921	7.949	1.545
9	5	0.157	49.429	40.921	7.949	1.545
11	0	0.689	62.232	32.243	4.601	0.234
11	1	0.623	61.969	32.464	4.7	0.244
11	2	0.614	61.876	32.453	4.807	0.251
11	3	0.614	61.876	32.453	4.807	0.251
11	4	1.209	63.249	30.838	4.474	0.229
11	5	1.209	63.249	30.838	4.474	0.229

Table C.1 continued from previous page

12	0	0.073	53.591	39.193	6.506	0.637
12	1	0.066	53.258	39.382	6.632	0.662
12	2	0.065	53.139	39.339	6.777	0.68
12	3	0.065	53.139	39.339	6.777	0.68
12	4	0.147	55.551	37.661	6.103	0.539
12	5	0.147	55.551	37.661	6.103	0.539
13	0	0.753	64.699	30.251	4.104	0.193
13	1	0.682	64.453	30.47	4.194	0.201
13	2	0.671	64.368	30.465	4.289	0.207
13	3	0.671	64.368	30.465	4.289	0.207
13	4	1.297	65.571	28.897	4.025	0.21
13	5	1.297	65.571	28.897	4.025	0.21
14	0	0.029	47.712	42.627	8.318	1.314
14	1	0.026	47.359	42.782	8.469	1.364
14	2	0.026	47.22	42.706	8.649	1.4
14	3	0.026	47.22	42.706	8.649	1.4
14	4	0.066	50.139	40.898	7.72	1.176
14	5	0.066	50.139	40.898	7.72	1.176
15	0	0.268	58.061	35.924	5.374	0.373
15	1	0.242	57.754	36.132	5.483	0.388
15	2	0.239	57.649	36.107	5.606	0.399
15	3	0.049	41.096	45.535	10.351	2.968
15	4	0.039	36.688	47.797	11.373	4.102
15	5	0.039	36.688	47.797	11.373	4.102
16	0	3.232	77.647	16.824	2.228	0.07
16	1	2.936	77.685	17.019	2.287	0.073
16	2	2.894	77.657	17.033	2.341	0.075
16	3	2.894	77.657	17.033	2.341	0.075
16	4	4.763	76.633	16.325	2.209	0.07
16	5	4.763	76.633	16.325	2.209	0.07
17	0	0.042	43.694	44.454	9.25	2.56
17	1	0.038	43.328	44.571	9.409	2.654
17	2	0.037	43.174	44.464	9.602	2.724
17	3	0.037	43.174	44.464	9.602	2.724
17	4	0.095	41.07	45.338	10.178	3.319
17	5	0.095	41.07	45.338	10.178	3.319
18	0	0.641	59.312	33.964	5.415	0.668
18	1	0.579	59.023	34.175	5.528	0.695

Table C.1 continued from previous page

18	2	0.57	58.914	34.151	5.651	0.714
18	3	0.57	58.914	34.151	5.651	0.714
18	4	1.119	60.132	32.706	5.342	0.701
18	5	1.119	60.132	32.706	5.342	0.701
19	0	0.971	59.599	32.734	5.6	1.096
19	1	0.878	59.321	32.943	5.717	1.141
19	2	0.864	59.204	32.916	5.844	1.173
19	3	0.864	59.204	32.916	5.844	1.173
19	4	1.923	60.002	31.031	5.704	1.34
19	5	1.923	60.002	31.031	5.704	1.34
20	0	0.027	45.11	44.004	9.075	1.784
20	1	0.024	44.751	44.139	9.235	1.85
20	2	0.024	44.604	44.045	9.428	1.899
20	3	0.024	44.604	44.045	9.428	1.899
20	4	0.064	46.234	42.976	8.882	1.845
20	5	0.064	46.234	42.976	8.882	1.845
21	0	0.17	53.56	38.746	6.606	0.918
21	1	0.154	53.226	38.933	6.734	0.954
21	2	0.151	53.102	38.886	6.881	0.98
21	3	0.151	53.102	38.886	6.881	0.98
21	4	0.06	30.364	50.634	12.795	6.147
21	5	0.06	30.364	50.634	12.795	6.147
22	0	0.288	57.307	36.226	5.657	0.522
22	1	0.26	56.996	36.43	5.772	0.543
22	2	0.256	56.885	36.401	5.9	0.558
22	3	0.256	56.885	36.401	5.9	0.558
22	4	0.234	52.315	39.228	7.187	1.037
22	5	0.234	52.315	39.228	7.187	1.037
23	0	0.194	55.261	37.747	6.131	0.667
23	1	0.175	54.937	37.942	6.252	0.693
23	2	0.173	54.82	37.905	6.39	0.712
23	3	0.173	54.82	37.905	6.39	0.712
23	4	0.479	57.019	35.928	5.883	0.691
23	5	0.479	57.019	35.928	5.883	0.691
24	0	1.336	64.888	28.887	4.414	0.475
24	1	1.209	64.672	29.111	4.512	0.495
24	2	1.191	64.581	29.104	4.615	0.509
24	3	0.248	50.402	39.65	7.61	2.09

