

**The Impact of Business Analytics in Information Security Risk
Management**



By

Ayesha Naseer

(Registration No: 00000169011)

Thesis Supervisor: Dr. Adil Masood Siddiqui

Department of Computer Software Engineering
Military College of Signals

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2023)

The Impact of Business Analytics in Information Security Risk Management



By

Ayesha Naseer

(Registration No: 00000169011)

A thesis submitted to the National University of Sciences and Technology, Islamabad,
in partial fulfilment of the requirements for the degree of

**Doctor of Philosophy in
Software Engineering**

Thesis Supervisor: Dr. Adil Masood Siddiqui

Department of Computer Software Engineering
Military College of Signals

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2023)

THESIS ACCEPTANCE CERTIFICATE

It is certified that final copy of PhD thesis written by **NS Ayesha Naseer**, Registration No. **NUST201590339TMCS1115F** of **Military College of Signals** has been vetted by undersigned, found complete in all aspect as Per NUST Statues / Regulations / PhD Policy, is free of plagiarism, errors and mistakes and is accepted as partial, fulfilment for award of PhD degree. It is further certified that necessary amendments as pointed by GEC members and Foreign / Local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: **Dr Adil Masood Siddiqui**

Date: _____

Signature of HoD with Stamp: _____

Date: **26 Dec 22**

Brig
Head of Dept of GSE
Mil College of Sig (NUST)

Countersigned By

Signature (Dean): _____

Date: _____

Brig
Dean, MCS (NUST)
(Asif Masood, PhD)



National University of Sciences & Technology

REPORT OF DOCTORAL THESIS DEFENCE

Name: Ayesha Naseer NUST Regn No 00000169011 School/College/Centre: Military College of Signal Rawalpindi

Title: The Impact of Business Analytics in Information Security Risk Management

DOCTORAL DEFENCE COMMITTEE

Doctoral Defence held on 16th February 2023

	QUALIFIED	NOT QUALIFIED	SIGNATURE
GEC Member 1: Prof Dr. Hammad Afzal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
GEC Member 2: Assoc Prof Dr. Naima Iltaf	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
GEC Member (External): Dr. M. Mukarram Khan	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Supervisor: Brig Adil Masood Siddiqui, PhD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Co-Supervisor: Assoc Prof Dr. Fahim Arif	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
External Evaluator 1: Dr. Faisal Bashir (Local Expert)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
External Evaluator 2: Dr. Asif Ullah Khan (Local Expert)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
External Evaluator 3: Dr. Gabriela Mogos (Foreign Expert)	<input type="checkbox"/>	<input type="checkbox"/>	
External Evaluator 4: Dr. Mohammad Hammoudeh (Foreign Expert)	<input type="checkbox"/>	<input type="checkbox"/>	

FINAL RESULT OF THE DOCTORAL DEFENCE (Appropriate box to be signed by HOD)

Head of Dept of CSS
College of Sigs (NUST) PASS FAIL

The student Ayesha Naseer Regn No 00000169011 is accepted for Doctor of Philosophy Degree.

Dated: 16/2/23

Brig
Dean, MCS (NUST)
(Asif Masood, Phd)
Dean/Commandant/Principal/DG

Distribution:

1 x original copy each for PGP Dte, Exam Branch Main Office NUST and Student's dossier at the School/College/Centre.
1x photocopy each for HoD, Supervisor, Co Supervisor (if appointed), sponsoring agency (if any) and 05 copies for insertion in Dissertation.

Note:

* Decision of External Evaluators (Foreign Experts) will be sought through video conference, if possible, on the same date and their decision will be intimated (on paper) to HQ NUST at a later date.

Certificate of Approval

This is to certify that the research work presented in thesis titled "The Impact of Business Analytics in Information Security Risk Management" was conducted by Ayesha Naseer, under the supervision of Brig Adil Masood Siddiqui, PhD. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Computer Software Engineering, Military College of Signals in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the field of Software Engineering, Department of Computer Software Engineering of MCS, National University of Sciences and Technology, Islamabad.

Student Name: Ayesha Naseer

Signature: _____



Examination Committee:

- a) External Examiner 1: **Dr. Faisal Bashir**
(Professor, Computer Science Department
Bahira University, Islamabad).
- b) External Examiner 2: **Dr. Asif Ullah Khan**
(Professor, Department Computer and Information Sciences
PIEAS University Pakistan).
- c) Internal Examiner 1: **Dr. Hammad Afzal**
(Professor, Department Computer Software
Engineering Military College of Signals (NUST)
Islamabad).

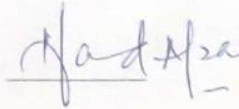
Signature: _____



Signature: _____

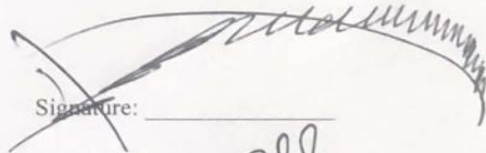


Signature: _____



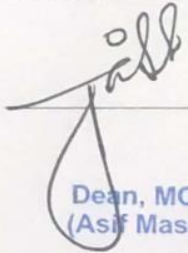
Supervisor Name: **Brig. Adil Masood Siddiqui, PhD**

Signature: _____



Name of Dean: **Brig. Asif Masood, PhD**

Signature: _____



**Brig
Dean, MCS (NUST)
(Asif Masood, PhD)**

AUTHOR'S DECLARATION

I Ayesha Naseer hereby state that my PhD thesis titled: "The Impact of Business Analytics in Information Security Risk Management." is my own work and has not been submitted previously by me for taking any degree from the National University of Sciences and Technology, Pakistan or anywhere else in the country / World.

At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my PhD degree.

Signature: _____

Name: Ayesha Naseer

Registration No: NUST201590339TMCS1115F


Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled “**The Impact of Business Analytics in Information Security Risk Management**” is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and that of National University of Sciences and Technology (NUST), Islamabad, towards plagiarism. Therefore I, as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred / cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of PhD degree, the University reserves the rights to withdraw / revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC / University Website on which names of students are placed who submitted plagiarized thesis.

Date: 26/12/22

Student/ Author Signature: 
Name: _____
(Ayesha Naseer)

DEDICATION

*This PhD thesis is dedicated to my honorable
teachers, family and friends for their love,
endless support, guidance, and inspiration.*

ACKNOWLEDGEMENTS

Thanks to Almighty ALLAH for all the uncountable blessings.

I would like to express my sincere gratitude to my supervisor Dr Adil Masood Siddiqui for his support and guidance during my studies. His comments and fruitful suggestions helped me complete my dissertation in a timely fashion.

I would also like to thank my GEC committee members Dr Hammad Afzal, Dr Naima Iltaf, Dr Fahim Arif, and Dr Mukarram Khan for their tremendous support and cooperation.

A special thanks also goes to Dr Humza Naseer for helping me with my research publications.

ABSTRACT

The organizations protect information resources and maintain competitive advantage by using risk driven and controlled centered security management systems. These systems are very useful in the prevention of threats that exploit common vulnerabilities. To react against attacks that are volatile, developing and complex for example *Advanced Persistent Threats*, they are not very effective. These dynamic and complex threats require a timely, agile, and sophisticated response capability to gather, integrate and analyze data to perform operational and strategic security operations. The modern organizations use *Real Time Analytics* as unique *Business Analytics Capability* that help them in gathering, combining, and analyzing business incidents efficiently. The capability of *Real Time analytics* to response important business information has achieved a lot of consideration in the existing literature. However, inadequate research has been done on how enterprises enhance agility in *Incident Response process*.

That research presents the research gap as mentioned above by exploring the research question: *How does use of real-time analytics in the incident response process improve enterprise cybersecurity performance?* To better understand how enterprises utilize *real time analytics capabilities* to infuse agile characteristics in their *incident response process*, this research gathered qualitative data from twenty experts' interviews and used data comparison process that employs simultaneous exploration and analysis. The results informed a theoretical framework that enlightens how organizations enable agile features of *swiftness, innovation, and flexibility* in incident response process using salient characteristics of *Real-time analytics* such as *complex event processing, decision automation, and continuous and on-demand data analysis*.

The *incident response dynamic strategies* collectively *real-time analytics capabilities* with help enterprises to identify and respond to cyber security incidents as-they-occur, which in turn, improve the overall organization security performance and gives both economic and strategic advantages.

The descriptions related to the proposed theoretical framework make contribution in the existin literature of *business analytics, agility in business operations* and *incident response strategies*. The findings of this study give a valuable guidance for future research on how agile characteristics are enhanced and developed in the *incident response process*.

TABLE OF CONTENTS

DEDICATION	i
ACKNOWLEDGEMENTS	ii
ABSTRACT.....	iii
LIST OF FIGURES	vi
LIST OF TABLES	vii
LIST OF ACRONYMS	viii
LIST OF PUBLICATIONS	ix
CHAPTER 1: INTRODUCTION.....	1
1.1 Motivation and Problem Statement	2
1.2 Contribution.....	4
CHAPTER 2: LITERATURE SURVEY.....	10
2.1 Business Analytics Capability	10
2.1.1 The Realtime Analytics Capability.....	13
2.2 Cybersecurity Incident Response Process	18
2.3 Deficiencies of Incident Response Process	25
2.4 Contingent Resource Based View Theory.....	27
CHAPTER 3: DESIGN AND METHODOLOGY	30
3.1 Research Methodology	30
3.2 Selection of Interviewees and Research Domain	33
3.3 Data Collection	37
3.4 Data Investigation process.....	39
3.5 The Real-time Analytics Capabilities.....	43
CHAPTER 4: RESEARCH CONTRIBUTIONS	47

4.1 The Theoretical Framework.....	47
4.2 Agile Characteristics in Incident Response... ..	48
4.3 Environmental Factors	50
4.4 Organizational Security Performance.....	53
4.5 The Theoretical Framework.....	55
CHAPTER 5: DISCUSSION AND FUTURE RESEARCH.....	66
5.1 Contribution of the Study	66
5.1.1 Contribution For Research.....	67
5.1.2 Contribution for Practice	68
5.2 Limitations and Future Research... ..	70
REFERENCES.	72
APPENDIX A: INTERVIEW GUIDE.....	80

LIST OF FIGURES

Figure 1.1 Overview of Research Methodology.....	5
Figure1.2. Real-time Analytics in Organizational Security Performance	6
Figure 1.3 Thesis Outline	10
Figure 2.1 Literature Integration.....	12
Figure 2.2 Decision Support Systems Evolution.....	14
Figure 2.3 Latency Vs Business Value.....	17
Figure 2.4 Incident Response Process Stages	22
Figure 2.5 Compromise Collection Cycle	23
Figure 3.1 Data Analysis Process	32
Figure 4.1 Data Structure.....	38
Figure 4.2 The Proposed Theoretical Framework	43

LIST OF TABLES

Table 2.1 Applications of Business Analytics in Various Industries	15
Table 2.4 Weaknesses of Information security Risk Management Process	21
Table 2.5 Weaknesses of Incident Response Process.....	25
Table 3.1 Interview Experts Profiles	30
Table 3.2 Data Analytics Process	34
Table 4.1 Interpretations from Qualitative Data.....	39

LIST OF ACRONYMS

Business Analytics Capabilities	BAC
Real Time Analytics Capabilities	RTAC
Incident Response Process	IRP
Incident Response	IR
Advanced Persistent Attacks	APAs
Information Security Risk Management	ISRM
Business Analytics	BA
Security Analytics	SA

LIST OF PUBLICATIONS

Following research papers have been published from this PhD thesis:

1. Naseer, A., Naseer, H., Ahmed, A., Maynard, S. B., Siddiqui, A. M. (2021). “Real-time Analytics, Incident Response Process Agility and Enterprise Security Performance: A Contingent Resource Based Analysis”. Published in International Journal of Information Management. (IF: 14.0)
HJRS Category: W, Medallion: Platinum
2. Naseer, A & Masood, A. (2022)., “THE EFFECT OF BIG DATA ANALYTICS IN ENHANCING AGILITY IN CYBERSECURITY INCIDENT RESPONSE”, 16th International Conference on Open-Source Systems and Technologies (ICOSST).
3. Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood, A. (2022), “Moving towards agile cybersecurity incident response: the enabling role of big data analytics as a dynamic capability”, Computers and Security, 2022. (IF: 5.1)
HJRS Category: W, Medallion: Gold

Introduction and Motivation

The modern organization have designated teams for incidence response process, which detect, examine, react, and gain knowledge from potential security event in a cost effective and timely way. That process is critical for organizations as they are not able to avoid a breach and hence a quick response to a security threat helps them to shun unspecified financial loss. It also helps the organizations to protect their organizational competitive advantage and reputation. To handle the security attacks and data breaches, organizations employ their security incidence response teams to identify, investigate and respond to security events effectively and efficiently. However, to efficiently identify and react to security incidences, designated incidence response teams are required to swiftly gather, integrate, and analyze the entire data relevant to a security incidence that has occurred or is occurring in their enterprise.

This ability plays a vital role in the development of IPR, since an enterprises' ability to attain superior security performance based on its reaction to security events inside a dynamic threat environment. The following sections give details of the significance of this study, the main center of attraction of the research, give an outline of the design of research, give the summary of research contributions, and discuss thesis organization.

1.1 Motivation and Problem Statement

Modern business environment is fast-paced and dynamic in which organizations employ their assets such as data, systems, and digital processes in attaining a competitive advantage. However, today's organizations execute their routine business tasks, these

assets are more vulnerable to evolving and complex security threats, such as embezzlement, fraud, theft, industrial espionage, and sabotage. Therefore, it is crucial for enterprises to save these assets to maintain their competitive advantage and effectively work in modern unpredictable threat environment. In order to do so, enterprises use the IRP that enables them to detect, examine and react to promising security events in a way that reduces damage and supports speed recovery.

Strategically, organization security in enterprises has focused on dealing with threats with an inclusive control system. The industry-endorsed checklists are used to develop the process of selection of controls to a very complicated process of risk management which demands the organization to: (1) detect important assets, (2) organize risk events based on severity, and (3) find out the cost-effective ways of managing vulnerability.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe cyber attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and protective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

However, they are not useful for dynamic response against complex, developing and unpredictable threats for example Advanced Persistent Attacks. They are organized, informed, and trained attackers which employ innovative and specialized methods to manage enterprise security threats. In the coming years the occurrence of this more complicated form of attack is supposed to increase extensively.

The dynamic and complex nature of such threats requires awareness of situation to react to the developing attacks. That demands the enterprises to build up a specialized ability to gather, integrate and analyze information to perform operational and strategic security techniques to be employed efficiently and effectively.

security incidence response (IR) teams exist in most of the organizations, their conventional role is mostly technology oriented and operational. The main objective of such teams is to help an organization to recover to routine business process. To contest argue, based on the whole of organizational response, paradigm shift is needed. In the 'response

paradigm', incidence response acts as a more strategic-level operation, which helps the organizations to respond the dynamic threat environment inside the strategic-business environment. To develop more strategic level process of incidence response, organizations must produce security information regarding the attacks and employing the IRP to leverage said information efficiently and effectively against APAs. As a result, this needs the IRP to have skills, tools and processes that make organization to collect, integrate and analyse all related data relevant to security events particularly data regarding the strategic-business environment.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe cyber attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and protective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Business analysis Capability assists enterprises to integrate process, technology and people in order to produce information that help business managers to take informed decisions efficiently and effectively. This organizational capability is required to collect, integrate, and analyse of huge collection enterprise data. One of the specialized BA is RTA that targets on streaming data therefore allowing enterprise to execute Business analysis in real-time and effectively makes decisions informally. Therefore, RTA helps organizations to attain the above mentioned paradigm shift by establishing an incidence response process that helps to collect, integrate, and analyze both security and business data in real time to moderate the threat of advanced persistent threats inside the strategic business environment.

Business analysis literature and practice have the idea of RTA for more than a decade, however the knowledge of this idea is still inadequate. The RTA is a growing phenomenon, many organizations are applying it to increase their operational performance. Therefore, a few organizations have realized that RTA is a unique business analysis capability which assists to enhance ability in business operations. Although the RTA has attained much consideration as a developing business analysis capability, however,

the research on using RTA to enhance ability in IRP to improve the entire organization security performance is less focused.

ability is important IRP, as an organizational security performance relies on its response to security events that have occurred or are occurring in an ever-changing threat environment. While organizations are giving more focus in enhancing ability in IRP, there is limited knowledge regarding how ability can be enhanced in IRP. Therefore, how enterprises enhance ability by using RTA in IRP crucially impacts an organization's security performance remains relatively less focused.

To fulfill the above-mentioned gap in the research, the fundamental research question is:

How enterprises enable agile characteristics in the incidence response process utilizing key features of analysis abilities?

There are many relevant concerns that require to be investigated, to answer the key research question. The first issue is: what are the fundamental characteristics of RTA in IRP? The second issue is: what are the essential phenomenon by which RTA enhances ability in IRP? And the third issue is: what are the key environmental factors that hinder or facilitate using of RTA in IRP? And the fourth issue is: how does using of RTA in IR affect entire organizational security performance?

Consequently, four subject matters have to be investigated to find the answer to highlighted question of research study.

- Main characteristics of analysis Capability: What are the salient characteristics of RTA in IRP?
- Agile characteristics of incidence Response: What are the fundamental techniques that help RTA enhance ability in IRP? In another way, why and how does RTA enhance ability in IRP?
- Contingent Environmental factors: What are the key environmental factors which hinder or support the use of RTA in IRP? Why are those key factors significant?
- Security performance of an enterprise: How does the use of RTA in IRP enhance entire organizational security performance?

1.2 Contribution

Integrating the existing literature with qualitative data analysis findings of our study a theoretical framework is developed, grounded on contingent resource based view theory, that explains the impact of analysis on enterprise cybe rsecurity performance through inter-mediating role of agile incidence response process, furthermore, the framework also explains the contingent factors of cyber threat environment (complexity and dynamism) positively moderate the use of analysis in security incidence response process. In order to explain the theoretical framework, following propositions are formulated:

Proposition 1: Complex event processing, decision automation, and on demand and continuous data analysis are critical elements of analysis capability.

Proposition 2: analysis capability enables organizations to execute agile incidence re- sponse by instilling the agile characteristics of swiftness, flexibility, and innovation in their security incidence response process and thereby respond to the complex and dy- namic cyber threat environment proactively.

Proposition 3: Increasing ability in the incidence response process enhances the efficiency and effectiveness of overall enterprise security performance.

Proposition 4: incidence response ability mediates the relationship between RTA and enterprise security performance.

Proposition 5a: Cyber threat environment complexity positively moderates the impact of analysis capability on incidence response ability.

Proposition 5b: Cyber threat environment dynamism positively moderates the impact of analysis capability on incidence response ability.

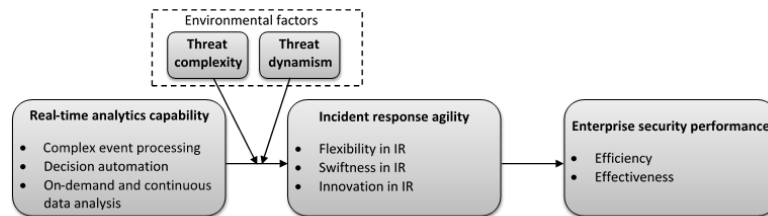


Figure 1.1: The Proposed Theoretical Framework

- Main features analysis capability. Three salient characteristics of RTA are identi-

fied by this research study including (“complex event processing, decision automation, and continuous and on demand data analysis”). Organizations use these characteristics to build, combine and reconfigure their security skills, resources, and functional abilities and hence enable ability in incidence response process of security.

- Agile characteristics of incidence response. RTA enabled agile features for example (swiftness, flexibility, and innovation) in IRP that results to enhance the ability in IRP.
- Contingent Environmental factors. Two environmental factors are indentified by this study including (threat complexity and threat dynamism). These factors balanced the affect of RTA on IRP.
- RTA is used to develop agile characteristics in IRP that help enterprises to enhance their organizational security performance. Organizational security performance links to the efficacy and effectiveness of security processes. ability IR process enhance the entire organizational security performance by minimizing the cost of prevention, remediation, and mitigation.

In general view, the descriptions of the proposed theoretical framework enhance and clarify the understanding of how the IRP reacts to both un-predictable and predictable attacks by building up the RTA abilities which infuse ability in IRP. Moreover, the information from this research enhances our knowledge of RTA ability and expands the former literature with highlighting its key areas in IRP by describing the (“complex event processing, decision automation, and continuous and on-demand data analysis”).

That research adds in the existing literature on strategies of IRP by highlighting RTA which infuse ability in IRP. Three analysis abilities have (complex event processing, decision automation, continuous and on-demand data analysis). Three agile incidence response strategies include (swiftness, flexibility and innovation). While [15] presents ability as a main feature of process of incidence response and highlights the growth of ability in IRP that handle dynamic and complex threats, that study expands the former literature by highlighting three main RTA abilities that infuse ability in IRP.

From a theoretical perspective, the proposed framework describes the connection of RTA and ability enabled IRP with organizational security performance and also describes

ability enabled IRP as a significant type dynamic capability. The enhanced ability in the IRP makes enterprise to redirect and reuse its security resources, alter its extant processes of incidence response, techniques, or build novel methods of reacting to both un-predictable and predictable security attacks effectively and efficiently. Hence, RTA instill agile features of (innovation, flexibility, and swiftness) in IRP which improve overall organizational security performance.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe cyber attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and protective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

From a practical perspective, the information from this study helps three groups of participants in practical scenario of IRP. To benefit incidence response teams, that research's findings have the broad perspective of the function of RTA. Instead of practicing RTA at the operational level to observe the threat environment continuously, incidence response teams are required to identify the impact of RTA at a strategic level in developing both detective and protective reaction plans.

To benefit the security executives, the implications from this research emphasize that for developing analytical abilities in IRP, executives are required to employ and/or educate security or analysis employees with knowledge and skills need to implement security analysis solutions produced by external vendors. To benefit security retailers, the information from this research propose that they must identify the potentially widespread creative function that their security solutions may supply to their organization. Developing security solutions which can incorporate threat intelligence data, apply complex algorithms, automate investigations and forensic analysis to find out the possible threats will facilitate their clients produce creative strategies for incidence response that can respond to the dynamism of threat environment.

For security executives, the implications from this research emphasize that to make IRP analysis enabled, executives require to appoint and/or educate security or analysis em-

employees with knowledge and skills need to implement security analysis solutions produced by external vendors. For security retailers, the information from this research proposes that they should identify the specific role that their security solutions can supply to their organization.

The increasing adoption of cloud, mobile services and Internet of Things is putting organizations at risk of threats more than ever before. The ongoing digitization of business operations is creating a larger attack surface for attackers to exploit, which has resulted in the need for ability in the response to security incidences. The process of security incidence response is used by organizations to identify, contain, eliminate and recover from security attacks. The incidence response process consists of a gathering of procedures aimed at detecting, examining and responding to most likely security attacks in a manner that reduces effect and helps fast recovery. In this paper, we claim that for the incidence response process to be efficient in tackling unknown, complicated and attacks, its basic phases (identification, control, elimination and recovery) must be carried out in an effective manner. This requires incidence response teams to have skills, tools and processes that make enterprises to gather, integrate and examine of all related data linked to security incidences to make informed decisions in an effective manner.

Big data analysis is an enterprise capability that assists in gathering, integration and examination of a large amount of business data generated in various forms at high speed to gain business information for informed decision making. The use of big data analysis helps to collect, integrate and analyze security data from a variety of sources such as logs, networks, endpoints, sensors, and cloud systems, security managers can discover useful information about security incidences. This information can help organizations to detect system vulnerabilities and attacks and execute incidence response in an agile manner.

The capability of big data analysis to enhance security has obtained much attention in both research and practitioner domains, research on the trans-formative effects of big data analysis on the ability of security incidence response is limited. These findings in the literature encouraged our study main research question: How can big data analysis improve ability in the process of security incidence response?

To address this research question, we carried out twenty-one detailed expert interviews with security professionals examining how the practice of big data analysis impacts

ability in the process of incidence response. Based on the qualitative data findings, we built a framework that describes the main characteristics and application of big data analysis capability in the incidence response process at three distinct levels i.e., manual analysis, basic analysis and advanced analysis. The features of the framework help to understand how organizations may operate at three different big data analysis-driven incidence response levels and what organizations can do to get to the next level. Further, the framework also explains how big data analysis instils the agile properties of flexibility, innovation, and swiftness in the process of incidence response.

In the subsequent sections, first, we explain the intersection of big data analysis and security. Then, we unpack the concept of the process of security incidence response ability. In the research technique section, we elaborate on the method of data gathering and assessment, and then describe the outcomes of the fieldwork. In the next section, we highlight implications for practice and theory. We conclude the paper by describing the shortcomings of this research work and guidelines for further research agenda.

Developing security solutions that may put together threat intelligence data, apply complex algorithms, automate forensic analysis and investigations to find out the possible attacks will facilitate their clients produce creative IRP strategies that can respond to dynamism of threat environment.

CHAPTER 2

Literature Review

This chapter presents the detailed literature survey of business analysis abilities (BA), Business Process ability (BPA) and security risk management (CSRM). In section 2.1, the basic ideas related to of BA are described together evolution of analysis capability that is a specialized business analysis capability. Section 2.2 explains security incidence response process in detail. In Section 2.3 the deficiencies in the process of security incidence response are analyzed. Section 2.4, contingent perspective of resource-based view theory is described in detail.

The weakness highlighted in the IRP make the foundation of that research's overarching research question: How enterprises enable agile characteristics in the incidence response process utilizing key features of analysis abilities?

2.1 Business analysis Capability

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require

to identify the more novel role of analysis abilities at strategic level in developing both detective and reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards. In Table 2-1, a comprehensive view of few published BA applications and the techniques by which organizations gained improved performance in various industries.