Table C.1 continued from previous page

24	4	0.42	51.128	39.067	7.38	2.005
24	5	0.42	51.128	39.067	7.38	2.005
25	0	2.081	70.867	23.664	3.262	0.126
25	1	1.887	70.753	23.889	3.34	0.131
25	2	1.858	70.692	23.896	3.418	0.135
25	3	1.858	70.692	23.896	3.418	0.135
25	4	3.087	70.412	23.118	3.255	0.127
25	5	3.087	70.412	23.118	3.255	0.127
26	0	0.489	59.523	34.299	5.226	0.462
26	1	0.442	59.232	34.51	5.335	0.481
26	2	0.435	59.127	34.489	5.454	0.495
26	3	0.435	59.127	34.489	5.454	0.495
26	4	0.733	59.704	33.825	5.265	0.472
26	5	0.733	59.704	33.825	5.265	0.472
27	0	0.361	59.774	34.413	5.07	0.382
27	1	0.326	59.478	34.623	5.175	0.397
27	2	0.321	59.376	34.604	5.291	0.408
27	3	0.321	59.376	34.604	5.291	0.408
27	4	0.541	59.996	33.961	5.112	0.39
27	5	0.541	59.996	33.961	5.112	0.39
28	0	1.799	71.042	23.92	3.159	0.08
28	1	1.63	70.91	24.141	3.235	0.083
28	2	1.606	70.85	24.148	3.31	0.086
28	3	1.606	70.85	24.148	3.31	0.086
28	4	3.784	73.454	19.971	2.707	0.084
28	5	3.784	73.454	19.971	2.707	0.084
29	0	0.034	46.253	43.363	8.749	1.601
29	1	0.031	45.896	43.507	8.905	1.662
29	2	0.03	45.752	43.42	9.092	1.706
29	3	0.03	45.752	43.42	9.092	1.706
29	4	0.007	23.714	54.628	15.17	6.481
29	5	0.007	23.714	54.628	15.17	6.481
30	0	4.34	81.464	12.547	1.625	0.024
30	1	3.951	81.64	12.714	1.67	0.026
30	2	3.895	81.64	12.728	1.711	0.026
30	3	3.895	81.64	12.728	1.711	0.026
30	4	5.73	77.71	14.473	2.005	0.082
30	5	5.73	77.71	14.473	2.005	0.082

Table C.1 continued from previous page

31	0	0.112	50.681	40.39	7.306	1.512
31	1	0.101	50.331	40.556	7.443	1.57
31	2	0.099	50.194	40.493	7.602	1.612
31	3	0.099	50.194	40.493	7.602	1.612
31	4	0.244	49.372	40.533	7.897	1.954
31	5	0.027	22.822	53.96	14.089	9.102
32	0	0.885	62.853	31.357	4.601	0.304
32	1	0.801	62.603	31.579	4.7	0.317
32	2	0.788	62.51	31.569	4.807	0.326
32	3	0.161	52.231	39.265	7.115	1.227
32	4	0.438	53.883	37.722	6.703	1.254
32	5	0.438	53.883	37.722	6.703	1.254
33	0	0.256	54.94	37.6	6.279	0.924
33	1	0.231	54.614	37.792	6.403	0.96
33	2	0.227	54.492	37.751	6.543	0.987
33	3	0.227	54.492	37.751	6.543	0.987
33	4	0.588	55.234	36.602	6.44	1.136
33	5	0.588	55.234	36.602	6.44	1.136
34	0	0.042	47.271	42.668	8.281	1.738
34	1	0.037	46.913	42.815	8.43	1.804
34	2	0.037	46.77	42.734	8.608	1.852
34	3	0.037	46.77	42.734	8.608	1.852
34	4	0.066	49.009	41.44	7.941	1.545
34	5	0.066	49.009	41.44	7.941	1.545
35	0	0.338	55.637	36.9	6.153	0.972
35	1	0.305	55.315	37.094	6.275	1.01
35	2	0.3	55.193	37.055	6.413	1.038
35	3	0.3	55.193	37.055	6.413	1.038
35	4	0.507	55.864	36.429	6.206	0.994
35	5	0.507	55.864	36.429	6.206	0.994
36	0	0.075	52.253	39.918	6.913	0.84
36	1	0.068	51.914	40.1	7.045	0.873
36	2	0.067	51.789	40.049	7.199	0.897
36	3	0.067	51.789	40.049	7.199	0.897
36	4	0.194	54.225	38.289	6.516	0.776
36	5	0.194	54.225	38.289	6.516	0.776
37	0	0.081	45.937	43.182	8.786	2.014
37	1	0.073	45.577	43.319	8.942	2.089