Based on the analytical perspective, BA is divided into three groups: first group is descriptive analysis, second group is predictive analysis, and third group is prescriptive analysis. It is helpful to discriminate between those groups as the dissimilarities have the useful directions for the technology, process, people, and structural design needed to implement BA.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe cyber attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing

Enterprise	Process/System	Strategies leads to competitive advantage and superior organization performance	Citation
Retail	Examination of click stream data produced by a website	Minimize customer shopping cart rejection	[ahmad2012incidence]
Logistics and Transport	Examination of parcel delivery data to prevail over packages BAKlog	Accurate customer errors and charge them for the service	[2]
Insurance	Un writing process of insurance	Optimal charges of insurance policies to reflect right risks	[4]
Airlines	Analysis of data about flights, reservations, and customers	Knowledge of profiles of preferably profitable clients personalized relations with clients	[5]
Supply Chain Management	Examination of customer data to design customer value frameworks	Personalized relations with customer to provide a specialized experience	[1]

Table 2.1: Concept Matrix: Applications of BA in different industries.

both detective and protective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The

relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

2.1.1 The analysis Capability

The applications of predictive, prescriptive, and descriptive analysis are important to business as they give information to both past investigation and upcoming preparation. Though, those applications have latency's for example decision, analysis and data latency, because data are initially stored to an analytical platform after that processed for information creation.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and reaction plans. The use of the variety of abilities which are allowed

by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe cyber attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and protectiv reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

Those applications are hence not useful for business activities which require to be examined when they happen such as (situational intelligence, event-based campaign, attacks detection and fraud). To minimize the data and analysis latency relies mainly on the analytical architecture and technologies. Current growths in analytical platforms give assistance in this regard. On the other hand, minimizing decision latency needs alter-

ations in how people utilize information in doing their business processes.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

To handle the decision latency is generally trickier than analysis and data latency. To answer this problem, Business analysis researchers have presented the idea of analysis abilities. The main goal of RT is minimizing the decision-making time to enhance business value [49]. When the business operations and processes are combined with the analytical processes in real time that make it possible to do remedial action before problems materialize.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

First, organizations are now able to capture new sources of data that they were not able to capture before. As a result, the rate of security data generation has significantly enhanced. The variety in sources of security data is extremely broad, for example operations data, social media, network logs, threat intelligence, NetFlow data, firewall logs, security information and event management (SIEM) data, intrusion detection system data, intrusion prevention system data. Most of this data has always been available, but organizations were not able to capture and integrate this into single source of truth until novel technologies and methods in big data analysis were developed and used in

security.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

Second, organizations now have to deal with increasingly huge volumes of data due to the growth in data sources. As storage costs have decreased significantly due to the introduction of cloud-based platforms and solutions, all the data that was once retained only for a finite time can now be stored in large data storage systems and data sets indefinitely.

Third, the increasing number of data sources and the rate of data generation has resulted in a larger variation in the types of data. Organizations now collect data that ranges from highly structured data sets to highly unstructured data sets. Historically, most data available for security analysis was in a structured format. However, the types of data being captured today range from highly structured and transnational data sets (customer relationship data, financial accounting data) to highly unstructured data extracted from social media, emails, threat feeds, and new data sources that are being created through a combination of existing data sources.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RT will assist IR teams execute the integration of avoidance, identification and reaction strate-

gies which may assist them to better handle with both unpredictable and predictable security attacks.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and reaction plans. The use of the variety of abilities which are allowed by RT will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

However, the main issue for organizations is not the high volumes of data, the several

types of data, the collection of data, or the storage of data; but rather how organizations harness this data to generate value. To drive value from big data analysis, organizations are increasingly using data to enable behavioural analysis so that they can make smarter decisions, maximize return on investments, minimize costs, and optimize operational performance. To summarize, organizations are increasingly discovering the role of big data analysis in improving their security processes and overall enterprise security performance.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

RTA has potential to provide major value and benefits to enterprises by enhancing business processes. Since the idea of RTA is still emerging and requires more examination, this research hence try to build and expand on our knowledge of RTA by investigating its role in emerging RTA that are essential to attain ability in IRP.

2.2 security incidence Response Process

That method is critical for organizations as they may not avoid vulnerability all the time and hence an efficient IRP to a security threat can assist them to prevent any financial loss and particularly, defend their reputation and competitive advantage. To handle the security data attacks and beaches, enterprises IRP teams are engaged to identify and eliminate the cyber-attacks. The main objective of IRP team is to reduce the damage of a security event. IRP teams are the “firefighters” inside an organization that identify, examine, react, and recover from security incidences.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is

when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems (MIS). After these systems the executive information systems (EIS) and decision support systems (DSS) are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing (OLAP, enterprise data warehouses, dashboards, data mining and scorecards.

The main objective of IRP is to swiftly reduce the loss of the threat, the recovery time of the threat, and to build guidelines that will assist in avoiding the security attacks in future. The phases of IRP according to are given in Figure 2-1 and descriptions of each phase of IRP are presented below.

In preparation phase the IRP team forms processes, tools and policies which may assist to avoid, identify, and react to several kinds of security attacks. One additional task in this stage is to educate the organization's workers. All workers of an enterprise must have knowledge of security policies and processes so that they know how to react when there is a security attack.

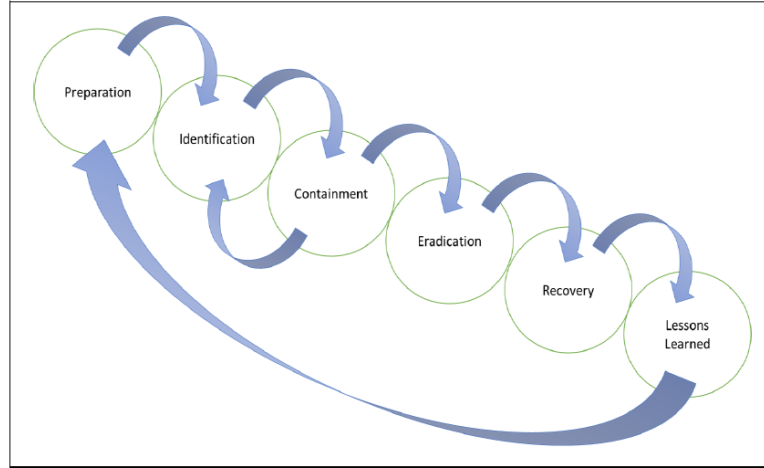


Figure 2.1: phases of incidence Response Process

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

In the phase of identification, the IRP team identify if the security event is really a security attack. For that, IRP team analyzes the available information related to the security event. Those indicators assist in detection of the malicious events on systems and networks. The examples of IOC may have (registry file changes, unusual network traffic, multiple failed login etc).

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will

assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

The collection is a recurrent process. First the IRP team gathers the primary information regarding the security attack, after that the detection scenarios are created. New BA are created with the help of these detected scenarios which Application of these scenarios assist the attack identification and collect more information related to it by performing data examination, therefore making a loop.

The compromised assets are restored to their original state in the eradication phase. That process includes deleting the malicious program, rebuilding the configuration, and deleting any artifacts that were caused by the malicious program. Such as, if software compromised a computer, the IRP team must remove the program, rebuild the compromised system registry and files to the initial state, and remove the installation files of the software.

The process of incidence response is one of the core areas of a successful security program. Organizations use the process of incidence response to recognize, examine, eliminate and

recover from potential security attacks in cost-effective and timely manner. This is a key business process as enterprises are not always able to avoid vulnerabilities and a timely reaction to an incidence can minimize the effect on their competitive advantage and reputation.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems (MIS). After these systems the executive information systems (EIS) and decision support systems (DSS) are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

To effectively address security attacks and data breaches, organizations require quick detection so that they can respond in an agile manner. The longer a security attack is left unidentified, the more challenging it is for enterprises to precisely measure the damage the attack may have caused both to itself, as well as to its customers and partners. The literature on the process of security incidence response reveals that the aim of the process of security incidence response, in various enterprises, is to advance in complicated protection targeted at fighting identified attacks, rather than in a complicated and dynamic reaction capability to deal unidentified, complicated and novel attacks. The use of prevention-oriented measures enables enterprises to better handle with security attacks that are static and known in nature. Though, they are more exposed to unknown, dynamic, volatile, and novel security attacks (e.g. zero-day attacks).

In their seminal paper described ability as a main property of the dynamic incidence response process. ability in the process of incidence response enables enterprises to contain attacks and eliminate and recover from the impacts of an attack to their enterprise assets in a swift and efficient manner. Even though enterprises are giving more focus to enable incidence response ability, the knowledge about how incidence response ability can be applied is inadequate. Therefore, we examine the utilization of big data analysis in improving ability in the incidence response process.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

In that last stage, the IRP team examines the security incidence thoroughly and implements strategies which will assist to avoid such security events in the future and modifies the security incidence response strategy for such kind of incidences. This process may include changing the enterprise assets configuration, security policies adjustment, and security training of enterprise workers.

2.3 The Deficiencies of incidence Response Process

With the increase of security incidences in enterprises, it is very important that enterprises can examine, identify, react, and prevent the security incidences in a cost effective and swift way. The analysis of IRP literature proposes that the main purpose of the IRP

strategies in many enterprises is to spend in complicated preventive process designed for controlling predictable risks instead in an adaptive response process to examine and prevent unpredictable emerging risks. Recent business discussions also propose that basic drawbacks present in the application of recent strategies in real-world handling of security incidences. The reason is that most of the IRP are structured utilizing a method based on linear plan beginning from preparation stage which directs to identification of security incidence.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

Organizations have been collecting increasingly large amounts of data as part of their

routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

Table 2-2 sum up the weaknesses detected in the incidence response process strategies.

Weaknesses in incidence Response Process	Citation
Do not provide adequate information regarding security events	[baskerville2014incidence]
Do not provide information for security incidence planning	[3]
Do not enhance the advantages of forensic abilities	[6]
Do not provide forensic evidence	[5]
Focus on complex threat prevention rather than response strategies to handle the complex threats	[7]

Table 2.2: Concept Matrix: Applications of BA in different industries.

2.4 Contingent Resource Based View Theory

The RB argues that organizations can generate competitive advantage by developing bundles of resources. These resources include tangible and intangible assets and abilities. Assets consist of people, infrastructure, and data, while abilities consist of processes and knowledge and skills of the people that use assets to do business activity. Organization's can achieve superior performance by developing abilities that are non-substitute, rare, unique, inimitable, and valuable which allow the organization to do activities more effectively and efficiently than its opponents.

The existing literature about RB reveals that it is static in nature. This means that RB is unable in recognizing the internal and external conditions in which abilities are most valuable. The concept of contingent conditions is highlighted in the contingency theory which refers those contingent factors will influence the organizational capability development, therefore organizations must adopt to changing environment. Scholars have proposed contingent RB to overcome the static nature of RB.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and reaction plans. The use of the variety of abilities which are allowed by RT will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the

first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing (OLAP, enterprise data warehouses, dashboards, data mining and scorecards.

The contingent perspective of RB is used in this research study for two reasons: (1) to improve the use of RB, and (2) for recognizing of the conditions that affect the effectiveness of different abilities. The internal and external factors are critical in attaining competitive advantage produced by abilities, especially in context of their selection and deployment. Furthermore, contingency research is accepted as vital for the development of secure information systems however, the contingent perspective on the RB is underdeveloped in incidence response literature.

CHAPTER 3

Design and Methodology

In that chapter the research design used for that study is explained and described. The section 3.1 justifies and explains the research design adopted to address the question of research that research focuses to explore how organizations enhance the IRP ability using RTA. Establishing on the focus of that research and unpredictable nature of the security environment, the inductive qualitative research by taking the fifteen interviews form security and business analysis experts is taken to answer the overarching question of research. In next section, the context of this research study is presented in detail and the reason behind the selection of twenty experts for interviews is explained in addition to that the participants profiles are also presented in this section. In the next two sections 3.3 and 3.4, a summary of analysis process and the process of data collection is explained.

3.1 Research Methodology

The focus of that research is to investigate how Enterprises enhance ability in IRP by implementing RTA. To address this research question, fifteen expert interviews are conducted according to the guidelines presented by. Based on their relevant industry experience the Interviewees were selected. Having experience in both security and BA was one of the key criteria of selection for this study.

Although the literature on BA is very rich, there is a deficiency of systematic framework to build the knowledge how RTA can assist enterprises to enhance ability in IRP, and that stimulates the selection of that study's research design to inductively establish a

framework. Qualitative approaches may assist in getting information into the complexity involved in utilizing RTA in IRP to improve ability, and assist the evolution of more and richer informative results.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Expert interviews are helpful when a phenomenon is complex and broad and demands comprehensive, detailed examination without manipulation and explicit control. One more important reason for choosing expert interviews to collect qualitative data is the kind of the research question which is being examined. Interviews are most suitable for examining "How" questions and therefore, in that case, the examination of how RTA enhance IRP ability is compatible with these definitions of the expert interviews methodology.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to

identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The goal of our research study is to examine how ability can be enhanced in the process of security incidence response using big data analysis. The security landscape is highly complex and dynamic, we used an inductive research technique to be open to unanticipated and new findings. We applied the strategies for inductive research described in. The aim of conducting inductive research is to create powerful chances for the discovery of new concepts and their relationships rather than assertion of existing concepts. In addition, inductive research helps to comprehend the meanings and ideas utilized by social actors in their real-life settings, rather than generating quantitative facts to assess hypotheses.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The

relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

That inductive and qualitative research method follows the guidelines that are like the method used by. The interviews' data is into three groups: descriptive data view, exploratory data view and explanatory data view. The main cause of using the descriptive data view is to highlight a comprehensive explanation of the process inside its domain, an exploratory data view is adopted to describe the questions and hypotheses of a following research or to find out the likelihood of the preferred research processes and the aim of an explanatory data view is to examine the underlying associations in the hypotheses. This research takes each expert interview as an individual analytical unit and formulates theory from the interviews data by iterative looping within the interviewee's data, following the guidelines of. This study uses the guidelines which presents for constructing theory that is based on the collected qualitative data.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related

dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Hence, that research utilizes main concepts from the literature on RTA and IRP that give the theoretical framing which is essential for developing knowledge of how enterprises enhance ability in IRP by implementing RTA.

3.2 Selection of Interviewees and Research Domain

In that study, the theoretical sampling is adopted to choose the enterprises where most recent comprehensive business analysis and security are used to enhance IRP decision formulation process. The relevance and applicability of that research's findings can be enhanced by using multiple cases. Moreover, multiple cases can improve our knowledge and description of a central issue.

The focus of this research is to investigate how enterprises enhance their entire enterprise security performance using RTA in their IRP. Taking into consideration that security attack environment is highly unpredictable, we employed an exploratory and inductive research approach to be open to new and unexpected findings. We followed the guidelines outlined in. Relied on the exploratory nature of that research study, we took twenty face-to-face semi-structure interviews (in international collaboration with University of Melbourne) with security and business analysis experts to gather the qualitative data.

Interviewees were chosen based on their relevant industry experience. Having experience in both security and BA was one of the key criteria of selection for this study. (Table

3-1) below gives the brief description of the interviewee's profiles.

ID	Role	Industry Sector	Experience (security, BA)
1	Senior security Manager	Finance	12 Years, 10 Years
2	Senior Security Architect	ICT	12 Years, 10 Years
3	Head of security	Insurance	12 Years, 10 Years
4	Chief Security Architect	Big Data and Cybersecurity	12 Years, 10 Years
5	Head of IT Risk	Finance	12 Years, 10 Years
6	Enterprise Security Architect	Cross Industry	12 Years, 10 Years
7	Director of security Risk	Cross Industry	12 Years, 10 Years
8	security Manager	Finance	12 Years, 10 Years
9	Data Scientist	Banking and Finance	12 Years, 10 Years
10	Senior security Analyst	Banking and Finance	12 Years, 10 Years
11	security Risk Manager	ICT	12 Years, 10 Years
12	Chief Information Security officer	Banking and Finance	12 Years, 10 Years
13	IT Risk Manager	Insurance	12 Years, 10 Years
14	General manager of IT Risk	Banking and Finance	12 Years, 10 Years
15	IT Risk Partner	Banking and Finance	12 Years, 10 Years
16	Senior security Analyst	ICT	12 Years, 10 Years
17	Threat Hunter	Banking and Finance	12 Years, 10 Years
18	security and IT Specialist	ICT	12 Years, 10 Years
19	Threat Intelligence Leader	Banking and Finance	12 Years, 10 Years
20	General Manager of Data science	Cross Industry	12 Years, 10 Years

Table 3.1: Interviewees Profile.

From each organization one or more security and business analysis expert is selected for interview. We used this research method as it facilitates this study to base on the most recent practice and gives comprehensive and detailed knowledge of the impact of analysis in IRP and how it enhances organizational security performance. We opted “snowball

sampling”; in which we started to contact the professionals in the industry, explained this research main goals with them, and required their assistance in highlighting more contributors for that research study.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will

assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Based on the concepts of RTA and IRP an interview guide was designed which also contained open-ended interview questions relevant to the BA and IRP. The semi-structured interviews of approximately one-hour were transcribed and audio-recorded. We also took comprehensive notes throughout the interviews. We used thematic content analysis to perform data analysis. The raw qualitative data was systematically converted into theoretical interpretations after several iterations of analyzing the data from first order concepts to final dimensions.

3.3 Data Collection

That study involved human informants, to gather data, the ethics approval was required. To work according to the guidelines of Human Ethics Advisory for data collection, research collaboration is conducted with security research group at University of Melbourne-Australia, that research team helped in data collection phase.

The information was gathered from the aforementioned experts over the period of a year beginning in June 2017 and finishing in July 2018. Information was gathered by from experts by taking interviews. Meeting related information documents were provided rely upon the interviewee request.

Moreover, the data available on the enterprises websites was also gathered that allowed to understand each enterprise strategies and practices regarding incidence response process (IRP). Overall, 20 interviews were conducted from security and business analysis experts. They highlighted the more informants that can assist that research study. The informants were chosen based on the benchmark that they all had practice understanding in both analysis and security areas and had adequate information to give information on behalf of the enterprise in which they worked. Many interviews conducted for that research continued about an hour.

The interviewees were asked to provide precise examples to get a deep knowledge of what important information was provided related to context. Moreover, comprehensive notes were prepared at the time of those interviews for reference in the phase of data analysis. The analysis of data and data collection were conducted according to the guidelines.

We employed purposeful sampling technique to select participants that had considerable experience in using big data analysis in the process of incidence response. The conditions for the collection of interviews for our research was that participants required to have minimum five years of industry practice in both big data analysis and security incidence response. In total, twenty-one participants from fifteen organizations were interviewed. The participants came from four distinct industry sectors including banking and finance, insurance, information and communication technology, and cross industry. The experts from consulting enterprises had a deep and various set of skills across these industry areas. While conducting the expert interviews, we asked the participants to indicate on their overall experiences rather than those just in their existing enterprise. Based on the

knowledge of big data analysis and relevant literature on security incidence response, an interview guide was formed containing open-ended questions. The approximately one-hour semi-structured interviews were conducted, transcribed and audio-recorded. We also formed comprehensive notes while conducting the interviews.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both de-

tective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The “Follow-up” conversations were conducted with the interview informants to get interpretations and gather more information. That research study gives evidence by presenting quotes in Chapter 4 to describe the research contributions generated from the analysis of qualitative data gathered based on the recommended practices in the studies of qualitative research.

3.4 Data Investigation Process

The first step in data investigation process is to review the BAKground information and interview notes along with the field transcript which were taken during the interview. In this phase, the specific objective is to find out indicators of how IRP teams were utilizing RTA in their daily security practices.

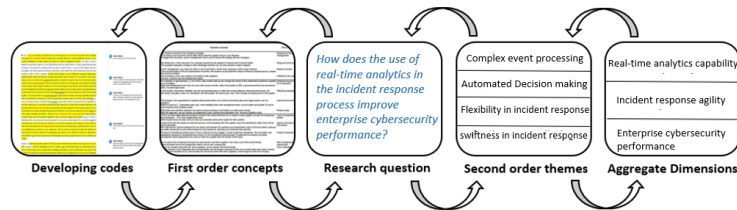


Figure 3.1: Data Investigation Process

Those lables were allocated to words, paragraphs, and sentences in the edges of the

interview notes. On whole, that research study generated 250 codes related to present the role of RTA in enhancing ability in IRP. Those codes were arranged into data tables in “Excel spreadsheets” which presents a single theme or topic across data sources. Each fresh statement was written under the suitable code. This coding process is continued till it was not probable to find out any more discrete, common patterns inside the information. In that fashion, theoretical code generation was achieved.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable

security attacks.

The four phases of data analysis process are used to convert the raw data into theoretical interpretations in detail following the guidelines presented. Analytical methods presented were used to produce information from each case and after that these information are compared with all the cases.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems. After these systems the executive information systems and decision support systems are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

The theoretical interpretations were derived from the raw qualitative data, after performing various cycles of examining the data from first order groups to second order themes and then to final dimensions. In the first phase, primary coding was done to

build first order groups from empirical data using the informants' terms and wordings. In next stage, we focus on data and the current literature to examine and build concepts that describe the data. We examined the linkages and overlap in first-order categories to compile these into higher-order themes. The second order themes are created after several iterations. while performing these iterations, the first-order categories were reviewed, integrated and sometimes left over in order to get a higher level of abstraction and to reach at eight second-order themes. Lastly, the eight second-order themes were integrated into two accumulated dimensions that highlight the key ideas relevant to knowledge of the role of big data analysis in enhancing IR process ability. Though the linear structure is followed in this paper, the whole process of data examination that we performed was iterative to enhance actionable information and generalized.

It should be observed that although we give only some examples of raw data, there are several examples of first order groups and second order themes. The themes comprised of theoretically distinct ideas that appeared from the data when examined at a more abstract level.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Based on each security and business analysis expert's response a rich case study is develop that have several kinds of data to explain the enterprises context, security response, analysis and the affect of utilizing the RTA in IRP to enhance ability. Three critical information generated from the expert interviews that assisted in further examination. First, security experts described what they imply by analysis and after that they highlighted the main characteristics of the RTA in the domain of IRP.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the

organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

Second, these higher-order abilities facilitated by RTA in IRP are built up over a long period of time. Moreover, the comparison of distinct security and business analysis expert’s interviews helped me to understand how RTA can be used in IRP. That information helped me to focus on the impact of those evolving abilities played in developing the IRP strategies.

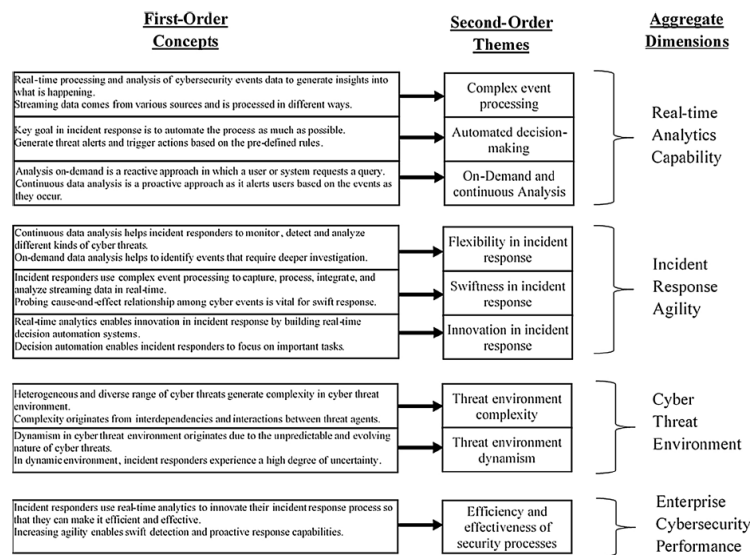


Figure 3.2: The Supporting Data Structure

3.5 The analysis abilities

Each phase of the incidence response process (IRP) is affected by the real time analysis abilities (RTA), from the senior information security analyst, security manager, and security officer, to security architects, they all require to gather, utilize, and investigate

Representative Quotes	First Order Concepts	Second Order Themes	Aggregate Dimensions
<p>“We use both continuous and on-demand real-time data analytics for making IR related decisions quickly... On-demand waits for the analyst to request a query and therefore is reactive. But in contrast, continuous analytics is more proactive as it generates threat alerts in real-time as the events are occurring”. (Expert 12)</p>	<ul style="list-style-type: none"> • Continuous data analysis helps incident responders to monitor, detect and analyze different kinds of cyber threats. • On-demand data analysis helps to identify events that require deeper investigation. 	Flexibility in incident response	
<p>“The complex event processing engine ingests the streaming data and analyzes it, correlates values and blends different cybersecurity events streams together... we also use complex event processing to analyze cause-and-effect relationships among cybersecurity events”. (Expert 20)</p>	<ul style="list-style-type: none"> • Incident responders use complex event processing to capture, process, integrate, and analyze streaming data in real-time. • Probing cause-and-effect relationship among cyber events is vital for swift response. 	Swiftness in incident response	Incident response agility
<p>“Real-time analytics helps in reducing the incident response time by automating and speeding up the whole decision-making process... this allows incident responders to focus on threat hunting and other valuable tasks”. (Expert 15)</p>	<ul style="list-style-type: none"> • Real-time analytics enables innovation in incident response by building real-time decision automation systems. • Decision automation enables incident responders to focus on important tasks 	Innovation in incident response	

Figure 3.3: Data supporting emergent concepts and themes.

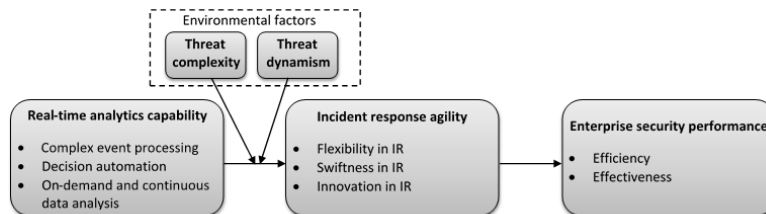


Figure 3.4: The Proposed Theoretical Framework

data to perform their duties and strategies. Therefore, the main decision makers such as security analysts and managers in main enterprises utilize RTA to investigate continuous data from several targets to identify malicious events which are harmful.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Enterprises also require to constantly checking the security activities to minimize the exposure of organizational assets to novel and developing attacks. That needs gathering, collection and investigation of security information to produce information which may assist security managers to examine and investigate events across all information assets.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems (MIS). After these systems the executive information systems (EIS) and decision support systems (DSS) are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both de-

tective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The organizations gather, store, and analyze the key business data to produce novel information regarding business and markets by using these applications. The analytical solutions which enterprises build up utilizing BA include data marts, online analytical processing enterprise data warehouses, dashboards, data mining and scorecards.