Table C.1 continued from previous page

37	2	0.072	45.428	43.228	9.128	2.144
37	3	0.072	45.428	43.228	9.128	2.144
37	4	0.197	46.913	42.06	8.663	2.167
37	5	0.197	46.913	42.06	8.663	2.167
38	0	1.568	67.691	26.59	3.854	0.296
38	1	1.42	67.512	26.815	3.943	0.309
38	2	1.399	67.434	26.815	4.034	0.318
38	3	1.399	67.434	26.815	4.034	0.318
38	4	1.709	61.983	30.544	5.002	0.762
38	5	1.709	61.983	30.544	5.002	0.762
39	0	0.974	60.046	32.549	5.478	0.953
39	1	0.88	59.773	32.761	5.593	0.992
39	2	0.866	59.66	32.737	5.718	1.019
39	3	0.866	59.66	32.737	5.718	1.019
39	4	1.951	60.663	30.692	5.533	1.161
39	5	1.951	60.663	30.692	5.533	1.161
40	0	0.239	42.184	44.589	9.834	3.154
40	1	0.216	41.819	44.695	10.001	3.269
40	2	0.212	41.658	44.574	10.203	3.354
40	3	0.212	41.658	44.574	10.203	3.354
40	4	0.345	43.537	43.543	9.611	2.964
40	5	0.345	43.537	43.543	9.611	2.964
41	0	0.16	51.284	40.09	7.353	1.113
41	1	0.144	50.942	40.265	7.492	1.156
41	2	0.142	50.81	40.207	7.654	1.188
41	3	0.142	50.81	40.207	7.654	1.188
41	4	0.283	52.664	38.89	7.106	1.057
41	5	0.283	52.664	38.89	7.106	1.057
42	0	0.466	56.271	36.088	6.127	1.047
42	1	0.421	55.956	36.284	6.25	1.089
42	2	0.414	55.833	36.247	6.387	1.119
42	3	0.414	55.833	36.247	6.387	1.119
42	4	0.699	56.457	35.599	6.175	1.07
42	5	0.699	56.457	35.599	6.175	1.07
43	0	0.247	51.341	39.536	7.3	1.577
43	1	0.223	50.996	39.707	7.437	1.638
43	2	0.219	50.858	39.645	7.597	1.682
43	3	0.219	50.858	39.645	7.597	1.682

Table C.1 continued from previous page

43	4	0.37	51.588	39.06	7.367	1.614
43	5	0.37	51.588	39.06	7.367	1.614
44	0	0.015	47.019	43.034	8.484	1.448
44	1	0.014	46.664	43.183	8.637	1.502
44	2	0.013	46.523	43.102	8.819	1.543
44	3	0.013	46.523	43.102	8.819	1.543
44	4	0.033	49.023	41.564	8.005	1.375
44	5	0.004	25.496	53.659	14.574	6.267
45	0	1.6	64.963	27.995	4.641	0.801
45	1	1.449	64.755	28.216	4.745	0.835
45	2	1.426	64.657	28.205	4.853	0.859
45	3	1.426	64.657	28.205	4.853	0.859
45	4	2.381	64.733	27.428	4.645	0.813
45	5	2.381	64.733	27.428	4.645	0.813
46	0	0.209	57.431	36.52	5.478	0.364
46	1	0.188	57.12	36.726	5.588	0.378
46	2	0.185	57.013	36.699	5.713	0.389
46	3	0.185	57.013	36.699	5.713	0.389
46	4	0.467	59.599	34.536	5.115	0.282
46	5	0.467	59.599	34.536	5.115	0.282
47	0	0.352	60.911	33.863	4.712	0.162
47	1	0.318	60.624	34.078	4.811	0.169
47	2	0.313	60.53	34.064	4.92	0.174
47	3	0.313	60.53	34.064	4.92	0.174
47	4	0.67	63.32	31.468	4.405	0.137
47	5	0.67	63.32	31.468	4.405	0.137
48	0	0.289	60.217	34.487	4.79	0.216
48	1	0.261	59.924	34.7	4.89	0.225
48	2	0.257	59.827	34.684	5	0.232
48	3	0.257	59.827	34.684	5	0.232
48	4	0.434	60.466	34.048	4.832	0.221
48	5	0.434	60.466	34.048	4.832	0.221
49	0	0.733	64.984	30.266	3.954	0.063
49	1	0.663	64.742	30.489	4.041	0.065
49	2	0.653	64.661	30.485	4.134	0.067
49	3	0.653	64.661	30.485	4.134	0.067
49	4	1.096	65.067	29.796	3.977	0.064
49	5	1.096	65.067	29.796	3.977	0.064