The main characteristics of RTA in security IRP observed by the interview experts in security organizations are discussed below.

Research Contributions

This last chapter demonstrates the key findings and results of the four phases of data analysis process as presented in the preceding chapter. Section 4.1 of that chapter explains the theoretical framework which that research builds up founded on the examination of qualitative data. The following parts describe each element of the theoretical framework thoroughly with supporting qualitative information.

Section 4.2 presents the salient characteristics of RTA (“automated decision making”, “complex event processing” and “on-demand and continuous data analysis”) in the IRP are described. The section 4.3 explains the three agile incidence response strategies (swiftness, flexibility, and innovation). Section 4.4 explains and identifies the environmental factors which facilitate and hinder the growth of ability in incidence response process (IRP) by using the real time analysis abilities (RTA). In the next section, the economic and strategic benefits which organization gained by using RTA in their IRP are presented. Section 4.6 describes the theoretical framework from enhancement in IRP ability perspective.

4.1 The Theoretical Framework

That research discovers the utilization of RTA in the IRP. The narrative that follows explains how the utilization of RTA in IRP assisted the enterprises to develop ability in their incidence response process. Moreover, it also describes the affect of utilizing RTA in IRP on entire organization performance. To further support that narrative, a data structure view (Figure 4-1), and a data table (Table 4-1) which supports developing con-

structs are also incorporated. Lastly, the key findings from the data examination process are incorporated with current literature to develop a theoretical framework of RTA to enhance ability in IRP. In the Figure 4-2 the theoretical framework that this research builds up grounded on the examination of qualitative data. All the interview experts have experience in working dynamic attack landscape that have the sophisticated, evolving and dynamic nature of security attacks (unpredictable and predictable) for example insider data theft, advanced persistent threats and zero-day attack. These enterprises react to that dynamic attack environment by the use of RTA in IRP. Particularly, they use RTA to develop higher order agile features such as (swiftness, innovation and flexibility) in their IRP which in turn, direct to positive results in organization security performance by giving economic and strategic advantages. Moreover, the theoretical framework also presents two types of environmental factors (threat complexity and threat dynamism) which hinder and facilitate the execution and growth of agile characteristics in security IRP by using RTA. The framework is described in detail below.

4.2 Agile Characteristics in incidence Response

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Enterprises also require to constantly checking the security activities to minimize the exposure of organizational assets to novel and developing attacks. That needs gathering, collection and investigation of security information to produce information which may assist security managers to examine and investigate events across all information assets.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is

the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems (MIS). After these systems the executive information systems (EIS) and decision support systems (DSS) are developed in mid 1960s. The relational database management systems were built up in late 1970s, these systems are used to capture huge amount of data and enhanced data designing capability.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Enterprises also require to constantly checking the security activities to minimize the exposure of organizational assets to novel and developing attacks. That needs gathering, collection and investigation of security information to produce information which may assist security managers to examine and investigate events across all information assets.

The knowledge of the idea of BA can be build up from the investigation of its heritage. Generally, the traditional views of BA are related to the analysis of data, with the purpose of enhancing and supporting business activities and processes, such as decision making. The data analysis processes are (examination, inference, or calculation). BA is the most recent in long list of technologies that are employed to enhance and support making of decisions relevant to business processes.

In 1950s the mainframe computers were developed; they were utilized to build up the first generation of data processing systems which helped manager level making of decisions labeled management information systems (MIS). After these systems the executive information systems (EIS) and decision support systems (DSS) are developed in mid 1960s. The relational database management systems were built up in late 1970s,

these systems are used to capture huge amount of data and enhanced data designing capability.

4.3 environmental Factors

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and pro-

ducing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

“If we went to the board and said that we want to spend some money to invest on some technology or product to develop a capability and the project is not mandatory [compliance requirement], getting their support and involvement is very difficult. That is why we need to convince them regarding why this project is of high priority so that they can give required budget and resources

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

“If the stakeholders do not understand the goals of project and are not committed to achieve them as the security team, this means that the stakeholders do not fully understand “why” behind the project.” (security senior manager, bank)

“We were able to show just broad evidence of from cross industry that there are many organisations that are ill prepared in been able to detect and respond to security breaches. In addition, we showed case studies of organizations that had been breached but had not discovered the breach for some time and then not particularly well prepared and been able to respond when they were aware that a loss event had taken place.”

The manager of security strategy and governance in Insurance further explained that: “The approach we take in communicating with key stakeholders is helping articulate their shared understanding of what the problem is, by providing some facts whether they are internal facts or broader industry weight of evidence, helping them understand what the options are and proposing or making a recommendation to our key stakeholders on what the solution may be. Now obviously when we are talking about board level directors, we are not talking at a deep technology level. We are basically talking about the abilities that we want to develop and how that helps support our business.”

Second, misaligned analysis and security skills can be a challenge for organizations

when they embark upon the journey of adding analytical abilities in security incidence response. The manager of IT and information security in Insurance highlighted the mismatch between their existing and required security and analysis skills as follows:

“In this day and age, we really need a person that has very strong analytical and communication skills, and business acumen. Someone that actually understands our business and security processes and has the ability to analyse data effectively.”

The focal organizations addressed this issue by hiring and/or training their analysis and security personnel:

4.4 Organizational Security Performance

This section examines how focal organizations reaped strategic and economic benefits and improved their overall enterprise security performance as a result of developing analysis enabled dynamic abilities and dynamic incidence response strategies using analysis.

The manager of security strategy and governance in Insurance stated that: “The concept of security risk management is so that we can operate our business processes in a manner with some assurance that we can actually be very confident in doing our daily business operations. The analogy is like where you have brakes on a car, it is actually the brakes that are there to allow you to go faster, it is not to slow you down. So, the benefit of using analysis is that we can actually manage our risks appropriately and we can have the confidence to innovate and operate our business processes in a manner that they can be very effective and efficient.”

The general manager of security strategy and governance in Insurance explained that real-time situational awareness and dynamic risk assessment enabled by analysis capability significantly improved their security awareness both at tactical and operational level: “Using analysis, we are improving our security awareness and that is changing the perception that risk management is a valuable capability in the organisation and not what we call a handbrake on the happiness.”

He further elaborated that:

“The key point for us with real-analysis is the thing that is really important is being able to change some of our decisions from experience and intuition to fact very quickly. That is the critical piece.”

“So, what we are doing is turning our security risk management and incidence response capability into it is almost like an opportunity, it is the upside instead of the downside, so if we have not managed our risks appropriately we would not have availed ourselves the business opportunities. We do not have the confidence of saying we have millions of customers if we don’t have appropriate risk management controls and how we manage our data.”

The General manager of security risk management in bank noted that analysis helped them to handle security threats in a proactive manner as follows: “analysis to us is like an early warning system. It helps us to identify what the next credible or significant threat to us might be. We can then take proactive approach and implement additional controls to prevent them from happening. So, it is managing the risk in a proactive way so that it does not become an issue.” (General manager of security risk management, bank) He further explained that:

“I think we have started getting real benefits of using analysis in our security incidence response in last 12 months. We also had the managed service, I mentioned that we have got an external service provider that has been doing some of the analysis for us. We have been able to use that information to better inform ourselves around what our gaps are. What our weaknesses are? And I can say in last 3 years we have got an evidence that we have been able to use analysis to proof a gap. And invest in a security controls that have reduced our security exposure or reduced the number of incidences that we have seen.” (General manager of security risk management, bank)

Manager of security strategy and governance in Insurance also highlighted that the use analysis has helped them to develop more efficient and robust user access models and thereby improve their access management: “I think the real benefits that we are seeing from security analysis right now like immediate term future is helping us our access management. So, our immediate opportunity that we see in applying more advanced analysis techniques is to try and develop more efficient and robust access models. That will then help us progressively reduce our risk of thing like fraud or accidental disclosure of information.”

The chief security architect of Insurance provided an example of how the use of analysis in the right manner can help organizations to gain economic benefits as follows:

When asked about the role of analysis in improving overall enterprise security perfor-

mance, the manager of security strategy and governance reported that: “It depends. If it is the commodity analysis then no. I will put it this way, if we don’t invest in analysis we cannot improve our security [performance] and we are at a competitive disadvantage. I think that our peer organisations will all be making similar investments in such technology to improve their security performance and if we don’t, then we are at competitive disadvantage.”

4.5 A Theoretical Framework

Based on the above mentioned narrative explained how modern security enterprises utilized the analysis abilities (RTA) to enhance ability in their security IRP which enabled them to enhance their entire organizational security performance. Integrating these information’s with existing literature enlightens a theoretical framework of impact of RTA on enterprise security performance by developing agile characteristics in security incidence response process (IRP), as presented in Figure 4-3. IRP may be considered dynamic as enterprises use RTA such as (“complex event processing, decision automation and on-demand and continuous data analysis”) to develop agile features such as (swiftness, innovation and flexibility) in their security incidence response process (IRP) in order to respond security incidences proactively and hence improve the overall enterprise security performance. The integration of qualitative data findings with existing literature are explained below.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

In order to respond to both known and unknown security attacks, Researchers have suggested a combination of detection, anticipation and reaction strategies. [10], [19]. Eventually, the chosen response strategy by security managers should be quick and agile in order to enhance the security performance [70].

Our findings provide one way to develop agile incidence response is by using the RTA in the IR process. The “complex event processing, automated decision making and on-demand and continuous data analysis” characteristics of RTA allow catching and handling of flowing data and assist to security incidences in real-time, hence allow ability in IR. security incidences are not always be known [3], [39]. In complex event processing, incidences function as a trigger, hence IR teams can react effectively to security incidences as they happen by adopting proactive response strategies for unpredictable incidences [42], [41].

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

Our findings give empirical indication for this opinion and recommend that the utilizing of RTA in the IR process needs added abilities (such as interoperability across multiple analytical platforms and in memory analysis, data virtualization) than given in a common security analysis design. For example, when data requires to move among different analytical tools and platforms in real-time, each tool needs some type of real-time capability (e.g., business rules, complex event processing and streaming input). Our findings extend the existing knowledge of RTA and expand the existing literature by explaining its main characteristics. Building on this, we build the following proposition:

Proposition 1: “Complex event processing, decision automation, and on demand and continuous data analysis are critical elements of analysis capability”.

Current research suggests that organizations that have developed process-oriented analytical abilities can to enhance ability in their business process this enable them to identify changes, attacks and chances in the security landscape which, in turn, assist

them to exploit chances for competitive and innovative response [30], [42]. Moreover, ability in business process is a significant process by which organizations can perform better than their competitors by reacting more efficiently to dynamic business landscapes [30].

Our study assists these concepts and proposes that RTA makes firms to adopt changing in their attack landscape and become swift in reacting to security attacks. Enhancing ability by using RTA develops the agile features of speed, innovation and flexibility in the IR process. It gives firms the capability to react efficiently to complex and unpredictable security incidences.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

The baseline level of big data analysis usage in incidence response is manual analysis. In manual analysis, there is no centralized repository to integrate and store data such as a data warehouse. Data are collected from multiple organizational units and stakeholders, for example, data center administrators, network teams, communication server teams and applications teams. The entire process is cumbersome and time consuming. There is no standard format or storage structure as there are many departments collecting data. Mostly, descriptive analysis is used to generate security information. security events and log data are captured only after the incidence is discovered. As data capture is reactive rather than proactive, the discovery of the original point of compromise is difficult. Organizations mostly rely on source tools with very little integration abilities to drive the manual analysis process. Table 4 below provides example quotes for analyzing incidence related data using manual analysis.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to

identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

As the data used for incidence related analysis is stored in flat files rather than in a standardized central repository such as a data warehouse, data manipulation for analytical purposes is difficult. Therefore, information generated from manual analysis are almost impossible to validate. At this level, incidence response teams can use big data analysis but have limited data for analysis. In manual analysis, the investigation focuses on the aftermath of the attack because the data are not completely integrated or simply not available to paint a holistic picture. In summary, manual analysis of collected data is time consuming, difficult and increases the cost of the investigation significantly, and

delivers incomplete results than those obtained in other levels.

At the basic analysis level, a centralized repository to integrate and store security data such as data warehouse exists but is still not the main source for data analysis. There are enterprise-wide standards for security data naming and storage management. Most organizations at this level have SIEM solutions to standardize retention, aggregation, correlation, and analysis of log data. Organizations can capture incidence related data either through standard capture tools or through more sophisticated security analysis solutions. Although incidence related data is available, it may not be comprehensive enough to paint a full picture and much of the context for that data remains unavailable. Both descriptive and predictive analysis are used to generate security information. At this level, some of the analytical tasks are automated but these are not yet integrated in the mainstream security processes. Incidence response teams have the specific skill sets required to utilize big data technologies and generate incidence specific information. Table 5 below provides example quotes for analyzing incidence related data using basic analysis.