Table C.1 continued from previous page

50	0	0.078	29.99	50.761	12.362	6.808
50	1	0.07	29.639	50.724	12.532	7.035
50	2	0.069	29.471	50.494	12.763	7.204
50	3	0.069	29.471	50.494	12.763	7.204
50	4	0.117	30.181	50.227	12.496	6.979
50	5	0.117	30.181	50.227	12.496	6.979
51	0	0.155	43.547	43.979	9.334	2.986
51	1	0.139	43.179	44.092	9.494	3.096
51	2	0.137	43.019	43.98	9.688	3.176
51	3	0.061	39.777	45.994	10.511	3.657
51	4	0.135	37.673	46.925	11.062	4.206
51	5	0.135	37.673	46.925	11.062	4.206
52	0	0.389	59.717	34.565	5.042	0.287
52	1	0.352	59.425	34.778	5.147	0.298
52	2	0.346	59.325	34.76	5.263	0.307
52	3	0.346	59.325	34.76	5.263	0.307
52	4	0.583	59.933	34.108	5.083	0.293
52	5	0.583	59.933	34.108	5.083	0.293
53	0	0.71	64.625	30.61	4	0.055
53	1	0.643	64.38	30.832	4.087	0.058
53	2	0.633	64.298	30.829	4.181	0.059
53	3	0.633	64.298	30.829	4.181	0.059
53	4	1.062	64.718	30.139	4.023	0.057
53	5	1.062	64.718	30.139	4.023	0.057
55	0	1.017	64.729	29.873	4.191	0.19
55	1	0.921	64.5	30.098	4.284	0.198
55	2	0.906	64.415	30.093	4.382	0.204
55	3	0.906	64.415	30.093	4.382	0.204
55	4	1.519	64.714	29.365	4.209	0.194
55	5	1.519	64.714	29.365	4.209	0.194
56	0	5.212	84.151	9.411	1.212	0.013
56	1	4.75	84.44	9.548	1.248	0.013
56	2	4.684	84.462	9.562	1.278	0.014
56	3	4.684	84.462	9.562	1.278	0.014
56	4	7.601	82.163	9.035	1.189	0.013
56	5	7.601	82.163	9.035	1.189	0.013
57	0	1.267	65.628	28.583	4.213	0.31
57	1	1.147	65.416	28.807	4.307	0.323

Table C.1 continued from previous page

57	2	1.129	65.331	28.803	4.406	0.332
57	3	0.269	44.863	42.399	9.341	3.128
57	4	0.132	37.776	46.886	11.038	4.168
57	5	0.132	37.776	46.886	11.038	4.168
58	0	1.358	65.805	28.209	4.242	0.387
58	1	1.229	65.598	28.433	4.337	0.403
58	2	1.21	65.511	28.428	4.436	0.415
58	3	1.21	65.511	28.428	4.436	0.415
58	4	2.023	65.659	27.674	4.251	0.393
58	5	2.023	65.659	27.674	4.251	0.393
62	0	1.425	66.886	27.264	3.994	0.431
62	1	1.29	66.69	27.486	4.085	0.449
62	2	1.27	66.606	27.483	4.178	0.462
62	3	1.27	66.606	27.483	4.178	0.462
62	4	2.122	66.705	26.734	4.001	0.438
62	5	2.122	66.705	26.734	4.001	0.438
63	0	0.016	44.612	44.237	9.145	1.99
63	1	0.015	44.25	44.366	9.304	2.064
63	2	0.015	44.101	44.268	9.497	2.119
63	3	0.015	44.101	44.268	9.497	2.119
63	4	0.025	44.907	43.782	9.246	2.041
63	5	0.025	44.907	43.782	9.246	2.041
64	0	3.322	77.805	16.608	2.196	0.068
64	1	3.019	77.852	16.803	2.254	0.071
64	2	2.976	77.826	16.817	2.308	0.073
64	3	2.976	77.826	16.817	2.308	0.073
64	4	4.895	76.752	16.109	2.176	0.068
64	5	4.895	76.752	16.109	2.176	0.068
65	0	0.117	52.655	39.478	6.837	0.913
65	1	0.105	52.317	39.66	6.968	0.949
65	2	0.104	52.191	39.611	7.12	0.975
65	3	0.104	52.191	39.611	7.12	0.975
65	4	0.288	54.339	37.885	6.557	0.931
65	5	0.288	54.339	37.885	6.557	0.931
69	0	0.273	52.375	38.871	7.04	1.44
69	1	0.246	52.035	39.048	7.175	1.496
69	2	0.242	51.9	38.992	7.329	1.537
69	3	0.027	42.724	44.664	9.64	2.946

Table C.1 continued from previous page

69	4	0.039	36.078	47.784	11.184	4.915
69	5	0.039	36.078	47.784	11.184	4.915

Appendix D

Insider Threat Risk Prediction Validation Workshop

Insider Threat Risk Prediction

Validation Workshop

02 Nov 2016

Loughborough University

Thank you for your participant, please go through each response case, and based on your experience rank the risk level to each case 1 is higher to 5 which is the lowest.

Case	Rare to be insider threat	Unlikely to be insider threat	Possible insider threat	Likely to be insider threat	Certain is insider threat
0	4	1	2	3	5
1	5	2	1	3	5
2	5	2	2	3	5
3	4	1	2	3	5
4	5	3	2	3	5
5	5	2	3	4	5
6	5	1	3	4	5
7	4	1	2	3	5
9	4	1	2	3	5
11	4	1	2	3	5
12	4	1	2	3	5
13	4	1	2	3	5
14	4	1	2	3	5
15	4	1	2	3	5
16	4	1	2	3	5
17	4	2	1	3	5
18	5	1	2	3	4
19	5	2	1	3	5
20	4	2	1	3	5
21	4	1	2	3	5
22	4	1	2	3	5
23	4	1	2	3	5
24	4	1	2	3	5
25	4	1	2	3	5
26	4	1	2	3	5
27	4	1	2	3	5
28	4	1	2	3	5
29	4	1	2	3	5
30	4	1	2	3	5
31	4	1	2	3	5
32	4	1	2	3	5

33	4		1		2		3		5						
34	4	4		1		2	2		3		5	5			
35	4	4		1	1		2	2		3	3	5	5		
36		4		1		1		2		3		5	5		
37		4		1	1			2	2		3	3	5	5	
38		4		1	1			2		3		5	5		
39		4		1		1		2		3	3		5	5	
40	5	4		2	2		1	2		3	3		4	4	
41		5		1		1		2		3	3		4	4	
42	5	5		1		1		2		3			4	4	
43		5		1		1		2		3			4	4	
44		5	5		1	1		2	2		3	3		4	4
45		5	5		1	1		2	2		3	3		4	4
46		5	5		1	1		2	2		3	3		4	4
47		5	5		1	1		2	2		3	3		4	4
48		5	5		1	1		2	2		3	3		4	4
49		5	5		1	1		2	2		3	3		4	4
50		5	5		1	1		2	2		3	3		4	4
51		5	5		1	1		2	2		3	3		4	4
52		5	5		1	1		2	2		3	3		4	4
53		5	5		1	1		2	2		3	3		4	4
55		5	5		1	1		2	2		3	3		4	4
56		5	5		1	1		2	2		3	3		4	4
57		5	5		1	1		2	2		3	3		4	4
58		5	5		1	1		2	2		3	3		4	4
62		5	5		1	1		2	2		3	3		4	4
63		5	5		1	1		2	2		3	3		4	4
64		5	5		1	1		2	2		3	3		4	4
65		5	5		1	1		2	2		3	3		4	4
69		5	5		1	1		2	2		3	3		4	4

Name: Shadha

Date: 2/11/16

Cloud Computing Security
by enhancing Access Control

Insider Threat Risk Prediction

Validation Workshop

02 Nov 2016

Loughborough University

Thank you for your participant, please go through each response case, and based on your experience rank the risk level to each case 1 is higher to 5 which is the lowest.

Case	Rare to be insider threat	Unlikely to be insider threat	Possible insider threat	Likely to be insider threat	Certain is insider threat
0	5	2	1	3	4
1	5	3	1	2	4
2	5	2	1	3	4
3	5	2	1	3	4
4	4	3	2	1 3	5
5	5	1	2	3	4
6	4	1	2	3	5
7	5	2	1	3	4
9	4	1	2	3	5
11	4	1	2	3	5
12	4	1	2	3	5
13	4	1	2	3	5
14	4	1	2	3	5
15	4	1	2	3	5
16	4	1	2	3	5
17	5	2	1	3	4
18	4	2	1	3	5
19	4	3	2	1	5
20	4	2	1	3	5
21	4	1	2	3	5
22	4	1	2	3	5
23	4	1	2	3	5
24	4	1	2	3	5
25	4	1	2	3	5
26	4	1	2	3	5
27	4	1	2	3	5
28	4	1	2	3	5
29	4	1	2	3	5
30	4	1	2	3	5
31	4	1	2	3	5
32	4	1	2	3	5

33	4	1	2	3	5
34	4	1	2	3	5
35	5	2	1	3	4
36	4	1	2	3	5
37	4	1	2	3	5
38	4	1	2	3	5
39	4	1	2	3	5
40	5	2	1	3	4
41	4	1	2	3	5
42	4	1	2	3	5
43	4	1	2	3	5
44	4	1	2	3	5
45	4	1	2	3	5
46	4	1	2	3	5
47	4	1	2	3	5
48	4	1	2	3	5
49	4	1	2	3	5
50	4	1	2	3	5
51	4	1	2	3	5
52	4	1	2	3	5
53	4	1	2	3	5
55	4	1	2	3	5
56	4	1	2	3	5
57	4	1	2	3	5
58	4	1	2	3	5
62	4	2	2	3	5
63	4	1	2	3	5
64	4	1	2	3	5
65	4	1	2	3	5
69	4	1	2	3	5

Name: Egab

Date: 2-11-2016

Secure routing protocol using
 Reputation & Trust systems in VANETS

Insider Threat Risk Prediction

Validation Workshop

02 Nov 2016

Loughborough University

Thank you for your participant, please go through each response case, and based on your experience rank the risk level to each case 1 is higher to 5 which is the lowest.