With basic analysis, more data is available for incidence specific investigations. Intrusion detection systems, intrusion prevention systems and firewall data are extracted and loaded into the SIEM for integration, aggregation, and correlation of data. In addition, network data is used to enrich the security alerts, and this helps in removal of false positives. Some threat intelligence data may also be incorporated to provide rich context. At a basic level, incidence related investigations are much easier and more complete. By using the combination of descriptive and predictive analysis, the initial vector of the compromise can often be determined. However, determination of the amount and type of exfiltrated data may not be possible if the attackers are using sophisticated and novel methods such as encryption for attack.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective and protective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable

and predictable security attacks.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

At this level, a centralized data store, such as a data warehouse, becomes the single source of truth and centralized repository of all security analysis initiatives. Data is sourced and integrated from multiple sources such as intrusion recognition systems, intrusion prevention systems, SIEM, network and antivirus software, and spam and application logs. There are no data silos in the analytical ecosystem and data are easily available for in-depth incidence investigations. Data capture routines are deployed at relevant source systems to capture relevant data as well as every available piece of meta-data. Therefore, incidence related data is available and considered complete. There are clear mechanisms in place to connect new data sets with existing data. The data retrieval process is optimized using indexes, and therefore it becomes highly searchable. To build comprehensive context, high-quality threat and reputation data are integrated while doing incidence investigations. Advanced analysis is different from the basic analysis level not only because the data is more readily searchable, but also because all incidence related data is available and enriched with reliable threat and reputation data.

Organizations do not simply move from the manual analysis level directly to advanced analysis level. Getting to advanced analysis level and to enhance ability in incidence response needs a combination of the right people, tools, processes, and training. Enterprises required to invest in building and integrating a big data analysis capability into their incidence response process and that takes time. In addition, organizations also need to develop an overarching analytical ecosystem architecture that can assist enter-

prises produce, disseminate, and take actions based on analytical information. Even though big data analysis usage at advanced analysis level makes incidence investigations easier and more complete, that only happens with highly trained and experienced security personnel.

For the IR teams work in the incidence response process, that research's implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Our findings propose that security managers require people in their incidence response teams that have business insight, effective analytical and communications skill so that they can comprehend their business and examine security attacks in an efficient and timely manner. Hence, security managers required to train and/or hire analysis or security employees with knowledge and skills required to build security analysis applications and combine and gain big data analysis solutions given by outside vendors. To perform this, managers can:

- Teach and up skill their present security employees that have a Background of traditional security how to know and use the more innovative analysis abilities.
- Hire employees that come from a big data analysis Background and explain them the processes of security.
- Managed security services enablers or acquire vendor if they cannot train or hire current workers to get these knowledge and skills while they develop their our own big data analysis abilities in process of incidence response.

Our findings propose that giving big data analysis knowledge to employees with security information is a good option as they can take advantage of the actionable information gathered from the environment of security and generate value to the business.

Organizations can quickly rebuild current processes or build novel ones to response to the dynamic attack landscape, with improvement of agile features in security IR process,

[79]. That kind of ability can be explained by quickness in detecting related incidences, investigating what is occurring and interpretation the affect and results for the firm, discovering possibilities, and creating decisions, and executing appropriate reactions.

The existing RB literature explains BA abilities' role in attaining competitive advantage, our research proposes that IR ability enabled by RTA is essential for protecting or sustaining competitive advantage. To summarize, the organization's ability to implement and leverage RTA determines, the ability to which it can quickly change its IR resources and processes. Thus, we suggest that:

Proposition 2: "analysis capability enables organizations to execute agile incidence response by instilling the agile characteristics of swiftness, flexibility, and innovation in their security incidence response process and thereby respond to the complex and dynamic threat environment proactively".

Organizations use ability in IR process to develop their tasks in a way that assists them to enhance the effectiveness and efficiency of their firm security performance. Organization security is related to all the attacks and attacks that can influence the main business of a firm [4]. These comprise human error, failed processes and both external and internal security attacks [3]. A firm's level of IR ability shows the manner and quickness with which it can react to dynamic attack landscape.

Organizations have been collecting increasingly large amounts of data as part of their routine activities, for example data related to supply chain, accounting and finance, operations, and customers. Today, maintaining large data repositories is part of the organizational business model. However, the collection of big data does not necessarily create value for organizations. What is new, and what makes big data valuable, is when organizations apply analysis to further their strategic objectives. Big data analysis gives organizations a holistic way to collect, integrate and analyze the data-related dimensions of 5V (velocity, volume, veracity, variety and value) and thereby generate actionable information for measuring performance, delivering continual value and producing competitive benefits. Below, we apply the key ideas of big data analysis to the field of security.

Our findings propose that a firm with the mature IR ability can react to dynamic attack landscape quickly and effectively. Furthermore, both IR process efficiency and effectiveness have been individually connected to improve the firm security performance by

either minimizing the cost of prevention, remediation and mitigation, or by minimizing the cost of damages [10]. Grounded on contingent RB theory, ability in IR process shows a valuable capability that can add to superior firm security performance. Hence, we suggest that:

Proposition 3: “Increasing ability in the incidence response process enhances the efficiency and effectiveness of overall enterprise security performance”.

Grounded on the contingent RB, BA abilities can affect organization performance by the intermediate role of other abilities and resources [70]. Our findings propose that RTA affects the firm security performance by the intermediate role of agile IR process. ability in IR depends on the firm’s ability to leverage and execute RTA. ability in IR process suggests the manner and quickness with which a firm reacts to complex and dynamic attacks. The enhancement in IR ability provides firms a distinctive opportunity to quickly detect security attacks and react to them in an effective fashion. Without IR ability, firms are less likely to attain superior organizational security performance and maintain their competitive advantage. Hence, we suggest that RTA has an indirect effect on firm security performance and that IR ability acts as an intermediary of this link. Building on this, the following proposition is developed:

Proposition 4: “incidence response ability mediates the relationship between RTA and enterprise security performance”.

[75] explain in their assessment and review of RB that “the moment we try to explain or predict the firm’s actual performance... the RB turns out to be incomplete because it ignores the material contingencies of the firm’s situation”. Our study explains this challenge by suggesting attack landscape dynamism and complexity as the contingent factors that impact the link between RTA and agile IR process.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Heterogeneity and different range of attacks that can expose firm assets refers to Complexity in the threat landscape [39]. Any incidence that can have an unpredictable affect on firm security is a risk. Furthermore, the distribution of assets among multiple targets, such as software, data, physical components and network increases the number of attack vectors and thereby dynamism [39].

Our findings propose that attack complexity makes larger insecurity and thus an added opportunity for RTA to use ability in IR process. Firms with a lesser number of targets for threat have small insecurity and hence a smaller threat complexity. However, firms with a greater number of targets for threat have larger insecurity. In this situations, firms that have improved RTA can respond to the complexity made by the greater number of targets in a better manner. To summarize, in threat landscape complexity, firms with improved RTA are able to deal with attacks in an effective and better manner and are hence more likely to develop ability in IR process. Building on this, we suggest that:

Proposition 5a: “ threat environment complexity positively moderates the impact of analysis capability on incidence response ability”.

For the IR teams work in the incidence response process, that research’s implications have the practical view of the impact of analysis abilities. Instead of using analysis abilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis abilities at strategic level in developing both detective reaction plans. The use of the variety of abilities which are allowed by RTA will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Threat environment dynamism is described by the emerging nature of security attacks [19], [3]. Our findings propose that in a highly unpredictable or dynamic attack environment, IR teams have greater amount of uncertainty and have a requirement for both real-time information and the ability to respond it. Therefore, in dynamic attack landscapes, RTA becomes extra important as it makes firms to identify security attacks as they occur and react to them in a proactive fashion. Moreover, when firms are open to evolving and dynamic attacks, they require to determine these new attacks and new forms of threats before they can create any loss [3]. To attain this, firms need regular

creation of new IR plan, reconfiguration of their IR process, and the capability to continuously investigate for innovative response strategies. Thus, larger attack dynamism is predictable to build highly unpredictable and evolving attacks, hence required improved RTA to identify and react to them. Building on this rationale we suggest the following: Proposition 5b: “Cyber threat environment dynamism positively moderates the impact of analysis capability on incidence response ability”.

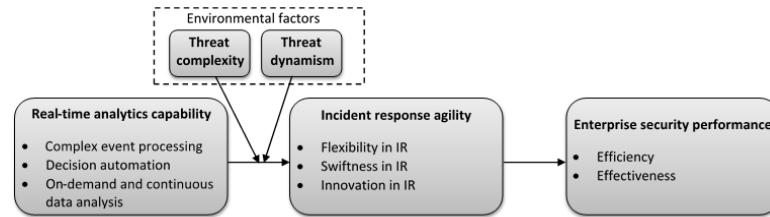


Figure 4.1: The Proposed Theoretical Framework

Discussion and Future Research

In the previous chapter the entire findings of this research were presented. The explanations of those research findings improve our existing knowledge of the impact that RTAC plays in enhancing cyber security IRP agility in three manners. The First way is, that research builds up a theoretical framework which connects RTAC with cyber security IRP agility. The proposed theoretical framework describes the key contribution of that study. Secondly, the descriptions of the proposed theoretical framework represent how agile characteristics are developed by implementing dynamic capabilities in the cyber security IRP. Finally, that study gives information which may contribute to practice the cyber security incident response strategies in industry. That chapter presents the implications of that research for both information systems practice and research.

5.1 Contributions of the Study

What is the practical and theoretical importance of that research study findings? Why and How are those research findings and information valuable? How do these build our knowledge of enhancing agility in security IRP using RTAC? Furthermore how are they vary from what was acknowledged about enhancing agility in IRP before the initiation of that research? The objective of that part is to highlight those key questions, starting with the practical and then the theoretical advantages of these research findings.

5.1.1 Contribution for Research

This research finding suggests many significant implications for information systems literature, with its analysis of enhancing IRP agility using RTAC.

First of all, that research presents key dimensions of RTAC and explains how enterprises implement agility in their IRP by investing and using RTAC. It presents how RTAC allowed dynamic capabilities can assist enterprises to move from a reactive method to a proactive method for cyber security event reaction plans. Secondly, [146] explains how agility can be developed using strong dynamic capabilities, that research analysis how RTAC allowed dynamic capabilities assist enterprises combine, create, and rebuild their organizational assets to enhance agility in their IRP. Particularly, that research presents RTAC enabled dynamic incident reaction plans to describe how enterprises may enhance agility in their IRP and hence improves their entire organizational security performance. Specifically, that research presents the research question by implementing a theoretical framework (in Figure 5-1) which describes that research's key contribution by integrating RTAC and IRP agility.

For the IR teams work in the incident response process, that research's implications have the practical view of the impact of analysis capabilities. Instead of using analysis capabilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis capabilities at strategic level in developing both detective reaction plans. The use of the variety of capabilities which are allowed by RTAC will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

With the help of proposed theoretical framework, that research describes how enterprises utilize RTAC are capable to implement higher order dynamic capabilities in IRP. That research also describes how RTAC enable agility in IR which help to develop dynamic cyber security incident reaction plans. That research describes applicable and value able findings relevant to the utilization of RTAC for enhancing IRP agility. Particularly, that research finding highlights on how enterprises with dynamic real-time capabilities developed by utilizing of RTAC enhance agility in IRP which, consecutively, improves the entire organizational security performance by producing economic and strategic advantages. The proposed theoretical framework also presents a detailed picture of the

factors which both hinder and facilitate the implementation of real-time capabilities in IRP.

This research enhances our knowledge of RTAC and expands the previous literature by describing its key areas in cyber security IRP such as (building supporting architecture, defining the real-time perspective, decision automation, and continuous and on-demand data analysis).

Moreover, that research adds to the literature on incident response reaction plans by describing RTAC allowed dynamic capabilities which develop agility in IRP and design dynamic incident reaction plans. Three analysis capabilities are (complex event processing,, continuous and on-demand monitoring, and automated decision making).

[15] explains agility as main feature of IRP and calls for the implementation of analysis capabilities in security landscape which experience sophisticated and complex attacks, that research expands the previous literature by highlighting three key RTAC enabled agile characteristics in IRP and describe how to develop agile incident reaction plans using these analysis capabilities and hence enhance agility in IRP.

That research highlights how the key dimensions of IRP and features of dynamic capability support the implementation of RTAC enabled dynamic incident identification and reaction plans. The modern security enterprises that have a well developed IRP and work together with attack intelligence sharing organizations have broader view of security attack environment and may react to cyber security events swiftly.

5.1.2 Contribution for Practice

The findings of that research have valuable practical advantages and add to three groups of collaborators in IR practice. For the vendors of security organizations, the results of that research propose that they should identify the contemporary and creative role that their security solutions can give to organizations. This innovative role of security solutions may combine attack related information, automate analysis and forensic investigations; implement intricate procedures and visual analysis to find the key security attacks, will assist their clients build creative security incident reaction plans which may handle with dynamic security landscape. The impact of the capabilities triggered by RTAC for example complex event processing, on-demand monitoring and decision automation, will enhance the requirement for data automation, integration, analysis and

visualization. Hence, security organization vendors who design security solutions require to vigilantly examine these requirements during the implementation their security responses.