Case	Rare to be insider threat	Unlikely to be insider threat	Possible insider threat	Likely to be insider threat	Certain is insider threat
0	5	1	2	3	4
1	5	2	1	3	4
2	5	2	1	3	4
3	5	2	1	3	4
4	5	2	1	3	4
5	5	1	2	3	4
6	5	1	2	3	4
7	5	2	1	3	4
9	5	2	1	3	4
11	5	1	2	3	4
12	5	1	2	3	4
13	5	1	2	3	4
14	5	2	1	3	4
15	4	1	2	3	5
16	4	1	2	3	5
17	5	2	1	3	4
18	5	2	1	3	4
19	4	1	2	3	5
20	5	2	1	3	4
21	4	1	2	3	5
22	4	1	2	3	5
23	4	1	2	3	5
24	4	1	2	3	5
25	4	1	2	3	5
26	4	1	2	3	5
27	4	1	2	3	5
28	4	1	2	3	5
29	4	1	2	3	5
30	4	1	2	3	5
31	4	1	2	3	5
32	4	1	2	3	5

	rare	unlikely	Possible	unlikely	Certain
33	4	1	2	3	5
34	4	1	2	3	5
35	4	1	2	3	5
36	4	1	2	3	5
37	4	1	2	3	5
38	4	1	2	3	5
39	4	1	2	3	5
40	5	2	1	3	4
41	4	1	2	3	5
42	4	1	2	3	5
43	4	1	2	3	5
44	4	1	2	3	5
45	4	1	2	3	5
46	4	1	2	3	5
47	4	1	2	3	5
48	4	1	2	3	5
49	4	1	2	3	5
50	4	1	2	3	5
51	4	1	2	3	5
52	4	1	2	3	5
53	4	1	2	3	5
55	4	1	2	3	5
56	4	1	2	3	5
57	4	1	2	3	5
58	4	1	2	3	5
62	5	2	1	3	4
63	4	1	2	3	5
64	4	1	2	3	5
65	4	1	2	3	5
69	4	1	2	3	5

Name: Mutlog

Date: 02 / 11 / 2016

Parfa Mining DS for Cyber Physical Systems.

Insider Threat Risk Prediction

Validation Workshop

02 Nov 2016

Loughborough University

Thank you for your participant, please go through each response case, and based on your experience rank the risk level to each case 1 is higher to 5 which is the lowest.

Case	Rare to be insider threat	Unlikely to be insider threat	Possible insider threat	Likely to be insider threat	Certain is insider threat
0	5	2	1	3	4
1	5	3	1	2	4
2	5	3	2	1	4
3	4	1	2	3	5
4	4	3	1	2	5
5	4	1	2	3	5
6	5	1	2	3	4
7	5	2	1	3	4
9	5	1	2	3	4
11	5	1	2	3	4
12	5	1	2	3	4
13	4	1	2	3	5
14	4	1	2	3	5
15	4	1	2	3	5
16	5	1	2	3	4
17	5	2	1	3	4
18	5	1	2	3	4
19	5	3	1	2	4
20	5	2	1	3	4
21	5	1	2	3	4
22	5	1	2	3	4
23	4	1	2	3	5
24	4	1	2	3	5
25	4	1	2	3	5
26	4	1	2	3	5
27	4	1	2	3	5
28	4	1	2	3	5
29	4	1	2	3	5
30	4	1	2	3	5
31	4	1	2	3	5
32	4	1	2	3	5

33	4	1	2	3	5
34	4	1	2	3	5
35	4	2	1	3	5
36	4	1	2	3	5
37	4	1	2	3	5
38	4	1	2	3	5
39	4	1	2	3	5
40	5	3	1	2	5
41	4	1	2	3	5
42	4	1	2	3	5
43	4	1	2	3	5
44	4	1	2	3	5
45	4	1	2	3	5
46	4	1	2	3	5
47	4	1	2	3	5
48	4	1	2	3	5
49	4	1	2	3	5
50	4	1	2	3	5
51	4	1	2	3	5
52	4	1	2	3	5
53	4	1	2	3	5
55	4	1	2	3	5
56	4	1	2	3	5
57	4	1	2	3	5
58	4	1	2	3	5
62	4	1	2	3	5
63	4	1	2	3	5
64	4	1	2	3	5
65	4	1	2	3	5
69	4	1	2	3	5

Name: Istisar Al-mandhari

Date: 2 / 11 / 10

Topic: enhancing cloud security under
IDS implementation.

Insider Threat Risk Prediction

Validation Workshop

02 Nov 2016

Loughborough University

Thank you for your participant, please go through each response case, and based on your experience rank the risk level to each case 1 is higher to 5 which is the lowest.

Case	Rare to be insider threat	Unlikely to be insider threat	Possible insider threat	Likely to be insider threat	Certain is insider threat
0	5	1	2	3	4
1	5	2	1	3	4
2	4	3	1	2	5
3	5	2	3	1	4
4	5	2	1	3	4
5	5	2	1	3	4
6	4	1	2	3	5
7	4	2	1	3	5
9	4	1	2	3	5
11	5	1	2	3	4
12	5	1	2	3	4
13	5	2	1	3	4
14	5	1	2	3	4
15	5	1	2	3	4
16	5	1	2	3	4
17	5	2	1	3	4
18	5	2	1	3	4
19	5	2	1	3	4
20	5	1	2	3	4
21	4	1	2	3	4
22	5	1	2	3	4
23	4	1	2	3	4
24	4	1	2	3	5
25	4	1	2	3	5
26	3	1	2	3	5
27	3	1	2	4	5
28	5	1	2	4	5
29	4	1	2	3	4
30	4	1	2	3	5
31	4	1	2	3	5
32	4	1	2	3	5

33	4	1	2	3	
34	4	1	2	3	
35	5	1	2	3	
36	4	1	2	3	
37	3	1	2	3	
38	4	1	2	3	
39	4	1	2	3	
40	5	2	1	3	
41	4	1	2	3	
42	4	1	2	3	
43	4	1	2	3	
44	4	1	2	3	
45	4	1	2	3	
46	4	1	2	3	
47	4	1	2	3	
48	4	1	2	3	
49	4	1	2	3	
50	4	1	2	3	
51	4	1	2	3	
52	4	2	1	3	
53	4	1	2	3	
55	4	1	2	3	
56	4	1	2	3	
57	4	1	2	3	
58	4	1	2	3	
62	4	1	2	3	
63	4	1	2	3	
64	4	1	2	3	
65	4	1	2	3	
69	4	2	2	3	

Name: _____

Date: _____

Appendix E

Ethics Approvals

Ethical Clearance Checklist

Has the Investigator read the 'Guidance for completion of Ethical Clearance Checklist' before starting this form?	Yes
---	-----

Project Details

1. Project Title: Insider Threat Prediction

Applicant(s) Details

2. Name of Applicant 1: Nebrase Elmrabit	10. Name of Applicant 2:
3. Status: PGR student	11. Status: Choose an item
4. School/Department: Computer Science	12. School/Department: Click here to enter text.
5. Programme (if applicable):	13. Programme (if applicable): Click here to enter text.
6. Email address: n.elmrabit@lboro.ac.uk	14. Email address: Click here to enter text.
7a. Contact address: Click here to enter text.	15a. Contact address: Click here to enter text.
7b. Telephone number: 07925352220.	15b. Telephone number: Click here to enter text.
8. Supervisor: Yes	16. Supervisor: Choose an item
9. Responsible Investigator: Yes	17. Responsible Investigator: Choose an item
List all other investigators (name/email address): Shuang-Hua Yang/ S.H.Yang@lboro.ac.uk Lili Yang/ L.Yang@lboro.ac.uk.	

Participants

Positions of Authority

18. Are researchers in a position of direct authority with regard to participants (e.g. academic staff using student participants, sports coaches using his/her athletes in training)?	No
--	----

Vulnerable groups

19. Will participants be knowingly recruited from one or more of the following vulnerable groups?	
Children under 18 years of age	No
Persons incapable of making an informed decision for themselves	No
Pregnant women	No
Prisoners/Detained persons	No
Other vulnerable group Please specify: Click here to enter text	No
If you have selected No to all of Question 19, please go to Question 23.	
20. Will participants be chaperoned by more than one investigator at all times?	Choose an item
21. Will at least one investigator of the same sex as the participant(s) be present throughout the investigation?	Choose an item
22. Will participants be visited at home?	Choose an item

Researcher Safety

23. Will the researcher be alone with participants at any time?	Yes
If Yes, please answer the following questions:	
23a. Will the researcher inform anyone else of when they will be alone with participants?	Yes
23b. Has the researcher read the Guidance Notes on 'Conducting Interviews Off-Campus and Working Alone' and will abide by the recommendations within?	Yes

Methodology and Procedures

24. Please indicate whether the proposed study:

Involves taking bodily samples (please refer to published guidelines)	No
Involves using samples previously collected with consent for further research	No
Involves procedures which are likely to cause physical, psychological, social or emotional distress to participants	No
Is designed to be challenging physically or psychologically in any way (includes any study involving physical exercise)	No
Exposes participants to risks or distress greater than those encountered in their normal lifestyle	No
Involves collection of body secretions by invasive methods	No
Prescribes intake of compounds additional to daily diet or other	No

dietary manipulation/supplementation	
Involves pharmaceutical drugs	No
Involves use of radiation	No
Involves use of hazardous materials	No
Assists/alters the process of conception in any way	No
Involves methods of contraception	No
Involves genetic engineering	No

Involves testing new equipment	No
--------------------------------	----

Observation/Recording

25a. Does the study involve observation and/or recording of participants?	Yes
If Yes:	
25b. Will those being observed and/or recorded be informed that the observation and/or recording will take place?	Yes

Consent and Deception

26. Will participants give informed consent freely?	Yes
---	-----

Informed consent

27. Will participants be fully informed of the objectives of the study and all details disclosed (preferably at the start of the study but, where this would interfere with the study, at the end)?	Yes
28. Will participants be fully informed of the use of the data collected (including, where applicable, any intellectual property arising from the research)?	Yes