Our study gives key contributions to the literature on security incident response research in several ways. First, our findings highlight the importance of using big data analysis in IR process to understand sense of attacks and incidents that generate from the threat environment. Second, we identify the key dimensions of big data analysis capability (data management, data integration, data analysis, insights consumption) that can be utilized to classify the use of big data analysis in incident response process at different levels, that is, manual analysis, basic analysis, advanced analysis. Third, following the work of [5] Describing the need for enabling agility in incident response, our findings explain how big data analysis assists enterprises to transform their process of incident response to identify and react to complicated, unidentified and new security attacks in an agile and proactive manner. Our research explains the research question (How can big data analysis enhance agility in the process of security incident response?) by developing a framework (see figure 1) that describes the key features and application of big data analysis in the process of incident response at different maturity levels. Through the framework, we explain how key dimensions of a big data analysis capability in the incident response process change at different maturity levels.

This paper explains the practice perspective that the key role of big data analysis in permitting agility in the incident response process. Big data analysis provides enterprises a distinctive opportunity to effectively identify the threats as they occur and react to them in an effective and timely fashion. The application of big data analysis makes enterprises to intensify their process of incident response in a way that develop flexibility, swiftness and innovation in their incident response process. These agile characteristics enables both known and unknown attacks.

Enhancing agility in incident response using big data analysis is a journey and an evolutionary process that starts by shortening the time to detect the security incidents. After an incident is detected, agile incident response ensures containment and remediation are not only faster than traditional approaches, but they are also more complete.

Our findings also suggest that even though many big data analysis tools and practices have been established in the past few years, their usage in the security incident

response process warrants new methods considering many aspects including zero-day attack detection, unified data architecture, data sharing across threat detection systems, sampling and dimensional reduction, real time analysis of data, automated response, and predictive analysis for anomaly detection.

For the IR teams work in the incident response process, that research's implications have the practical view of the impact of analysis capabilities. Instead of using analysis capabilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis capabilities at strategic level in developing both detective reaction plans. The use of the variety of capabilities which are allowed by RTAC will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

5.2 Limitations and Future Research

That part is focused at stimulating future research on the idea of how enterprises enhance agility in their IRP, a theme proposing a big chance for academic investigation. The promising themes for further research grounded on the results and limitations of that research are described below.

For the IR teams work in the incident response process, that research's implications have the practical view of the impact of analysis capabilities. Instead of using analysis capabilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis capabilities at strategic level in developing both detective reaction plans. The use of the variety of capabilities which are allowed by RTAC will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

Hence, the generalization of the results of that research in other domains that entail the implementation of RTAC should be performed carefully as the results can be specific to the particular features of IRP, and to the industry experts that were considered in that study. Such as, that research identifies that the choice of enterprises from banking, finance and assurance sector, the utilization of related IR techniques in the enterprises

considered as well as their great degree of development in IRP and in implementing RTAC can restrict the generalized of that research's results.

That research's results can not implement better to enterprises which utilize different IRP techniques and are at different stage of development in the implementation of RTAC. Hence, further research is required which might increase, support or refuse that research's results in other enterprises and organizational sectors. A part from these limitations, that study proposes that the implementation of analysis capabilities in IRP encloses a novel transformation for IR research that deals with the affects of analysis in developing swift incident response strategies, and the results from that research will provide a foundation for further study which may be considered to confirm, challenge and expand that research's findings.

Further research is required to examine the environmental factors which hinder or support the development of agile features in IRP. Future study may examine how several practices and expertise of IR units influence the implementation of dynamic IR strategies. Moreover, each of the IR unit's experts in that research has practised a data-driven IR capability no fewer than 9 months and no more than two years prior to starting of that research. Therefore, many of the information that evolved in that research identify the findings of that technique. Further research is required to examine the key features of data-driven IR techniques.

Lastly, this research gives key bases for high-level quantitative research which may examine key components which may assist enterprises enhance IR agility using RTAC. The connection between developing agility using RTAC and enterprises security performance is a focus of existing research. Future study is also required to detect main difference between dynamic real-time capabilities and other dynamic strategies to attain information regarding how RTAC can provide diverse capabilities.

For the IR teams work in the incident response process, that research's implications have the practical view of the impact of analysis capabilities. Instead of using analysis capabilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis capabilities at strategic level in developing both detective reaction plans. The use of the variety of capabilities which are allowed by RTAC will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and

predictable security attacks.

- once the criminal has access to the network, the length of time it takes to identify the threat.
- once the security incident has been identified, the speed at which a reaction and elimination can be executed. Big data analysis assists in handling both components by minimizing the time taken to identify and react to security attacks, which ultimately helps to cost savings and improve data protection.

Our research study generates queries about the generalized of the suggested framework, therefore need further work to enhance it. Generalizing from our research findings should be performed with great care as they do not give a detailed information about the working of the organizations. Further research is required to further improve the proposed framework. This can be done by performing several in-depth case studies. Case studies will give in-depth organizational context hence adding more information to the proposed framework by giving actionable information on:

- components that enable or hinder the growth of agile features in incident response using big data analysis.
- the knowledge and skills needed by the teams of security to use big data analysis in incident response.
- conditions which hinder the utilization of big data analysis in the incident response.

Finally, our study gives a solid platform for broader quantitative research studies that can examine key aspects that assist enterprises enhance incident response agility using big data analysis and its effect on overall organizational security performance. Relating big data analysis abilities and enterprise performance is a direction of future research. Moreover, research is also required to detect main differences between big data analysis and other technologies to acquire actionable information into how big data analysis can give unique capabilities. Using big data analysis enables a model shift in the process of decision-making, additional in-depth knowledge is needed to examine its potential along with the challenges it causes to enterprises.

For the IR teams work in the incident response process, that research's implications have the practical view of the impact of analysis capabilities. Instead of using analysis

capabilities at operational level to constantly observe attack landscape, IR teams require to identify the more novel role of analysis capabilities at strategic level in developing both detective reaction plans. The use of the variety of capabilities which are allowed by RTAC will assist IR teams execute the integration of avoidance, identification and reaction strategies which may assist them to better handle with both unpredictable and predictable security attacks.

In the end, the researcher expects that results of that research formulate constructive contribution to both practice and theory in the urge of a good knowledge of how RTAC enhance agility in IRP. The security attack landscape is complex and dynamic and does not make itself to being effortlessly pinned or understood through business rules. No other way exists by which enterprises may recognize what kind of security threats they are heading to experience in the future. Though, what they may do is, implement proactive strategy to handle security threats by utilizing analysis. That will make certain that they are innovative, rapid and flexible in their security response plans.

REFERENCES

- [1] Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective," *Computers and Security* (42), pp. 27–39.
- [2] Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. 2012. "Incident Response Teams - Challenges in Supporting the Organisational Security Function," *Computers and Security* (31:5), pp. 643–652.
- [3] Ahmad, A., Maynard, S. B., and Park, S. 2014. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," *Journal of Intelligent Manufacturing* (25:2), pp. 357–370.
- [4] Ahmad, A., Maynard, S. B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management* (35:6), pp. 717–723.
- [5] Jalali, M. S., Siegel, M., and Madnick, S. 2019. "Decision-Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment," *The Journal of Strategic Information Systems*, pp. 1–17.
- [6] Ahmad, A., Ruighaver, T., and Teo, W. T. 2005. "An Information - Centric Approach to Data Security in Organizations," in *In TENCON 2005-2005 IEEE Region 10 Conference. IEEE*.
- [7] Anderson-Lehman, R., Watson, H. J., Wixom, B. H., and Hoffer, J. A. 2004. "Continental Airlines Flies High With Real-Time Business Intelligence," *MIS Quarterly Executive* (3:4), pp. 163–176.
- [8] Anderson, E. E., and Choobineh, J. 2008. "Enterprise Information Security Strategies," *Computers & Security* (27:1–2), pp. 22–29.
- [9] Aragon-Correa, J. A., and Sharma, S. 2003. "A Contingent Resource-Based View of Proactive Corporate Environmental Strategy," *Academy of Management Review* (28:1), pp. 71–88.
- [10] Bärenfänger, R., Otto, B., and Österle, H. 2014. "Business Value of In-Memory Technology- Multiple-Case Study Insights," *Industrial Management and Data Systems* (114:9), pp. 1396–1414.
- [11] Barney, J. B., Wright, M., and Ketchen, J. D. 2001. "The Resource-Based View of the Firm: Ten Years after 1991," *Journal of Management* (27:6), pp. 625–641.

- [12] Barreto, I. I. 2010. "Dynamic Capabilities: A Review of Past Research and an Agenda for the Future," *Journal of Management* (36:1), pp. 256–280.
- [13] Baskerville, R. 2005. "Information Warfare," *Journal of Information System Security* (1:1), pp. 23–50.
- [14] Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," *Information and Management* (51:1), pp. 138–151.
- [15] Battleson, D. A., West, B. C., Kim, J., Ramesh, B., and Pamela, S. 2016. "Achieving Dynamic Capabilities with Cloud Computing : An Empirical Investigation," *European Journal of Information Systems* (25:3), pp. 209–230.
- [16] Bharadwaj, A. S. 2000. "A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation," *MIS Quarterly* (24:1), p. 169.
- [17] Bojanc, R., and Jerman-Blažič, B. 2008. "An Economic Modelling Approach to Information Security Risk Management," *International Journal of Information Management* (28:5), pp. 413–422.
- [18] Bojanc, R., and Jerman-Blažič, B. 2013. "A Quantitative Model for Information-Security Risk Management.," *Engineering Management Journal* (25:2), pp. 25–37.
- [19] Bronzo, M., de Resende, P. T. V., de Oliveira, M. P. V., McCormack, K. P., de Sousa, P. R., and Ferreira, R. L. 2013. "Improving Performance Aligning Business Analytics with Process Orientation," *International Journal of Information Management* (33:2), pp. 300–307.
- [20] Casey, E. 2005. "Case Study: Network Intrusion Investigation - Lessons in Forensic Preparation," *Digital Investigation*, pp. 254–260.
- [21] Casey, E. 2006. "Investigating Sophisticated Security Breaches," *Communications of the ACM* (49:2), pp. 48–55.
- [22] Chakravarty, A., Grewal, R., and Sambamurthy, V. 2013. "Information Technology Competencies, Organizational Agility, and Firm Performance: Enabling and Facilitating Roles," *Information Systems Research* (24:4), pp. 976–997.
- [23] Chen, H., Chiang, R. H., and Storey, V. C. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* (36:4), pp. 1165–1188.

- [24] Chen, P., Desmet, L., and Huygens, C. 2014. "A Study on Advanced Persistent Threats," *Communications and Multimedia Security* (8735), pp. 63–72.
- [25] Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., and Chow, W. S. 2013. "IT Capability and Organizational Performance: The Roles of Business Process Agility and Environmental Factors," *European Journal of Information Systems* (23:January 2012), pp. 326–342.
- [26] Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. 2008. "Performance Measurement Guide for Information Security," *NIST Special Publication* (800–55:July).
- [27] Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2," *NIST Special Publication* (800–61).
- [28] Cosic, R., Shanks, G., and Maynard, S. 2012. "Towards a Business Analytics Capability Maturity Model," *ACIS 2012 : Location, Location, Location : Proceedings of the 23rd Australasian Conference on Information Systems 2012*, pp. 1–11.
- [29] Cosic, R., Shanks, G., and Maynard, S. 2015. "A Business Analytics Capability Framework," *Australasian Journal of Information Systems* (19), pp. S5–S19.
- [30] Davenport, T. H., Harris, J. G., and Morison, R. 2010. "Analytics at Work: Smarter Decisions, Better Results," *Harvard Business Press*, Harvard Business Press.
- [31] Dobrev, K., and Hart, M. 2015. "Benefits, Justification and Implementation Planning of Real-Time Business Intelligence Systems.," *Electronic Journal of Information Systems Evaluation* (18:2), pp. 104–118.
- [32] Dube, L., and Paré, G. 2003. "Rigor in Informatin Systems Positivist Case Research: Current Practices, Trends, and Recommendations," *MIS Quarterly* (27:4), pp. 597–635.
- [33] Eastman, R., and Versace, M. 2015. "Big Data and Predictive Analytics : On the Cybersecurity Front Line," *IDC White Paper* (February).
- [34] Eckerson, W. 2010. *Performance Dashboards : Measuring, Monitoring, and Managing Your Business*, John Wiley & Sons, Inc.