29. For children under the age of 18 or participants who are incapable of making an informed decision for themselves:	
a. Will consent be obtained (either in writing or by some other means)?	Choose an item
b. Will consent be obtained from parents or other suitable person?	Choose an item
c. Will they be informed that they have the right to withdraw regardless of parental/guardian consent?	Choose an item
d. For studies conducted in schools, will approval be gained in advance from the Head-teacher and/or the Director of Education of the appropriate Local Education Authority?	Choose an item
e. For detained persons, members of the armed forces, employees, students and other persons judged to be under duress, will care be taken over gaining freely informed consent?	Choose an item

Deception

30. Does the study involve deception of participants (i.e. withholding of information or the misleading of participants) which could potentially harm or exploit participants?	No
If Yes:	
31. Is deception an unavoidable part of the study?	Choose an item
32. Will participants be de-briefed and the true object of the research revealed at the earliest stage upon completion of the study?	Choose an item
33. Has consideration been given on the way that participants will react to the withholding of information or deliberate deception?	Choose an item

Withdrawal

34. Will participants be informed of their right to withdraw from the investigation at any time and to require their own data to be destroyed?	Yes
--	-----

Storage of Data and Confidentiality

35. Will all information on participants be treated as confidential and not identifiable unless agreed otherwise in advance, and subject to the requirements of law?	Yes
36. Will storage of data comply with the Data Protection Act 1998?	Yes
37. Will any video/audio recording of participants be kept in a secure place and not released for any use by third parties?	Yes
38. Will video/audio recordings be destroyed within ten years of the completion of the investigation?	Yes
39. Will full details regarding the storage and disposal of any human tissue samples be communicated to the participants?	N/A
40. Will research involve the sharing of data or confidential information beyond the initial consent given?	No
41. Will the research involve administrative or secure data that requires permission from the appropriate authorities before use?	No

Incentives

42. Will incentives be offered to the investigator to conduct the study?	No
43. Will incentives be offered to potential participants as an inducement to participate in the study?	No

Work Outside of the United Kingdom

44. Is your research being conducted outside of the United Kingdom?	No
If Yes:	
45. Has a risk assessment been carried out to ensure the safety of the researcher whilst working outside of the United Kingdom?	Choose an item
46. Have you considered the appropriateness of your research in the country you are travelling to?	Choose an item
47. Is there an increased risk to yourself or the participants in your research study?	Choose an item
48. Have you obtained any necessary ethical permission needed in the country you are travelling to?	Choose an item

Information and Declarations

Checklist Application Only:

If you have completed the checklist to the best of your knowledge, and not selected any answers marked with an *, # or †, your investigation is deemed to conform with the ethical checkpoints. Please sign the declaration and lodge the completed checklist with your Head of Department/School or his/her nominee.

† Checklist with Additional Information to the Secretary:

If you have completed the checklist and have only selected answers which require additional information to be submitted with the checklist (indicated by a †), please ensure that all the information is provided in detail below and send this signed checklist to the Secretary of the Sub-Committee.

Checklist with Generic Protocols Included:

If you have completed the checklist and selected one or more of the answers marked with this symbol # a full Research Proposal needs to be submitted to the Ethical Approvals (Human Participants) Sub-Committee unless you, or one of the investigators on this project, are a named investigator on an existing Generic Protocol which covers the procedure. Please download the Research Proposal form from the Sub-Committee's web page. **A signed copy of this Checklist should accompany the full proposal to the Sub-Committee.**

If you, or one of the investigators on this project, are using a procedure covered by a generic protocol, please ensure the relevant individuals are on the list of approved investigators for that Generic Protocol. Include the Generic Protocol reference number and a short description of how the proposal will be used at the end of the checklist in the space provided for additional information.

The completed checklist should be lodged with your Head of Department/School or his/her nominee.

*** Full Application needed:**

If on completion of the checklist you have selected one or more answers which require the submission of a full proposal (indicated by a *), please download the Research Proposal form from the Sub-Committee's web page. A signed copy of this Checklist should accompany the full Research Proposal to the Sub-Committee.

Space for Information on Generic Proposals and/or Additional Information as requested:

Click here to enter text.

For completion by Supervisor

Please tick the appropriate boxes. The study should not begin until all boxes are ticked.

- The student has read the University's Code of Practice on investigations involving human participants
- The topic merits further research
- The student has the skills to carry out the research or are being trained in the requires skills by the Supervisor
- The participant information sheet or leaflet is appropriate
- The procedures for recruitment and obtaining informed consent are appropriate

Comments from supervisor:

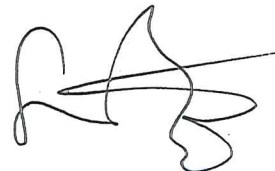
Signature of Applicant:



Signature of Supervisor (if applicable):



Signature of Head of School/Department or his/her nominee:



Date: 9/9/2015.

Appendix F

A Snap-shot of Bayes Network for Case 4



Appendix G

A Snap-shot of Bayes Network for Case 22