- [35] Eckerson, W. 2012. *The Secrets of Analytical Leaders: Insights from Information Insiders*, Technics Publications.
- [36] Eckerson, W. W. 2004. "Gauge Your Data Warehouse Maturity.," *DM Review* (14:11), pp. 34–51.
- [37] Eisenhardt, K. M., and Graebner, M. E. 2007. "Theory Building from Cases: Opportunities and Challenges," *Academy of Management Journal* (50:1), pp. 25–32.
- [38] Eisenhardt, K. M., and Martin, J. A. 2000. "Dynamic Capabilities: What Are They?," *Strategic Management Journal* (21:10–11), pp. 1105–1121.
- [39] Elahi, E. 2013. "Risk Management: The next Source of Competitive Advantage," *Foresight* (15:2), pp. 117– 131.
- [40] Elyas, M., Ahmad, A., Maynard, S. B., and Lonie, A. 2015. "Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework," *Computers and Security* (52), pp. 70–89.
- [41] Elyas, M., B., M. S., Atif, A., and Andrew, L. 2014. "Towards A Systemic Framework for Digital Forensic Readiness," *Journal of Computer Information Systems* (54:3), pp. 97–105.
- [42] Eriksson, T. 2014. "Processes, Antecedents and Outcomes of Dynamic Capabilities," *Scandinavian Journal of Management* (30:1), pp. 65–82.
- [43] Fink, L., and Neumann, S. 2007. "Gaining Agility through IT Personnel Capabilities : The Mediating Role of IT Infrastructure Capabilities," *Journal of the Association for Information Systems* (8:8), pp. 440–462.
- [44] Friedberg, I., Skopik, F., Settanni, G., and Fiedler, R. 2014. "Combating Advanced Persistent Threats : From Network Event Correlation to Incident Detection," *Computers & Security* (48), pp. 35–57.
- [45] Garg, A., Curtis, J., and Halper, H. 2003. "Quantifying the Financial Impact of IT Security Breachesnull," *Information Management & Computer Security* (11:2), pp. 74–83.
- [46] George, Alexander and Bennet, A. 2005. *Case Studies and Theory Development in the Social Sciences*, MIT Press. Cambridge.

- [47] Germann, F., Lilien, G. L., and Rangaswamy, A. 2013. "Performance Implications of Deploying Marketing Analytics," *International Journal of Research in Marketing* (30:2), pp. 114–128.
- [48] Gioia, D. a., Corley, K. G., and Hamilton, A. L. 2013. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), pp. 15–31.
- [49] Gonzalez, J. J. 2005. "Towards a Cyber Security Reporting System – A Quality Improvement Process," in *International Conference on Computer Safety, Reliability, and Security*, Springer, Berlin, Heidelberg, pp. 368–380.
- [50] Gordon, L. a., and Loeb, M. P. 2006. "Budgeting Process for Information Security Expenditures," *Communications of the ACM* (49:1), pp. 121–125.
- [51] Grispos, G., Glisson, W. B., and Storer, T. 2014. "Rethinking Security Incident Response: The Integration of Agile Principles," in *20th Americas Conference on Information Systems, AMCIS 2014*, pp. 1–9.
- [52] Gupta, M., and George, J. F. 2016. "Toward the Development of a Big Data Analytics Capability," *Information and Management* (53:8), pp. 1049–1064.
- [53] Hahn, G. J., and Packowski, J. 2015. "A Perspective on Applications of In-Memory Analytics in Supply Chain Management," *Decision Support Systems* (76), pp. 45–52.
- [54] Helfat, C. E., Finkelstein, S., Mitchell, W., Peteraf, M., Singh, H., Teece, D., and Winter, S. G. 2009. *Dynamic Capabilities: Understanding Strategic Change in Organizations*, John Wiley & Sons.
- [55] Helfat, C. E., and Winter, S. G. 2011. "Untangling Dynamic and Operational Capabilities: Strategy for the (N)Ever-Changing World," *Strategic Management Journal* (32:11), pp. 1243–1250.
- [56] Holsapple, C., Lee-Post, A., and Pakath, R. 2014. "A Unified Foundation for Business Analytics," *Decision Support Systems* (64), pp. 130–141.
- [57] Humphreys, E. 2008. "Information Security Management Standards: Compliance, Governance and Risk Management," *Information Security Technical Report* (13:4), pp. 247–255.
- [58] Inmon, W. H. 2002. *Building the Data Warehouse*, John Wiley & Sons, Inc.
- [59] Institution, B. S. 2013. *ISO/IEC 27001:2013 - Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements.*, British International Institute.

- [60] Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., and Longva, O. H. 2009. "A Framework for Incident Response Management in the Petroleum Industry," *International Journal of Critical Infrastructure Protection* (2:1), pp. 26–37.
- [61] Khansa, L., and Liginlal, D. 2009. "Valuing the Flexibility of Investing in Security Process Innovations," *European Journal of Operational Research* (192:1), pp. 216–235.
- [62] Kevin, B., Yang, C., Olson, D., and Sheu, C. 2014. "The Impact of Advanced Analytics and Data Accuracy on Operational Performance: A Contingent Resource Based Theory (RBT) Perspective," *Decision Support Systems* (59), pp. 119–126.
- [63] Kohavi, R., Rothlender, N., and Simoudis, E. 2002. "Emerging Trends in Business Analytics," *Communications of the ACM* (45:8), pp. 45–48.
- [64] Kohli, R. 2007. "Innovating to Create IT-Based New Business Opportunities at United Parcel Service.," *MIS Quarterly Executive* (6:4), pp. 199–210.
- [65] Krishnamoorthi, S., and Mathew, S. K. 2018. "Business Analytics and Business Value: A Comparative Case Study," *Information and Management* (55:5), pp. 643–666.
- [66] Lee, O. K., Sambamurthy, V., Lim, K. H., and Wei, K. K. 2015. "How Does IT Ambidexterity Impact Organizational Agility?," *Information Systems Research* (26:2), pp. 398–417.
- [67] Lemay, A., Calvet, J., Menet, F., and Fernandez, J. M. 2018. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors," *Computers and Security* (72), pp. 26–59.
- [68] Lim, E.-P., Chen, H., and Chen, G. 2013. "Business Intelligence and Analytics: Research Directions," *ACM Transactions on Management Information Systems* (3:4), pp. 1–10.
- [69] Lu, Y., and Ramamurthy, K. R. 2011. "Understanding the Link Between Information Technology Capability and Organizational Agility: An Empirical Examination," *MIS Quarterly* (35:4), pp. 931–954.
- [70] Mathiassen, L., and Pries-Heje, J. 2006. "Business Agility and Diffusion of Information Technology," *European Journal of Information Systems*, pp. 116–119.

- [71] Maynard, S., Onibere, M., and Ahmad, A. 2018. "Defining the Strategic Role of the Chief Information Security Officer," *Pacific Asia Journal of the Association for Information Systems* (10:3), pp. 61–85.
- [72] Nazir, S., and Pinsonneault, A. 2012. "IT and Firm Agility: An Electronic Integration Perspective," *Journal of the Association for Information Systems* (13:3), pp. 150–171.
- [73] Newbert, S. 2007. "Empirical Research on the Resource-Based View of the Firm: An Assessment and Suggestions for Future Research," *Strategic Management Journal* (28:2), pp. 121–146.
- [74] Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., and Ruhl, R. 2012. "The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches," in *Proceedings of Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom), IEEE.*, pp. 734–741.
- [75] Oliveira, M. P. V. De, McCormack, K., and Trkman, P. 2012. "Business Analytics in Supply Chains - The Contingent Effect of Business Process Maturity," *Expert Systems with Applications* (39:5), pp. 5488– 5498.
- [76] Onibere, M., Ahmad, A., and Maynard, S. 2017. "The Chief Information Security Officer and the Five Dimensions of a Strategist," in *PACIS 2017 Proceedings*, pp. 1–13.
- [77] Overby, E., Bharadwaj, A., and Sambamurthy, V. 2006. "Enterprise Agility and the Enabling Role of Information Technology," *European Journal of Information Systems* (15:2), pp. 120–131.
- [78] Paré, G. 2004. "Investigating Information Systems with Positivist Case Study Research," *Communications of the Association for Information Systems* (13:1), pp. 233–264.
- [79] Park, S., Ruighaver, A. B., Maynard, S. B., and Ahmad, A. 2012. "Towards Understanding Deterrence: Information Security Managers' Perspective," in *International Conference on IT Convergence and Security* (Vol. September), pp. 21–37.
- [80] Park, Y., El Sawy, O. A., and Fiss, P. 2017. "The Role of Business Intelligence and Communication Technologies in Organizational Agility," *Journal of the Association for Information Systems* (18:9), pp. 648–686.
- [81] Patton, M. Q. 2015. *Qualitative Evaluation and Research Methods*, Beverly Hills, CA: Sage.

- [82] Pavlou, P. A., and El Sawy, O. A. 2006. "From IT Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development," *Information Systems Research* (17:3), pp. 198–227.
- [83] Pavlou, P. A., and El Sawy, O. A. 2011. "Understanding the Elusive Black Box of Dynamic Capabilities," *Decision Sciences* (42:1), pp. 239–273.
- [84] Peteraf, M., Di Stefano, G., and Verona, G. 2013. "The Elephant in the Room of Dynamic Capabilities: Bringing Two Diverging Conversations Together," *Strategic Management Journal* (34:12), pp. 1389–1410.
- [85] Phillips-Wren, G., Lakshmi S., I., Kulkarni, U., and Ariyachandra, T. 2015. "Business Analytics in the Context of Big Data: A Roadmap for Research," *Communications of the AIS* (37:1), pp. 448–472.
- [86] Piccoli, G., and Watson, R. T. 2008. "Profit from Customer Data by Identifying Strategic Opportunities and Adopting the 'Born Digital' Approach," *MIS Quarterly Executive* (7:3), pp. 113–122.
- [87] Pierazzi, F., Casolari, S., Colajanni, M., and Marchetti, M. 2016. "Exploratory Security Analytics for Anomaly Detection," *Computers & Security* (56), pp. 28–49.
- [88] Popovič, A., Hackney, R., Simões, P., and Jakli, J. 2012. "Towards Business Intelligence Systems Success: Effects of Maturity and Culture on Analytical Decision Making," *Decision Support Systems* (54), pp. 729–739.
- [88] Raschke, R. L. 2010. "Process-Based View of Agility: The Value Contribution of IT and the Effects on Process Outcomes," *International Journal of Accounting Information Systems* (11:4), pp. 297–313.
- [89] Rees, J., and Allen, J. 2008. "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation," *Journal of Organizational Computing and Electronic Commerce* (18:4), pp. 255–277.

APPENDIX A. INTERVIEW GUIDE

This appendix presents the questionnaire that was used to guide the semi-structured interviews. Please note that this questionnaire was an approximate guide only, and its purpose was to encourage the interviewees to reflect on the research themes, rather than constrain this discussion. The phrasing of the questions varied based on the role of the interviewee and the organizational context. Depending on the interviewee's role and experience (e.g., top-level managers, middle level senior managers, cybersecurity analysts and data analysts), the focal themes also varied from interview to interview. Not all questions were necessarily covered in every interview, and some themes were covered in greater depth than others.

How does use of real-time analytics in the incident response process improve enterprise cybersecurity performance?

Interview Guide

Interviewee Background

Please describe your background and current role in the organization (incl. educational and professional background, cybersecurity related experience, business analytics related experience, current role, reporting line, key deliverables).

Theme 1: Real-Time Analytics in Cybersecurity Incident Response

1. What does real-time analytics mean to you?
2. Describe the evolution of analytics in your organization?
 - a. What were the key milestones that you targeted and achieved?
 - b. What is the status at present?
3. Describe the potential role that analytics may play in the process of cybersecurity incident response.
4. Describe how you have integrated real-time analytics into your incident response process.
 - a. How much were you and other top management team members involved in this integration?
 - b. What are the major challenges and obstacles you encountered? How did you or your top leadership team overcome these challenges?
 - c. What are the sources of data for real-time analytics? How do you manage your cybersecurity data and analytical architecture?
 - d. What kind of reporting and analysis are you performing on cybersecurity data related to risk management and incident response? What type of analytical models are you using?
5. Who are the consumers of insights generated from analytics applications? How are insights delivered? (Dashboards, reports, scorecards etc.)
6. Describe the importance of self-service analytics in building real-time analytics capability?

Theme 2: Impact of Using Real-time Analytics on Cybersecurity Incident Response

2. Describe the incident response process from initial identification to closure.
3. Describe how important it is to be proactive and dynamic when it comes to executing cybersecurity incident response?
4. What role does analytics play in becoming dynamic in cybersecurity risk management and incident response?
5. Give some examples of situations when top leadership involvement was critical for implementing new analytics related initiative. How was leadership involvement solicited and managed?
6. What are some of the key risk indicators that you monitor, analyze and measure? Why?
7. Describe how you determine if your risk management and incident response process is effectively protecting your enterprise.
8. What cybersecurity risk assessment methods and techniques are you using in your organization?
9. Give a few examples of innovative ideas that you have incorporated into your incident process that have resulted in better execution of your incident response process?
10. Describe what you did in a situation where a significant threat was discovered. Specifically, how was the threat discovered? How did you decide it was significant? How did you decide what to do about it? And how did you determine if your actions were successful or not?

INTERVIEW GUIDE

Theme 3: Enterprise Security Performance:

1. What specific benefits have you realized by using analytics in your cybersecurity incident response process?
 - a. Can you give some examples on how the use of analytics has influenced the quality of cybersecurity related decisions in your enterprise?
 - b. Can you give any figures on the value analytics brings (e.g., \$ saved/lost, time saved/wasted, performance optimization etc.)?
2. Describe what measures do you use to evaluate the performance of your cybersecurity processes?
3. Describe how analytics in cybersecurity has impacted your enterprise's security performance during the last 2 or 3 years.
4. What do you think would be the best way to determine Return on Security Investment? Are there any other ways to do it?
5. Describe how you develop your cybersecurity budget? How do you justify spending and resource requests to the business?
6. Give some examples of organizational cybersecurity measures. Which of these measures describe the overall enterprise security performance the best?

Thank you for finding time to contribution!